

Miranda HARIZAJ
PËR MARRJEN E GRADËS
“DOKTOR”
NË “INXHINIERI ELEKTRIKE”
DREJTIMI “AUTOMATIZIM I INDUSTRIË”

DISERTACION

NJË VËZHGIM NË PËRDORIMIN E TEKNOLOGJIVE TË KONTROLLIT TË
AVANCUAR PËR IDENTIFIKIMIN DIXHITAL NË INFRASTRUKTURËN
ROBUSTE

Udhëheqës Shkencor
Prof.Dr. Petrika MARANGO

Tiranë, 2017



**REPUBLIKA E SHQIPËRISË
UNIVERSITETI POLITEKNIK I TIRANËS
FAKULTETI I INXHINIERISË ELEKTRIKE**

Disertacioni
i paraqitur në Universitetin Politeknik të Tiranës
për marrjen e gradës shkencore
“Doktor”
Në Inxhinierinë Elektrike, drejtimi “Automatizim i Industrisë”
nga Znj. Miranda HARIZAJ

TEMA

**NJË VËZHGIM NË PËRDORIMIN E TEKNOLOGJIVE TË KONTROLLIT TË
AVANCUAR PËR IDENTIFIKIMIN DIXHITAL NË INFRASTRUKTURËN
ROBUSTE**

Mbrohet më datë 09/06/ 2017 para jurisë së miratuar nga rektori i UPT me shkresën
Nr. Prot.319/1 Datë 30.03.2017

Juria

I aprovuar nga

Prof. Dr. Aida SPAHIU	Kryetari i Jurisë
Prof. Dr. Orion ZAVALANI	Anëtar i Jurisë
Prof. Dr. Aleksandër XHUVANI	Anëtar i Jurisë
Prof. Assoc. Dr. Indrit ENESI	Anëtar i Jurisë, (oponent)
Prof. Assoc. Dr. Ana KTONA	Anëtar i Jurisë (oponent)

PËRMBAJTJA

PËRMBAJTJA.....	iii
LISTA E FIGURAVE.....	vi
LISTA E TABELAVE.....	xi
FALENDERIME	xii
ABSTRACT.....	xiii
PËRMBLEDHJE	xv
KAPITULLI 1 HYRJE.....	17
1.1 Hyrje	17
1.2 Motivimi i punimit.....	19
1.3 Qëllimi dhe kontributi i punimit	20
1.4 Struktura e punimit	21
KAPITULLI 2 TEKNOLOGJITË E KONTROLLIT TË AVANCUAR	22
2.1 Teknologjia dhe sistemet biometrike	22
2.1.1 Koncepte dhe përkufizime	22
2.1.2 Modalitetet biometrike	23
2.1.3 Arkitektura e sistemeve biometrike.....	25
2.1.3.1 Arkitektura e sistemit biometrik	26
2.1.4 Sistemet e identifikimit nëpërmjet biometrisë së shumëfishtë	29
2.1.5 Kufizimet dhe dobësitë e sistemeve biometrike.....	31
2.1.6 Vlerësimi i sistemeve biometrike	32
2.1.7 Sfidat në të ardhmen.....	38
2.2 Teknologjia e kartave inteligjente.....	38
2.2.1 Kartat inteligjente	38
2.2.2 Karakteristikat fizike	39
2.2.3 Kartat e kujtesës.....	39
2.2.4 Kartat pa kontakt(Contactless)	40
2.2.5 Kartat inteligjente përballë RFID	41
2.2.6 Kartat inteligjente me elementin biometrik: gjurmë papilare	41
2.2.7 Ndërveprimi me teknologjinë biometrike.....	41
2.2.8 Token(çelësi) personal	42
2.3 Teknologjia kriptografike	42

2.3.1 Kriptografia shkenca e sekretit	42
2.3.2 Kriptografia simetrike dhe asimetrike	43
2.3.3 Zbatime	43
2.3.4 Primitivët bazë të kriptografisë.....	43
2.3.5 Ndërveprimi me kartat inteligjente	45
2.3.6 Ndërveprimi me biometrinë.....	46
2.4 Sistemet krypto-biometrike	46
2.4.1 Skemat me Key release	48
2.4.2 Skemat me Key generation	49
KAPITULLI 3 ZGJIDHJE ROBUSTE PËR IDENTIFIKIMIN DIXHITAL.	
RASTE STUDIMORE.....	51
3.1 Hyrje	51
3.2 Standarti ISO/IEC 24745 - Mbrojtja e template-it biometrik	52
3.3 Zgjidhja e integruar në kartën inteligjente.....	53
3.3.1 ToC-Template on card (template-i në kartën inteligjente)	53
3.3.2 MoC-Match on card (krahasimi në kartën inteligjente)	54
3.3.3 SoC-System on card (sistemi në kartën inteligjente).....	55
3.3.4 Pse zgjidhja Match-on-Card?	55
3.3.5 Disa kufizime.....	56
3.4 Zgjidhja SBMoC-Secure Biometric Match on Card–Raste studimore.....	56
3.4.1 Letërnjoftimi elektronik - kartë inteligjente e standartit ISO/IEC 7816.....	56
3.4.2 Infrastruktura e Çelësit Publik	58
3.4.3 Platforma e shërbimeve elektronike e-Aleat – rast studimor.....	61
3.4 Vlerësimi i performancës së zgjidhjes MoC	62
3.4.1 MINEX I.....	62
3.4.2 MINEX II.....	63
KAPITULLI 4 BIOMETRIA E GJURMËS PAPILARE.....	66
4.1 Hyrje	66
4.2. Karakteristika dhe veçori të gjurmës papilare.....	67
4.2.1 Karakteristikat kryesore të gjurmës papilare	71
4.2.2 Sistemi i identifikimit biometrik me gjurmë papilare.....	75
4.2.1 Regjistrimi i gjurmëve papilare.....	76

4.2.2	Parapërpunimi	77
4.2.3	Ekstraktimi i karakteristikave.....	79
4.2.4	Krahasimi i gjurmës papilare	80
4.3	Problematika që kërkojnë zgjidhje.....	81
KAPITULLI 5 PËRMIRËSIMI I IMAZHIT TË GJURMËS PAPILARE		82
5.1	Hyrje	82
5.2	Teknikat më të përdorura të përmirësimit të imazhit	83
5.2.1	Përmirësimi në rrafshin e hapësirës	84
5.2.2	Përmirësimi në rrafshin e frekuencës	84
5.3	Teknika përmirësimi të imazhit të gjurmës papilare.....	84
5.3.1	Teknika e përmirësimit sipas L.Hong.....	84
5.3.2	Teknika e përmirësimit sipas S.Chikkerur nëpërmjet analizës STFT	91
5.3.3	Teknika e përmirësimit në dy-etapa duke mësuar nga imazhi fillestar	99
5.4	Një krahasim i teknikave të analizuara	105
5.5	Teknika e përmirësimit me piramidat e imazhit të Laplas-it	105
5.5.1	Piramidat e imazhit të Laplas-it	106
5.5.2	Zbatimi i piramidave të imazhit të Laplas-it në skemën me dy-etapa	109
5.5.3	Përmbledhje	110
KAPITULLI 6 ZBATIME, EKSPERIMENTE DHE INTERPRETIME PËR		
TEKNIKAT E PËRMIRËSIMIT.....		111
6.1	Ambienti i testimit.....	111
6.2	Krahasimi i metrikave dhe parametrave të cilësisë.....	112
6.3	Inspektimi Vizual.....	112
6.4	Parametra të matur	124
KAPITULLI 7 PËRFUNDIME DHE OBJEKTIVA.....		134
7.1	Përfundime të punimit.....	134
7.2	Objektiva për të ardhmen.....	136
LITERATURA		137
SHTOJCA.....		142
Kode në MATLAB		142
Baza e të dhënave publike FVC2004.....		161

LISTA E FIGURAVE

Figura 1-1. Inovacioni dhe industria SMART	18
Figure 2-1. Disa modalitete biometrike. Nga e majta në të djathtë, lart poshtë, fytyra, gjurmëpapilare, ecje, dinamika e shtypjes së tastierës, ADN, irisi, nyja e gishtit dhe informacioni për venat e dorës.....	23
Figura 2-2. Biometritë sipas karakteristikave fizike dhe të sjelljes.....	24
Figura 2-3.Shembuj të template-ve biometrike.....	25
Figura 2-4. Arkitektura e përgjithshme e sistemit biometrik.....	26
Figura 2-5. Skema logjike e sistemit biometrik	27
Figura 2-6. Procesi i përpunimit të gjurmës papilare.....	27
Figura 2-7. Krahasoni me bazë minutiae	28
Figura 2-8. Arkitektura e sistemit multimodal (a)seri; (b) parallel.....	29
Figura 2-9.Sinteza e e identifikimit nëpërmjet biometrisë së shumëfishtë (a)karakteristike (b) rezultati (c) vendimi	30
Figura 2-10. Pika të mundshme sulmi të identifikuar në një sistem biometrik(model sipas Ratha).....	32
Figura 2-11. Një gisht proteze krijuar nga latex	32
Figura 2-12.Vlerësimi i sistemeve biometrike	33
Figura 2-13. Cilësia e vlerësimit biometrik të të dhënave	33
Figure 2-14. Vlerat e FNMR dhe FMR për një vlerë të dhënë të pragut(t)	36
Figura 2.15. Kurba ROC: FAR kundrejt FRR	36
Figura 2-16. Paraqitja grafike CMC për tre sisteme biometrike	37
Figura 2-17. Prodhimi i kartave inteligjente	39
Figura 2-18. Arkitektura e një karte memorie.....	40
Figura 2-19. Arkitektura e ndërfaqes së komunikimit të një karte pa kontakt.....	40
Figura 2-20. Modeli i enkriptimit simetrik Shanon	44
Figura 2-21 Modeli i enkriptimit asimetrik.....	44
Figura 2-22. Modeli me funksionet Hash.....	44
Figura 2-23 Nënshkrimi dixhital	45
Figura 2-24. Koncepti bazë i sistemeve kriptobiometrike (a) me publikim të çelësit; (b) me gjenerim të çelësit	47
Figura 2-25. Diagramat skematike të fazave të aplikimit dhe autentifikimit në sistemet kriptobiometrike.....	47
Figura 2-26. Skema bazë e operimit Fuzzy Vault.....	48
Figura 2-26. Skema bazë e operimit Fuzzy Commitment.....	49

Figura 3-1. Pikat e dobëta ku paraqiten kërcënimet gjatë identifikimit dixhital.....	51
Figura 3-2. Arkitektura ISO/IEC 24275	52
Figura 3-3. Procesi i identifikimit me zgjidhjen ToC në kontrollin në kufi	54
Figura 3-4. Procesi i identifikimit me zgjidhjen MoC në kontrollin në kufi	54
Figura 3-5. Procesi i identifikimit me zgjidhjen SoC në kontrollin në kufi.....	55
Figura 3-6. Një specimen i letërnjoftimit elektronik.....	57
Figura 3-7. Bllokskema e identifikimit dixhital SBMoC.....	57
Figura 3-8. Protokolli gjatë krahasimit lokal biometrik në chip-in me kontakt në letërnjoftimin elektronik (MoC)	58
Figura 3-9. Konfiguracioni i Autoritetit certifikues (CA).....	59
Figura 3-10. Protokolli i identifikimit dixhital gjatë leximit të chip-it pa kontakt në pikat e kalimit kufitar.....	61
Figura 3-11. Bllokskema funksionale e infrastrukturës së platformës e-Aleat.....	62
Figura 3-12. Rezultatet e saktësisë MINEX II(më e saktë vlera më e ulët).....	64
Figura 3-13. Rezultatet e kohës së përgjigjes MINEX II.....	65
Figura 4-1. Lëkura e lëmuar.....	66
Figura 4-2. Lëkura e majës së gishtit.....	66
Figura 4-3. Imazhi gri i gjurmës papilare	68
Figura 4-4. Imazhi i gjurmës papilare i përmirësuar dhe i qartësuar	68
Figura 4-5. Vijat papilare fundore dhe degëzim	68
Figura 4-6. Procesi i krahasimit të minutiae-ve	69
Figura 4-7. Një çift gjurmësh papilare identike me minutiae të përputhura në maksimum... 70	
Figura 4-8. Një çift gjurmësh të ndryshme me shumë pak minutiae të përputhura	70
Figura 4-9. Harta orientuese - Niveli 1 i karakteristikave.....	71
Figura 4-10. Matja e orientimit të vijës papilare.....	72
Figura 4-11. Veçoritë e laqeve.....	72
Figura 4-12. Veçoritë e deltave.....	73
Figura 4-13. Vijë papilare fundore (a) me rreth të bardhë:degëzim (b) me katror të zi.....	74
Figura 4-14. Karakteristikat e nivelit 3	75
Figura 4-15. Struktura bazë e një sistemi identifikimi biometrik me gjurmë papilare	76
Figura 4-16. Sensorë të ndryshëm të regjistrimit të gjurmëve papilare	76
Figura 4-17. Sensorët me gjendje-solidë	77
Figura 4-18. Sensorët optikë.....	77
Figura 4-19. Shembuj të imazheve të gjurmëve papilare me cilësi të ulët.....	78
(a) gisht i thatë, (b) gisht i lagësht, dhe (c) gisht me shumë rrudha	78

Figura 4-20. Procesi i qartësimit të imazhit dhe ekstraktimit të karakteristikave të gjurmës papilare.....	79
Figura 4-21 Skema e ekstraktimit të karakteristikave të nivelit 1 dhe nivelit 2.....	79
Figura 4-22. Krahësim i suksesshëm me një rezultat = 614	80
Figura 4-23.Krahësim i pasuksesshëm me një rezultat = 7.....	81
Figura 5-1. Skanim me cilësi të mirë të gjurmës papilare.....	82
Figura 5-2. Procesi i përmirësimit të imazhit të gjurmës papilare	83
Figura 5-3. Diagrama e L.Hong përkemën e përmirësimit të gjurmës papilare	85
Figura 5-4. Rezultati i normalizimit (a) imazhi i hyrje; (b) imazhi i normalizuar	86
(M0=100, VAR0=100)	86
Figura 5-5. Vlerësimi i orientimit në pixel(x, y).....	86
Figura 5-6. Metoda e dritares së orientuar për të matur frekuencën e vijës papilare	87
Figura 5-7. Gjurma papilare origjinale e skanuar	91
Figura 5-8. Imazhi i përmirësuar i gjurmës papilare.....	91
Figura 5.10 Diagrama e skemës së përmirësimit me analizë STFT.....	93
Figura 5-11. (a) Imazhi origjinal i skanuar i gjurmës papilare; (b) Imazhi i orientuar; (c) Imazhi i filtruar në bazë të energjisë së zonave; (d) Imazhi pas filtrimit në frekuencë; (e) Imazhi i matur në koherencë këndore; (f) Imazhi përfundimtar i përmirësuar.....	97
Figura 5-12. (a) dhe (b) Imazhi origjinal i skanuar i gjurmës papilare dhe imazhi i përmirësuar (107 FVC2004DB1) ; (c) dhe (d) Imazhi origjinal i skanuar i gjurmës papilare dhe imazhi i përmirësuar (109 FVC2004DB1)	98
Figura 5-13. (a) dhe (b) Imazhi origjinal i skanuar i gjurmës papilare dhe imazhi i përmirësuar (101 FVC2004DB4) ; (c) dhe (d) Imazhi origjinal i skanuar i gjurmës papilare dhe imazhi i përmirësuar (104 FVC2004DB4)	98
Figura 5-14. Bllokskema e përmirësimit me dy-etapa	99
Figura 5.15. Dritarja përgjatë orientimit lokal të vijës papilare.....	102
Figura 5-16 Rezultatet e skemës së përmirësimit me dy-etapa :(a) imazhi origjinal 109.....	104
FVC2004DB1; (b) imazhi i përmirësuar); (c) imazhi origjinal 104 FVC2004DB1; dhe (d) imazhi i përmirësuar)	104
Figura 5-17. Piramida e Gaus-it.....	106
Figura5-18. Gjashtë nivelet e para të piramidës së Gaus-it për imazhin "Lena"	107
Figura 5-19. Katër nivelet e piramidës së Laplas-it për imazhin Lena"	108
Figura 5-20. Bllokskema funksionale e propozuar për zbërthimin me piramidat e Laplas-it	109
Figura 5-21. Bllokskema funksionale me shumë-etapa, me bazë LPD	110

Figura 6-1. Gjurmë papilare origjinale FVC2004DB1105	112
Figura 6-2. Imazh i përmirësuar me filtrimin Gabor	112
Figura 6-3. Imazhi i përmirësuar në skemën me dy-etapa	113
Figura 6-4. Imazhi i përmirësuar në skemën me shumë-etapa (LPD)	113
Figura 6-5. Gjurmë papilare me cilësi shumë të ulët FVC2004DB1101	114
Figura 6-6. Përmirësim i imazhit bazuar në analizën STFT	114
Figura 6-7. Përmirësim i imazhit me skemën me shumë-etapa (LPD)	115
Figura 6-8. Imazhi fillestar i gjurmës papilare 102 nga FVC2004DB1.....	115
Figura 6-9. Imazhi i piramidës së Laplas-it Niveli 1.....	115
Figura 6-10. Imazhi i piramidës sëLaplas-it Niveli 2	116
Figura 6-11. Imazi i piramidës së Laplas-it Niveli 1 i përmirësuar	116
Figura 6-12. Imazhi i piramidës së Laplas-itNiveli 2 i përmirësuar	116
Figura 6-13.Imazhi përmirësuar me analizën STFT me shtrembërime të theksuara	117
Figura 6-14. Imazhi përmirësuar me skemën me shumë-etapa (LPD), me më pak shtrembërime.....	117
Figura 6-15. (a) Imazhi origjinal 104 FVC2004 DB1; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD).....	118
Figura 6-16. (a) Imazhi origjinal 107 FVC2004 DB1; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD)	118
Figura 6-17. (a) Imazhi origjinal 101 nga FC2004 DB2; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD).	118
Figura 6-18. (a) Imazhi origjinal 104 FVC2004 DB2; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën e re me shumë-etapa (LPD).....	119
Figura 6-20. (a) Imazhi origjinal 104 FVC2004 DB3; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD)	119
Figura 6-21. (a) Imazhi origjinal 105 FVC2004 DB3; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD).....	120
Figura 6-22. (a) Imazhi origjinal 103 FVC2004 DB3; (b) Përmirësimi me analizën STFT; (c) Përmirësimi me skemën me dy-etapa; (d) Përmirësimi me skemën me shumë-etapa (LPD).	121
Figura 6-23. Minutia-t e ekstraktuara në katër imazhe gjurme papilare (a) Imazhi origjinal; (b) Imazhi përmirësuar me filtrin Gabor; (c) Imazhi i përmirësuar me analizën STFT; (d) Imazhi i përmirësuar me skemën me shumë-etapa (LPD)	122

Figura 6-24. Veprimi i qartësisë në (a) imazhin original 101FVC2004DB2; (b) përmirësimi i skemës me teknikën e filtrimit Gabor; (c) skema e përmirësimit me shumë-etapa (LPD)	123
Në figurën 6-25 tregohen minutiae-t e ekstraktuara nga imazhet e qartësuara të vëzhguara në figurën 6.24.	123
Figura 6-25. Minutia-t e ekstraktuara nga imazhi i qartësuar (a) imazhi original 101 FVC2004 DB2; (b) përmirësimi i skemës me teknikën e filtrimit Gabor; (c) skema e	123
Figura 6-26. Minutiae të nxjerra nga (a) imazhi original 103 FVC2004DB1, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)	125
Figura 6-27. Minutiae të nxjerra nga (a) imazhi origjinal 105 FVC2004DB2, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)	126
Figure 6-28. Minutiae të nxjerra nga (a) imazhi original 102 FVC2004DB3, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)	127
Figura 6-29 Krahاسimi i raporteve të minutiae TMR, FMR dhe mesatarja e tyre	130
Figura 6.30. Krahاسimi i rezultateve dhe shkallës së përmirësimit të parametrut EER(%)..	131
Figura 6-31. Grafiku i kohës mesatare për leximin, përpunimin e përmirësimit dhe ekstraktit të karakteristikave të imazheve	133

LISTA E TABELAVE

Tabela 2-1. Studimi krahasues i modaliteteve biometrike	24
Tabela 3-1 Mekanizmat të kontrollit të avancuar	59
Tabela 3-2 Rezultatet dhe krahasimet e performancës sipas MINEX II.....	64
Tabela 6-1 Llogaritja e minutiae të dedektuara për imazhe të bazës së të dhënave.....	128
Tabela 6-2 Numri i minutiae-ve të rreme të dedektuara në imazh.....	128
Tabela 6-3 Tabela e krahasimit të raporteve të minutiae TMR, FMR dhe mesatarja e tyre	129
Tabela 6.4 Rezultatet dhe shkalla e përmirësimit të parametrin EER (%).....	130
Tabela 6-5 Koha e përpunimit të imazheve sipas teknikave të përmirësimit.....	132

FALENDERIME

Përzemërsisht shpreh mirënjohjen time të thellë për udhëheqësin shkencor Prof.Dr. Petrika MARANGO për kontributin, ndihmën dhe mbështetjen e pamasë në realizimin e punimit.

Mirënjohje të veçantë për kontributin, bashkëpunimin dhe përkrahjen e vazhdueshme, drejtuesit të Fakultetit të Inxhinierisë Elektrike, Prof.Dr.Orion ZAVALANI dhe përgjegjësit të departamentit , Prof.Dr. Aida SPAHIU.

Një falenderim shkon për të gjithë miqtë e kolegët e Fakultetit të Inxhinierisë Elektrike dhe Fakultetit të Teknologjisë së Informacionit, në mënyrë të veçantë departamentin e Automatikës për kontributin dhe mbështetjen e dhënë.

Falenderoj familjen time që më ka mbështetur ngrohtësisht në çdo moment.

Miranda HARIZAJ

ABSTRACT

In the last decade we have distinguished specific aspects of the different processes automation, beyond the ordinary concept of "industrial processes". The theory and practice of automatic control has preceded this flow and has successfully solved the issues posed.

Interesting is the fact that these processes, which at first glance deviate from the "industrial" idea, still retain the same constituent elements. So they have a set of equipment and technology, where flows a process in space and in time, they have a product targeted to the market, and other defined elements in this classification.

On the basis of the requirements for these directions, special systems of automatic control have been constructed, of course with closed-loop signal flow, but with special specifications and with unusual products. We can say that the first contours were dictated by the financial system, the banking system, and the various sell-purchases. Further, with a rapid burst, automatic systems for identifying and verifying various parameters were established, the basic principles of which lie in the theory of automatic control. These systems have two distinct specifications:

1. Specific analogue and digital signals, converting from electric to audio or video, to images and continuous conversion.
2. A specific output product that does not coincide with common knowledge such as speed, flow, level, temperature, etc.

The particular purpose of this automation is the safety and authenticity of the product, which is the main objective of their implementation. Moreover, this fact today is a fundamental problem in scientific research, where in most cases is completed with very special and high-cost patents.

Harassment on these systems are two types:

- Common harassment as internal or external concerns, well-known by the theory of automatic control;
- Internal or external harassment, caused by intentional interference, intentionally for the reorganization of the existing structures for the benefit of another objective.

If the first group of harassments has as "defense" the theory of automatic control, analysis and synthesis of the structure, the second group enriches this theory with many new mathematical elements in terms of active protection of the designed automation.

Exactly, the second orientation of these automation structures is the object of this thesis, with a modest contribution to reasoning and a series of experiments carried out. In this point of view, as the main harassment of the second group are treated thefts and fraud in terms of identity of persons, more simply, the legal

protection of the person and his data by additional components in the construction and automation of a process.

Meanwhile, population growth and the use of information technology-based services have revealed a growing risk of identity theft and fraud. The system qualifies as both the user and the intruder as the disturbing harassments to be faced by the closed automation contour.

With the above specifications, in this thesis, advanced control technologies in these areas have been analyzed, and further, a robust solution for digital identification is proposed. The core idea is based on advanced control and assessment of individual identity through digital control and local biometric comparison, based on the smart card.

Thus, to achieve this, a set of parameters that have to be kept in control and improved constantly have been evaluated, where among them, the main is the quality of the biometric image recorded.

Over the years, researchers have considered fingerprints as unique to each individual and have used them as a basic control element in their biometric identification systems through the use of a proper mathematical model for fingerprint orientation.

The quality of the recorded image has a major impact on the results of comparison and identification and therefore improving quality and eliminating noise in the recorded image is crucial to guaranteeing a reliable digital identification process in robust infrastructure.

In this work, several techniques have been implemented to improve the image quality of fingerprints and after evaluating and comparing the measured results, an improvement scheme is proposed as a robust one by combining the two stages of improvement in the space and frequency domain with pyramid of images techniques.

Evaluated and proposed techniques as most efficient for improvement of the image of the captured fingerprints are implemented in MATLAB. The results are obtained by measuring various image quality parameters such as image processing time, True Minute Ratio (TMR), and False Minute Ratio (FMR), etc for images taken from the FVC2004, a public fingerprints database. The conclusions are drawn on the basis of comparison of their efficiency and improvements dedicated by each technique.

I conclude with the modesty that the presented work finalises the studies and the research accomplished at the Department of Automation, Faculty of Electrical Engineering.

PËRMBLEDHJE

Në dhjetëvjecarin e fundit dallojmë aspekte të veçanta të automatizimit të proceseve të ndryshme përtej konceptit të zakonshëm si “proceset industriale”. Teoria dhe praktika e kontrollit automatik i ka paraprirë kësaj prurje dhe i ka zgjidhur me sukses problemet e parashtruara.

Është interesant fakti, që edhe këto procese, që në pamje të parë devijojnë nga idea “industriale”, përsëri ruajnë po ato elemente përbërës. Kështu ata kanë një tërësi pajisjesh dhe teknologji, ku rrjedh një proces në hapësirë dhe në kohë, ata kanë një produkt me objektiv tregun, dhe elemente të tjerë të përkufizuar në këtë klasifikim.

Mbi bazën e kërkesave për këto drejtime janë konstruktuar sisteme të veçanta të kontrollit automatik, sigurisht me rrjedhje të sinjalit në kontur të mbyllur, por me specifika të veçanta dhe me produkte jo të zakonshme. Mund të themi se konturet e para u diktuan nga sistemi finaciari, sistemi bankar dhe shit-blerjet e ndryshme.

Me tej, me një hov të shpejtë u ngritën sisteme automatike të identifikimit dhe verifikimit të parametrave të ndryshme, parimet bazë të cilave qëndrojnë në teorinë e kontrollit automatik. Këta sisteme kanë dy specifika të dallueshme:

1. Sinjale të veçanta analoge dhe dixhitale, që kalojnë nga elektrike në audio ose video, në imazhe dhe konvertim të vazhdueshëm.
2. Një produkt specifik në dalje që nuk përkon me njohuritë e zakonshme si shpejtësi, prurje, nivel, temperaturë, etj.

Qëllimi i veçantë i këtij automatizimi është siguria dhe vërtetësia, e produktit, kjo përbën dhe objektivin kryesor të ndërtimit të tyre. Për më tepër ky fakt sot është problem themelor në kërkimin shkencor, ku në shumicën e rasteve përfundohet me patenta shumë të veçanta e me kosto të lartë.

Ngacmimet mbi këto sisteme janë dy llojesh:

- Ngacmime të zakonshme si shqetësime të brendshme ose të jashtme, të mirënjohura nga teoria e kontrollit automatik;
- Ngacmime të brendshme ose të jashtme, të shkaktuara nga ndërhyrje të qëllimshme, me dashje për ti riorganizuar strukurat ekzistuese në dobi të një objekti tjetër.

Në qoftëse grupi i parë i ngacmimeve ka si “mbrojtje” teorinë e kontrollit automatik, analizën dhe sintezën e strukturës, grupi i dytë e pasuron këtë teori me shumë elemente të rinj matematikore në drejtim të mbrojtjes aktive të automatizimit të projektuar.

Pikërisht, drejtimi i dytë i këtyre strukturave të automatizimit, përbën dhe objektin e këtij punimi, me një kontribut modest në arsyetim dhe me një sërë eksperimentesh të realizuara. Në këtë trajtim, si ngacmime kryesore të grupit të dytë janë trajtuar vjedhjet dhe mashtrimet në drejtim të identitetit të personave, më

thjesht, mbrojtja juridike e personit dhe e të dhënave të tij nga komponentë shtesë në konstruktimin e automazimit e një procesi.

Ndërkaq, rritja e popullsisë dhe përdorimit të shërbimeve me bazë teknologjinë e informacionit, kanë bërë të dukshme një rrezik të madh në rritje të vjedhjes së identitetit dhe mashtrimeve. Sistemi kualifikon në të njëjtën mënyrë si përdoruesin, po ashtu dhe keqbërësin, si ngacmim shqetësues që duhet përballur nga konturi i mbyllur i automatizimit.

Me specifikat e mesipërme, në këtë punim janë analizuar teknologjitë e avancuara të kontrollit në këto fusha dhe me tej propozohet një zgjidhje robuste për identifikimin dixhital. Ideja kryesore bazohet në teknikat e avancuara të kontrollit dhe vlerësimin e identitetit të individit nëpërmjet kontrollit dixhital dhe krahasimit lokal biometrik me bazë kartën inteligjente.

Kështu, për të arritur këtë, janë vlerësuar një sërë parametrash të cilët duhen mbajtur në kontroll dhe përmirësuar vazhdimisht, ku ndër kryesorët është cilësia e imazhit biometrik të regjistruar.

Ndër vite, studiuesit i kanë konsideruar gjurmët papilare si unike për çdo individ dhe i kanë përdorur si element bazë kontrolli në sistemet e tyre të identifikimit biometrik nëpërmjet përdorimit të modelit të duhur matematikor për orientimin e gjurmëve papilare.

Cilësia e imazhit të regjistruar ka një ndikim kryesor në rezultatet e krahasimit dhe identifikimit dhe për këtë arsye përmirësimi i cilësisë dhe eliminimi i zhurmave në imazhin e regjistruar është vendimtare në garantimin e procesit të identifikimit dixhital të besueshëm në një infrastrukturë robuste.

Në punim janë marrë në studim disa teknika të përdoruara për përmirësimin e cilësisë së imazhit të gjurmës papilare dhe pas vlerësimit dhe krahasimit të rezultateve të matura është propozuar si më robuste një skemë përmirësimi me anë të kombinimit të dy etapave të përmirësimit në fushën e hapësirës dhe frekuencës dhe më përdorimin e teknikave të piramidave të imazhit.

Teknikat e vlerësuara dhe të propozuara si më efikase për përmirësimin e imazhit të gjurmës papilare të regjistruar në hyrje janë implementuar në ambientin MATLAB. Rezultatet merren nga matja e parametrave të ndryshëm të cilësisë së imazhit si koha e përpunimit të imazhit, raporti i minutiae të vërteta (TMR) dhe raporti i minutiae të jo të vërteta (FMR) për imazhet e marra nga baza e të dhënave publike të gjurmëve papilare FVC2004. Përfundimet nxirren në bazë të krahasimit të efikasitetit të tyre dhe përmirësimet e sjella nga secila teknikë.

Përfundoj, me modesti, që punimi i paraqitur të kurorëzohet shkollën e doktoraturës që kam kryer pranë Departamentit të Automatikes, Fakulteti i Inxhinierise Elektrike.

KAPITULLI 1

HYRJE

1.1 Hyrje

Sistemet e kontrollit industrial[1] monitorojnë dhe kontrollojnë procese të natyrave tëndryshme, shpesh në infrastruktura kritike si termocentrale dhe rrjeti energjitik, sistemet e shpërndarjes së ujit, naftës dhe gazit, monitorimi i ndërtesave, sistemet e prodhimit të ushqimit, makinave e produkteve të tjera. Dështime të hërëpashërëshme në sigurinë e infrastrukturave kritike kanë shkaktuar pasoja në jetët njerëzore dhe kanë sjellë dëme në objektet industriale, për shkak të sulmeve kibernetike dhe ndërhyrjeve të paautorizuara. Raportet e fundit të publikuara tregojnë që këto infrastruktura kritike nuk janë të mbrojtura mjaftueshëm kundrejt sulmeve kibernetike dhe ndërhyrjeve të paautorizuara.

Sipas një raporti të publikuar në vitin 2012, nga Departamenti i Drejtësisë së Shteteve të Bashkuara të Amerikës[5] afro 2700 organizata që monitorojnë infrastrukturën kritike në ShBA, identifikuan që vetëm në vitin 2009 afro 13 milion incidente të krimit kibernetik shkaktuan një humbje monetare prej 288 milion dollarë dhe mosfunksionim të sistemeve për rreth 150 000 orë.

Numri në rritje i incidenteve të sigurisë[1] në sistemet e kontrollit industrial shkaktohet ngakombinimi i dobësive teknologjike dhe organizative, që lejojnë devijimin e procesit industrial nga ndërhyrjet e paautorizuara.

Me zhvillimet e fundit teknologjike, nëpërmjet industrisë dhe shërbimeve "smart" [2] [3] [4] [5] dhe në "cloud", identifikimi dixhital i përdoruesve dhe klientëve, është konsideruar tashmë një domosdoshmëri, si pjesë e pandarë e zgjidhjes robuste të sistemeve të ndryshme të kontrollit. Disa nga zgjidhjet dhe tendencat e fundit të teknologjisë të së ardhmes, të cila janë ilustruar dhe në figurën 1-1 janë:

- Fabrikat e të ardhmes;
- Pajisjet dhe sistemet “e gatshme”;
- Sistemet e integruara në rrjet të qëndrueshëm ;
- Virtualizimi and clusterizmi “Cloud”;
- Printimi 3D ;
- Integrimi dydrejtimësh me sistemet e biznesit(informacion mbi prodhimin/konsumin);
- Menaxhimi i informacionit me vlerë, analiza e performancës së lartë, raportimi etj;

- Bashkëpunimi ndërmjet bizneseve virtuale;
- Dyqane me fleksibilitet të lartë për të akomoduar ndërmarrjet virtuale;
- Ofrimi i të gjitha shërbimeve nëpërmjet teknologjive smart.



Figura 1-1. Inovacioni dhe industria SMART

Evolimi i mëtejshëm i sistemeve të kontrollit industrial, shtrirja dhe përmasat gjithmonë e më të mëdha të aksesit në internet sjellin me vete riskun për ndërhyrje të pautorizuara[5][6][7]. Për këtë arsye, në mënyrë që të shmanget devijimi i procesit industrial nga ndërhyrjet e paautorizuara, si dhe rreziku i madh në rritje i vjedhjes së identitetit dhe mashtrimeve është identifikuar se janë të domosdoshme përmirësimet e nevojshme për këto sisteme, minimumi një hap para keqbërësve, si dhe zbatimi si pjesë e sistemit të kontrollit me zgjidhje nëpërmjet teknologjive të avancuara [6][7] dhe në përputhje me zhvillimet teknologjike, në mënyrë që të garantohen një zgjidhje robuste për identifikimin dixhital të besueshëm të individëve në përgjithësi dhe përdoruesve të sistemeve në veçanti.

Zgjidhjet tradicionale të përdorura për identifikimin dixhital të përdoruesve vërtetojnë identitetin e tyre në bazë të njohurive dhe token-ave të tilla, si fjalëkalime e karta inteligjente, të cilat janë të prekshëm nga vjedhjet dhe kopjet, edhe pse janë mbrojtur me mekanizma dhe përafrime kontrolli.

Vlen të theksojmë se për më shumë se një shekull, njohja biometrike me gjurmë papilare është përdorur me sukses në procesin e identifikimit të të dyshuarve dhe viktimave në zbatimet mjeko-ligjore dhe të zbatimit të ligjit.

Identifikimi me anë të gjurmëve papilare është realizuar[9][22][29] kryesisht në teknikat e krahasimit të bazuar në tipare, të cilat kanë një interpretim fizik dhe ekstrahojnë tipare të qarta nga imazhi nën vlerësim dhe shifrojnë këto tipare në një grup karakteristikash, të cilat përdoren për krahasim. Gjurmët papilare, të cilat regjistrohen në hyrje si një imazh, në shumicën e rasteve janë nën efektin e zhurmave dhe korruptohen prej tyre.

Tipari biometrik i gjurmës papilare[8][12][16] është provuar të jetë zgjidhja më e përdorur dhe e suksesshme, pasi gjurmët papilare nuk ndryshojnë me kalimin e moshës, struktura e vijave papilare në secilin gisht është unike edhe ndërmjet binjakëve identikë. Duhet theksuar fakti që procesi i krahasimit të gjurmëve papilare është relativisht jo i shtrenjtë në krahasim me format e tjera të biometrisë.

Nevojat në rritje dhe zhvillimet e fundit[42] në sistemet automatike të identifikimit me gjurmë papilare (Automatic Fingerprint Identification System-AFIS) janë shoqëruar me rritjen e nevojës për identifikim të besueshëm të identitetit të individëve dhe kanë sjellë përdorimin në një shkallë të gjerë të këtyre sistemeve të identifikimit.

Ndër vite, me përdorimin e njohjes biometrike me gjurmë papilare në fusha e sisteme të ndryshme kontrolli janë identifikuar probleme të ndryshme, të cilat duhen adresuar dhe trajtuar, për të cilat studiues të ndryshëm kanë propozuar teknika e përafrime të ndryshme përmirësimi.

1.2 Motivimi i punimit

Në ditët e sotme, sisteme të ndryshme industriale dhe ato të teknologjisë së informacionit kanë zhvilluar teknika të reja me funksionalitete të avancuara kontrolli për sigurinë dhe mbrojtjen e tyre. Nevoja për zgjidhje që garantojnë mbrojtjen dhe aksesin e autorizuar jo vetëm në sistemet dhe aplikimet industriale, por edhe në ato të sigurisë, të transportit publik dhe të jetës sonë të përditshme janë objekt vlerësimi për shumë studiues për projektimin e infrastrukturave robuste dhe të besueshme për identifikimin dixhital të individëve dhe përdoruesve të autorizuar nëpërmjet teknologjive të avancuara të kontrollit. Identifikimi dixhital i individit në një infrastrukturë robuste është një prej zgjidhjeve që garantojnë mbrojtjen, aksesin e autorizuar në sisteme dhe privatësinë e të dhënave, me anë teknikave të avancuara të kontrollit në këtë fushë.

Identifikimi dixhital me gjurmë papilare është një nga teknikat e avancuara të kontrollit që bazohet në tipare, të cilat kanë një interpretim fizik.

Një teknikë krahasimi e bazuar në tipare, ashtu siç emërtohet ekstrahon tipare të qarta nga imazhi nën vlerësim dhe shifron këto tipare në një grup karakteristikash, të cilat më tej përdoren për krahasim. Proces i krahasimit të gjurmëve papilare ka avantazhet dhe disavantazhet e tij. Studime të ndryshme tregojnë se janë identifikuar raste të shumta kur vetë sistemet biometrike të identifikimit kanë rënë pre e sulmeve të prezantuara, duke kompromentuar në disa raste efikasitetin dhe përdorimin e tyre. Një nga dobësitë e këtyre sistemeve, që në rastin më të mirë ul performancën e sistemit të identifikimit dixhital është cilësia jo e lartë e imazhit të regjistruar dhe kjo për arsye të ndryshme.

Për këtë arsye është identifikuar nevoja për përmirësim jo vetëm të teknikave dhe algoritmeve të kontrollit të template-ve biometrike në sistemet e identifikimit, por dhe të përmirësimit të cilësisë së imazhit të regjistruar. Duke qenë se gjurmët papilare regjistrohen si

një imazh, është pothuaj e sigurt që ato do të korruptohen nga zhurma. Cilësia e imazhit të marrë të gjurmës papilare ndikohet nga një sërë faktorësh në hyrje, si tipi i sensorit dhe shtrembërime të vijës papilare nga një gisht i thatë ose me lagështi.

Cilësia e imazhit të regjistruar të gjurmës papilare ka një ndikim të rëndësishëm në rezultatet e krahasimit dhe identifikimit dixhital dhe për këtë arsye shmangia e zhurmave nga imazhi i marrë dhe përmirësimi i cilësisë së imazhit është vendimtare për të garantuar një infrastrukturë robuste për identifikimin dixhital.

1.3 Qëllimi dhe kontributi i punimit

Në këtë punim janë analizuar dhe vlerësuar zgjidhjet aktuale dhe teknologjitë e avancuara të kontrollit për identifikimin dixhital të tilla si: kriptografia, njohja biometrike dhe karta inteligjente, si dhe ndërveprimi i tyre në zgjidhjet e vlerësuara si robuste për identifikimin dixhital.

Në këtë punim kemi vlerësuar dhe ilustruar me raste studimore zgjidhjen më efikase për identifikimin dixhital, që bazohen në përdorimin e kartës inteligjente në një infrastrukturë robuste të Çelësit Publik, ku çelësi privat është i mbrojtur me identifikim lokal biometrik (match on card) dhe realizohet nëpërmjet mekanizmave kriptografikë të kontrollit të avancuar në chipin e kartës inteligjente.

Kjo zgjidhje realizohet me përdorimin e teknologjive dhe mekanizmave të avancuar të kontrollit, që kanë si element bazë të kontrollit, tiparin biometrik të gjurmës papilare. Identifikimi dixhital nëpërmjet kësaj zgjidhje të propozuar është bazuar në diçka që është unike për secilin individ dhe kërkon prezencën e tij gjatë procesit të identifikimit dixhital. Kjo është edhe një zgjidhje praktike, pasi eliminon nevojën që përdoruesi të mbajë mend ndonjë informacion të fshehtë dhe shmang humbjen apo dekonspirimin e tij.

Nevoja e identifikuar për përmirësimin e cilësisë së imazhit të regjistruar në hyrje të sistemit të identifikimit dixhital është përkthyer në shtimin e një hallke për përmirësimin e cilësisë së imazhit të regjistruar në hyrje të tij.

Në këtë punim janë marrë në studim teknikat më të përdorura të përmirësimit të cilësisë së imazhit të cilat janë vlerësuar dhe është krahasuar performanca e tyre nëpërmjet rezultateve të matura. Një nga skemat e përmirësimit të propozuara si më efikase në fushën e hapësirës ka si objekt kryesor rindërtimin e vijave papilare të thyera nga lëmimi i imazhit, ndërsa përmirësimi në fushën e frekuencës ka si objektiv eliminimin e zhurmës nëpërmjet përdorimit të filtrit brezlejuar të drejtuar që mat orientimin dhe frekuencën e vijave të gjurmëve papilare.

Teknika e propozuar si zgjidhja më robuste për identifikimin dixhital është përmirësimi i cilësisë së imazhit nëpërmjet përdorimit të piramidave të imazhit të Laplas-it për zbërthimin (LPD) dhe rindërtimin e imazhit (LPR) të gjurmës papilare në skemën e përmirësimit me shumë-etapa, si dhe janë evidentuar nevojat për përmirësim të mëtejshëm në të ardhmen.

1.4 Struktura e punimit

Pjesa e mbetur e punimit është e organizuar në kapitujt si më poshtë:

- Në kapitullin e dytë prezantohen, analizohen dhe vlerësohen teknologjitë e avancuara të kontrollit si sistemet biometrike, kriptografia, karta inteligjente, si dhe zhvillimet, ndërveprimet teknologjike dhe përmirësimet ndër vite.
- Në kapitullin e tretë është propozuar integrimi dhe ndërveprimi i teknologjive të trajtuara të kontrollit të avancuar të identifikimit dixhital, si zgjidhje robuste, që ilustrojnë rastet studimore të pëzgjedhura. Infrastruktura më efiçente e propozuar për identifikimin dixhital është zgjidhja që bazohet në përdorimin e kartave inteligjente në një infrastrukturë robuste të Çelësit Publik, me anë të identifikimit lokal biometrik (match on card) dhe nëpërmjet mekanizmave të kontrollit të avancuar në chipin e kartës inteligjente.
- në kapitullin e katërt përshkruhen biometria e gjurmës papilare, karakteristikat më të rëndësishme të një gjurme papilare dhe të sistemit e krahasimit të tyre;
- në kapitullin e pestë shpjegohet nevoja për përmirësimin e imazheve të gjurmëve papilare, në një sistem identifikimi biometrik dhe analizohen katër teknika të ndryshme të përmirësimit të imazhit të gjurmës papilare. Gjithashtu në këtë kapitull prezantohen dhe algoritmet përkatëse të përmirësimit të teknikave të vlerësuara. Në këtë kapitull prezantohet si zgjidhja më robuste, teknika e propozuar me piramidat e imazhit të Laplasit për zbërthimin dhe rindërtimin e imazhit të gjurmës papilare në skemën e propozuar me shumë etapa.
- Në kapitullin e gjashtë zbatohen, eksperimentohen dhe interpretohen rezultatet për teknikat e përmirësimit të vlerësuara, me imazhe me cilësi të ndryshme të marra nga baza e të dhënave publike FVC2004, si dhe krahasohen rezultatet për të nxjerrë përfundimet mbi performancën dhe efiçensën e teknikave të përmirësimit;
- Së fundi, paraqiten përfundimet e punimit dhe objektivat e punës në të ardhmen.

KAPITULLI 2

TEKNOLOGJITË E KONTROLLIT TË AVANCUAR

2.1 Teknologjia dhe sistemet biometrike

Biometria[8] konsiderohet si një zgjidhje premtuese midis metodave tradicionale të bazuara në "atë që ne kemi" (si një çelës) ose "çfarë ne dimë" (si një fjalëkalim). Ajo është e bazuar në "ajo që ne jemi" dhe "si sillemi". Pak njerëz e dinë se për shumë vite biometritë janë përdorur për qëllime të identifikimit ose të nënshkrimeve dixhitale. Në vitin 1928, shenjat e gishtave janë përdorur për gratë klerike punonjëse të departamentit të policisë në Los Angeles. Shenjat e gishtave janë të përdorur si një nënshkrim për shkëmbimet tregtare në Babiloni (3000 para lindjes së Krishtit). Alphonse Bertillon propozoi për herë të parë në vitin 1879 që informacionet antropometrike të përdoreshin për hetimet e policisë.

Në ditët e sotme, të gjitha forcat policore në botë e përdorin këtë lloj informacioni për të hetuar e zbuluar krimet. Prototipet e para të terminaleve që siguronin një përpunim automatik të zërit dhe modeleve numerike të gjurmëve papilare kanë marrë formën e tanishme në mes të viteve 1970. Në ditët e sotme, sistemet biometrike të identifikimit kanë gjetur shumë zbatime si në kontrollin kufitar, aksesin e autorizuar, e-tregti[9] etj. Përfitimet kryesore të kësaj teknologjie janë rritja e sigurisë dhe lehtësimi i procesit të vërtetimit të identitetit dixhital të një përdoruesi qoftë në sistemet dhe aplikimet industriale dhe në ato të jetës së përditshme. Kjo pasi është shumë më e vështirë të kopjohen karakteristikat biometrike të një individi, në krahasim me shumicën e metodave të tjera të identifikimit të tilla si fjalëkalimet.

Pavarësisht nga përparësitë e dukshme të sistemeve biometrike, përdorimi i tyre në këto vite nuk ka qenë në nivelet e synuara. Pengesë kryesore ka qenë pasiguria e rezultatit të identifikimit(verifikimit) dixhital[10][11]. Në kontrast me kontrollin e fjalëkalimit, verifikimi i të dhënave biometrike të marra nga një individ është subjekt i gabimeve të mundshme që nuk garanton një rezultat 100% të saktë. Të tjera kufizime lidhen me çështjet e përdorshmërisë [41][42][43][44]. Veç kësaj, që të përdoret në një kontekst industrial, sistemi biometrik duhet të përcaktohet me saktësi të lartë. Ne kemi nevojë për një metodologji vlerësimi të besueshme, në mënyrë që të duket qartësisht përfitimi nga përdorimi i një sistemi të ri identifikimi dixhital.

Disa pyetje të ngritura: A duhet t'i besojmë kësaj teknologjie për përdorimin gjatë identifikimit dixhital? Çfarë lloj modalitetesh biometrike mund të përdoren? Cilat janë tendencat në këtë fushë? Këto janë disa nga pyetjet, përgjigjet e të cilave do të trajtojmë nëpërmjet një metodologjie vlerësimi të sistemeve biometrike.

2.1.1 Koncepte dhe përkufizime

Fjala biometri[8] rrjedh nga greqishtja dhe ajo bashkon "bios" me "metron" dhe ka kuptimin "matje e jetës". Në kuptimin e saj të parë, ajo ishte përkufizuar si pjesë e shkencës

biologjike e cila zbaton metoda statistikore dhe formula probabilitare në qeniet e gjalla. Në sigurinë kompjuterike, biometria i referohet teknikave të identifikimit që mbështeten në karakteristikat e matshme fizike, të cilat mund të kontrollohen me teknika të automatizuara.

2.1.2 Modalitetet biometrike

Çdo informacion biometrik që mund të diskriminojë individin është konsideruar si një modalitet biometrik[11]. Një shembull i modaliteteve biometrike është paraqitur në figurën 2-1. Një informacion biometrik "i përsosur" duhet të respektojë cilësitë e mëposhtme:

- Universaliteti: të gjithë individët duhet të karakterizohen nga ky informacion;
- Uniciteti: ky informacion duhet të jetë aq i ndryshëm dhe në të njëjtën kohë dhe unik për çdo individ;
- Qëndrueshmëria: informacioni biometrik duhet të jetë i pranishëm gjatë gjithë jetës së një individi;
- Mbledhshmëria: informacioni biometrik duhet mbledhur që të mund të matet në mënyrë të lehtë;
- Pranueshmëria: të bëjë të mundur përdorim të vërtetë nga ana e individit.



Figure 2-1. Disa modalitete biometrike. Nga e majta në të djathtë, lart poshtë, fytyra, gjurmëpapilare, ecje, dinamika e shtypjes së tastierës, ADN, irisi, nyja e gishtit dhe informacioni për venat e dorës

Teknologjitë e identifikimit biometrik janë metoda të automatizuara të verifikimit ose të njohjes së identitetit të një individi bazuar në karakteristikat fizike dhe të sjelljes si në figurën 2-2.

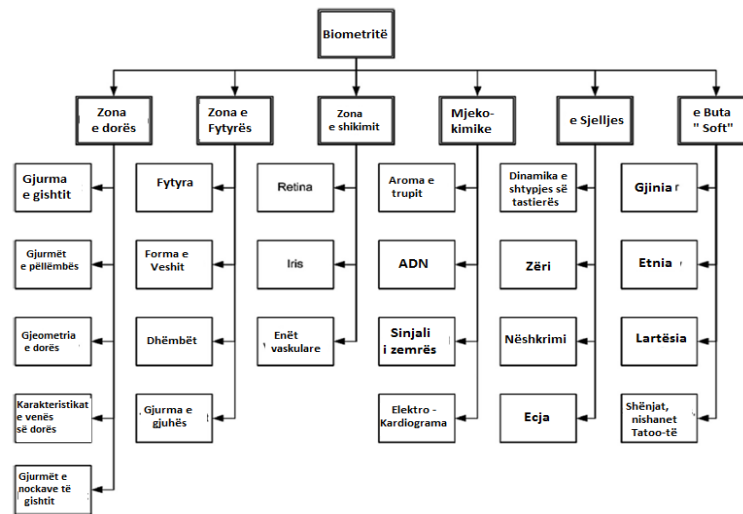


Figura 2-2. Biometritë sipas karakteristikave fizike dhe të sjelljes

Në tabelën 1-1 paraqiten rezultatet e një studimi krahasues të modaliteteve biometrike në drejtim të universalitetit, unicitetit, qëndrueshmërisë, mbledhshmërisë dhe pranueshmërisë[12] [39][40][43]. Nga kjo tabelë, mund të nxjerrim përfundimin se asnjë prej informacioneve biometrike nuk përmbush, në të njëjtën kohë të gjitha këto cilësi. Për shembull, analiza e ADN-së është një nga teknikat më efikase për të verifikuar identitetin e një individi apo për ta identifikuar individin.

Megjithatë, ajo nuk mund të përdoret për kontroll logjik apo akses kontrolli fizik jo vetëm për arsye të llogaritjes kohore, por edhe sepse e kemi të vështirë të gjejmë individë të gatshëm për të dhënë template-in e nevojshëm të gjakut për të bërë verifikimin. Për këtë arsye, duhet të zgjedhim një modalitet të veçantë për një aplikim të veçantë dhe për një grup të veçantë individësh.

Tabela 2-1.Studimi krahasues i modaliteteve biometrike

Informacioni	Univer.	Unic.	Qëndr.	Mbledh.	Pranuesh.	Perform
ADN	Po	po	Po	E dobët	E dobët	*****
Ecje	Po	Jo	E dobët	Po	Po	***
Dinamika e shtypjes së tastierës	Po	Po	E dobët	Po	Po	*****
Zëri	Po	Po	E dobët	Po	Po	*****
Iris	Po	Po	Po	Po	E dobët	*****
Fytyra	Po	Jo	E dobët	Po	Po	*****
Gjeometria e dorës	Po	Jo	Po	Po	Po	*****
Gjurma papilare	Po	Po	Po	Po	Mjaftueshëm	*****

2.1.3 Arkitektura e sistemeve biometrike

Procesi i identifikimit biometrik[20][25][46] në sistemet biometrike është i kategorizuar në tre procese kryesore :

Regjistrimi

Regjistrimi përbën procesin fillestar të regjistrimit të template-tit(modeli numerik të karakteristikave të elementit biometrik) të të dhënave biometrike nga një individ, i cili ekstrahet në një template reference që përfaqëson një identitet të përdoruesit dhe që më vonë do të përdoret për krahasim në sistemin e identifikimit. Një shembull i template-ve të modaliteteve të ndryshme të individëve është dhënë në figurën 2-3., ku nga e majta në të djathtë, nga lart poshtë ilustrohen minutiae-t nga një gjurmë papilare, kodi iris, grafik me bazë fytyrën, duke përdorur pika kyçe, vokali dhe sinjalet dinamike të tastierës.

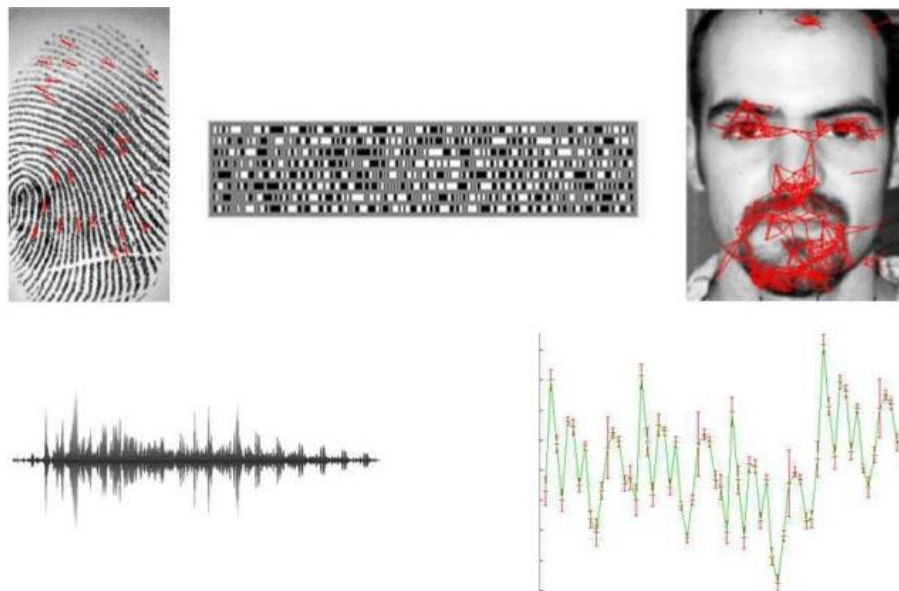


Figura 2-3.Shembuj të template-ve biometrike

Verifikimi

Verifikimi siguron rezultatin e përputhjes midis template-it biometrik të marrë nga individ dhe template-it të tij të ruajtur në bazën e të dhënave. Rezultati i përputhjes ndodhet ndërmjet vlerave 0% dhe 100% (100% është e pamundur të arrihet).

Identifikimi

Identifikimi është përcaktimi i identitetit të një individ të panjohur në një bazë të dhënash e pararegjistruara. Në këtë rast, sistemi ose i atribuon identitetin që i korrespondon profilit kandidat, më të ngjashëm të gjetur në bazën e të dhënave, individit të panjohur (ose një listë të profileve më të ngjashme), ose refuzon individin.

2.1.3.1 Arkitektura e sistemit biometrik

Arkitektura e përgjithshme e sistemit biometrik e ilustruar[47][48] në figurën 2-4, ka komponentët bazë si më poshtë:

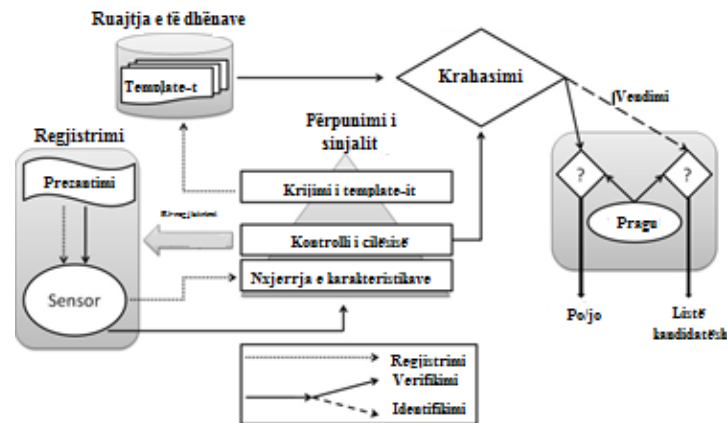


Figura 2-4. Arkitektura e përgjithshme e sistemit biometrik

- **Moduli i Kapjes**

Ky modul përbëhet nga kapësi i të dhënave biometrike që na mundëson të ekstraktojmë një përfaqësim numerik nga imazhi i elementit biometrik. Ky përfaqësim përdoret pastaj për regjistrim, verifikim ose identifikim.

- **Moduli i procesimit të sinjalit**

Ky modul lejon uljen e përfaqësimit numerik të ekstraktuar në mënyrë që të optimizojë sasinë e të dhënave të ruajtura gjatë fazës së regjistrimit, ose për të lehtësuar kohën e përpunimit gjatë fazave të verifikimit dhe identifikimit. Ky modul është i pajisur një funksion test të cilësisë për të kontrolluar të dhënat biometrike të kapura.

- **Moduli Storage**

Ky modul shërben për të ruajtur template-t biometrike të individëve.

- **Modul i përputhjes**

Ky modul shërben për të krahasuar të dhënat e nxjerra biometrike të një ose më shumë templateve biometrike të mëparshme. Prandaj ky modul përcakton shkallën e ngjashmërisë ose divergjencës ndërmjet dy vektorëve biometrike.

- **Moduli i vendimit**

Ky modul shërben për të përcaktuar nëse indeksi i ngjashmërisë është i mjaftueshëm për të përcaktuar identitetin e një individi. Një sistem biometrik është një sistem identifikimi, i cili krahason karakteristikat e dukshme ose diskriminuese të template-it të ri të regjistruar (që do të verifikohet/ identifikohet) me karakteristikat e template-ve të para-ruajtura (baza e të dhënave), e cila paraqitet në figurën 2-5. Në mënyrë specifike, sistemi biometrik ruan të dhënat referencë të një individi/përdoruesi, të gjeneruara gjatë procesit të regjistrimit, për ti krahasuar gjatë procesit të verifikimit/ autentifikimit ose identifikimit me të dhënat e reja të regjistruara të kandidatit.

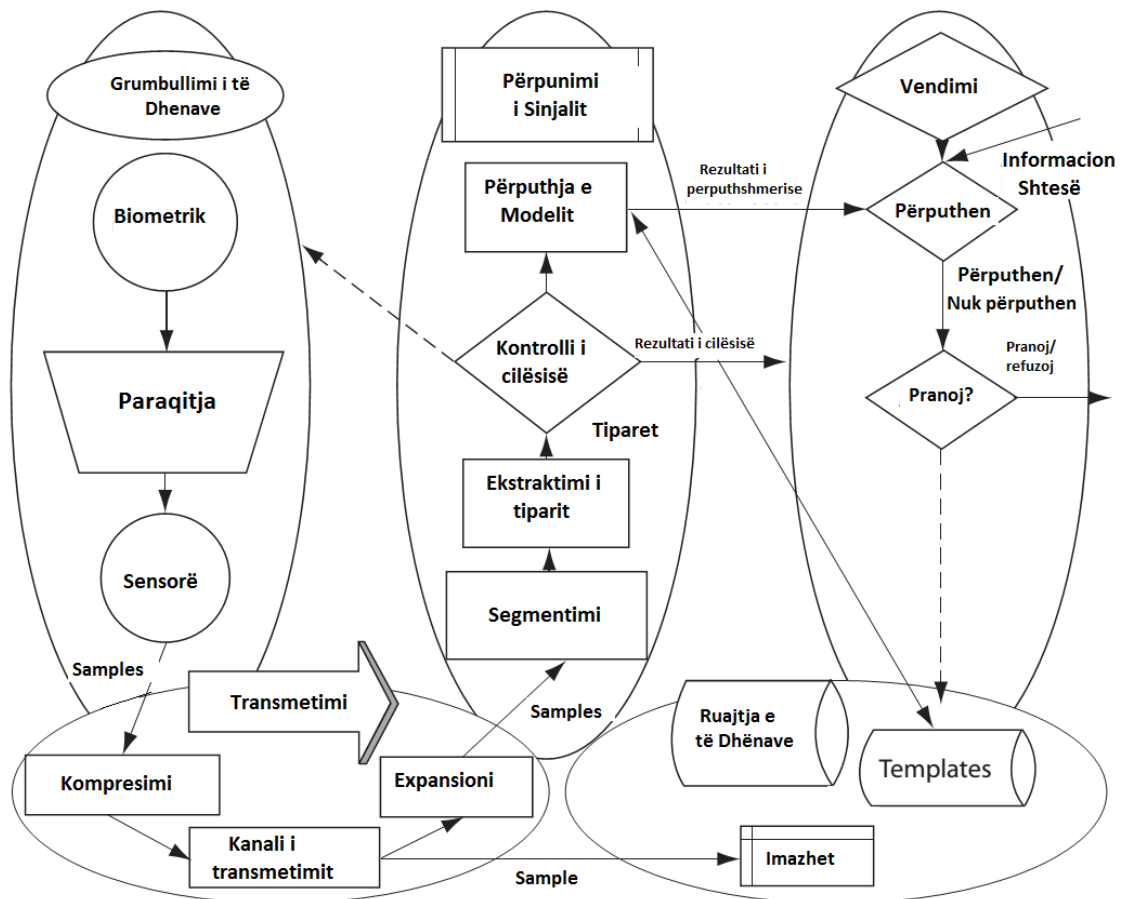


Figura 2-5. Skema logjike e sistemit biometrik

Algoritmi i ekstraktimit

Algoritmi i emërtuar si i ekstraktimit [37][73][85] përpunon sinjalin në hyrje të biometrisë origjinale për të ekstraktuar karakteristikat e qarta të përsëritura dhe ndërton një template. Qëllimi tjetër i përdorimit të këtij algoritmi është minimizimi i përdorimit të hapësirës së memories dhe bandwidth-it të komunikimit, nëpërmjet kompresimit të informacionit. Imazhi i regjistruar i gjurmës papilare është afro 100 kB (rreth 12 kB pas kompresimit, i ruajtur në chip-in e pasaportës), paraqitet me një template minutiae prej 250 B.

$$TP_{tef} = Ekstrakt(IM_{ref})$$

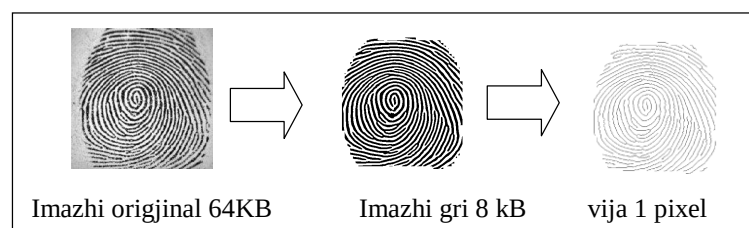


Figura 2-6. Procesi i përpunimit të gjurmës papilare

Në figurën 2-6 përshkruhet përpunimi klasik i imazhit që aplikohet në imazhin biometrik për të ekstraktuar minutiae-t. Procesi i ekstraktimit është një funksion me një imazh si hyrje dhe në dalje jep një template.

Algoritmi i krahasimit

Algoritmi i emërtuar si i krahasimit [37][73][85] realizon krahasimin e dy template-e biometrikë për të përcaktuar nëse janë ose jo nga i njëjti burim biometrik. Transformime matematikore të këtij algoritmi zbatohen në template-in e kandidatit për të vlerësuar distancën nga një template referencë.

Në varësi të distancës dhe threshold-it(pragut të pranimit), merret një vendim suksesi apo dështimi për krahasimin. Në figurën 2-7 ilustron krahasimi i minutiae-ve ndërmjet dy gjurmëve papilare. Procesi i krahasimit është një funksion me dy template në hyrje dhe në dalje jepet një vendim, ose një rezultat:

$$Score = Match(TP_{kand}, TP_{ref})$$

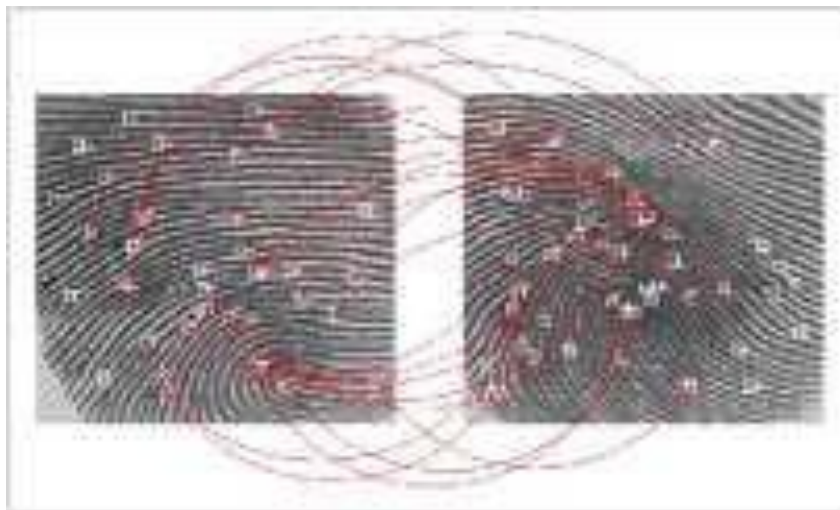


Figura 2-7. Krahasimi me bazë minutiae

Për arsye sigurie të sistemit biometrik, dalja tipike është një vendim dhe rezultati përdoret vetëm nga sistemi për krahasim me threshold (pragu).

2.1.4 Sistemet e identifikimit nëpërmjet biometrisë së shumëfishtë

Si një alternativë e përmirësimeve të mëdha në teknologjinë biometrike, sistemet e identifikimit të bazuara në krahasimin me një biometri nuk mund të garantojnë 100 % saktësi[16][17][77]. Kjo për shkak të faktorëve të ndryshëm, disa prej të cilëve janë si më poshtë:

1. Të dhëna me gabime (prezenca e zhurmës);
2. Ndryshime të brendshme;
3. Dallueshmëria;
4. Jo – universaliteti;
5. Sulmet për akses të pautorizuar dhe mashtrime.

Një sistem identifikimi, nëpërmjet biometrisë së shumëfishtë[13][14][33] mbështetet në natyrën e metodat e përzgjedhura për automatizimin e procesit të identifikimit. Këto sisteme, në bazë të karakteristikave të elementëve biometrik, klasifikohen në kategoritë e mëposhtme:

1. Sistem me shumë-sensorë;
2. Sistem me shumë-algoritme;
3. Sistem me shumë-istanca;
4. Sistem me shumë-template;
5. Sistem multimodalë.

Arkitektura e sistemit biometrik multimodal të identifikimit biometrik është paraqitur në figurën 2-8:

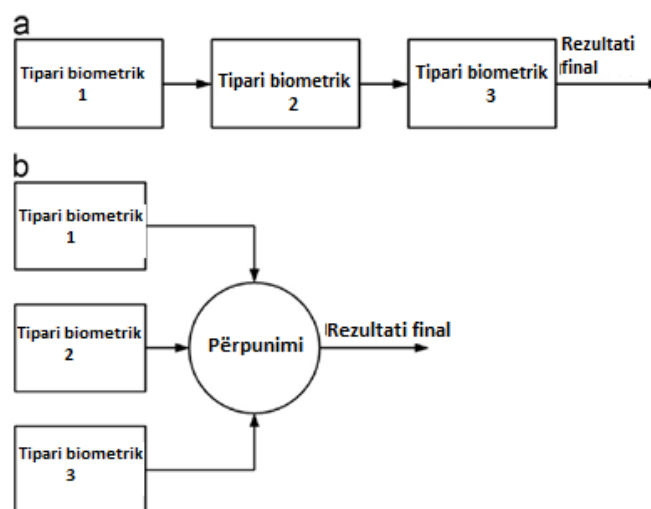


Figura 2-8. Arkitektura e sistemit multimodal (a)seri; (b) parallel.

Sistemet e identifikimit kanë avancuar nëpërmjet biometrive të shumëfishta të regjistruara nga burime të ndryshme, të cilat mund të kombinohen bashkë në nivele të ndryshme, siç ilustrohen dhe në figurën 2-9:

1. Në nivel sensori;
2. Në nivel karakteristikash;
3. Në nivel rezultatesh të gjetura;
4. Në nivel vendimi.

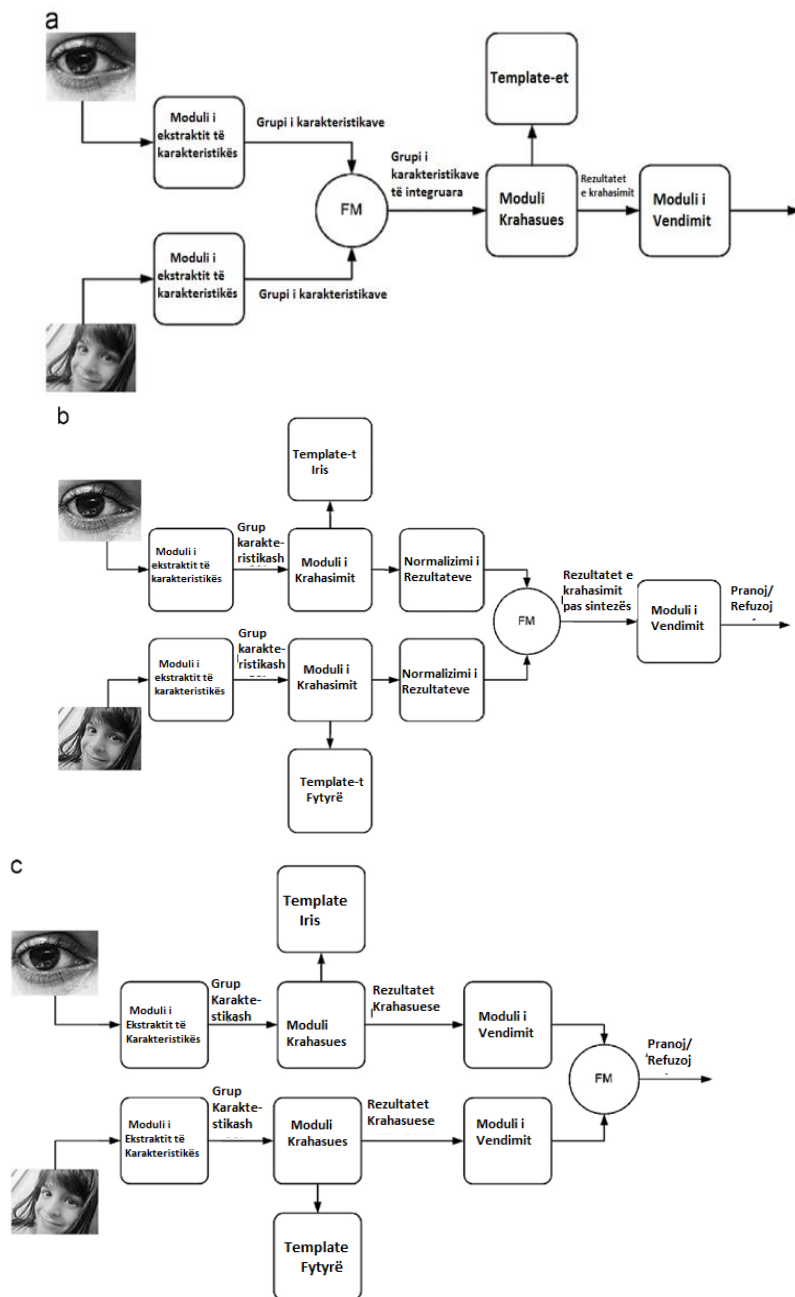


Figura 2-9.Sinteza e e identifikimit nëpërmjet biometrisë së shumëfishtë
(a)karakteristike (b) rezultati (c) vendimi

2.1.5 Kufizimet dhe dobësitë e sistemeve biometrike

Megjithë avantazhet e sistemeve biometrike që janë të lehtë për t'u përdorur dhe për të ofruar një siguri më të lartë për identifikimin dixhital në krahasim me zgjidhjet tradicionale, përdorimi i tyre në ditët e sotme është i kufizuar për aplikime specifike, kjo edhe për shkak se këto sisteme vuajnë nga disa kufizime, të cilat nëse nuk eliminohen mund të ngushtojnë gamën e përdorimit të tyre si:

- **Kufizimi në performancë**

Në ndryshim me verifikimin e fjalëkalimit, verifikimi i të dhënave biometrike është subjekt i gabimeve dhe shprehet me anë të një përqindje pragu për identifikimin (100% nuk është arritur). Gabimet e vërejtura[20][25] ndodhin për shumë arsye të tilla si ndryshimet e karakteristikave të njeriut, faktorët e mjedisit dhe ndërveprimi me pajisjet e regjistrimit. Këta faktorë[12], nëse nuk kontrollohen mund të ndikojnë ndjeshëm performancën e sistemeve biometrike.

- **Kufizimet e pranueshmërisë**

Në bazë të studimeve të realizuara[40][41][42], siç ilustron dhe në tabelën 1-1 u konfirmua se jo të gjitha modalitetet biometrike janë pranuar nga individët në përdorim. Megjithatë, pranimi është i lidhur ngushtësisht edhe me qëllimin e përdorimit dhe popullsinë e përzgjedhur. Në punimin e tij Jain(2004)[15] i kategorizon kufizimet në biometri në tri kategori kryesore:

1. saktësi në aspektin e gabimeve;
2. shkalla ose madhësia e bazave të të dhënave;
3. përdorimi në kuptimin sa e lehtë është në përdorim, pranueshmëria, etj.

Një qeveri mund të vendosë që një individ do të identifikohet me anë të të dhënave biometrike të ngarkuara në pasaportë. Për të realizuar procesin e kontrollit logjik apo fizik në një kompani, është më e vështirë të imponohet një sistem që nuk do të pranohet nga individët.

- **Kufizime arkitekturore**

Disa punime ekzistuese [14][15][20][24][112] tregojnë dobësitë e sistemeve biometrike. Ratha[14] ka identifikuar tetë pikat e sulmeve të mundshme në një sistem të përgjithshëm biometrik siç është paraqitur në figurën 2-10. Maltoni[112] ka paraqitur në punimin e tij të meta të sistemeve biometrike që lidhen me shmangien, cilësinë e biometrisë së regjistruar, etj.

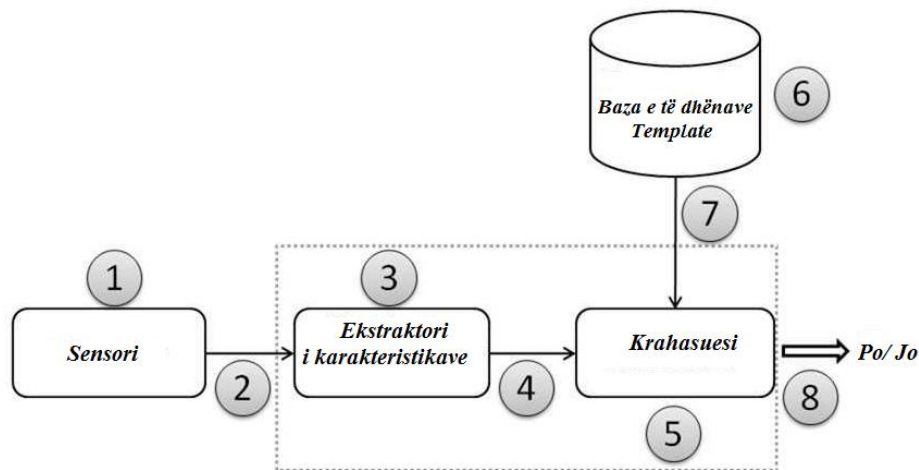


Figura 2-10. Pika të mundshme sulmi të identifikuara në një sistem biometrik(model sipas Ratha)

Përveç këtyre kërcënimeve të paraqitura, disa punime të tjera[24][33][51] paraqesin sulmet e mundshme ndaj sistemeve biometrike në pikat e identifikuara në skemë e paraqitur në skemën e mësipërme. Një shembull i sulmeve të tipit 1(sensor) është dhënë në figurën 2-11.



Figura 2-11. Një gisht proteze krijuar nga latex

2.1.6 Vlerësimi i sistemeve biometrike

Siç u trajtua dhe në seksionin e mëparshëm, sistemet biometrike kanë disa kufizime të cilat nëse nuk eliminohen apo minimizohen, të cilat ndikojnë në zbatimet e tyre në industri dhe në jetën reale. Për këtë arsye, aspektet e vlerësimit të sistemeve biometrike mund të ndahet si në figurën 2-12, në kategoritë e mëposhtme:

1. cilësia e të dhënave;
2. përdorshmëria;
3. siguria.

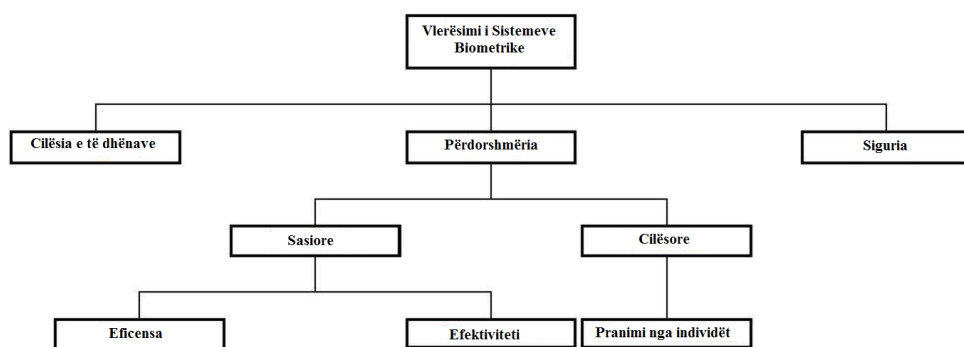


Figura 2-12. Vlerësimi i sistemeve biometrike

2.1.7.1 Cilësia e të dhënave

Vlerësimi i cilësisë së të dhënave biometrike po merr gjithnjë e më shumë vëmendje, pasi konsiderohet si një nga faktorët kryesorë që ndikojnë në performancën e përgjithshme të sistemeve biometrike. Kjo ndodh kryesisht për shkak të humbjeve dhe zhurmave në procesin e regjistrimit të elementëve biometrik nga faktorë të tillë si ndriçimi, rezolucioni etj. Për këtë arsye kontrolli dhe përmirësimi i cilësisë së të dhënave biometrike është një domosdoshmëri në ditët e sotme. Duke përdorur një informacion biometrik cilësor, template-et me cilësi të dobët mund të eliminohen gjatë fazës së regjistrimit ose refuzohen gjatë verifikimit. Një informacion i tillë mund të përdoret edhe për biometritë e buta dhe qasjet multimodale[18][20].

Sipas Organizatës Ndërkombëtare të Standarteve[14] cilësia e të dhënave biometrike karakterizohet nga tre veti, të ilustruara në figurën 2-13:

- Karakteristika: i referohet cilësisë së tipareve fizike dhe individuale;
- Përpikmëria: i referohet shkallës së ngjashmërisë ndërmjet template-it biometrik dhe burimit të tij;
- Përdorimi: i referohet ndikimit të template-it individual biometrik në performancën e përgjithshme të sistemit biometrik.

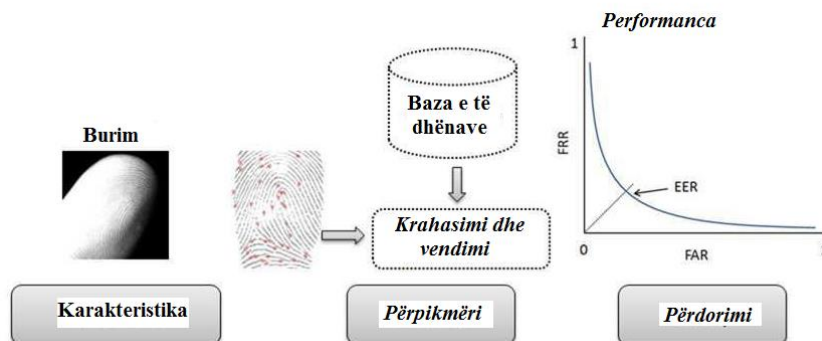


Figura 2-13. Cilësia e vlerësimit biometrik të të dhënave

Në trajtimin e biometrisë ka një konsensus ndërkombëtar në lidhje me faktin që template-i biometrik duhet të jetë i lidhur me performancën e identifikimit[9]. Në këtë punim është paraqitur një vështrim i përgjithshëm i metrikës së cilësisë, me bazë morfologjinë dhe e vlerësuar nga dobia e përdorimit.

Në punimin e tij Alonso-Fernandez[10] prezanton një pamje të përgjithshme të metrikës së cilësisë aktuale të gjurmës papilare. Në këtë punim prezantohet ndikimi i template-eve me cilësi jo të mirë në performancën e sistemit biometrik.

Aktualisht përafrime dhe algoritme të ndryshme ekzistojnë që vlerësojnë efektivitetin e cilësisë së imazheve të gjurmëve papilare, ku veçojmë një shembull të këtyre metrikave, që është NIFQ - Fingerprint Image Quality Metric (Metrika e cilësisë së Imazhit biometrik. NIFQ ka për detyrë vlerësimin e cilësisë së gjurmës papilare.

He[26] prezanton një model hierarkik të vlerësimit të cilësisë biometrike të template-it në tre nivele: bazë të dhënash, lloj dhe nivel të cilësisë së imazhit. Në punimin e tyre Zhang dhe Wang[12] prezantuan një metodë vlerësimi të cilësisë së imazhit bazuar në asimetrinë e imazheve të fytyrës. Kjo metodë përdor dekriptuesin SIFT për vlerësim cilësor.

Abed, Giot, Hemery, Charrier dhe Rosenberger[39] prezantuan së bashku metodën e vlerësimit bazuar në dy tipe informacioni, në atë të cilësisë së imazhit dhe cilësisë së bazuar në strukturë duke përdorur dekriptuesin SIFT. Metrika e prezantuar ka avantazhet e të qenit multimodale (fytyrë, gjurmë papilare dhe venat/vijat e dorës) dhe e pavarur nga sistemi identifikues i përdorur.

2.1.7.2 Përdorimi

Sipas standartit ISO 13407:1999 (1999)[29], përdorimi përcaktohet si “shtrirja sipas së cilës një produkt i përdorur nga individë specifik për të arritur synime specifike me efektivitet, efikasitet dhe kënaqësi në një kontekst specifik përdorimi”, ku:

- Efikasiteti nënkupton që përdoruesit duhet ta kenë të mundur të përmbushin detyrat lehtësisht në një kohë të përshtatshme. Kjo zakonisht matet si koha e detyrës.
- Efektiviteti nënkupton që përdoruesit e kanë të mundur të plotësojnë detyrat që dëshirojnë pa shumë sforcim. Kjo matet në përgjithësi me metrika të zakonshme që përfshijnë raportin e plotësuar dhe numrin e gabimeve (FTE).
- Pranueshmëria e individit mat pranimin e përdoruesit dhe kënaqësinë në lidhje me sistemin. Matet zakonisht duke studiuar disa cilësi si lehtësia në përdorim, besimi, etj.

2.1.7.2.1 Performanca dhe metrikat

Sistemet biometrike janë subjekt i disa llojeve të gabimeve. Disa prej parametrave [48][49] që vlerësojnë performancën e tyre ose metrikat i kategorizojmë si më poshtë:

Parametrat bazë të performancës

- FTE-Failure-to-enroll-rate(përqindja e dështimit në regjistrim): pjesa e popullsisë për të cilën sistemi biometrik nuk arrin të kapë informacion të përmbledhur nga template-i biometrik.
- FTA-Failure-to-acquire-rate(përqindja e dështimit të kapjes): pjesa e përpjekjeve të verifikimit ose identifikimit për të cilat sistemi biometrik e ka të pamundur të kapë një template apo të lokalizojë një imazh a sinjal me cilësi të kënaqshme.
- FMR-False-match-rate(përqindja e gjetjes jo të vërtetë): raporti i përputhjeve pozitive jokorrekte me anë të algoritmit të përputhjes të tentativave të krahasuara të një template-i të vetëm.
- FNMR-False-non-match-rate(përqindja e mosgjetjes jo të vërtetë): raporti i përputhjeve negative jokorrekte me anë të algoritmit të përputhjes të tentativave krahasuese të një template-i të vetëm.

Përvec këtyre metodave të matjes së gabimit përdoren edhe metoda të tjera për të siguruar përdorimin operacional të sistemit biometrik të tilla si: koha mesatare e regjistrimit, koha mesatare e verifikimit, madhësia mesatare dhe maksimale e template-it dhe sasia maksimale e memories se alokuar.

Matjet e performancës të verifikimit të sistemit

- FRR-False rejection rate(përqindja e refuzimit jo të vërtetë): pjesa e përdoruesve autentikë që janë mohuar gabimisht. Nëse një operacion verifikues bëhet vetëm njëherë, FRR do të jepet me anë të:

$$FRR(\tau) = FTA + FNMR(\tau) * (1 - FTA) \quad (2.1)$$

- FAR-False acceptance rate(përqindja e pranimi jo të vërtetë)pjesa e mashtrimeve që janë pranuar nga sistemi biometrik. Nëse një operacion verifikimi bëhet vetëm një herë FAR, siç ilustruhet në figurën 2-14, do të llogaritet me:

$$FAR(\tau) = FMR(\tau) * (1 - FTA) \quad (2.2)$$

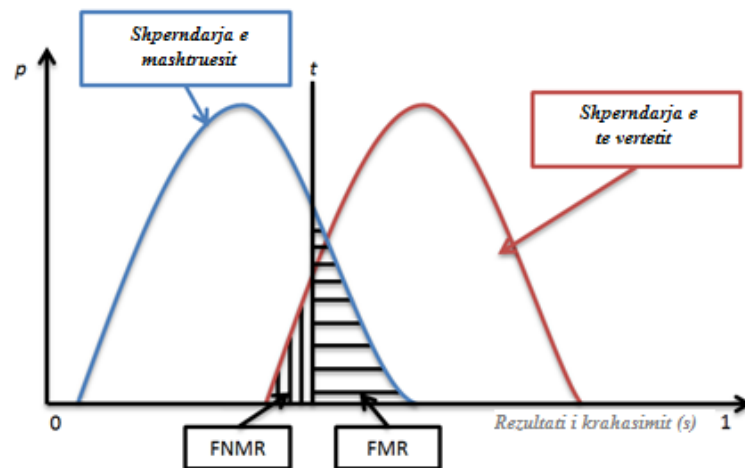


Figure 2-14. Vlerat e FNMR dhe FMR për një vlerë të dhënë të pragut(t)

- ROC-Receiver operating characteristic curve(Kurba karakteristike funksionale e marrësit) është paraqitur në planin koordinativ, në figurën 2-15.

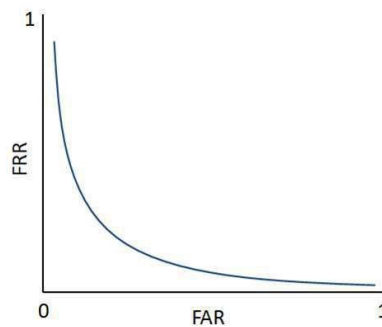


Figura 2.15. Kurba ROC: FAR kundrejt FRR

- EER-Error Equal Rate(Përqindja e gabimit të barabartë) është përqindja e gabimit që i korrespondon pikës në të cilën FAR dhe FRR priten. Ky parametër përdoret gjerësisht për të vlerësuar dhe krahasuar sistemet biometrikë të identifikimit. Sa më shumë t'i afrohet EER 0% aq më e mirë është performanca e sistemit.

Matjet e performancës të identifikimit të sistemit

- IR-Identification rate(Përqindja e identifikimit) shënohet me r dhe përcaktohet si pjesa e operacioneve të identifikimit nga përdoruesit e regjistruar në sistem në të cilin identifikuesi i saktë i përdoruesit është ndërmjet të kthyerve.
- FNIR-False-negative-identification-error-rate (Përqindja e gabimit të identifikimit negativ jo të vërtetë) është pjesa e operacioneve të identifikimit nga përdoruesit e regjistruar në sistem në të cilin kandidati i saktë i përdoruesit nuk është ndërmjet

të kthyerve. Për një operacion identifikimi të përbërë nga një provë kundrejt bazës së të dhënave me madhësi N ajo jepet me anë të barazimit:

$$FNIR(\tau) = FTA + (1 - FTA) * FNMR(\tau) \quad (2.3)$$

- FPIR-False-positive-identification-error-rate(Përqindja e gabimit të identifikimit pozitiv jo të vërtetë) është pjesa e operacioneve të identifikimit nga përdoruesit e paregjistruar në sistem, ku një kandidat është rikthyer. Për një operacion identifikimi të përbërë nga një provë kundrejt bazës së të dhënave me madhësi N ajo jepet me anë të barazimit:

$$FPIR = (1 - FTA) * (1 - (1 - FMR)^N) \quad (2.4)$$

- CMC-Cummulative Match Curve(Kurba karakteristike e përputhjes kumulative) është prezantimi grafik i rezultateve të një testi me detyrë identifikimi jepet në figurën 2-16.

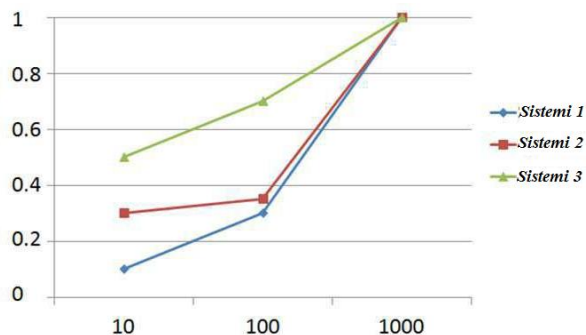


Figura 2-16. Paraqitja grafike CMC për tre sisteme biometrike

2.1.7.3 Siguria

Sistemet biometrike paraqesin disa dobësi dhe kufizime të cilat mund të ulin ndjeshëm përdorimin e tyre në një mënyrë eficiente. Prandaj, është e rëndësishme që sistemet biometrike të jenë të ndërtuara për të përballuar kërcënimet e paraqitura, sidomos në aplikimet e sigurisë kritike në industri dhe për të garantuar një siguri të vazhdueshme për sistemin biometrik. Një sërë studimesh dhe përafrimesh që kanë të bëjnë me çështjen e sigurisë së sistemeve biometrike janë realizuar ndër vite. Në këtë punim ne kemi sjellë disa prej tyre.

Dimitriadis dhe Polemi (2004)[46], në punimin e tyre paraqesin një studim krahasues të sigurisë të disa teknologjive biometrike, në mënyrë që të përdoren si sisteme kontrolli në stadione. Metoda e propozuar prej tyre mund të përdoret lehtë në krahasimin e sistemeve biometrike pasi ajo është një metodë sasiore.

Abed(2012)[48], në punimin e tij prezanton një platformë online për vlerësimin e sigurisë së sistemeve biometrike(Security EvaBio). Kjo platformë zbaton një metodë sasiore bazuar në vlerësimin e sigurisë, mbështetur në nocionin e faktorëve të rrezikut, për të mundësuar vlerësimin dhe krahasimin e sistemeve

biometrike. Kjo platformë përmban një bazë të dhënash të kërcënimeve të përbashkëta dhe dobësive të sistemeve biometrike.

2.1.7 Sfida në të ardhmen

Sistemet biometrike janë një zgjidhje premtuese për identifikimin e besueshëm dixhital të individëve. Megjithatë, përdorimi i tyre nuk është në nivelet e synuara. Në këtë kapitull shohim se teknologjia biometrike paraqet disa të meta të cilat mund të ulin shkallën e përdorimit në aplikime të jetës reale. Për këtë arsye, vlerësimi i sistemeve të tilla është konsideruar si një sfidë kryesore në këtë fushë kërkimore. Në përgjithësi, shumica e studimeve aktuale kanë për qëllim të paraqesin një algoritëm njohje të mirë në drejtim të performancës(p.sh., duke përdorur EER) pa marrë parasysh aspektet e tjera të vlerësimit në aspektin e cilësisë së të dhënave, pranimin nga përdoruesi dhe sigurinë. Nga punimet e prezantuara mund të vënë në vëmendje këto çështje:

- Për aspektin e cilësisë, ne shohim se shumica e metrikave ekzistuese të cilësisë janë të varur nga metrikat (të tilla si NFIQ). Një hap përpara është paraqitur nga Abed, se cilat paraqesin një metrikë cilësore multimodale për të vlerësuar cilësinë e të dhënave biometrike. Megjithatë, metrika e paraqitur nuk do të zbulojë ndryshimin e ndriçimit, e cila konsiderohet si një ndryshim i rëndësishëm, veçanërisht në një modalitet të fytyrës. Përveç kësaj, ne besojmë se janë të nevojshme më shumë veprime për tu ndërmarrë në këtë aspekt të vlerësimit për të siguruar saktësinë e aplikimeve duke përdorur vetëm një informacion biometrik si referencë (p.sh., një imazh të fytyrës në e-pasaportë).
- Për aspektin e sigurisë, ne shohim gjithashtu se shumica e veprimeve ekzistuese synojnë të paraqesin skenarët e sulmeve në sistemet biometrike. Të pakta janë materialet dedikuar vlerësimit të sigurisë së sistemeve të tilla. Në këtë kuadër gjykohet se duhet të bëhet më shumë në këtë fushë të kërkimit për të siguruar saktësinë e sistemeve biometrike.

Së fundi duke marrë parasysh aspektet e paraqitura të vlerësimit kur krahasojmë sistemet biometrike të identifikimit, theksojmë se një sistem biometrik që na siguron 0% gabime, por që nuk është e lehtë për t'u përdorur, nuk mund të gjejë zbatim.

2.2 Teknologjia e kartave inteligjente

2.2.1 Kartat inteligjente

Një kartë inteligjente është një celës(token) identifikimi dhe është pasardhësi i fundit i kartave plastike dhe me shirit magnetik. Kartat plastike[57] u përdorën fillimisht dhe gjerësisht në aplikimet bankare duke përdorur një numër unik identifikimi në formën e karaktereve të gdhendura në trupin e kartës. Më tej u shfaqën

në përdorim karta me shirit të afta për të ruajtur informacion numerik prej disa kB të tillë si emri i mbajtësit, datëlindja, numri i llogarisë. Një kartë inteligjente është një minikompjuter, me përbërje silikoni e aftë të ruajë në mënyrë dinamike dhe të procesojë në ditët e sotme një informacion prej afro 100 kB.

2.2.2 Karakteristikat fizike

Një kartë inteligjente nuk është më shumë se një pjesë silikoni në një copë plastike. Në figurën 2-17 paraqitet prodhimi i kartave inteligjente: një chip prej silikoni i lidhur me një modul me kontakt, i tëri i futur në trupin e kartës plastike ose polikarbonat.

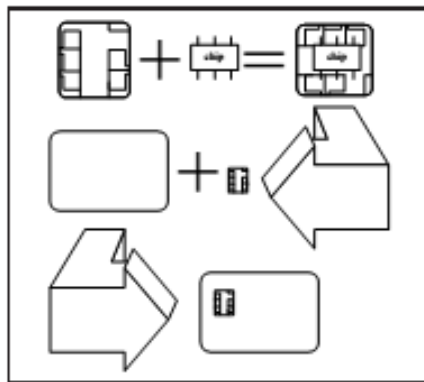


Figura 2-17. Prodhimi i kartave inteligjente

2.2.3 Kartat e kujtesës

Kartat e para inteligjente të përdorura në sasi të konsiderueshme ishin kartat e kujtesës për aplikime telefonike. Të dhënat e nevojshme për aplikimin ruhen në një memorie, që është zakonisht një kujtesë EEPROM. Aksesit në kartë kontrollohet nga një llogjikë sigurie, që në rastin më të thjeshtë konsiston vetëm në mbrojtjen nga shkrimi apo fshirja e pjesëve të caktuara ose të memories në tërësi. Kjo lloj karte u përdor më tej masivisht në transportin publik, makinat shitëse të të gjitha tipeve, parkimet e makinave etj.

Avantazhi i kësaj karte qëndron në teknologjinë e thjeshtë dhe koston e ulët. Më tej logjika sigurie më të avancuara për këto karta u implementuan që përfshinin dhe teknika enkriptimi. Kartat aktuale të memories përdorin protokollin serial në bazë të standartit ISO/IEC 7816[132]. Arkitektura e përgjithshme e një kartë memorie jepet në figurën 2-18.

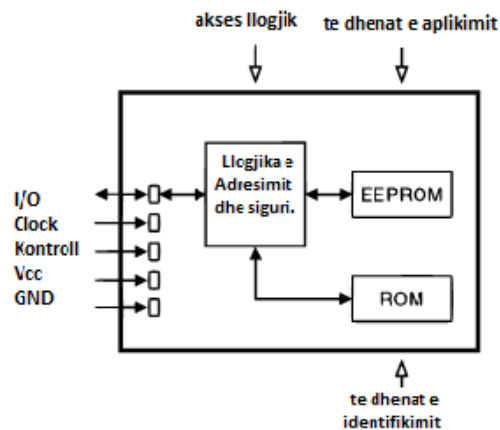


Figura 2-18. Arkitektura e një karte memorie

2.2.4 Kartat pa kontakt(Contactless)

Një kartë inteligjente e quajtur ndryshe dhe kartë inteligjente pa kontakt ndryshon nga kartat klasike me kontakt nga ndërfaqja e komunikimit. Në këto karta, kujtesa dhe mikroprocesori mund të përdorin një ndërfaqe pa kontakt, shpesh e identifikueshme nga mungesa e fletëve të arta të kontaktit. Këto karta, siç ilustron në figurën 2-19, ku energjia dhe të dhënat transmetohen pa pasur asnjë kontakt fizik ndërmjet kartës dhe terminalit kanë arritur në dekadën e fundit statusin e produkteve shumë të kërkuara në treg, duke lejuar që shumë aplikime të favorshme në të cilat jo domosdoshmërisht karta duhet të mbahet në dorë nga mbajtësi, por mund të qëndrojë në xhepin apo portofolin e tij.

Aplikimet më të shumta janë në kontrollin e aksesit të transportit publik, transaksionet bankare, dokumentet e identitetit (kartat e identitetit, pasaportat).

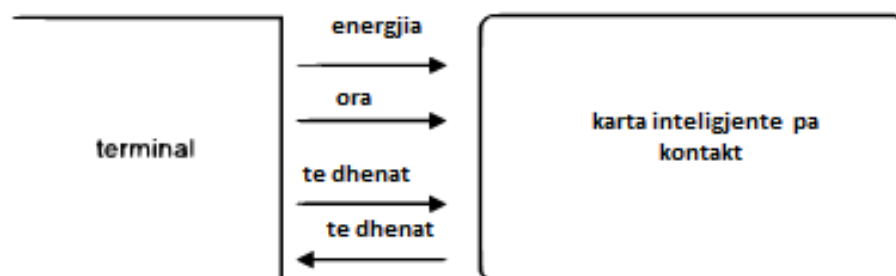


Figura 2-19. Arkitektura e ndërfaqes së komunikimit të një karte pa kontakt

2.2.5 Kartat inteligjente përballë RFID

Shpeshherë, në mënyrë të pasaktë, dikush mund të quajë një kartë inteligjente pa kontakt si kartë RFID ose të kundërtën, ku shembulli më i mire është pasaporta biometrike që shpesh referohet si nja pajisje RFID. Një pajisje RFID -Radio Frequency Identification (Identifikim në radio-frekuencë) realizon identifikimin nëpërmjet përdorimit të një pajisje që lexon me radio, të tillë si si një kod regjistrimi elektronik. Shumica e pajisjeve RFID nuk janë të mbrojtura nga ndërhyrjet, janë të klonueshme dhe të lira në ndryshim nga kartat inteligjente pa kontakt që janë pajisje reale me siguri të lartë me aftësi përpunuese dhe/ose hapësirë kujtese të mbrojtur.

2.2.6 Kartat inteligjente me elementin biometrik: gjurmë papilare

Me përdorimin e sensorëve me bazë silikoni për regjistrimin e gjurmëve papilare dhe integrimin e chip-it në silikon, në mënyrë natyrale u shfaq nevoja e zëvendësimit ose plotësimit të identifikimit dixhital me kod PIN, me kartat inteligjente biometrike. Sfida mekanike e integritetit dhe rezistencës ndaj lakimit dhe përdredhjes u kalua me sukses, megjithatë vazhdojnë sfidat përtej marrjes së imazhit, konsumimit të energjisë të chip-eve të tilla (për kartat autonome dhe pa kontakt) dhe në mënyrë të veçantë procesimi i imazhit të nevojshëm për krahasimin është jashtë mundësive teknike të kartave inteligjente klasike.

2.2.7 Ndërveprimi me teknologjinë biometrike

Kompania Gemplus prodhoi në vitin 1997, lexuesit e parë që kishin të integruar funksionet e sensorit të regjistrimit të gjurmëve papilare dhe lexues i kartave inteligjente[57].

Aplikimi origjinal ishte efikas për kontrollin llogjik të aksesit dhe zëvendësimin e kërkesës për kodin PIN me gjurmën papilare të regjistruar për aplikimin e identifikimit dixhital të përdoruesve në sistemin e kompanisë. Duke pasur parasysh rëndësinë e sigurisë, template referencë u vendos të ruhej në kartën inteligjente të mbajtësit në vend të laptopit të klientit. Megjithëse jo shumë e përshtatshme (mungesa e kartës = pamundësi identifikimi dixhital të përdoruesve në sistemin e kompanisë), rezultoi mjaft e sigurt.

Përvec ruajtjes të template-it referencë, një kërkesë e realizueshme për çdo teknologji konkurrese (p.sh karta e memories optike, bardkodi), një kartë inteligjente me një mikroprocesor mund të përfitojë nga potencialet e saj procesuese për të tejkaluar konkurrencën. Më tej u studiua kompleksiteti i komponentëve bazë të programeve si ekstraktimi dhe krahasimi i gjurmëve papilare[15][84], në mënyrë që të

gjendeshin rrugët e duhura për zhvillimin e këtyre programeve në një të limituar si karta inteligjente. Ishte pikërisht kjo arsyeja pse u përzgjodh si zgjidhja me efikase Mach-on-Card (krahasimi në kartë) pasi karta inteligjente jo vetëm ruan template-in origjinal, por është e aftë dhe të realizojë krahasimin.

Kjo zgjidhje e re ka shfaqur disa çështje që duhet të trajtohen të tilla si: performanca në kartat inteligjente (p.sh chip-i i kartës ushqehet nga fusha RF, sa më pak energji e barabartë me fuqi konsumi më e vogël) performanca me anë të makinave virtuale (p.sh zbatime për kartën java dhe .Net) janë më të ngadalta për veprimet intensive.

Në këtë kuadër zgjidhja me efikase, është që në vend të marrjes së informacionit nga burime të jashtme të pasigurta, kartat inteligjente mund të lexohen në sensorë siç u përshkrua dhe në paragrafin më lart. Kjo zgjidhje sjell arkitekturat e shumëfishta si: karta inteligjente autonome, ndërveprim i sigurt me lexues të kartave inteligjente me fuqi të lartë, në mënyrë që të mos lejohen veprime komplekse të tilla si ekstraktimi i të dhënave nga imazhi origjinal, ndërveprimi i sensorit kur karta inteligjente me kontakt vendoset në një lexues.

2.2.8 Token(çelësi) personal

Funksioni më i rëndësishëm i kartave inteligjente në skemën biometrike është roli i saj si token personal. Në shumë aplikime jo-qeveritare, direktiva nga organizata të fushës së mbrojtjes së të dhënave personale nuk lejojnë krijimin e bazave të të dhënave biometrike. Këto direktiva përcaktojnë edhe përdorimin e detyrueshëm të token personal, shpesh kartë inteligjente për të "shpërndarë" bazën e të dhënave biometrike të përdoruesve.

Në Francë, Komisioni Kombëtar i Informatikës dhe Lirisë, këshillon përdorimin e teknologjisë match-on-card(krahasim lokal i biometrisë në kartën inteligjente), së bashku me kartat inteligjente, për sigurinë e mbajtësit, pasi ai është mbajtës i referencës së tij biometrike dhe në këtë mënyrë kontrollon mekanizmin e krahasimit.

2.3 Teknologjia kriptografike

2.3.1 Kriptografia shkenca e sekretit

Objektivi themelor i kriptografisë[62][63][64] është të mundësojë komunikimin mes dy individëve në një kanal të pasigurt, në mënyrë të tillë që njëri prej individëve të mos kuptojë çfarë po komunikon individi tjetër.

Kriptografia[62] është përdorur historikisht në komunikimet ushtarake dhe diplomatike dhe më së fundmi prej disa dhjetëvjeçarësh ka gjetur zbatim në sigurinë e sistemeve të ndryshme të kontrollit dhe të teknologjisë së informacionit e më gjerë. Aplikimet të tilla përfshijnë enkriptimin e komunikimit, nënshkrimin dixhital dhe identifikimin e përdoruesit/pajisjes.

2.3.2 Kriptografia simetrike dhe asimetrike

Në ditët e sotme ekzistojnë dy tipe kriptosistemesh[62], i pari që përdoret që nga lashtësia, ku një çelës sekret shkëmbehet ndërmjet palëve që komunikojnë, që shpesh është quajtur si Kriptografia e Çelësit Sekret ose Kriptografia Simetrike.

I dyti, më i mëvonshmi u bë i njohur në 1976 nga Whitfield Diffie dhe Martin Hellman. Kjo skemë e re përdor dy çelësa komplementarë, çelësin publik dhe çelësin privat, të tillë që vetëm çelësi publik nevojitet për përpunime të caktuara, si enkriptimi dhe çelësi privat është i nevojshëm për përpunime të tjera, si dekriptimi. Ky kriptosistem është quajtur shpesh si Kriptografia e Çelësit Publik ose Kriptografia asimetrike.

2.3.3 Zbatime

Aplikimet e sotme të sistemeve të kontrollit dhe teknologjisë së informacionit përdorin gjerësisht kriptografinë[64], si konvencionale dhe moderne dhe më së shumti kanë gjetur zbatim në aplikimet bankare, telefoninë celulare, transmetimet video, shërbimet elektronike qeveritare, dokumentat e identitetit, kontrolli i aksesit, siguria në internet, etj. Në përgjithësi një aplikim i tillë shoqërohet me element shtesë sigurie të aftë për të ekzekutuar algoritmet kriptografike dhe/ose për të ruajtur çelësat kriptografikë dhe më shpesh i përdorur është karta inteligjente me chip elektronik.

2.3.4 Primitivët bazë të kriptografisë

2.3.4.1 Funksione të Enkriptimit/Dekriptimit

Enkriptimi është procesi i transformimit të informacionit të qartë(plaintext ose mesazh) në një informacion tëpalexueshëm(Ciphertextose Kriptogram), përveç për atë që ka informacionin e nevojshëm (Çelës). Në figurën 2-20 paraqitet sistemi i enkriptimit/dekriptimit simetrik ndryshe i referuar si modeli Shanon, ndërsa në figurën 2-21 paraqitet sistemi i enkriptimit/dekriptimit asimetrik, ku dërguesi përdor çelësin publik për të enkriptuar, ndërsa marrësi përdor çelësin e tij privat për të dekriptuar.

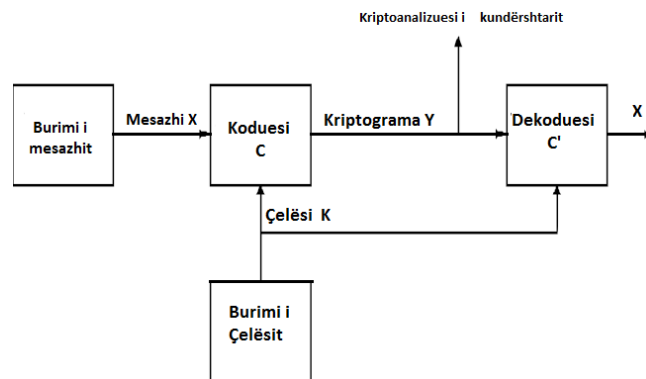


Figura 2-20. Modeli i enkriptimit simetrik Shanon

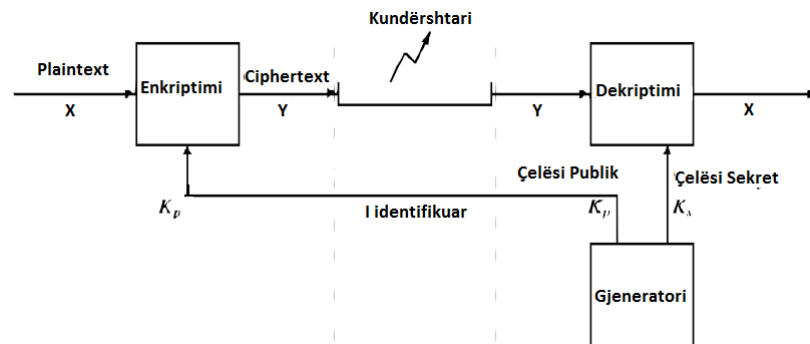


Figura 2-21 Modeli i enkriptimit asimetrik

2.3.4.2 Funkzionet Hash

Hashing është procesi i transformimit dhe reduktimit të informacionit të pastër, mesazhit, në një formë të shkurtuar të dhënave të mesazhit përgjithësisht 128, 160 ose 256 bite që e referojmë si vlera Hash.

Funksioni Hash siç ilustron dhe në figurën 2-22 është njëdrejtimësh (nuk mund të merret mesazhi origjinal nga vlera Hash e tij) dhe është unik për çdo mesazh.

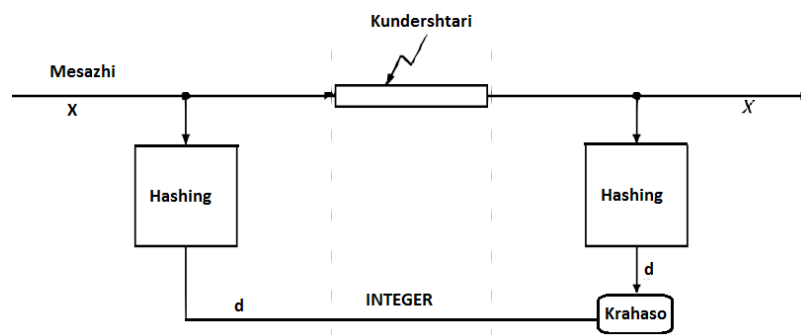


Figura 2-22. Modeli me funksionet Hash

2.3.4.3 Kodet e identifikimit të mesazhit (MAC)

MAC është kryesisht një funksion hash me kod. Një mënyrë e saktë si të ndërtohet një MAC nga një mesazh është të enkriptosh me funksion hash dhe vlerën hash ta enkriptosh me një çelës sekret. Ky model enkriptimi siguron mesazhin për integritetin dhe identifikimin në të njëjtën kohë.

2.3.4.4 Nënshkrimet dixhitale

Një nënshkrim dixhital është një skemë matematikore për të dëshmuar origjinalitetin e mesazhit dixhital apo dokumentit. Një nënshkrim dixhital i vlefshëm i jep marrësit një arsye për të besuar që mesazhi është krijuar nga një dërgues i njohur dhe që nuk është ndryshuar gjatë rrugës, siç paraqitet në figurën 2-23. Në thelb, nënshkrimi dixhital është e kundërta e skemës asimetrike të enkriptimit.

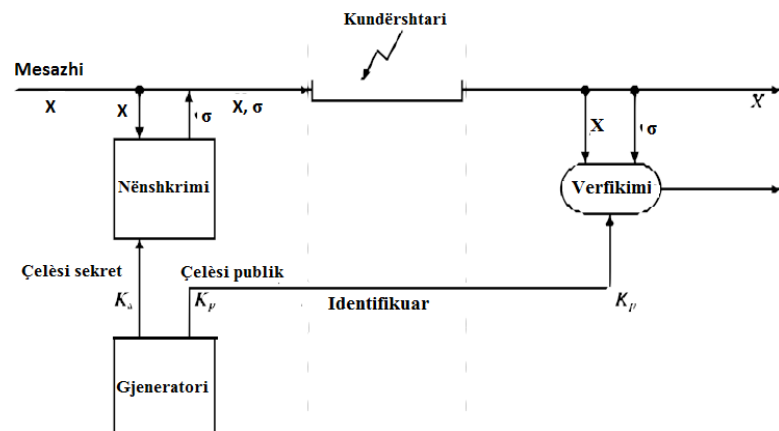


Figura 2-23 Nënshkrimi dixhital

2.3.5 Ndërveprimi me kartat inteligjente

Ndërveprimi ndërmjet kartave inteligjente dhe kriptografisë është prej shumë vitesh një fushë në studim. Një njeri nuk mund të mbajë mend numra të mëdhenj, të tillë si ato që duhen për çelësat e sigurt kriptografik dhe nuk mund ti manipulojë lehtësisht këto numra në mënyrë që të gjejë një zgjidhje për këtë problem. Një kartë inteligjente është mbajtësi dhe gjeneruesi më i sigurt i çelësve të tillë përpunues i veprimeve të tilla për identifikim. Një kartë inteligjente është e aftë, brenda disa sekondash të gjenerojë një çift çelësash për kriptosistemin RSA dhe është i aftë, brenda një sekonde të përcaktojë një çelës me një sistem tjetër dixhital.

Algoritme dhe mjete kriptografike të tilla si DES, 3DES, AES, RSA, MD%, SHA-1 janë implementuar në kriptoprosesorët e kartave inteligjente. Kartat inteligjente OPT janë shndërruar në standartit bazë për identifikimin e sigurt në

distancë. Aktualisht kartat inteligjente luajnë plotësisht rolin e token-it personal, sepse sistemi identifikon objektin në zotërim në vend të përdoruesit real.

Megjithatë vetëm një sekret (p.sh një kod PIN) i vendosur nga përdoruesi në kartë do të aktivizojë atë për procesuar një identifikim online. Kartat inteligjente dhe kriptografia do të arrijë më tej një identifikim me faktor që nënkupton diçka që ke dhe diçka që di. Përtej identifikimit njerëzor, identifikimi i përbashkët i pajisjeve dixhitale të instaluar në sistemet komunikuese përdor gjerësisht për identifikim, kartat SAM-Secure Access Modules (Modulet e Aksesit të Sigurt), nëpërmjet elementëve transparentë dhe të sigurisë.

2.3.6 Ndërveprimi me biometrinë

Ndërveprimi ndërmjet biometrisë dhe kriptografisë[86] është një fushë gati e re dhe e paeksploruar mjaftueshëm. Këto dy teknologji janë paksa paradoksale: në njërin anë kriptografia ka nevojë për të dhëna të shpërndara në mënyrë uniforme dhe të riprodhueshme në mënyrë identike, ndërkohë që nga ana tjetër të dhënat biometrike nuk mund të riprodhohen në mënyrë identike (në masim një distancë ndërmjet template-eve) dhe nuk shpërndahen në mënyrë uniforme. Në mënyrë më klasike, në aplikimet më të fundit të tilla si pasaporta biometrike, kriptografia ndihmon në ruajtjen e të dhënave biometrike në mënyrë të sigurt.

Përtej këtyre aplikimeve të zakonshme, kërkimi për ndërveprime me teknologji të avancuara mund të na çojë në zgjidhje jopraktike, ashtu sikurse shpesh është cituar nga njerëz të pa informuar të përdorim gjurmët papilare si një çelës kriptografie ose fjalëkalim (dhe në mënyrë specifike të firmosim në mënyrë dixhitale me gjurmën tonë biometrike), pa pasur idenë për çështjet e konfidencialitetit dhe riprodhimit, ose të përdorim kodet e korrigjimit të gabimit për të gjetur 'çelësin' original, të dhënat biometrike.

Në mënyrë më reale, të dhënat biometrike duke qenë që asnjëherë nuk riprodhohen të njëjta, dikush mund ti përdorë një imazh biometrik si një burim të rastësisë për të gjeneruar çelësa, psh nga hashing i të dhënave. Teknikat e mbulimit për të fshehur të dhënat biometrike referencë dhe gjetja e tyre duke përdorur një sekret dhe të dhënat e kandidatit, është një përgjigje pozitive për sfidën nëse kandidati është i duhuri.

2.4 Sistemet krypto-biometrike

Kriptosistemet[50] e bazuara në biometrinë grupohen në dy kategori kryesore, të emërtuara respektivisht key release (publikim të çelësit) dhe key generation (gjenerim të çelësit), skema logjike dhe diagramat skematike të aplikimit dhe autentifikimit të sistemeve kriptobiometrike paraqiten në figurat 2-24 dhe 2-25:

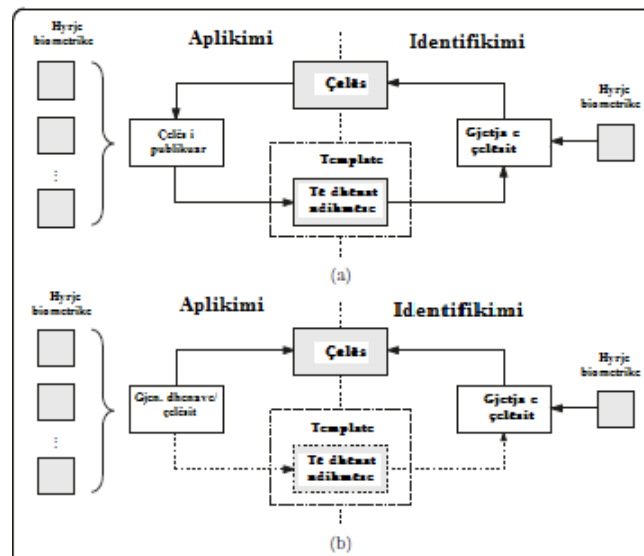


Figura 2-24. Koncepti bazë i sistemeve kriptobiometrike (a) me publikim të çelësit; (b) me gjenerim të çelësit

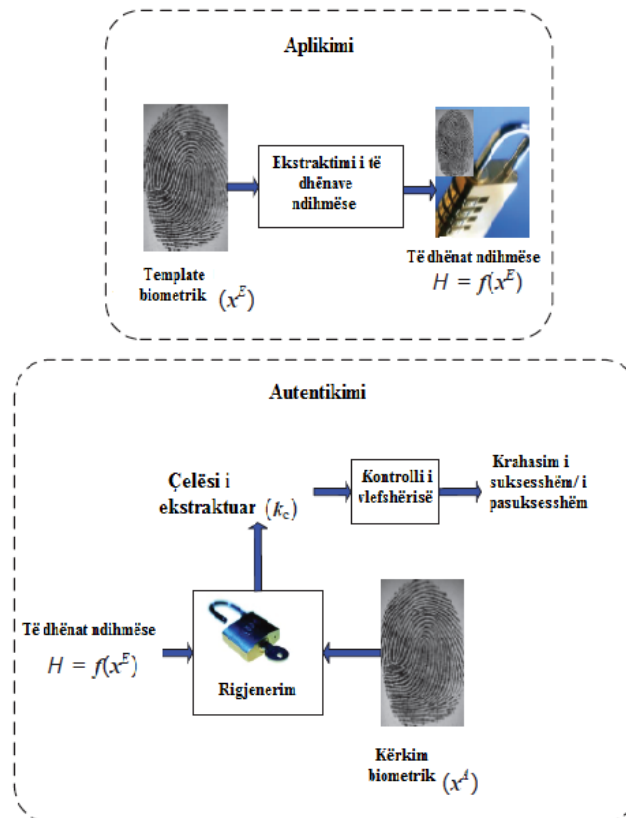


Figura 2-25. Diagramat skematike të fazave të aplikimit dhe autentifikimit në sistemet kriptobiometrike

2.4.1 Skemat me Key release

Në grupin e parë, një çelës kriptografik i krijuar në mënyrë të rastësishme është mbrojtur nga ndërhyrja e pautorizuar me të dhënat biometrike të përdoruesit. Në këtë grup përfshihen skemat e mbrojtjes Fuzzy vault(dhomë i mbrojtur) [53][91][92] dhe fuzzy commitment (e militarizuar)[52][82][83].

2.4.1.1 Skema Fuzzy vault

Në skemën bazë fuzzy vault, siç ilustron në figurën 2-26, të dhënat biometrike (p.sh pikat minutiae) janë konsideruar si një grup i parenditur:

$S^E = x_1, x_2, x_3, \dots, x_n$ të r elementëve.

Çelësi sekret(k_v) prej k bit-ësh është transformuar në një polinom të shkallës k . Të gjithë elementët s_E vlerësohen në polinom dhe vlera e matur polinomiale $P(x_i)$ dhe x_i janë pikat $(x_i, P(x_i))$ të cilat janë të mbrojtura me disa pika të fshehura të gjeneruara në mënyrë të rastësishme $(a_j, b_j)_{j=1}^q$, që nuk varen nga polinomi P (p.sh $b_j \neq P(a_j)$ dhe $a_j \notin S^E, \forall j = 1, 2, \dots, q$).

Pikat origjinale $(x_i, P(x_i))$ dhe pikat ngacmuese të gjeneruara (a_j, b_j) formojnë mbrojtjen fuzzy vault. Siguria e kësaj dhome varet nga vështirësitë e përlogaritjes kompjuterike të zgjidhjes së problemit të rindërtimit polinomial.

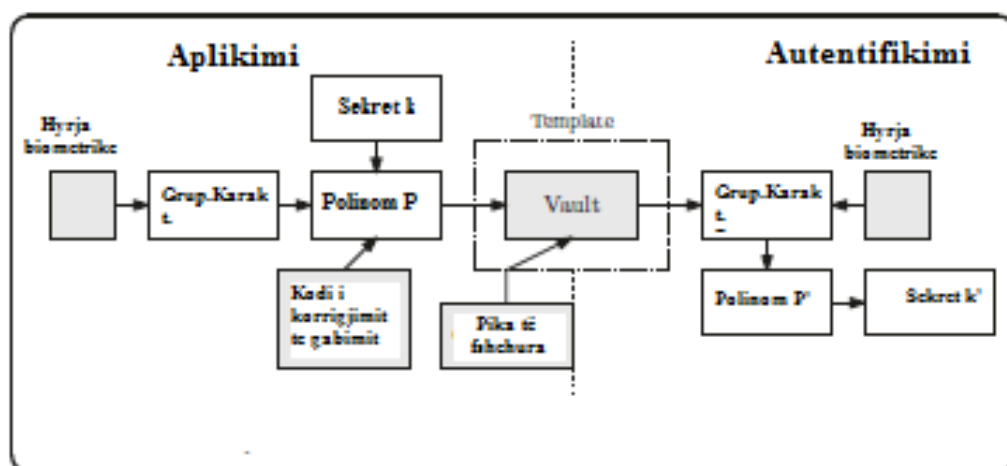


Figura 2-26. Skema bazë e operimit Fuzzy Vault

Çelësi sekret lëshohet vetëm kur kërkimi biometrik është pranë grupit S^E . Shumica e skemave aktuale fuzzy vault me bazë-biometrinë përdorin vlerat e koordinatave (x,y) të pikave minutiae [52,53], ku veçojmë Nandakumar[90] e cila propozon një skemë fuzzy vault me bazë-biometrinë ku përdoren në të njëjtën kohë koordinatat (x,y) dhe orientimi (θ) i pikave minutiae.

2.4.1.2 Skema Fuzzy commitment

Nga ana tjetër, në skemën fuzzy commitment, siç ilustron figura 2-26, të dhënat biometrike paraqiten në një vektor binar b_E dhe ky vektor është i kyçur me një çelës sekret të rastësishëm ose bite të barabartë të b_E me veprimin XOR. Në përafrimet e propozuara [82][83], kodi i i iris-it është kombinuar me çelësin e rastit duke përdorur veprimin XOR dhe në përdorimin e kërimit të kodit të irisit, çelësi sekret ekstrahet nga kodi i kombinuar i iris-it.

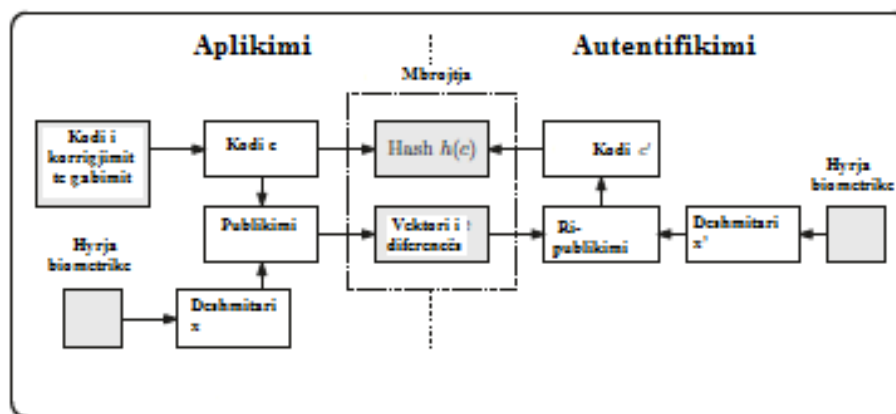


Figura 2-26. Skema bazë e operimit Fuzzy Commitment

2.4.2 Skemat me Key generation

Një numër i kufizuar përafrimesh janë propozuar ndër vite për të gjeneruar çelësa kriptografik nga tiparet biometrike[52][53][91]. Monroe[100] propozon një përafrim për të gjeneruar çelës kriptografik nga zëri i përdoruesit ndërsa flet një fjalëkalim. Feng[60] propozon një kriptosistem që quhet BioPKI, ku në kohë reale, nënshkrimi i përdoruesit përdoret për të gjeneruar një çelës privat. Në përafrimet [16,32], biometria e njohjes së fytyrës përdoret për të ekstraktuar një çelës kriptografik me gjatësi të përshtatshme.

Në disa përafrime të tjera[87][88], iris-i përdoret në të njëjtën kohë për gjenerimin e çelësit kriptografik nga veçoritë e tij. Rathgeb[70] në përafrimin e tij analizon vektorin e karakteristikave të iris-it dhe dedekton bit-et me të besueshme në kodin binar të iris-it për të ndërtuar çelësin kriptografik. Gjurma papilare, biometria me universale dhe e pranuar, është përdorur për të marrë një çelës kriptografik nga template i anulueshëm i gjurmës papilare. Problemi kryesor i këtyre përafrimeve është se nuk janë të aftë të gjenerojnë çelësa të revokueshëm për komunikimin në distancë.

Në studimet e fundit, biometritë mulimodale ose të shumëfishta janë përdorur në sistemet krypto-biometrike[13][18][32][50]. A.Jagadeesan[99] propozon një metodë ku përdoren biometritë e shumëfishta (gjurmë papilare dhe iris). Në këtë metodë u zbatua sinteza në nivel karakteristike e pikave minutiae dhe veçoritë e karakteristikave të iris-it për të gjeneruar template-t biometrike multimodale dhe çelësi gjenerohet nga ky template. Në një punim tjetër të Jagadeesan[101], përdoren të njëjtat biometri, por metodë tjetër për të gjeneruar template-in e transformuar.

Veprimi i përfaqësimit realizohet nga vlerat e karakteristikave të irisit, të cilat janë përdorur si numrat bazë dhe koordinatat e minutiae-ve janë përdorur si përfaqësues. Atëherë numri i ardhshëm primar përlogaritet për çdo rezultat përfaqësimi dhe template-i multimodal gjenerohet duke përdorur shumëzimin e rezultanteve të dy numrave primar për të gjeneruar një çelës 256 bit. Ky përafrim është nën ndikimin e problemit të ndarjes së çelësit të kriptografisë simetrike tradicionale.

Në përafrimin e tij, Dutta[93] prezantoi një metodë të kriptografisë me bazë gjurmën biometrike dhe sigurinë në komunikimin në distancë. Në këtë metodë merren në trajtim dhe vlerësim gjurmët papilare të dërguesit dhe marrësit. Gjurma papilare e marrësit transmetohet tek dërguesi, dhe shkrihet me gjurmët papilare të dërguesit për të gjeneruar një çelës kriptografik prej 128 bit-ësh duke përdorur funksionin standart hash (MD5). Në përafrimin e tyre, çelësi kriptografik së bashku me një vektor të rastit shkrihen në gjurmët papilare origjinale dhe imazhi i mbrojtur dërgohet tek pritësi. Kjo metodë nuk është e sigurt duke qenë se biometria origjinale përdoret si imazh mbrojtës për fshehjen e të dhënave. Duke qenëse çelësi dhe vektori i sekuencës së rastit përgjithësisht transmetohen në kanale jotë sigurta me teknika të fshehjes së të dhënave, gjë që mund të shkaktojë risqe për sigurinë gjatë transmetimit të mesazhit nëse gjurmët papilare të përdoruesit kompromentohen nga një palë e tretë, në çdo mënyrë. Në këtë përafrim, gjurmët papilare të marrësit i dërgohen dërguesit dhe gjurmët papilare të dërguesit përdoren si imazh mbrojtës dhe imazhi i mbrojtur që përmban çelësin master dhe vektori i rastit, i dërgohen marrësit. Si rrjedhim, gjurmët papilare të dërguesit i bëhen të njohura marrësit dhe e kundërta. Një palë e tretë (man-in-middle) mund të gjenerojë çelësin duke përdorur funksionin kriptografik hash dhe duke njohur gjurmët papilare të dërguesit dhe marrësit. Për më tepër, ky përafrim nuk ka trajtuar dhe zgjidhur çështjen e revokimit.

Gjerësisht në studimet dhe përafrimet e tyre, studiues të ndryshëm dalin në përfundimin që për shumë arsye duhet të shmagen zgjidhjet që përpunojnë dhe transmetojnë të dhënat biometrike, qoftë dhe të mbrojtur me mekanizma të avancuar kriptografikë, qoftë dhe në rrjetat të komunikimit enkriptuara dhe rekomandohen si më eficientë dhe robuste zgjidhjet për krahasimin lokal si element identikimi.

KAPITULLI 3

Zgjidhje robuste për identifikimin dixhital. Raste studimore

3.1 Hyrje

Kërcënimet dhe sfidat kryesore të identifikuar [42] në ditët e sotme që shqetësojnë dhe ndikojnë në performancë dhe saktësinë e infrastrukturës së identifikimit dixhital megjithë përdorimin e teknikave të avancuara të kontrollit të trajtuara në punim janë si më poshtë :

- Saktësia (FMR/FNMR) e sistemit;
- Mbrojtja e template biometrik;
- Dedektimi i kërcënimeve të paraqitura.

Në figurën 3-1 ilustrohen pikat kyçe, ku paraqiten kërcënimet të ndryshme (mashttrimet dhe sulmet) në sistemet e identifikimit dixhital.

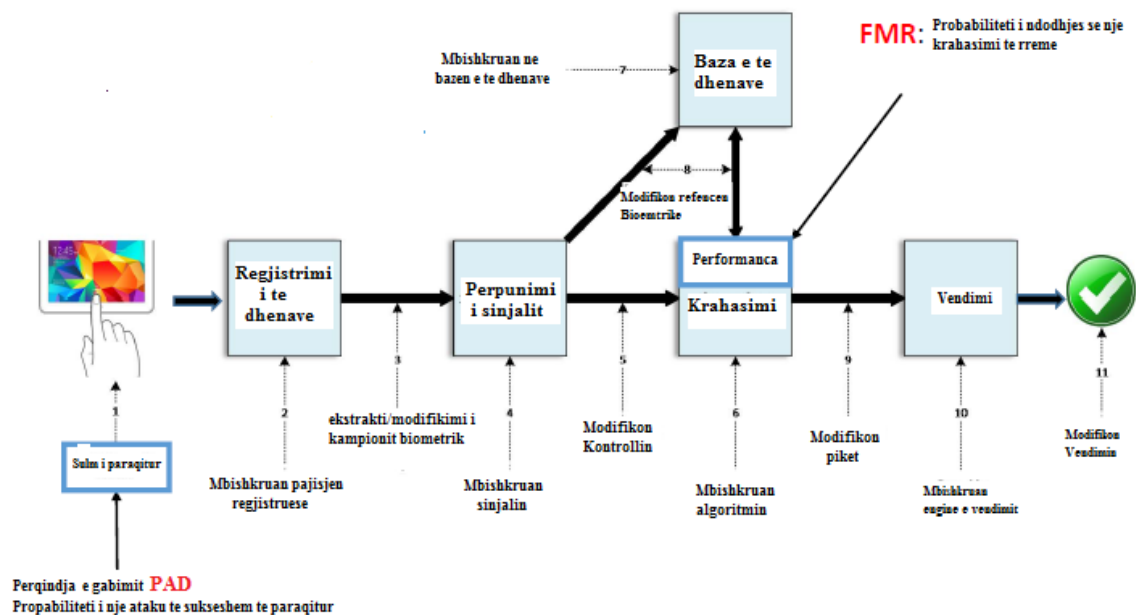


Figura 3-1. Pikat e dobëta ku paraqiten kërcënimet gjatë identifikimit dixhital

3.2 Standarti ISO/IEC 24745 - Mbrojtja e template-it biometrik

Standarti ISO/IEC24745:2011[39], përcakton kërkesat minimale dhe jep rekomandime për mbrojtjen e informacionit biometrik gjatë ruajtjes dhe transferimit të tij, në sistemet e identifikimit nëpërmjet biometrisë. Sipas këtij standarti skema ideale e mbrojtjes të template-it biometrik, arkitektura e të cilës jepet në figurën 3-2 duhet të plotësojë parametrat e mëposhtme:

Mos-invertimi: Nuk duhet të jetë e mundur (e përealizueshme teknikisht) rindërtimi i template-it biometrik origjinal nga template i mbrojtur;

Revokimi: Duhet të jetë i mundur revokimi i një template biometrik të kompromentuar dhe zëvendësimi i tij me një template të ri që merret nga të dhëna të njëjta biometrike;

Diversiteti: Nuk duhet të jetë e mundur të krahasosh me baza të dhënash të tjera një template biometrik të mbrojtur.

Performanca: Integrimi i një skeme mbrojtje për template-in biometrik në sistemin e identifikimit nëpërmjet biometrisë nuk duhet të ketë një efekt negativ në saktësinë e sistemit (FAR dhe FRR).

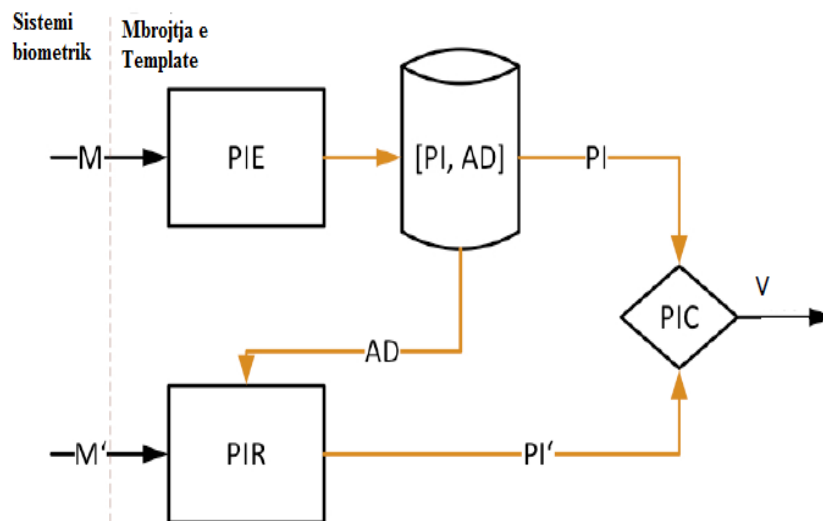


Figura 3-2. Arkitektura ISO/IEC 24745

Relacionete mëposhtme për skemën e propozuar nga ky standart janë:

$$[PI, AD] = PIE(M) \quad (3.1)$$

$$[PI'] = PIR(M', AD) \quad (3.2)$$

$$v = \text{PIC}(PI, PI') \quad (3.3)$$

ku PIE-Pseudonymous identifier Encoder (Koduesi i Identifikuesit me Pseudonim), M është e dhëna biometrike e matur gjatë procesit të regjistrimit, PI- Pseudonymous Identifier është identifikuesi me pseudonim dhe Additional data-AD është e dhëna shtesë, M' është e dhëna biometrike e kontrolluar, v rezultati i përputhshmërisë, si dhe [PI,AD] - template i mbrojtur.

3.3 Zgjidhja e integruar në kartën inteligjente

Në mënyrë që minimizojmë riskun e kopjimit dhe përpunimit të paautorizuar të informacion biometrik që është një e dhënë sensitive, në vend që të mbështetemi në baza të dhënash të qendëruara, ku secili nga ofruesit e shërbimit të identifikimit dixhital krijon bazën e të dhënave biometrike, është më e sigurt dhe rekomandohet nga organizma ndërkombëtare[36][60] mbajtja prej zotëruesve të të dhënave biometrike.

Një zgjidhje e propozuar nga kombinimi i tre teknologjive të avancuara është ruajtja e të dhënave biometrike në memorien e një pajisje portative të mbrojtur me algoritme kriptografike të avancuar të tillë si karta inteligjente.

Kjo zgjidhje sipas punimeve të shumta shkencore[15][58][62][64][65][91] nëpërmjet integritetit të tre teknologjive të avancuara si biometria, algoritmet kriptografike dhe karta inteligjente ka avantazhe të shumta si: zgjidhja më e besueshme dhe robuste për identifikimin e identitetit të mbajtësit, siguria e lartë dhe mobiliteti. Në të njëjtën kohë, kjo zgjidhje i mundëson mbajtësit të kartës inteligjente një shkallë të lartë kontrolli mbi aksesin në të dhënat e tij biometrike dhe minimizon shqetësimin në rritje për ruajtjen e privatësisë[46][58].

Zgjidhjet kryesore që kombinojnë tre teknologjitë e avancuara do të analizohen në vazhdim:

3.3.1 ToC-Template on card (template-i në kartën inteligjente)

Në këtë zgjidhje të propozuar, i gjithë procesi i regjistrimit të të dhënave biometrike, ekstraktimi i karakteristikave dhe krahasimi i tyre realizohet në anën e lexuesit të kartës inteligjente. Megjithatë gjatë fazës së regjistrimit, template-i origjinal që përpunohet në lexues ruhet në chip-in (me ose pa kontakt) e kartës inteligjente. Gjatë krahasimit, lexuesi do të paraqesë kërkesën për leximin e template-it origjinal, i cili më tej krahasohet me template-in e ri të regjistruar.

Në figurën 3-4 paraqitet procesi i identifikimit me anë të sistemit MoC në kontrollin e dokumenteve biometrikë në pikat kufitare.

Vijat e ndërprera në skemë tregojnë applet firewall (aplikimin e murit mbrojtës) që kufizon aksesin në applet (hapësirë memorie e dedikuar) e krahasimit gjatë kërkesës për krahasim të template-it të gjurmës papilare. Rezultati i krahasimit do të dërgohet nga applet-i i krahasimit në applet-in e krahasimit të pasaportës me metoda enkriptimi të sigurt të aplikuar në applet-in e krahasimit.

Në këtë mënyrë as template-i original i gjurmës papilare dhe as rezultati i krahasimit nuk publikohet jashtë kartës inteligjente. Secili prej applet-eve garanton komunikim të sigurt nëpërmjet mekanizmave të avancuar të kontrollit dhe realizon transferim të sigurt të të dhënave.

3.3.3 SoC-System on card (sistemi në kartën inteligjente)

Në këtë zgjidhje të propozuar, karta inteligjente përmban lexuesin biometrik, procesorin dhe algoritmin e përpunimit. Prandaj i gjithë procesi i regjistrimit të të dhënave biometrike, ekstraktimi i karakteristikave dhe krahasimi realizohet në kartën inteligjente. Brenda kartës inteligjente përlllogariten template-i origjinal dhe ai që do të krahasohet. Në figurën 3-5 paraqitet procesi i identifikimit me anë të sistemit SoC në kontrollin e dokumenteve biometrikë në pikat kufitare.

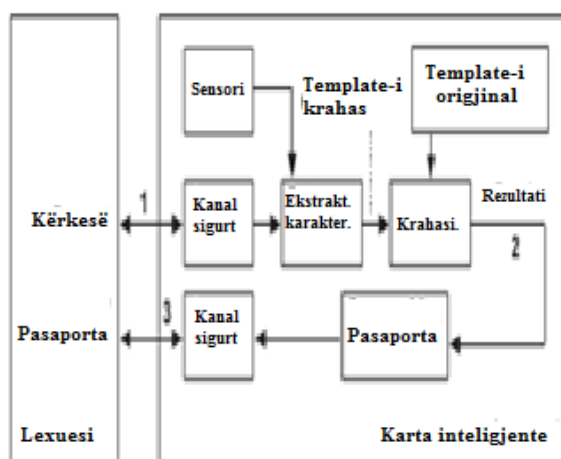


Figura 3-5. Procesi i identifikimit me zgjidhjen SoC në kontrollin në kufi

3.3.4 Pse zgjidhja Match-on-Card?

Siguria në sistemet biometrike mbështetet shumë në faktin se ku ndodh ekstraktimi dhe krahasimi i karakteristikave të gjurmës papilare[27][57]. Kur vlerësojmë vetëm sigurinë, zgjidhja ToC ofron ambientin më pak të sigurt, ndërsa SoC ambientin më të sigurt. Është e kuptueshme që SoC garanton zgjidhjen më të sigurt pasi përpunimi i të gjithë informacionit biometrik realizohet në kartën

inteligjente dhe asgjë nuk transmetohet jashtë saj. Megjithatë, kostoja e lartë e kartës inteligjente, pasi përmban një sensor dhe një processor të fuqishëm në mënyrë që të plotësojë ngarkesën e kërkuar për përpunimin biometrik e limiton përdorimin e gjerë të kësaj zgjidhjeje. Nga ana tjetër zgjidhja MoC garanton një nivel më të lartë sigurie se zgjidhja ToC, me një kosto më të përballueshme, duke e bërë një zgjidhje më praktike.

3.3.5 Disa kufizime

Zhvillimi i teknologjisë MoC[57] ka kufizime për shkak të limitimit në kapacitet të komponentëve përbërës të kartës inteligjente si fuqia përlogaritëse, memoria dhe energjia elektrike. Duhet theksuar fakti që secila kompani që operon në tregun e sistemit të identifikimit mund të zhvillojë në një kohë të shkurtër një sistem ToC, duke qenë se template-i ruhet në kartën inteligjente. Kjo gjë nuk është e mundur për tu realizuar në sistemin MoC për shkak të problemeve të ndryshme teknologjike që kërkojnë zgjidhjen e duhur për procesin e identifikimit. Për këtë arsye, MoC duke pasur zgjidhje specifike dhe më strikte për kartën inteligjente, nëse është e nevojshme mund të konvertohet në një sistem ToC, ndërkohë që e kundërta nuk është e mundur, pasi realizimi kërkon zhvillime dhe testime të mëtejshme.

3.4 Zgjidhja SBMoC-Secure Biometric Match on Card-Raste studimore

3.4.1 Letërnjoftimi elektronik - kartë inteligjente e standartit ISO/IEC 7816

Letërnjoftimi elektronik[130], i ilustruar me anë të një specimeni në figurën 3-6 është një kartë inteligjente në përputhje me standartin ISO/IEC7816[132] dhe karakteristikat teknike dhe funksionale si më poshtë:

- ☐ Kartë polikarbonat e gdhendur me teknologji Laser;
- ☐ Chip pa kontakt 80 kB
 - Të dhëna dhe funksionalitete sipas ICAO 9303
 - Aplikimi: Dokument Udhëtimi
- ☐ Chip me kontakt 80 kB
 - Bazuar në platformën Java 2.1.1
 - Mbajtësi i të dhënave elektronike (e-ID applet)
 - i) Informacioni personal dhe i dokumentit
 - ii) Certifikatat e identifikimit dhe nëshshkrimit elektronik
 - iii) MoC për shënjen e gishtit(fingerprint)
 - Funksionalitetet për identifikimin dhe nëshkrimin elektronik
- ☐ Hapësirë boshe për aplikime të tjera(e limituar)



Figura 3-6. Një specimen i letërnjoftimit elektronik

Sipas rekomandimeve të standartit NIST Special Publication 800-76 [73][130], letërnjoftimi elektronik si kartë inteligjente për verifikimin e identitetit (PIV) duhet të ketë në chip-in me kontakt elementët e detyrueshëm për identifikim dixhital të sigurt si më poshtë:

- Kodin PIN: përdoruesi gjithmonë duhet të vendosë kodin e tij PIN për ta aktivizuar;
- ID unike të mbajtësit të dokumentit, CHUID-Cardholder Unique Identifier (Identifikuesi unik i mbajtësit të kartës inteligjente);
- Të dhënat e autentikimit (një çift çelësash asimetrik dhe çertifikatën korresponduese, duke përdorur 1024-bit RSA dhe ECDSA);
- dy template gjurmë papilare.

Blokkema funksionale e identifikimit dixhital e zbatuar në kartën inteligjente Secure Biometric Match on Card e rastit tonë studimor dhe protokolli i ndjekur gjatë krahasimit lokal biometrik të gjurmëve papilare jepet përkatësisht në figurat 3-7 dhe 3-8.

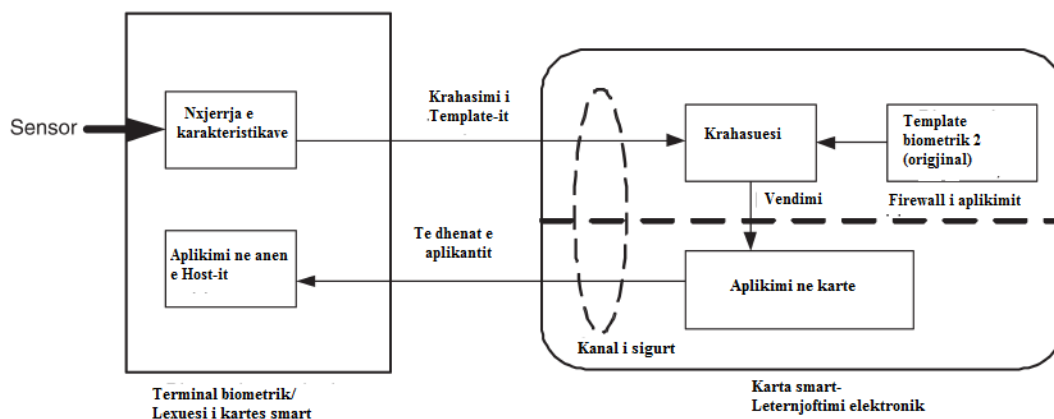


Figura 3-7. Blokkema e identifikimit dixhital SBMoC

Letërnjoftimi elektronik

Sistemi

regjistron gjurmën e gishtit
ekstrakton T,

merr një numer të rastit C

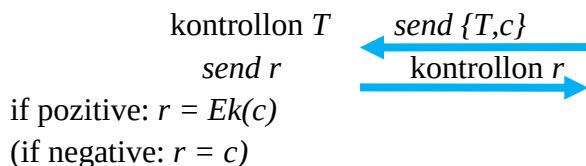


Figura 3-8. Protokolli gjatë krahasimit lokal biometrik në chip-in me kontakt në letërnjoftimin elektronik (MoC)

3.4.2 Infrastruktura e Çelësit Publik

Sistemi kriptobiometrik i instaluar në Qendrën e Personalizimit të dokumentave biometrikë shqiptarë (letërnjoftim elektronik dhe pasaporta biometrike) është i bazuar aktualisht në dy elementë kontrolli biometrik (gjurmën papilare dhe njohjen e fytyrës). Pjesë e zgjidhjes është Infrastruktura e Çelësit Publik [127], e cila ka në përdorim çelësat kriptografik me parametra të avancuara dhe qëllimin e përdorimit si më poshtë:

- Çelësi i autentifikimit asimetrik (RSA Ron Rivest, Adi Shamir, and Leonard Adleman) [1024];
- Një çelës për autentifikimin simetrik (CBC-Cryptography Block Cipher mode-një algoritëm që siguron konfidencialitetin dhe origjinalitetin e informacionit të shkëmbyer);
- Një çelës asimetrik për nënshkrimin elektronik, për nënshkrimin e dokumentave dhe mesazheve (RSA [1024]);
- Një çelës menaxhimi për kartën për të mbështetur personalizimin e kartës dhe përditësimet pas lëshimit (CBC-Cryptography Block Cipher mode-një algoritëm që siguron konfidencialitetin dhe origjinalitetin e informacionit të shkëmbyer).

Infrastruktura e Çelësit Publik për të dy dokumentat (letërnjoftim elektronik dhe pasaportë biometrike) përbëhet nga:

- Konfiguracioni i Autoritetit certifikues (CA) Root, që është Ministria e Punëve të Brendshme, e ilustruar në figurën 3-9, për të dy dokumentet e identifikimit biometrik janë:
 - Çelësi i Root është offline;
 - Çelësi zotërohet nga Autoriteti-Ministria e Punëve të Brendshme.
- Citizen Signature CA
 - Nën-CA e Root CA;

- Firmosja e certifikatave të nënshkrimit elektronik në e-id.
- Citizen Authentication CA
 - Nën-CA e Root CA;
 - Firmosja e certifikatave të autentifikimit elektronik në e-id.

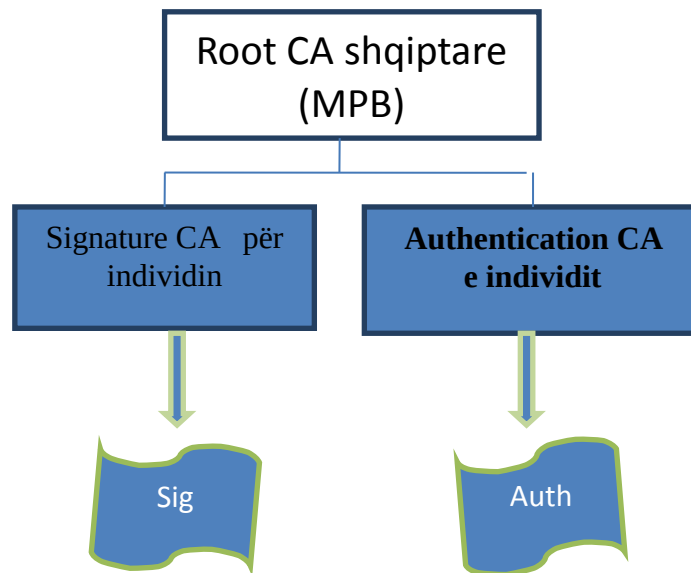


Figura 3-9. Konfiguracioni i Autoritetit certifikues (CA)

3.4.2.1 Mekanizmat e kontrollit të avancuar në pasaportën biometrike

Mekanizmat e kontrollit të avancuar[127] në grup të dhënave të mbajtësit të pasaportës biometrike gjatë identifikimit në pikat e kalimit kufitar paraqiten në tabelën 3.1

Tabela 3-1 Mekanizmat të kontrollit të avancuar

DG	E dhena	Kontrolli i aksesit (mekanizmat e avancuar të kontrollit)
DG1	MRZ-Machine Readable Zone (Zona që lexohet nga makina)	BAC/PACE
DG2	Imazhi i fytyrës	BAC/PACE
DG3	Gjurmet papilare	BAC/PACE + EAC
DG4	Imazhi i Iris	BAC/PACE + EAC(nuk është aktive)

Ku mekanizmat e avancuar të kontrollit janë:

1. BAC-Basic access control (Kontrolli bazë i aksesit) është një mekanizëm kontrolli që siguron që vetëm palët e autorizuar mund të lexojnë me teknologji ëireless informacionin personal nga pasaportat me chip të teknologjisë RFID- Radio Frequency Identification (Identifikimi në radio-frekuencë).
2. EAC-Extended Access Control (Kontrolli gjerë i aksesit) është një mekanizëm kontrolli që përbëhet nga një grup karakteristikash sigurie të avancuar për pasaportat elektronike që mbrojnë dhe kufizojnë aksesin në të dhënat personale sensitive që ruhen në chip-in e teknologjisë RFID. Në ndryshim me të dhënat personale si foto, emër, datëlindje e mbajtësit etj, të cilat mund të mbrohen me mekanizmat bazë, të dhënat më sensitive, të tilla si gjurmët papilare dhe iris, duhet të mbrohen me mekanizma më të avancuar kontrolli, në mënyrë që të parandalojnë aksesin e paautorizuar dhe sulmet. Një chip i mbrojtur me mekanizmin e kontrollit EAC do të lejojë që të dhënat sensitive të lexohen, nëpërmjet një kanali të enkriptuar, vetëm nga një sistem identifikimi i autorizuar.
3. SAC-Supplemental Access Control (Kontrolli shtesë i aksesit) është një mekanizëm kontrolli që përbëhet nga një grup karakteristikash sigurie të përcaktuar nga ICAO- International Civil Aviation Organization (Organizata Ndërkombëtare e Aviacionit Civil) për të mbrojtur të dhënat që përmbajnë dokumentat elektronike të udhëtimit. SAC përcakton protokollin PACE-Passëord Authenticated Connection Establishment (Vendosja e lidhjes së identifikuar me fjalëkalim), e cila plotëson dhe përmirëson mekanizmin e kontrollit BAC për të parandaluar sulme të ndryshme.

Një shembullin e ilustruar në figurën 3-10, identifikimi dixhital me anë të leximit të chipit pa kontakt në терминаlet e pikave të kalimit kufitar realizohet në mënyrë të sigurt nëpërmjet protokollit që aktivizon mekanizmat e kontrollit të avancuar EAC, në infrastrukturën e Çelësit publik (offline).

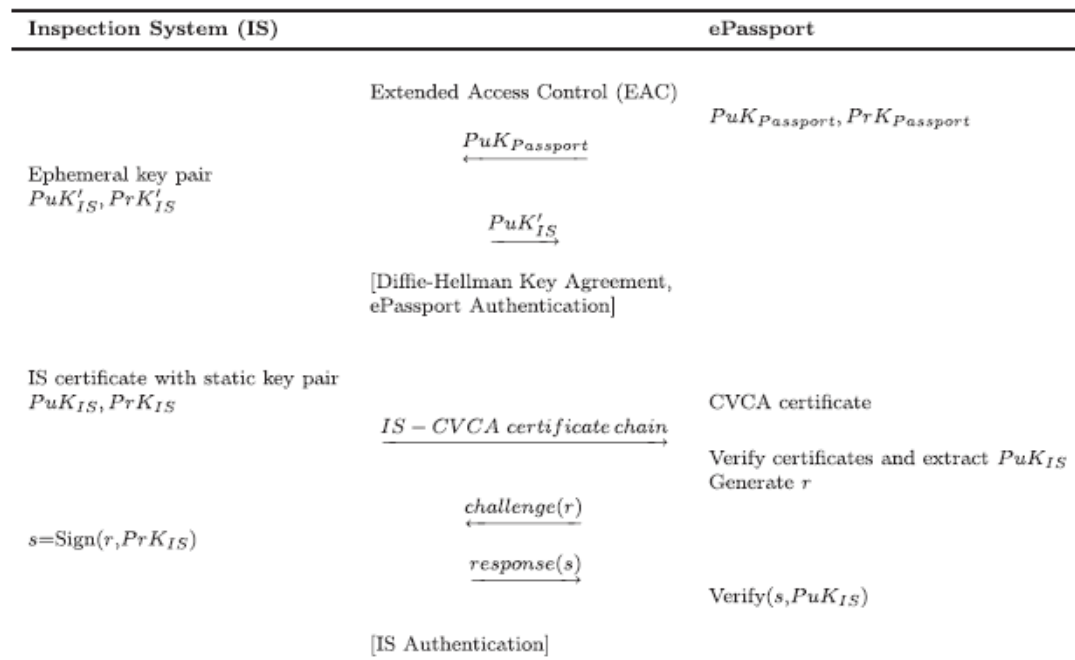


Figura 3-10. Protokoli i identifikimit dixhital gjatë leximit të chip-it pa kontakt në pikat e kalimit kufitar

3.4.3 Platforma e shërbimeve elektronike e-Aleat – rast studimor

Letërnjoftimi elektronik që prej Janar 2014 në chipin me kontakt kur mbyllet chip-i pakontakt, gjatë shpërndarjes së letërnjoftimit, ku bëhet paraprakisht krahasimi lokal biometrik i suksesshëm, ka të ngarkuara 2 certifikata elektronike (citizen and signature) të domosdoshme për aktivizimin dhe përdorimin e shërbimeve elektronike si më poshtë:

- Identifikimi dixhital
- (3 faktor identifikimi)
- Nënshkrimi elektronik (3 faktor identifikimi)
- Revokimi i certifikatave elektronike
- E-aktivizimi

Aktualisht kjo platformë është integruar në platformën e ndërveprimit të sistemeve qeveritare për të mundësuar shërbimin e identifikimit dixhital si pjesë e sistemeve dhe shërbimeve qeveritare. Këto shërbime elektronike momentalisht janë në fazën pilot përkatësisht disa prej tyre janë:

- Nënshkrimi elektronik – noterët;
- Identifikimi dixhital për shërbimet qeveritare, si pjesë e integruar e portalin e-Albania, së shpejti do kalojë live;
- Sistemi bankar: Raifeissein, FIB, etc

Blokskema funksionale e infrastrukturës së platformës e-Aleat jepet në figurën 3.11:

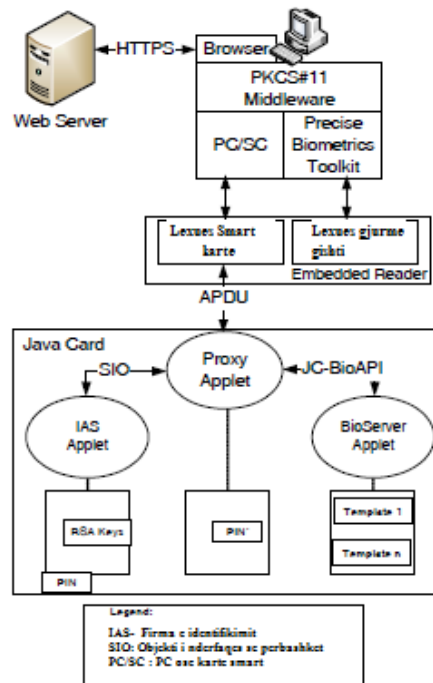


Figura 3-11. Blokskema funksionale e infrastrukturës së platformës e-Aleat

3.4 Vlerësimi i performancës së zgjidhjes MoC

Programi MINEX - Minutiae Interoperability Exchange (Shkëmbimi dhe interoperabiliteti i minutiae-ve) është një program i NIST-National Institute of Standards and technology(Instituti Kombëtar i Standartve dhe Teknologjisë) të Shteteve të Bashkuara të Amerikës, për vlerësimin dhe zhvillimin e aftësive të teknikave krahasuese të minutiae-ve të gjurmës papilare që ekzekutohen në kartat inteligjente të standartit ISO/IEC 7816 (letërnjoftimi shqiptar është një prej tyre).

3.4.1 MINEX I

Objektivi kryesor i MINEX I është analiza dhe vlerësimi i interoperabilitetit të formatit të minutia ANSI 378(American National Standards Institute-Instituti Amerikan për Standartet Kombëtare)[57][73], në algoritmet e krahasimit dhe gjenerimit të vendorëve të ndryshëm. Është e njohur që ndërveprimi i të dhënave të imazheve të gjurmëve biometrike garanton interoperabilitetin më të mirë ndërmjet sistemeve të ndryshëm të identifikimit biometrik. Megjithatë, në ditët e sotme ekzistojnë standarte që specifikojnë zonën dhe formatin e të dhënave të lokalizuara të minutiae-ve ose tempalte-ve të përpunuara për qëllime krahasimi.

Për shumë aplikime, template-t ofrojnë një alternativë më praktike se imazhet e papërpunuara, pasi nuk zënë shumë memorie, alokojnë më pak resource dhe janë më pak të kushtueshëm.

Testi për shkëmbimin dhe interoperabilitetin e minutiae-ve u realizua për të përcaktuar nëse është e realizueshme përdorimi i template-ve standarte të minutiae-ve për informacion gjurmësh papilare të shkëmbyeshëm ndërmjet sistemeve të ndryshëm identifikues të gjurmëve papilare. Disa nga rezultatet janë:

- Për FMR të caktuara, FNMR ndahet nga 2 në 5, template-t e patentuara të krahasuara me template-t standarte. Kjo provoi epërsinë e templatëve të patentuara, megjithatë ky ndryshim nuk ishte shumë tregues dhe është edhe më i vogël kur përdoret një zgjidhje me dy-gjurmë papilare(dhe rregull të fusion-it kur të dy gjurmët duhet të identifikohen);
- Pjesa më e madhe e zbatimeve që përdorin gjurmët papilare ruajnë të paktën dy gjurmë për arsye sigurie(në rast dëmtimi). Kjo është arsyeja pse ideja e vlerësimit të nivelit të saktësisë të përdorimit të dy gjurmëve në vend të një gjurme mund të jetë e përshtatshme;
- Alternativat e formatit të minutiae-ve sipas standartit ANSI 378 janë:
 - Vendodhjet e laqeve dhe deltave;
 - Numri i vijave papilare.

Këto alternativa japin më shumë informacion për një template dhe rrisin saktësinë e tij. Megjithatë ruajtja e një informacioni të tillëështë e kushtueshme. Për këtë arsye MINEX I propozoi vlerësimin e efikasitetit të përdorimit të numrit të vijave papilare, si alternativë shtesë e vendndodhjes së minutiae-ve. Në rastet e vlerësuara me të dy alternativat saktësia rritet në vlerë të vogël, që nuk justifikon përdorimin e alternativës shtesë.

3.4.2 MINEX II

Në vijim të MINEX I, objektivi kryesor ishte përcaktimi nëse template-t referencë të standartizuara të minutiae-ve mund të krahasohen më tej përkundrejt një template-i të njëvëndori tjetër. MINEX II këtë objektiv e zbatoi vetëm për një klasë të kufizuar algoritmesh krahasues dhe gjenerues të gjurmëve papilare, atë të vendorëve me teknika krahasuese të minutiae-ve të gjurmës papilare që ekzekutohen në kartat inteligjente të standartit ISO/IEC 7816.

Nga ana tjetër MINEX II vlerëson performancën e MoC me shkallë e vogël të FAR. Rezultatet e matura dhe krahasuara ndërmjet teknologjive më të avancuara të

kartave inteligjente dhe algoritmet më të fundit kriptografike të ekstraktimit dhe match on card të template-it të gjurmës papilare jepet përkatësisht në tabelën 3-2.

Tabela 3-2. Rezultatet dhe krahasimet e performancës sipas MINEX II

(a) FNMR at FMR = 0.01

Column = MATCH-ON-CARD algorithm, Row = INCITS 378 generator

Nfing	MX2D	MX2E	MX2G	MX2H	MX2I	MX2J	MX2K	MX2M	MX2N	MX2O	MX2P	MX2Q	MX2R	MX2S	MX2T	MX2N ³	MX2T ³
2																	
A	0.0038	0.0065	0.0427	0.0324	0.0140	0.0146	0.0156	0.0399	0.0073	0.0041	0.0048	0.0047	0.0466	0.0523	0.0016	0.0127	0.0014
B	0.0020	0.0070	0.0168	0.0159	0.0080	0.0082	0.0086	0.0207	0.0066	0.0037	0.0041	0.0030	0.0356	0.0416	0.0031	0.0098	0.0053
C	0.0030	0.0112	0.0237	0.0231	0.0118	0.0119	0.0128	0.0270	0.0095	0.0056	0.0056	0.0035	0.0482	0.0561	0.0065	0.0101	0.0126
D	0.0015	0.0029	0.0105	0.0066	0.0046	0.0046	0.0048	0.0156	0.0038	0.0021	0.0025	0.0023	0.0175	0.0197	0.0013	0.0092	0.0030
E	0.0040	0.0065	0.0195	0.0143	0.0093	0.0096	0.0102	0.0514	0.0063	0.0041	0.0044	0.0040	0.0343	0.0387	0.0026	0.0078	0.0034
F	0.0030	0.0112	0.0234	0.0225	0.0115	0.0117	0.0125	0.0271	0.0094	0.0055	0.0056	0.0035	0.0481	0.0557	0.0066	0.0102	0.0126
G	0.0025	0.0080	0.0205	0.0152	0.0102	0.0105	0.0083	0.0310	0.0079	0.0042	0.0044	0.0031	0.0439	0.0508	0.0041	0.0099	0.0069
N	0.0049	0.0121	0.0224	0.0168	0.0116	0.0118	0.0123	0.0343	0.0114	0.0069	0.0059	0.0050	0.0499	0.0561	0.0063	0.0146	0.0094
1C	0.0030	0.0054	0.0254	0.0194	0.0087	0.0088	0.0092	0.0425	0.0049	0.0031	0.0040	0.0036	0.0314	0.0359	0.0022	0.0044	0.0036
1D	0.0052	0.0201	0.0315	0.0267	0.0177	0.0181	0.0190	0.0354	0.0147	0.0103	0.0102	0.0055	0.0611	0.0688	0.0128	0.0154	0.0211
1F	0.0046	0.0140	0.0315	0.0248	0.0158	0.0162	0.0170	0.0392	0.0126	0.0075	0.0077	0.0052	0.0548	0.0618	0.0075	0.0166	0.0096
1G	0.0046	0.0140	0.0315	0.0249	0.0158	0.0162	0.0170	0.0393	0.0126	0.0075	0.0077	0.0052	0.0548	0.0619	0.0075	0.0166	0.0096
1J	0.0032	0.0132	0.0272	0.0210	0.0133	0.0133	0.0140	0.0270	0.0087	0.0048	0.0075	0.0043	0.0484	0.0633	0.0086	0.0114	0.0188
1L	0.0023	0.0058	0.0201	0.0146	0.0093	0.0096	0.0101	0.0295	0.0057	0.0031	0.0040	0.0033	0.0355	0.0417	0.0023	0.0084	0.0034
1M	0.0022	0.0056	0.0197	0.0151	0.0071	0.0071	0.0074	0.0268	0.0064	0.0039	0.0038	0.0030	0.0474	0.0538	0.0031	0.0095	0.0062
1N	0.0038	0.0123	0.0290	0.0228	0.0134	0.0136	0.0143	0.0312	0.0077	0.0049	0.0064	0.0044	0.0485	0.0557	0.0062	0.0074	0.0114
1T	0.0022	0.0039	0.0174	0.0130	0.0078	0.0079	0.0060	0.0306	0.0048	0.0029	0.0030	0.0027	0.0246	0.0302	0.0019	0.0052	0.0036
1Y	0.0020	0.0046	0.0166	0.0124	0.0079	0.0080	0.0061	0.0274	0.0055	0.0033	0.0034	0.0028	0.0426	0.0482	0.0025	0.0088	0.0049
2A	0.0030	0.0112	0.0237	0.0231	0.0118	0.0119	0.0128	0.0270	0.0095	0.0056	0.0056	0.0035	0.0482	0.0561	0.0065	0.0101	0.0126

A = Cogent	E = Neurotechnology	1C = LI/identix	1J = BIO-Key	1T = Neurotechnology
B = Dermalog	F = Innovatrics	1D = Precise Biometrics	1L = Motorola	1Y = Aware
C = Bioscrypt	G = NEC	1F = XTec	1M = Aware	2A = ImageWare
D = Sagem	N = Crossmatch	1G = Secugen	1N = Sonda	(ANSI 378 generators)

3.4.2.1 Rezultatet e saktësisë dhe shpejtësisë

MINEX II vlerëson saktësinë dhe shpejtësinë e algoritmave të identifikimit (ekstraktues/ krahasues) match on card. Në figurën 3-12 ilustrohen saaktësia e MoC me zbatimin me dy gjurmë papilare. Vijat e plota i korrespondojnë rezultateve të arritura kur përdorim një gjenerues Cogent në fazën e regjistrimit dhe gjenerator Sagem në krahasim. Vijat e ndërprera i korrespondojnë rezultateve të marra kur përdorim gjenerator Innovatrics në aplikim dhe gjenerator Sageem në krahasim.

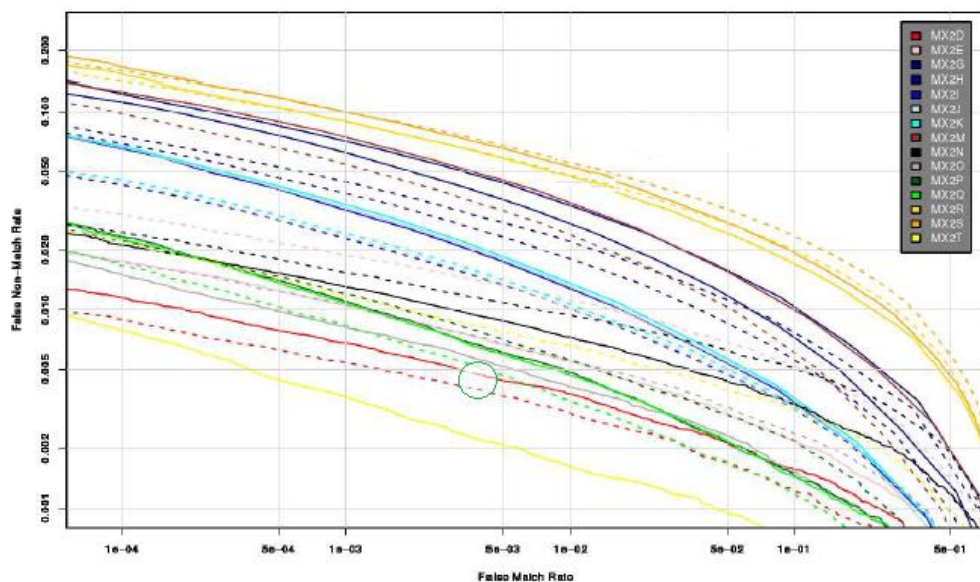


Figura 3-12. Rezultatet e saktësisë MINEX II(më e saktë vlera më e ulët)

Nga grafiku dallohet se vija e plotë e verdhë është një zgjidhje më robuste (kartat inteligjente Cogent dhe Gemalto). Vija e ndërprerë e verdhë është më e përshatshme pasi nuk është gjenerator referencë Cogent. Zbatime më robuste të matura (saktësi më e lartë) janë Cogent(e verdhë), Sagem(e kuqe), ID3(jeshile) dhe Innovatrics(e zezë).

Në figurën 3-13 paraqiten rezultatet e kohës së zgjidhjeve MoC. Koha mesatare e përgjigjes është ndërmjet 0.5 dhe 1 sekond. Ndërkohë në figurë me kuti me ngjyrë të hapur raportohet koha për krahasimet e suksesshme dhe me ngjyrë të errët për krahasimet e pasuksesshme.

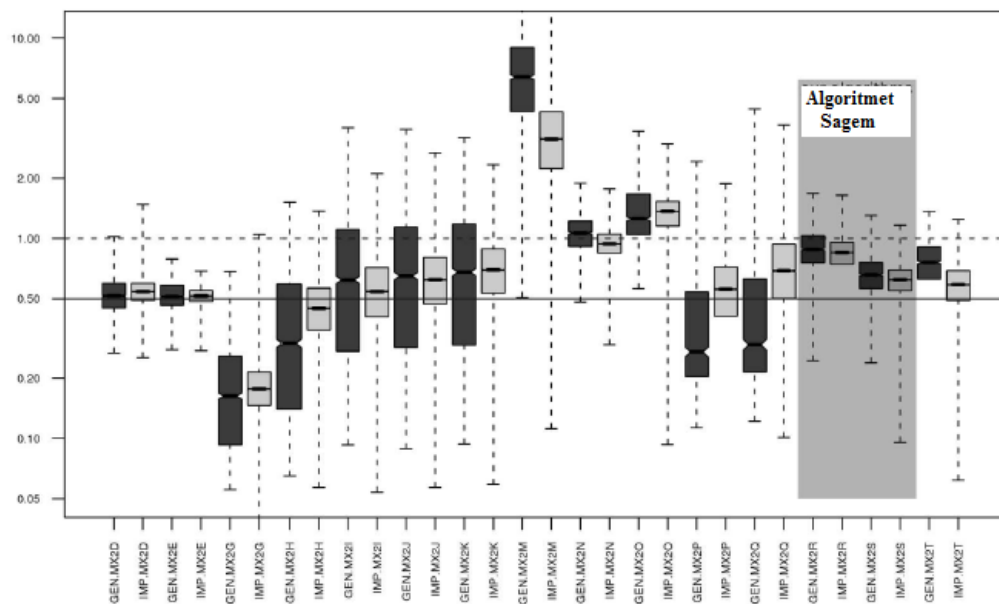


Figura 3-13.Rezultatet e kohës së përgjigjes MINEX II

KAPITULLI 4

Biometria e gjurmës papilare

4.1 Hyrje

Teknologjia e skanimit dhe krahasimit të gjurmëve papilare është teknologjia biometrike e përdorur më gjerësisht, me një numër të konsiderueshëm zgjidhjesh për identifikimin dixhital[78], kjo pasi biometria e gjurmës papilare ofron një nivel të lartë të saktësisë në identifikim[33]. Në përgjithësi ekzistojnë dy tipe lëkure në trup[79], e ilustruar në figurën 4-1, e para lekure e lëmuar, me qime dhe gjendra yndyrë dhe e dyta lëkurë e cila nuk ka asnjërën prej tyre, Lëkura e tipit të dytë është ajo që gjendet në majat e gishtërinjve dhe quhet gjurmë papilare. Gjurma papilare është një model i strukturuar i vijave dhe brazdave papilare që ndërthuren në majën e gishtit siç tregohet dhe në figurën 4-2.



Figura 4-1. Lëkura e lëmuar



Figura 4-2. Lëkura e majës së gishtit

Sipas shumë studimeve të kryera gjurmët papilare ofrojnë individualitet potencial, ku dy individë nuk mund të kenë gjurmë papilare të njëjta. Përdorimi i gjerë i tyre për identifikimin e individëve filloi vetëm në shekullin e 20-të. Në fillimet e veta, gjurmët papilare merreshin duke shenjuar gishtat e dorës të lyer me bojë në një letër, por në ditët e sotme kjo është zëvendësuar me teknologji të avancuar të pajisjeve të regjistrimit të imazhit (sensorëve)[74], që ka mundësuar së fundmi projektimin e sensorëve kompaktë dhe të lirë.

Tregu në rritje i sensorëve me përmasa të vogla dhe me kosto të ulët ka bërë të mundur përdorimin e gjurmës papilare si element kontrolli në një gamë të gjerë zbatimesh, të tilla si tregtia elektronike, aksesit fizik, identifikimi dixhital i individëve në pikat e kalimit kufitar (nëpërmjet dokumentave biometrik), përdoruesve të autorizuar në sistemet industriale dhe të teknologjisë së informacionit, etj.

Me përdorimin e këtyre sensorëve, sistemet e identifikimit automatik të gjurmëve papilare u zhvilluan më tej, për të përmirësuar efikasitetin dhe saktësinë e krahasimit të gjurmëve papilare. Aktualisht, pothuaj çdo agjenci e zbatimit të ligjit, në çdo vend të botës, mbështetet në këto sisteme për të krahasuar gjurmët papilare.

Shqetësimi në rritje për sigurinë publike dhe mashtrimet e konsumatorëve kanë treguar nevojën e përdorimit të gjurmës papilare si element kontrolli, në sistemet biometrike të identifikimit dixhital, për shumë zbatime të tjera, të ndryshme nga ato mjeko-ligjore.

Në ditët e sotme, sistemet biometrike të identifikimit dixhital me element kontrolli gjurmën papilare janë bërë kaq të njohur dhe të përdorur, sa janë bërë sinonim i nocionit të identifikimit biometrik në gjykimin e publikut të gjerë[74].

Modeli i vijave papilare të çdo gishti pohohet sipas shumë studimeve në fushë të jetë unik dhe i pandryshueshëm duke mundësuar përdorimin e tij si shenjë të padiskutueshme të identitetit të individit. Nga studimet rezulton që edhe binjakët identikë mund të dallohen nga gjurmët e tyre papilare. Dëmtimet sipërfaqësore të tilla si prerjet dhe djegiet në sipërfaqen e gishtit ndryshojnë përkohësisht modelin e tyre, vetëm në zonën e dëmtuar, pasi me shërimin e dëmtimeve[74], struktura e vijave papilare rishfaqet përsëri.

4.2. Karakteristika dhe veçori të gjurmës papilare

Identifikimi me gjurmë papilare bazohet tërësisht në krahasimin e karakteristikave të përdorura të cilat kanë një interpretim fizik. Kjo metodë ekstrakt karakteristika të qarta nga imazhi që analizohet dhe i kodon në një grup karakteristikash, të cilat përdoren më tej për krahasim, në skemën e kontrollit. Në figurën 4-3 paraqitet imazhi gri i një gjurme papilare [74].



Figura 4-3. Imazhi gri i gjurmës papilare

Për një ekstraktim optimal të karakteristikave, imazhi përmirësohet dhe qartësohet për tu paraqitur si një imazh i skeletit të vijave papilare, në të cilën çdo vijë papilare paraqitet me një pixel gjerësi si në figurën 4-4.



Figura 4-4. Imazhi i gjurmës papilare i përmirësuar dhe i qartësuar

Vendodhjet ku një vijë papilare shfaqet, përfundon, ndahet ose bashkohet me një vijë tjetër papilare përkufizohen si karakteristikat e vijës papilare ose minutiae. Përveç vendndodhjes, një minutiae ka dhe dy parametra të tjerë: drejtimin dhe llojin. Drejtimi i minutiae ndjek të njëjtin drejtim si orientimi lokal i vijës papilare. Në figurën 4-5 tregohen dy llojet kryesore të minutiae: fundore dhe degëzim [74].



Figura 4-5. Vijat papilare fundore dhe degëzim

Një grup minutiae, që përbëhet nga të gjithë minutiae në një gjurmë papilare, është një paraqitje abstrakte e skeletit të vijave papilare. Këto paraqitje me bazë minutiae përdoren gjerësisht në sistemet e automatizuara të identifikimit biometrik kryesisht për arsyet e mëposhtme:

- Minutiae veçon shumicën e informacionit dallues ose unik në gjurmën papilare;
- paraqitjet me bazë minutiae zënë pak hapësirë memorie;
- ekstraktimi i minutia është mjaft i qëndrueshëm ndaj burimeve të ndryshme të degradimit.

Kur imazhi i qartësuar i vijës papilare është me cilësinë e duhur, pixel- at e vijës papilare me tre pixela fqinjë të vijës papilare identifikohen si degëzime të vijës papilare dhe ato me një pixel fqinj të vijës papilare identifikohen si funde të vijës papilare. Grupi i minutiae krahasohet më tej me një template për të përlogaritur rezultatin e krahasimit bazuar në pikat korresponduese minutiae. Në figurën 4-6 paraqitet procesi i krahasimit të minutiae-ve[74][77].

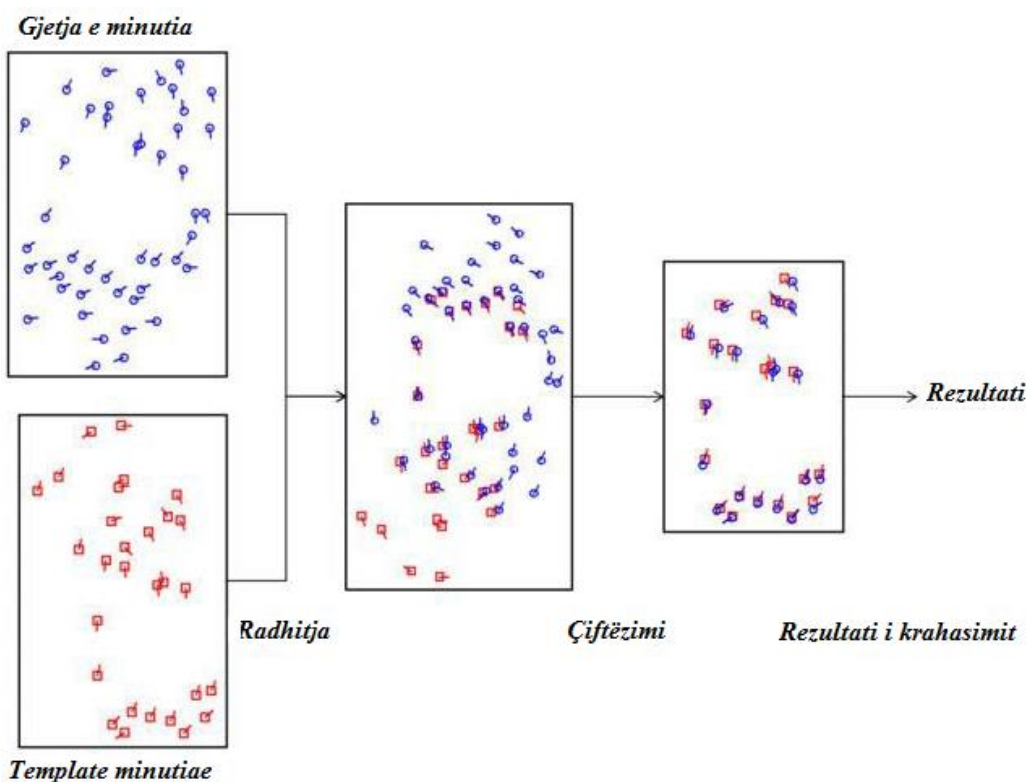


Figura 4-6. Procesi i krahasimit të minutiae-ve

Algoritmet kompjuterike të krahasimit të imazhit[74] përdoren për të krahasuar karakteristika të çiftëzuara të imazhit të gjurmës papilare. Në figurat e paraqitura 4-7 dhe 4.8 tregohet qartë se kur dy gjurmë papilare përputhen gjenerohet rezultat i lartë pikësh dhe kur nuk përputhen gjenerohet rezultat i ulët pikësh[74][78].

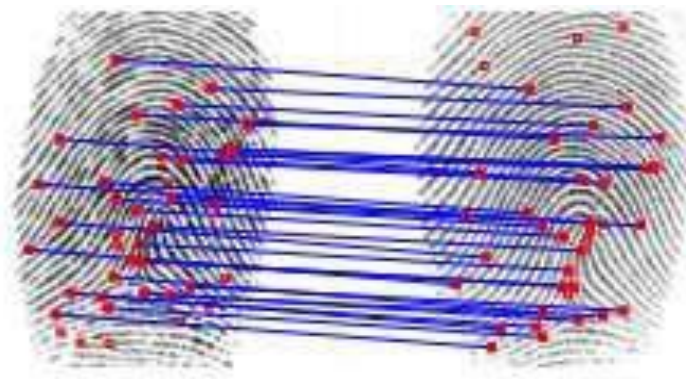


Figura 4-7. Një çift gjurmësh papilare identike me minutiae të përputhura në maksimum

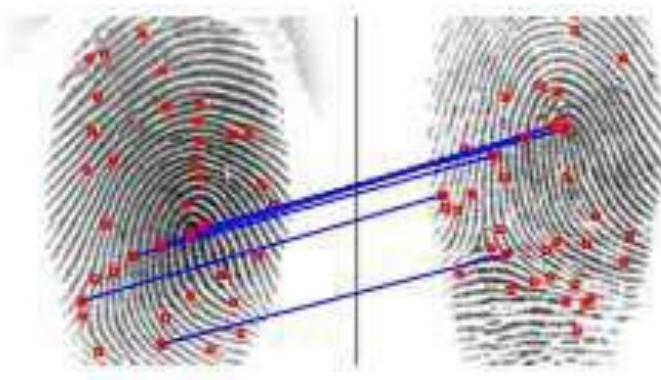


Figura 4-8. Një çift gjurmësh të ndryshme me shumë pak minutiae të përputhura

Identifikimi biometrik, qoftë kur bëhet manualisht nga një ekspert ose kur bëhet automatikisht nga një makinë, kryesisht është një metodë që bazohet në karakteristika(në ndryshim nga ato që bazohen tek imazhi) dhe karakteristikat e përdorura kanë një interpretim fizik. Termat me bazë-karakteristikë dhe bazë-imazhi janë gjerësisht të përdorura në literaturën e vizualizimit kompjuterik për të treguar metodat e përdorura për paraqitjen dhe krahasimin e imazheve të tilla si gjurmët papilare.

Një metodë me bazë-karakteristikën ekstraktin karakteristika të veçanta nga imazhi i analizuar dhe kodon këto karakteristika një një grup karakteristikash, e cila përdoret në vazhdim për krahasim. Nga ana tjetër një metodë me bazë-imazhi përdor direkt imazhin për krahasim pa ekstraktuar në mënyrë të veçantë asnjë karakteristike nga imazhi [74].

Së pari, nga një gjurmë papilare mund të ekstraktohen kategori të ndryshme karakteristikash, të cilat shoqërohen nga një përshkrim i histologjisë së lëkurës së vijës papilare dhe formacionit të saj. Njohuritë mbi këto dy çështje janë të domosdoshme për kuptimin e unicitetit dhe qëndrueshmërisë së modeleve të vijave papilare, të cilat janë faktorët kryesorë në njohjen biometrike [78].

4.2.1 Karakteristikat kryesore të gjurmës papilare

Karakteristikat në një gjurmë papilare mund të kategorizohen në tre nivele të ndryshme duke filluar nga më të dukshmet tek më të imëtat. Në kushte ideale, karakteristikat e nivelit të dukshëm mund të derivohen nga nivelet e imëta të paraqitjes së gjurmës papilare.

4.2.1.1 Karakteristikat e nivelit 1

Në nivelin e parë, një gjurmë papilare paraqitet si një hartë orientuese, si - figurën 4-9. Harta orientuese regjistron orientimin lokal të vijës papilare dhe frekuencën lokale të vijës papilare në çdo vendndodhje në gjurmën papilare. Një gjurmë papilare shpesh është referuar si një model orientues, që bazohet në formën dhe strukturën globale të saj. Në detajet e nivelit 1 dallohen vetëm drejtimi dhe frekuenca e vijës papilare, ndërsa vendndodhja e saktë dhe detajet dimensionale të vijës papilare nuk merren parasysh. Për të gjeneruar dhe vlerësuar karakteristikat e nivelit 1 të gjurmës papilare[74] përdoren sensorë për imazhe me rezolucion të ulët 250 ppi.

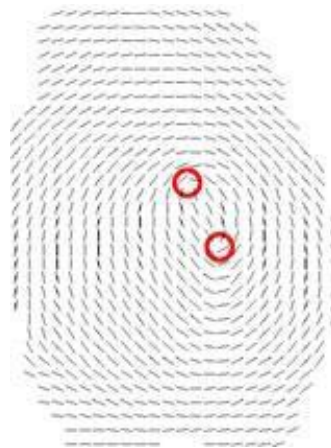


Figura 4-9. Harta orientuese - Niveli 1 i karakteristikave

Orientimi lokal i vijës papilare në një pixel(x,y) paraqet drejtimin tangencial të vijave papilare që kalojnë nëpër pixel (x,y). Orientimi i vijës papilare përcaktohet në diapazonin $[0, \pi)$.

Si rrjedhim harta orientuese e vijave papilare mund të shihet si një vektor gjatësie njësi, drejtimi i të cilit përcaktohet ndërmjet 0 dhe π . Frekuenca lokale e vijës papilare në (x,y) është numri mesatar i vijave papilare për njësi gjatësie përgjatë një segmenti vijë të qendëruar në (x,y) dhe pingul me orientimin lokal të vijës papilare. Frekuenca e vijës papilare është e anasjellta e periodës së vijës papilare.

Orientimi i vijës papilare në një pixel p është ilustruar në figurën 4-10, në të cilën paraqitet një pjesë e gjurmës me vija papilare të treguara me vija të errëta me orientimin e vijës papilare θ dhe periodën e vijës papilare 'ab'(e anasjellta e frekuencës së vijës papilare) i shënuar në një pixel p . Përgjithësisht, informacioni i orientimit të vijës papilare vlerësohet si më i rëndësishëm se informacioni i frekuencës së vijës papilare për qëllime krahasimi dhe klasifikimi të gjurmës papilare.

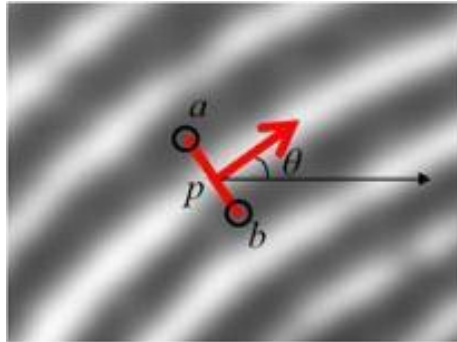


Figura 4-10. Matja e orientimit të vijës papilare

Një hartë orientuese e vijës papilare përmban vendndodhje të dukshme, në të cilat orientimet e vijave papilare ndryshojnë menjëherë. Këto vendndodhje të dukshme janë përcaktuar si pika singulare. Ekzistojnë dy lloje kryesore të pikave singulare lakore dhe delta që janë të dallueshme vizualisht. Një pikë singulare lakore, që quhet qendër, i referohet një zone lokale ku një grup vijash papilare hyjnë nga një drejtim dhe dalin në të njëjtin drejtim siç tregohet edhe në figurën 4-11.

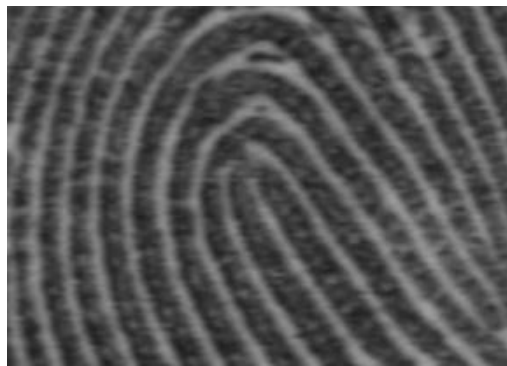


Figura 4-11. Veçoritë e laqeve

Një lak në një gjurmë papilare mund të përdoret si një pikë referimi për të përcaktuar qendrën e gjurmës papilare. Përgjithsisht, pika e qendrës i korrespondon pikës singulare të tipit lakor, më në veri në një gjurmë papilare. Nëse një gjurmë

papilare nuk përmban asnjë pikë singulare, qendra zakonisht i referohet pikës së lakimit maksimal të vijës papilare. Megjithatë, termi qendër në vetvete përdoret shpesh për të treguar në praktikë veçoritë e tipit lakor. Një veçori e tipit delta tregon një zone lokale ku tre sistemet e vijave papilare shfaqen dhe takohen siç tregohen në figurën 4-12.

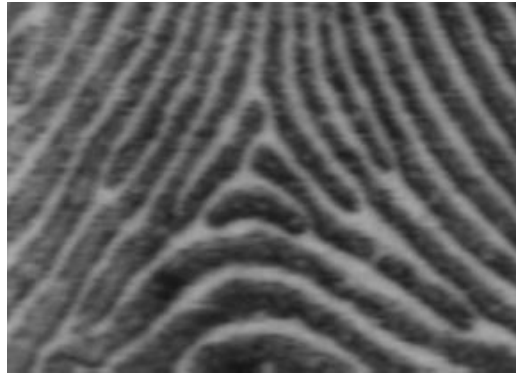


Figura 4-12. Veçoritë e deltave

Grupi i pikave të veçanta në një gjurmë papilare mund të shihet si një paraqitje abstrakte e hartës orientuese, si rrjedhim ajo mund të parashikohet afërsisht bazuar në numrin dhe vendndodhjen e pikave të veçanta. Një paraqitje edhe më abstrakte e hartës orientuese është tipi i modelit (shpesh i referuar dhe si një klasë e gjurmës papilare), e cila mund të nxirret bazuar në numrin e laqeve dhe deltave, si dhe lidhjes hapësinore ndërmjet tyre.

Veçoritë në shumë gjurmë papilare mund të dallohen kur plotësohen kufizimet: (a) numri i laqeve dhe deltave në një gjurmë të plotë janë të njëjta; me fjalë të tjera, laqet dhe deltat shfaqen çift; dhe (b) numri total i pikave të veçanta janë ose 0, 2, 4 [74].

4.2.1.2 Karakteristikat e nivelit 2

Në nivelin e dytë, një gjurmë papilare paraqitet si një imazh i strukturuar i vijës papilare, ku çdo vijë papilare është vetëm një pixel e gjerë siç e pamë në figurën 4-4. Në këtë nivel, vendndodhjet e sakta të vijave papilare regjistrohen, por detajet gjeometrike dhe dimensionale të vijave papilare nuk merren parasysh. Vendndodhjet ku një vijë papilare shfaqet, ndahet ose bashkohet me një vijë tjetër papilare janë përcaktuar si karakteristika të vijës papilare ose minutiae. Përveç vendndodhjes së saj minutiae ka dhe dy veçori të tjera: drejtimin dhe tipin. Drejtimi i një minutiae është përgjatë orientimit lokal të vijës papilare. Ekzistojnë dy tipe bazë të minutiae: fundore dhe degëzim që tregohen në figurën 4-13.

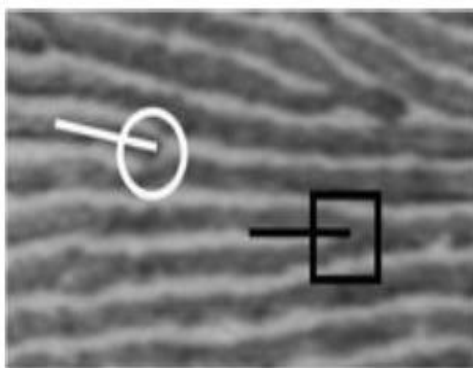


Figura 4-13. Vijë papilare fundore (a) me rreth të bardhë:degëzim (b) me katror të zi

Çdo minutiae mund të karakterizohet nga:

- a) vendndodhja e saj në imazh;
- b) drejtimi;
- c) tipi.

Detajet e nivelit 2 të një gjurme papilare mund të dallohen në imazhet e marra nga sensorë me rezolucion prej 500 ppi. Numri i minutiae që gjenden në një gjurmë papilare varion sipas metodës së regjistrimit dhe faktorëve të tjerë[74]. Një grup minutiae, që përbëhet nga të gjitha minutiae-t në gjurmën papilare, është një paraqitje abstrakte e strukturës së vijës papilare në kuptimin që grupi i minutiae-ve që regjistron informacionin më dallues në nivelin 2, dhe struktura e vijës papilare mund të derivohet vetëm nga informacioni i minutiae-ve.

Shpërndarja hapësinore e minutiae-ve në një gjurmë papilare është një çështje me interes të madh studimi, që ka tërhequr vëmendjen për shkak të nevojës për të vlerësuar individualitetin e gjurmëve papilare duke përdorur vetëm informacionin e minutiae-ve.

4.2.1.3 Karakteristikat e nivelit 3

Në nivelin e tretë, një gjurmë papilare paraqitet duke përdorur vrimat e brendshme(poret e e djersës) dhe konturet e jashtme(kufinjte) e vijës papilare. Kështu që vijat papilare nuk shihen më si të thjeshta, imazhe strukture një pixel të gjera. Për më tepër, informacioni që përmbahet brenda vijave papilare vëzhgohet më në detaje.Vijat papilare dhe pikat përfshihen gjithashtu në këtë nivel. Vijat papilare fillestare janë vija papilare të pazhvilluara, të cilat janë më të holla se të zhvilluarat dhe nuk përmbajnë pore djerse.

Një pikë është një vijë papilare e shkurtër që përmban vetëm një njësi të vetme vije papilare. Me zhvillimet teknologjike në regjistrimin e gjurmëve papilare, shumë sensorë të mëdhenj janë të pajisur tani me aftësinë e skanimit me 1000 dpi që është e

duhura për të kapur detajet e nivelit 3 në një gjurmë papilare[74]. Në figurën 4-14 jepet një gjurmë papilare me karakteristika të nivelit 3 të tilla si: kufinjtë, poret dhe pikat.

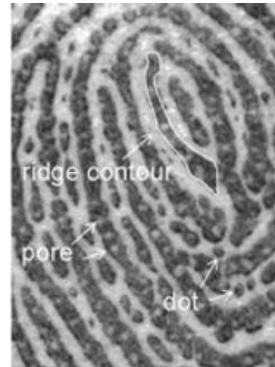


Figura 4-14 Karakteristikat e nivelit 3

4.2.1.4 Karakteristikat shitesë

Gjurmët papilare shpesh kanë karakteristika të tjera shitesë të tilla si rrudha, të prera dhe shenja. Ndërsa këto karakteristika nuk janë të pandara nga formacioni i gjurmës papilare, ato mund të bëhen të përhershme në varësi të thellësisë së të prerës dhe shenjës. Megjithatë, duke qenë se këto karakteristika nuk janë aq universale sa tre nivelet e karakteristikave të diskutuara me herët, përdorimi i tyre në krahasimin e gjurmëve papilare është i kufizuar. Në fakt, të tilla anomali janë shpesh burim gabimi gjatë krahasimit[74].

4.2.2 Sistemi i identifikimit biometrik me gjurmë papilare

Modulet kryesore të sistemit të identifikimit biometrik me gjurmë papilare janë:

- a) regjistrimi i gjurmëve papilare, në të cilën gjurma papilare e një individi regjistrohet nga një skaner për të prodhuar një paraqitje numerike të papërpunuar;
- b) parapërpunimi, në të cilën vlerat në hyrje të gjurmës papilare përmirësohen dhe përshtaten për të thjeshtësuar detyrën e ekstraktimit të karakteristikave;
- c) ekstraktimi i karakteristikave, në të cilën gjurmët papilare përpunohet më tej për të gjeneruar karakteristika dalluese, që quhen ndryshe dhe vektorët e karakteristikave;
- d) krahasimi, në të cilën vektori i karakteristikave të hyrjes së gjurmës papilare krahasohet përkundrejt një ose më shumë template-ve ekzistues.

Template-t e përdoruesve të aprovuar të sistemit të identifikimit biometrik regjistrohen zakonisht në bazën e të dhënave dhe quhen klientë. Klientët mund të deklarojnë një identitet dhe gjurmët e tyre papilare mund të krahasohen përkundrejt gjurmëve papilare të regjistruara[33]. Në figurën 4-15 ilustron struktura bazë e një sistemi identifikimi biometrik me gjurmë papilare.

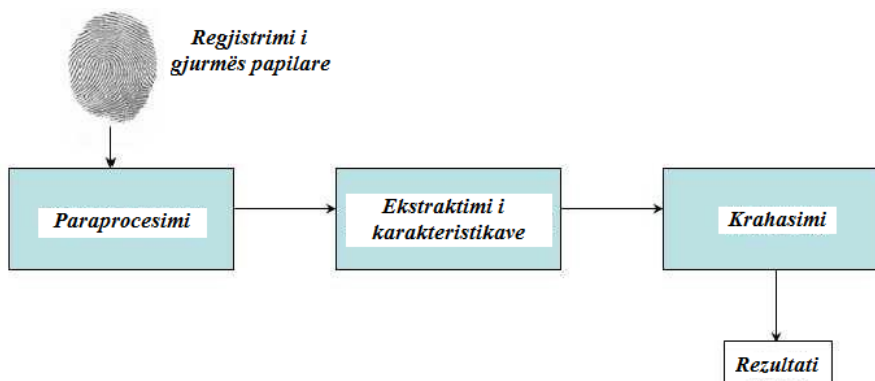


Figura 4-15. Struktura bazë e një sistemi identifikimi biometrik me gjurmë papilare

4.2.1 Regjistrimi i gjurmëve papilare

Regjistrimi i imazheve të gjurmëve papilare[77] është realizuar historikisht nga ngjyrosja me bojë e majës së gishtit dhe shtypja e tij në një kartë letre. Karta e letrës më tej skanohet, dhe rezulton në një paraqitje numerike. Ky proces është i njohur si regjistrimi offline dhe përdoret akoma në aplikimet e zbatimit të ligjit. Në ditët e sotme është e mundur të regjistrosh imazhet e gjurmës papilare duke shtypur gjurmën papilare në sipërfaqen e sheshtë të një sensori elektronik të gjurmës papilare. Ky proces është i njohur si një regjistrim online[33]. Ekzistojnë lloje të ndryshme të sensorëve të gjurmës papilare, sië ilustron dhe në figurën 4-16.



Figura 4-16. Sensorë të ndryshëm të regjistrimit të gjurmëve papilare

Tipet më të njohura janë sensorët me gjendje-solide dhe sensorët optikë. Sensorët me gjendje solide kanë gjetur zbatim në aparaturat e teknologjisë së fundit të telefonisë celulare (smartphones dhe gadgets), pasi ato janë kompakte dhe nuk kanë komponentë optikë. Sensori me gjendje-solide ka një pllakëz capacitive që përbëhet

nga pixela të cilët konvertojnë informacionin nga kontakti vijë-brazdë papilare në një sinjal elektrik. Në figurën 4-17 ilustron parimi i një sensori me gjendje-solide.

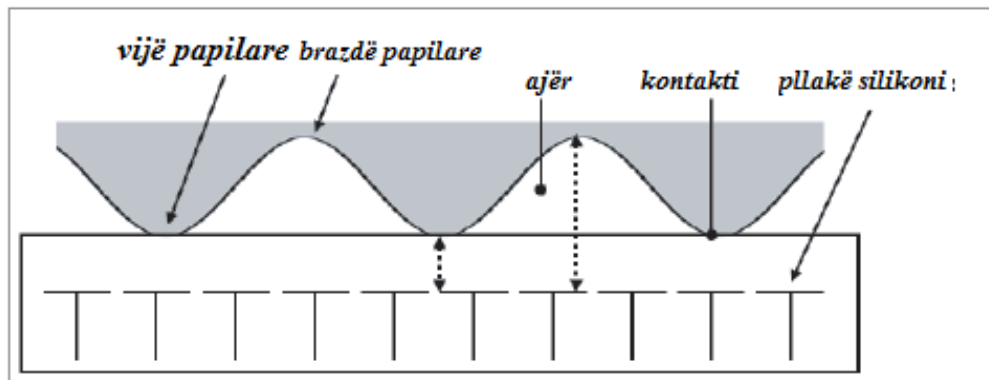


Figura 4-17. Sensorët me gjendje-solide

Sensorët optikë janë shumë më të saktë, por nuk janë kompaktë. Në këtë rast gjurma papilare prek një prizëm xhami, i cili ndriçohet me dritën e difuzuar, e cila reflektohet në brazdat dhe absorbohet në vijat papilare. Drita e reflektuar fokusohet mbi një sensor imazhi, i cili gjeneron imazhin e gjurmës papilare. Sensorët e imazhit janë pajisje CCD (Charge Couple Device) ose CMOS (Complementary Metal Oxide Semiconductor). Parimi i punës së një sensori optik paraqitet në figurën 4-18.

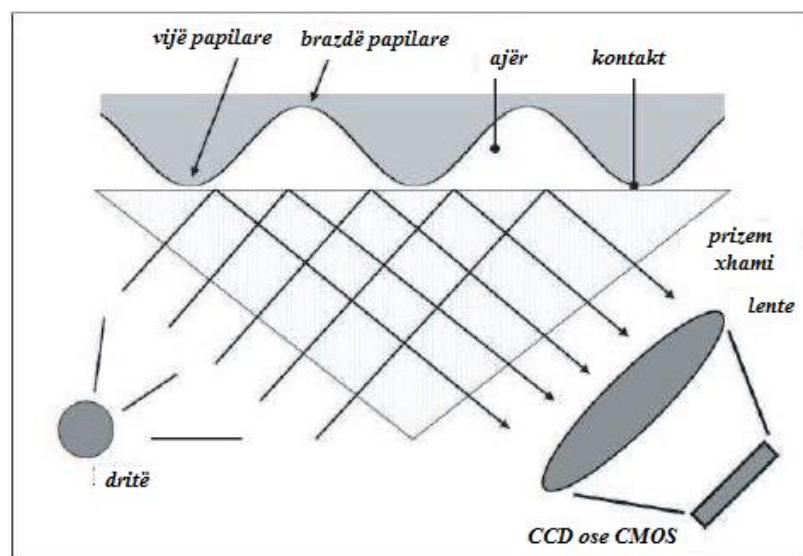


Figura 4-18. Sensorët optikë

4.2.2 Parapërpunimi

Cilësia e imazhit të regjistruar të gjurmës papilare ka një impakt të rëndësishëm në performancën e procesit të ekstraktimit të karakteristikave dhe

krahasimit të tyre. Faktorë të rëndësishëm që përcaktojnë cilësinë e gjurmës papilare përfshijnë rezolucionin e imazhit, zonës së gjurmës dhe qartësia e modelit të vijave papilare[33].

Në aplikimet biometrike dhe mjeko-ligjore, një rezolucion prej 500 ppi(pixel per inch) është i domosdoshëm për një përpunim dhe krahasim të suksesshëm të imazheve dhe karakteristikave. Në këtë rezolucion distanca ndërmjet vijave papilare fqinje është afërsisht 9 pixela. Aktualisht, agjencitë e zbatimit të ligjit kanë filluar të skanojnë gjurmët papilare me 1 000 ppi në mënyrë që të regjistrojnë edhe karakteristikat e nivelit 3. Në aplikimet civile përdoren shpesh sensorët e gjurmëve papilare me rezolucion më të ulët se 500 ppi për të ulur koston e sensorit[74].

Zona e gjurmës së regjistruar të një imazhi gjurme papilare është gjithashtu një faktor i rëndësishëm që ndikon në cilësinë e imazhit. Qartësia e modelit të vijës papilare është një faktor tjetër i rëndësishëm i cilësisë. Lëkura e gishtit dhe sensori kanë një impakt të madh në qartësinë e vijës papilare.

Në një gjurmë papilare me cilësi të mirë, vijat papilare rrjedhin vazhdimisht dhe vijat fqinje janë të ndara qartësisht. Kur gishti është i lagësht, vijat papilare fqinje mund të bashkohen; kur është i thatë, vijat papilare mund të kenë shumë të çara; dhe cilësia objektive e disa gishtave është e dobët. Në figurën 4-19 tregohen disa gjurmë papilare me cilësi të ulët.

Algoritmet e ekstraktimit të karakteristikave mbështeten në cilësinë e imazhit për të qenë të aftë për të ekstraktuar në mënyrë të besueshme karakteristikat e minutiae-ve. Etapa e parapërpunimit përmirëson imazhet me cilësi të ulët që trajtohen nga algoritmet e ekstraktimit të karakteristikave, në imazhe gjurmësh papilare me cilësi të mirë.

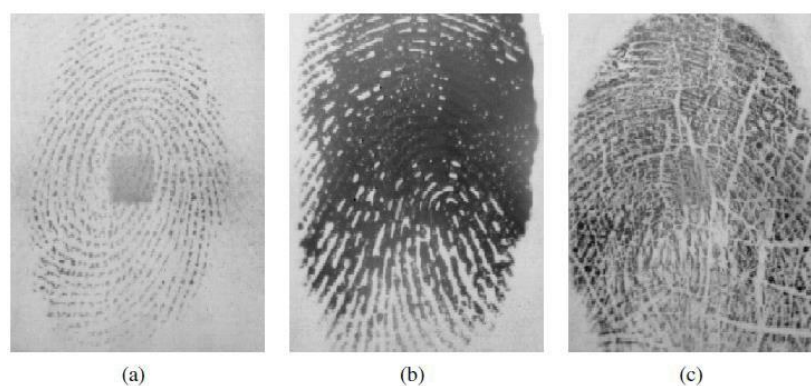


Figura 4-19. Shembuj të imazheve të gjurmëve papilare me cilësi të ulët

(a) gisht i thatë, (b) gisht i lagësht, dhe (c) gisht me shumë rridha

4.2.3 Ekstraktimi i karakteristikave

Pasi imazhi i gjurmës papilare është parapërpunuar, realizohet ekstraktimi i karakteristikave të gjurmës papilare. Shumica e sistemeve të identifikimit biometrik me gjurmë papilare janë të bazuara në krahasimin e minutiae-ve, kështu që ekstraktimi i minutiae-ve të besueshme është një domosdoshmëri. Imazhet e gjurmëve papilare të parapërpunuara konvertohen në një imazh binar, i cili më tej qartësohet duke përdorur morfologjinë. Etapa e qartësimit zvogëlon trashësinë e vijës papilare në një pixel, duke lejuar dedektimin e drejtpërdrejtë të minutiae-ve. Në figurat 4-20 dhe 4-21 tregohet procesi i ekstraktimit të karakteristikave [33][74].



Figura 4-20. Procesi i qartësimit të imazhit dhe ekstraktimit të karakteristikave të gjurmës papilare

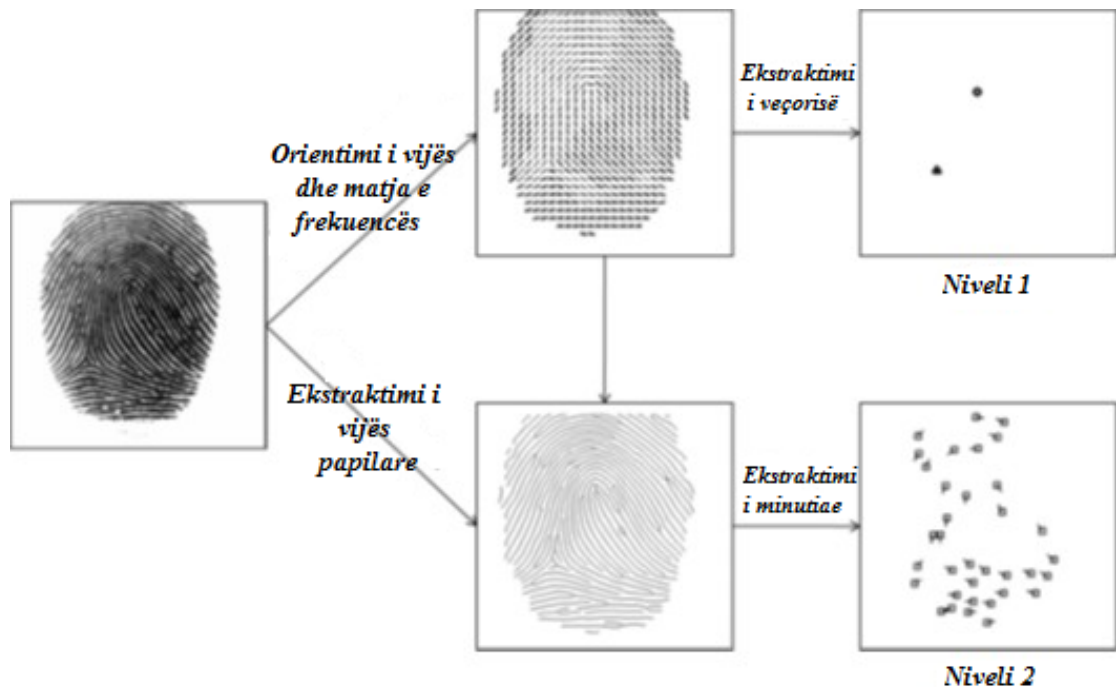


Figura 4-21 Skema e ekstraktimit të karakteristikave të nivelit 1 dhe nivelit 2

4.2.4 Krahاسimi i gjurmës papilare

Në fazën e krahasimit, karakteristikat e ekstraktuara nga gjurma papilare krahasohen përkundëjt atyre në një template të pararegjistruar, e cila paraqet një përdorues të vetëm (i gjetur nga baza e të dhënave të sistemit bazuar në identitetin e deklaruar).

Rezultati i një procedure të tillë është ose një shkallë ngjashmërie, e quajtur ndryshe dhe rezultati i krahasimit ose një vendim pranimi apo refuzimi. Në ditët e sotme ekzistojnë teknika krahasimi të gjurmëve papilare që krahasojnë direkt imazhet gri (ose nën-imazh) duke përdorur metodat me bazë-korrelacioni, në të cilën template i gjurmës papilare përkon me imazhin gri.

Megjithatë, shumica e algoritmeve të krahasimit të gjurmëve papilare përdorin karakteristika që ekstrahohen nga imazhi gri[33]. Përafrimet me bazë-minutiae janë metodat më të njohura dhe të përdorura gjerësisht për krahasimin e gjurmëve papilare, duke qenë se ato janë analoge me mënyrën sesi ekspertët mjeko-ligjor krahasojnë gjurmët papilare[74]. Një gjurmë papilare modelohet si një grup minutiae, të cilat paraqiten zakonisht nga koordinatat e saj hapësinore dhe këndi ndërmjet tangentes së vijës papilare në pozicionin e minutiae dhe akset horizontale dhe vertikale.

Për të krahasuar dy gjurmë papilare, grupet e minutiae-ve, së pari rreshtohen, duke kërkuar përlllogaritjen e zhvendosjes dhe rrotullimit[74]. Në figurën 4-22 tregohet një krahasim i suksesshëm, ndërsa në figurën 4-23 paraqitet një krahasim i pasuksesshëm.

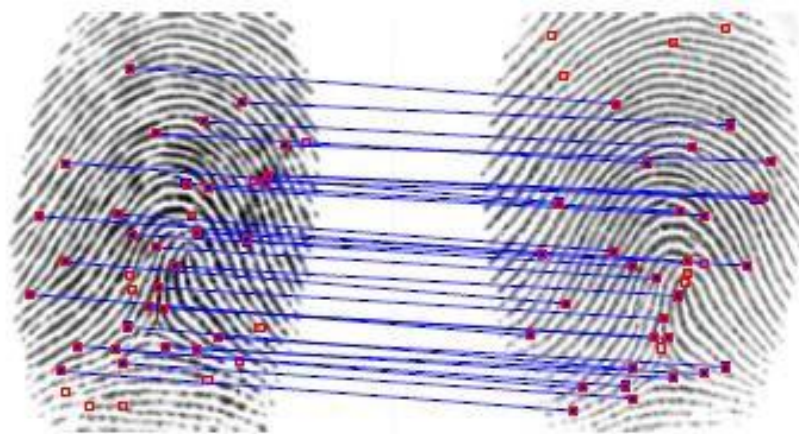


Figura 4-22. Krahasim i suksesshëm me një rezultat = 614

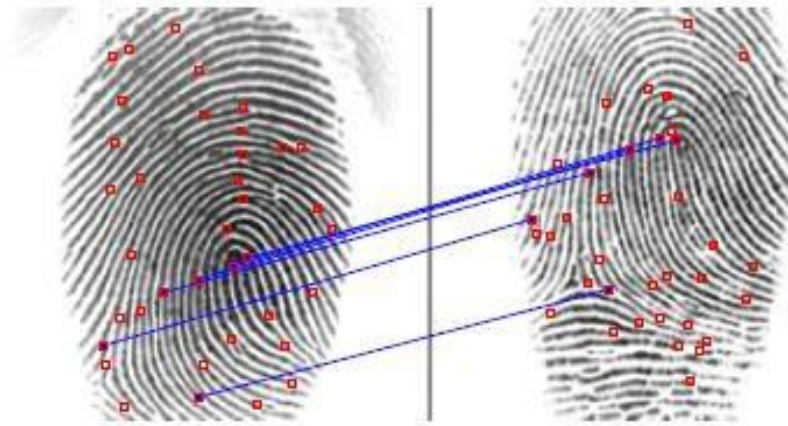


Figura 4-23. Krahasim i pasuksesshëm me një rezultat = 7

4.3 Problematika që kërkojnë zgjidhje

Një nga çështjet e hapura në identifikimin biometrik është qëndrueshmëria ndaj degradimit të cilësisë së imazhit[74]. Performanca e një sistemi identifikimi biometrik me gjurmë papilare ndikohet shumë nga cilësia e imazhit të regjistruar të gjurmës papilare.

Faktorë të ndryshëm përcaktojnë cilësinë e një imazhi gjurme papilare janë kushtet e lëkurës (p.sh thatësira, lagështira, papastërtia, të çara dhe blana), kushtet e sensorit (p.sh papastërtia, zhurma, madhësia), bashkëpunimi i përdoruesit etj. Disa prej këtyre faktorëve nuk mund të mënjanohen dhe disa ndryshojnë më kalimin e kohës. Imazhet me cilësi të dobët rezultojnë në karakteristika të rreme dhe të humbura, të cilat degradojnë performancën e sistemit në tërësi.

Për këtë arsye është shumë e rëndësishme për një sistem identifikimi biometrik me gjurmë papilare të vlerësojë cilësinë dhe vlefshmërinë e imazheve të regjistruara të gjurmëve papilare. Imazhet e degraduara mund të refuzohen ose të përmirësohen, në disa prej etapave të sistemit të identifikimit bazuar në cilësinë e matur[33] [74].

KAPITULLI 5

Përmirësimi i imazhit të gjurmës papilare

5.1 Hyrje

Krahasimi automatik i gjurmëve papilare varet në karakteristikat e vijës papilare lokale dhe relacionet e tyre për të realizuar një identifikim dixhital të individit. Një proces kritik në krahasimin e gjurmëve papilare është eksraktimi në mënyrë automatike dhe të besueshme i minutiae-ve nga imazhet e regjistruara në hyrje të gjurmëve papilare. Performanca e teknikës së përdorur për ekstraktin e minutiae-ve mbështetet tërësisht në cilësinë e imazheve të marra të gjurmëve biometrike. Në një imazh të përsosur të gjurmës papilare, vijat dhe brazdat papilare alternohen dhe rrjedhin në një drejtim lokal konstant dhe minutiae-t janë anomali të vijave papilare, p.sh, fundet dhe degëzimet e vijave papilare. Në situata të tilla, vijat papilare mund të dedektohen lehtësisht dhe minutiae-t mund të lokalizohen saktësisht në vijat e qartësuara[33][97]. Në figurën 5-1 ilustron një skanim imazhi gjurmë papilare me cilësi të mirë.

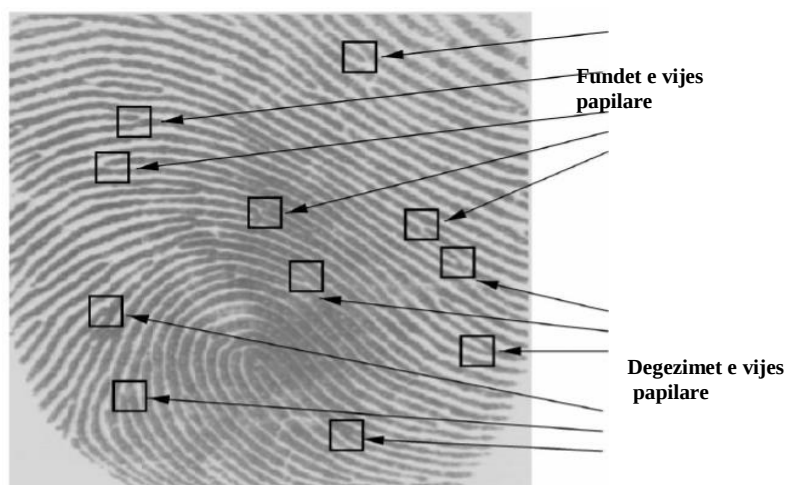


Figura 5-1. Skanim me cilësi të mirë të gjurmës papilare

Në praktikë, për shkak të ndryshimeve në konfigurimin e vijave papilare, kushtet e lëkurës (formacione të devijuara të vijave papilare të epidermës në gjurmët papilare, shenjat pas lindjes, shenjat nga profesioni), pajisjet e regjistrimit dhe sjellja jo-bashkëpunuese e individëve etj, një përqindje e konsiderueshme e gjurmëve papilare të regjistruara, nga eksperiencia afërsisht 10 % është me cilësi të ulët.

Strukturat e vijave papilare në imazhet e gjurmëve me cilësi të ulët nuk janë gjithmonë të mirë-përcaktuara, prandaj ato nuk mund të dedektohen. Në mënyrë që të garantojmë që teknika e përdorur për ekstraktimin e minutiae-ve nga imazhi i regjistruar i gjurmëve papilare të jetë robuste është i domosdoshëm përmirësimi i cilësisë së imazhit të regjistruar, qartësisë së strukturave të vijave papilare [33][98].

Përmirësimi i imazhit të gjurmës biometrike mund të realizohet ose në imazhet binare të vijave papilare ose në imazhet gri. Binarizimi përpara përmirësimit do të gjenerojë një numër më të madh minutiae të rreme dhe do humbasë një pjesë të informacionit origjinal, të vlefshëm të gjurmës papilare. Në të njëjtën kohë do të sjellë më shumë vështirësi për procedurën e mëvonshme të përmirësimit, duke kufizuar procesin e përmirësimit.

Teknika të ndryshme [96][97][99][102][108][109][112][119][120] për përmirësimin e imazheve gri të gjurmëve papilare janë propozuar duke supozuar që frekuenca dhe orientimi lokal i vijës papilare mund të maten me saktësi. Disa nga arsyet kryesore pse është i nevojshëm përmirësimi i imazhit të gjurmës papilare është eliminimi i zhurmës në imazhet e gjurmëve papilare, ndriçimi i vijave dhe brazdave papilare paralele dhe mbrojtja e konfigurimit të tyre origjinal, e ilustruar në figurën 5-2.



Figura 5-2. Procesi i përmirësimit të imazhit të gjurmës papilare

5.2 Teknikat më të përdorura të përmirësimit të imazhit

Në ditët e sotme nuk ka një teori të përgjithshme për përmirësimin e imazhit. Kur një imazh përpunohet për interpretime vizuale, eksperti i fushës është ai që gjykon se sa efëiente është përdorimi i një teknike të caktuar përmirësimi. Shumica e teknikave të kontrollit të cilësisë së imazhit janë përdorur si kritere, të cilat përcaktojnë refuzimin e imazhit ose një vlerësim të performancës së metodës së përdorur për përmirësimin e imazhit.

Ndër vite, studime të ndryshme janë realizuar me qëllim eliminimin e zhurmës dhe rritjes së kontrastit ndërmjet vijave dhe brazdave papilare në imazhet gri të gjurmëve papilare. Ndër teknikat më të njohura dhe të përdorura janë teknikat e përmirësimit në fushën e hapësirës dhe të frekuencës [106] [108].

5.2.1 Përmirësimi në rrafshin e hapësirës

Rrafshi i hapësirës i referohet planit të vetë imazhit and metodat e përpunimit të imazhit në këtë kategori punojnë me principin e përpunimit direkt të pixel-ave në një imazh. Fusha e hapësirës mund të paraqitet me formulën (5.1)[106] [108]:

$$g(x,y) = T[f(x,y)] \quad (5.1)$$

ku $f(x,y)$ është imazhi në hyrje, $g(x,y)$ është imazhi në dalje dhe T është një operator i përcaktuar një zonë të afërt të pikës (x,y) .

5.2.2 Përmirësimi në rrafshin e frekuencës

Rrafshi i frekuencës i referohet parimit të modifikimit të transformimit Furie të një imazhi dhe më pas përllogaritja e transformimit invers të tillë si Transformimi Diskret Furie [20] për të marrë imazhin në hyrje. Në këtë mënyrë kur jepet një imazh numerik $f(x,y)$, i madhësisë $M \times N$, ekuacioni bazë i filtrimit ka formën (5.2) [30][19] [28]:

$$g(x,y) = \tau^{-1}[H(u,v)F(u,v)] \quad (5.2)$$

ku τ^{-1} është Transformimi Diskret Invers Furie, $F(u,v)$ është Transformimi Diskret Furie i imazhit në hyrje $f(x,y)$, $H(u,v)$ është funksioni filtër dhe $g(x,y)$ është imazhi i filtruar në dalje.

5.3 Teknika përmirësimi të imazhit të gjurmës papilare

5.3.1 Teknika e përmirësimit sipas L.Hong

Teknika e përmirësimit të parametrave të gjurmës papilare është një metodë e përdorur nga L.Hong [16], e cila është bazuar në konvolucionin e imazhit me filtrat e Gabor [111] e taruar për frekuencën dhe orientimin e vijës papilare. Etapat kryesore të skemës së përmirësimit të kësaj teknike përfshijnë normalizimin, matjen e orientimit dhe frekuencës së vijës papilare, si dhe filtrimin, ashtu siç ilustruhet në diagramën e algoritmit të përmirësimit të përdorur në figurën 5-3.

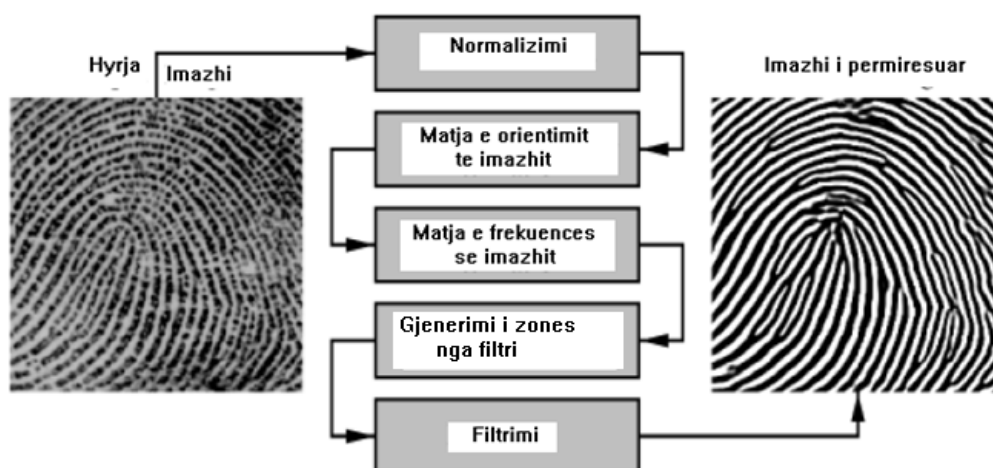


Figura 5-3. Diagrama e L.Hong për skemën e përmirësimit të gjurmës papilare

5.3.1.1 Normalizimi

Do të themi që një imazh gjurme papilare në hyrje, është normalizuar kur ka një mesatare dhe variancë të paracaktuar. Normalizimi përdoret për të standartizuar vlerat e intensitetit në një imazh duke përshtatur vlerat e serisë së nivelit gri në mënyrë që të shtrihet brenda një intervali të dëshiruar vlerash. Le të jetë $I(i, j)$ vlera e nivelit gri në $\text{pixel}(i, j)$, dhe $G(i, j)$ vlera e normalizuar e nivelit gri në $\text{pixel}(i, j)$. Imazhi i normalizuar përcaktohet nga formula (5.3):

$$G(i, j) = \begin{cases} M_0 + \sqrt{\frac{\text{VAR}_0(I(i, j) - M)^2}{\text{VAR}}} & \text{nëse } I(i, j) > M \\ M_0 - \sqrt{\frac{\text{VAR}_0(I(i, j) - M)^2}{\text{VAR}}} & \text{përndryshe} \end{cases} \quad (5.3)$$

ku M dhe VAR janë mesatarja dhe varianca e matur e $I(i, j)$ dhe M_0 dhe VAR_0 janë respektivisht vlerat e mesatares dhe variancës së dëshiruar. Normalizimi nuk ndryshon strukturën e vijave papilare në një gjurmë papilare, por realizon standartizimin e niveleve dinamike të ndryshimit të vlerave të nivelit gri, e cila lehtëson përpunimin në etapat e tjera të përmirësimit të imazhit[97], ashtu siç ilustruhet në figurën 5-4.

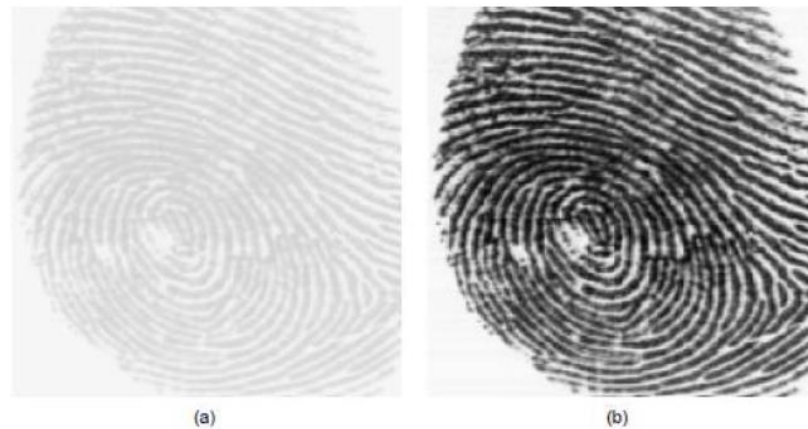


Figura 5-4. Rezultati i normalizimit (a) imazhi i hyrje; (b) imazhi i normalizuar

(M0=100, VAR0=100)

5.3.1.2 Matja e orientimit të imazhit

Orientimi i imazhit siç ilustrohet në figurën 5-5 paraqet një karakteristikë të brendshme të imazheve të gjurmëve papilare dhe përcakton koordinatat e pandryshueshme për vijat dhe brazdat papilare në një zonë të afërt lokale.

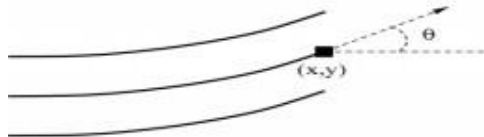


Figura 5-5. Vlerësimi i orientimit në pixel(x, y)

Duke e parë një imazh si një strukturë të orientuar, është zhvilluar një teknikë matje [97] për orientimin me metodën e mesatares së katrorëve më të vegjël. Kur jepet një imazh i normalizuar, G, hapat kryesorë të algoritmit të përmirësimit janë si më poshtë:

1. Ndaj G në blloqe të madhësisë $W \times W$ (16x16);
2. Llogarit gradientët $\delta_x(i,j)$ dhe $\delta_y(i,j)$ në çdo pixel(i,j);
3. Mat orientimin lokal të secilit bllok të qendëruar në pixel(i,j) duke përdorur ekuacionet (5.4) (5.5) (5.6):

$$\mathcal{V}_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u, v)\partial_x(u, v) \quad (5.4)$$

$$\mathcal{V}_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \left(\partial_x^2(u, v)\partial_y^2(u, v) \right) \quad (5.5)$$

$$\theta(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{\mathcal{V}_y(i, j)}{\mathcal{V}_x(i, j)} \right) \quad (5.6)$$

Ku $\theta(i, j)$ është matja me katror më të vegjël e orientimit lokal të vijës papilare në bllokun e qendëruar në pixel (i, j) . Matematikisht, ajo paraqet drejtimin që është ortogonal me drejtimin dominant të spektrit Furie të dritares $w \times w$. Për shkak të pranisë së zhurmës, strukturat e korruptuara të vijave dhe brazdave papilare, minutiae, etj në imazhin në hyrje, si dhe orientimi lokal i matur i vijës lokale mund të mos jenë gjithmonë të sakta.

Duke qenë se orientimi i vijave lokale ndryshon ngadalë në një zonë të afërt lokale, ku nuk shfaqen pika të dukshme, një filtër i brezit të ulët mund të përdoret për të ndryshuar orientimin e pasaktë të vijave lokale[97].

5.3.1.3 Matja e frekuencës së imazhit të vijës papilare

Nivelet gri përgjatë vijave dhe brazdave papilare mund të modelohen si një valë në formë sinusoidale sipas drejtimit normal të orientimit lokal të vijës, e ilustruar dhe në figurën 5-6.

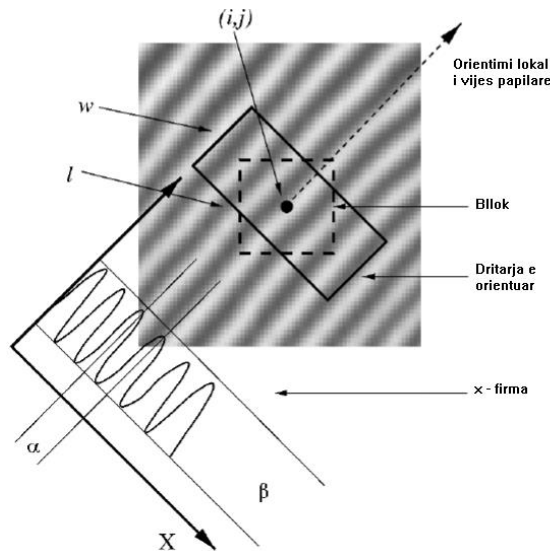


Figura 5-6. Metoda e dritares së orientuar për të matur frekuencën e vijës papilare

Prandaj frekuenca e vijës papilare lokale është një tjetër karakteristikë e brendshme e imazhit të gjurmës papilare. Le të jetë G imazhi i normalizuar dhe $O(i, j)$ orientimi i imazhit, atëherë hapat e përfshirë në matjen e frekuencës së vijës papilare

lokale janë si më poshtë[97] :

1. Ndaj G në blloqe të madhësisë $w \times w$ (16x16);
2. Për çdo bllok të qendëruar në pixel(i, j), llogarit një dritare të orientuar të madhësisë $l \times w$ (32x16), që përcaktohet në sistemin koordinativ të vijës papilare;
3. Për çdo bllok të qendëruar në pixel(i, j), llogarit x-signature, $X[0], X[1], \dots, X[l-1]$ të vijës dhe brazdës brenda dritares së orientuar, ku:

$$X[k] = \frac{1}{w} \sum_{d=0}^{w-1} G(u, v), \quad k = 0, 1, \dots, l-1 \quad (5.7)$$

$$u = i + \left(d - \frac{w}{2}\right) \cos O(i, j) + \left(k - \frac{l}{2}\right) \sin O(i, j) \quad (5.8)$$

$$v = j + \left(d - \frac{w}{2}\right) \sin O(i, j) + \left(\frac{l}{2} - k\right) \cos O(i, j) \quad (5.9)$$

Nëse nuk shfaqet asnjë minutiae apo pikë e dukshme në dritaren e orientuar, x-signatures formojnë një valë diskrete në formë sinusoidale, e cila ka frekuencë të njëjtë me vijat dhe brazdat papilare në dritaren e orientuar. Prandaj, frekuenca e vijave dhe brazdave papilare mund të vlerësohet nga x-signature.

Le të jetë $\tau(i, j)$, numri mesatar i pixel-ave ndërmjet 2 majave të njëpasnjëshme të dedektuar nga x-signature, atëherë frekuenca, $\Omega(i, j)$, llogaritet nga formula:

$$\Omega(i, j) = \tau^{-1}(i, j) \quad (5.10)$$

Atëherë nëse nuk dedektohen maja të njëpasnjëshme nga x-signature, frekuencës në fjalë i caktohet një vlerë -1, për ta dalluar atë nga vlerat e vlefshme të frekuencës.

5.3.1.4 Gjenerimi i maskës zonale

Një pixel(ose një bllok) në një imazh gjurme papilare në hyrje mund të jetë në një zonë të rikuperueshme ose në një zonë të parikuperueshme. Klasifikimi i pixel-ave në kategori të rikuperueshme dhe të parikuperueshme mund të realizohet nga vlerësimi i formës së valës të formuar nga vijat dhe brazdat papilare. Në këtë teknikë të përdorur, tre parametra përdoren për të karakterizuar valën në formë sinusoidale: amplituda(α), frekuenca(β) dhe varianca(γ).

Le të jetë $X[1], X[2], \dots, X[l]$, x-signature e një blloku të qendëruar në (i, j) . Te tre parametrat që i korrespondojnë pixel(blok)(i,j) llogariten si më poshtë [13]:

1. α = lartësia mesatare e majave-thellësia mesatare e brazdave;
2. ku $\beta = \tau^{-1}(i, j)$, ku $\tau(i, j)$ është numri mesatar i pixel-ave ndërmjet dy majave të njëpasnjëshme;
3. $\gamma = \frac{1}{l} \sum_{i=0}^l \left(X[i] - \left(\frac{1}{l} \sum_{i=0}^l X[i] \right) \right)^2$

5.3.1.5 Filtrimi

Strukturat e vijave dhe brazdave papilare paralele me frekuencë dhe orientim të mirë-përcaktuara në një imazh gjurme papilare japin informacion të rëndësishëm që ndihmon për zhdukjen e zhurmës së padëshiruar. Valët me formë sinusoidale të vijave dhe brazdave papilare ndryshojnë ngadalë në një orientim lokal konstant.

Kështu që një filtër brezlejues i cili është taruar në orientimin dhe frekuencën korresponduese mund të reduktojë me efikasë zhurmën e padëshiruar dhe të ruajë strukturat e vërteta të vijës dhe brazdës papilare.

Filtrat e Gabor-it, në të njëjtën kohë, kanë parametra zgjedhës për orientimin dhe frekuencën. Prandaj përdorimi i filtrave të Gabor si filtra brezlejues janë zgjidhja e duhur për të eliminuar zhurmën dhe për të ruajtur strukturat e vijës apo brazdës papilare[97] [106] [111].

Forma e përgjithshme e filtrit Gabor jepet në formulën (5.11):

$$h(x, y; \phi, f) = \exp \left\{ -\frac{1}{2} \left[\frac{x_\phi^2}{\delta_x^2} + \frac{y_\phi^2}{\delta_y^2} \right] \right\} \cos(2\pi f x_\phi) \quad (5.11)$$

ku ϕ është orientimi i filtrit të Gabor, f është frekuenca e një vale sinusoidale në plandhe δ_x dhe δ_y janë konstantet e hapësirës së mbështjellës Gaussianë respektivisht përgjatë akseve x dhe y . Funkcioni transferues i modulimit (MTF-Modulation Transfer Function) të filtrit të Gabor mund të paraqitet në (5.12)[97] [111]:

$$H(u, v; \phi, f) =$$

$$2\pi \delta_x \delta_y \exp \left\{ -\frac{1}{2} \left[\frac{(u_\phi - u_0)^2}{\delta_u^2} + \frac{(v_\phi - v_0)^2}{\delta_v^2} \right] \right\} +$$

$$2\pi \delta_x \delta_y \exp \left\{ -\frac{1}{2} \left[\frac{(u_\phi - u_0)^2}{\delta_u^2} + \frac{(v_\phi - v_0)^2}{\delta_v^2} \right] \right\} \quad (5.12)$$

$$u_\phi = u \cos \phi + v \sin \phi \quad (5.13)$$

$$v_{\Phi} = -u \cos \Phi + v \sin \Phi \quad (5.14)$$

$$u_0 = \frac{2\pi \cos \Phi}{f} \quad (5.15)$$

Ku $\delta_u = \left(\frac{1}{2\pi}\right) \delta_x$ dhe $\delta_v = \left(\frac{1}{2\pi}\right) \delta_y$.

Në mënyrë që të zbatojnë filtrin e Gabor në një imazh, parametrat që duhen përcaktuar janë:

1. f , frekuenca e valës sinusoidale të planit;
2. θ , orientimi i filtrit,;
3. δ_x dhe δ_y , devijimet standarte të mbështjelljes Gaussianë.

5.3.1.6 Zbatimi

Në këtë algoritëm, f është përcaktuar nga hapi i matjes së frekuencës së vijës papilare, θ është përcaktuar nga hapi i matjes së orientimit të vijës papilare, dhe vlerat e δ_x dhe δ_y janë përafruar bazuar në të dhënat empirike. Le të jetë G imazhi i normalizuar, O imazhi i orientuar, F të jetë imazhi i frekuencës, R të jetë maska e rikuperueshme, dhe w_g të jetë madhësia e filtrit të Gaborit. Imazhi i përmirësuar E merret nga (5.16) [97]:

$$E(i, j) = \begin{cases} 255 & \text{nëse } R(i, j) = 0 \\ \sum_{u=-w_g/2}^{w_g/2} \sum_{v=-w_g/2}^{w_g/2} h(u, v; O(i, j), F(i, j)) G(i - u, j - v) & \text{përndryshe} \end{cases} \quad (5.16)$$

5.3.1.7 Rezultatet e matura

Në figurën 5-7 jepet imazhi origjinal i një gjurme papilare i skanuar me sensor. Në mënyrë vizuale mund të dallojmë se imazhi është shumë i mjegullt dhe karakteristikat kryesore të kërkuara nga sistemi i identifikimit me gjurmë papilare nuk mund të ekstrahohen nga ky imazh.



Figura 5-7. Gjurma papilare originale e skanuar

Në figurën 5-8 paraqitet imazhi që rezulton në dalje pas përmirësimit me këtë algoritëm. Karakteristikat e vijës papilare në këtë imazh të përmirësuar janë më të dallueshme.



Figura 5-8. Imazhi i përmirësuar i gjurmës papilare

5.3.2 Teknika e përmirësimit sipas S.Chikkerur nëpërmjet analizës STFT

Një teknikë tjetër përmirësimi është ajo e propozuar nga Chikkerur[99], e cila bazohet në metodën e analizimit të imazhit nëpërmjet Transformimit të Shpejtë Furie (STFT), e cila është një teknikë e mirënjohur në përpunimin e sinjalit, për analizimin e sinjaleve të paqëndrueshëm.

Në këtë zbatim është shtrirë përdorimi i tij në imazhet e gjurmëve papilare dy

dimensionale. Kjo teknikë mat në të njëjtën kohë të gjithë karakteristikat e brendshme të gjurmës papilare të tilla si imazhet dy-dimensionale të gjurmëve papilare. Në të njëjtën kohë maten parametrat kryesore të imazhit si maska zonale së zgjedhur, orientimi dhe frekuenca lokale e vijës papilare[99].

Kjo teknikë është bazuar në filtrimin e kushtëzuar në rrafshin Furie. Imazhi i gjurmës papilare mund të supozohet si një sistem i strukturave të orientuara me karakteristika të paqëndrueshme. Prandaj analiza tradicionale Furie nuk është e përshtatshme për të analizuar imazhin e plotë, pasi duhet të përzgjidhen karakteristikat e imazhit, në kohë dhe në frekuencë. Analiza tradicionale kohë-frekuencë e imazhit një dimensional duhet të shtrihet në sinjalet e imazhit dy dimensional për të kryer analizën e shkurtër (kohë/hapësirë)-frekuencë[99].

Kur analizojmë një sinjal një-dimensional të paqëndrueshëm supozojmë që është përafërsisht i qëndrueshëm, në intervalin e kohës të një dritare të përkohshme $w(t)$. Transformimi i shpejtë Furie i $x(t)$ paraqitet tani nga vlerat e frekuencës në kohë $X(\tau, \omega)$ dhe jepet prej (5.17):

$$X(\tau, \omega) = \int_{-\infty}^{\infty} x(T) W^*(t - \tau) e^{-j\omega t} dt \quad (5.17)$$

Në rastin e sinjaleve dy-dimensionale të tillë si imazhi i një gjurme papilare, vlerat hapësirë-frekuencë jepen prej (5.18):

$$X(\tau_1, \tau_2, \omega_1, \omega_2) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} I(x, y) W^*(x - \tau_1, y - \tau_2) e^{-j(\omega_1 x + \omega_2 y)} dx dy \quad (5.18)$$

Ku τ_1 dhe τ_2 paraqesin pozicionin në hapësirë të dritares dy-dimensionale, $W(x, y)$ dhe ω_1, ω_2 paraqesin parametrat hapësinorë të frekuencës. Në figurën 5-9 ilustron sesi parametrizohet dritarja spektrale. Në çdo pozicion të dritares, ajo mbivendos pixel-at e OVRLP me pozicionin e mëparshëm.

Kjo siguron vazhdueshmërinë e vijës papilare dhe eliminon efektet 'bllok' të ngjashme me veprimet e tjera të përpunimit të bllokut të imazhit. Çdo analizë e tillë jep një vlerë të vetme të orientimit dominant dhe frekuencën në zonën përreth (τ_1, τ_2) . Megjithatë, në ndryshim nga transformimi i rregullt Furie, rezultati i transformimit të shpejtë Furie varet nga zgjedhja e dritares $w(t)$.

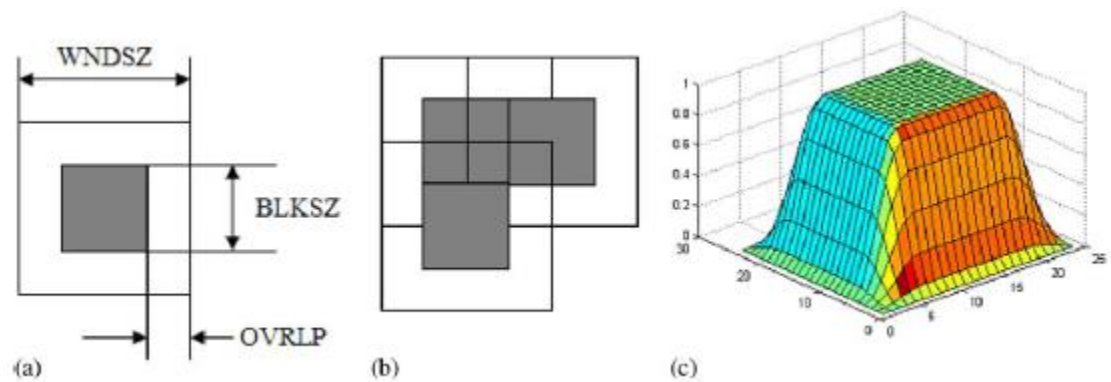


Figura 5-9. (a) Parametrat e dritares së mbivendosjes që përdoret në analizën STFT, (b) ilustrim i mënyrës se si dritaret e analizës lëvizin gjatë saj, dhe (c) dritarja spektrale e përdorur gjatë analizës STFT

Etapat kryesore të kësaj teknike janë përlllogaritja e imazheve të orientimit dhe frekuencës së vijës papilare, përcaktimi i një maske zonale duke llogaritur një imazh energjie për të dalluar zonat e gjurmëve papilare nga sfondi, llogaritja e imazhit të koherencës për të përshtatur gjerësinë e brezit këndor të filtrit drejtues dhe kryerja e përmirësimit më STFT për të gjeneruar imazhin përfundimtar të përmirësuar.

Në figurën 5-10 jepet diagrama e kësaj teknike [120].

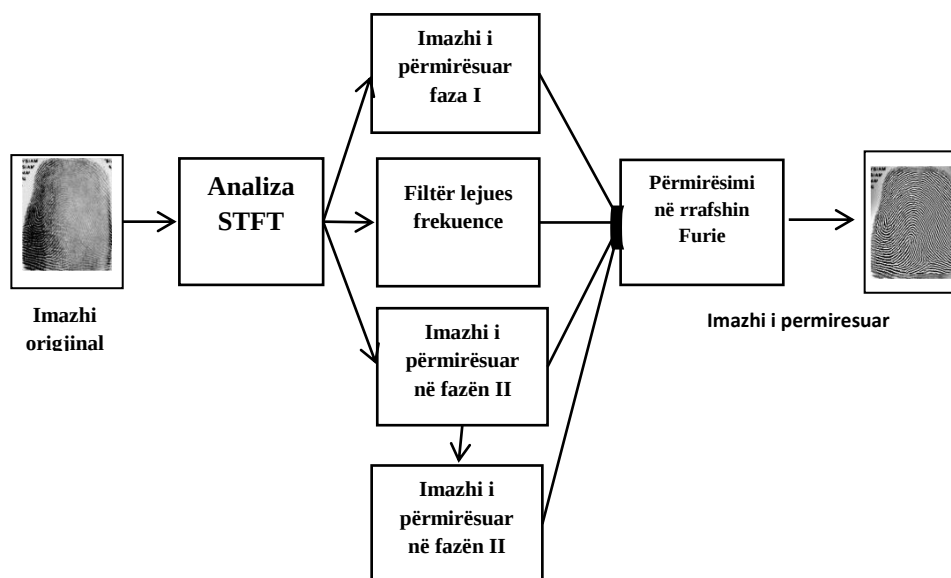


Figura 5.10 Diagrama e skemës së përmirësimit me analizë STFT

5.3.2.1 Imazhi sipas orientimit të vijës papilare

Për të llogaritur orientimin e vijës papilare të imazhit, orientimi θ supozohet si

një variabël i rastit që ka funksion densiteti të probabilitetit $p(\theta)$. Vlera e pritshme e orientimit $E(\theta)$ mund të përftohet nga kryerja e njëmesatarizimi të vektorit sipas (5.19) [99].

$$E\{\theta\} = \frac{1}{2} \tan^{-1} \left\{ \frac{\int_{\theta} p(\theta) \sin(2\theta) d\theta}{\int_{\theta} p(\theta) \cos(2\theta) d\theta} \right\} \quad (5.19)$$

Termat $\sin(2\theta)$ dhe $\cos(2\theta)$ janë përdorur për të zgjidhur orientimin ndërmjet dy drejtimeve, ndërmjet orientimeve $\pm 180^\circ$. Megjithatë, nëse ekziston një rrudhë në gjurmët papilare qëkërkon disa dritare analize, matja e orientimit mund të jetë përsëri e gabuar.

Matja do të jetë përsëri e pasaktë, kur dritarja përbëhet plotësisht nga zona të parikuperueshme me struktura vijë papilare të dobëta ose kontrast të dobët të vijës papilare. Në raste të tilla, orientimi i vijës papilare mund të vlerësohet duke konsideruar orientimin e fqinjit më të afërt. Imazhi i orientuar që rezulton $O(x,y)$ lëmohet më tej duke përdorur mesatarizim të vektorit. Duke konsideruar $W(x,y)$ si një kernel lëmues Gaussian, imazhi i lëmuar $O'(x,y)$ merret nga (5.20) [17]:

$$O'(x,y) = \frac{1}{2} \tan^{-1} \left\{ \frac{\sin(2O(x,y)) * W(x,y)}{\cos(2O(x,y)) * W(x,y)} \right\} \quad (5.20)$$

5.3.2.2 Imazhi sipas frekuencës së vijës papilare

Frekuenca mesatare matet në të njëjtën mënyrë si orientimi lokal. Supozojmë që frekuenca e vijës papilare r merret si vlerë e rastit me funksion densiteti të probabilitetit $p(r)$ [17].

Vlera e pritshme e frekuencës së vijës papilare jepet nëpërmjet:

$$E\{r\} = \int p(r) r dr \quad (5.21)$$

Harta e frekuencës që merret është e lëmuar nga procesi i difuzionit izotropik. Lëmime të thjeshta nuk mund të zbatohen duke qenë se frekuenca e vijës papilare nuk është përcaktuar në zonat e sfondit. Konsideroni kernelin lëmues Gaussian $W(x,y)$, variablin tregues $I(u,v)$ që garantojnë që të merren në konsideratë vetëm frekuencat e sakta të vijës papilare dhe imazhi sipas frekuencës $F(u,v)$, i lëmuar të merret nga ekuacioni (5.22) [17]:

$$F'(x, y) = \frac{\sum_{u=x-1}^{x+1} \sum_{v=y-1}^{y+1} F(u, v) W(u, v) I(u, v)}{\sum_{v=y-1}^{y+1} W(u, v) I(u, v)} \quad (5.22)$$

5.3.2.3 Maska zonale

Imazhi i gjurmës papilare mund të segmentohet lehtësisht bazuar në përfundimin se modeli i sipërfaqes së valës, nuk i merr në konsideratë zonat, ku nuk ekzistojnë vijat papilare. Në zonat e sfondit dhe të zhurmës ekziston vetëm një përmbajtje e vogël energjie në spektrin Furie.

Ne mund të përcaktojmë një imazh energjitik $E(x, y)$, ku çdo vlerë tregon përmbajtjen e energjisë të një blloku korrespondues. Zona e gjurmës papilare mund të diferencohet nga sfondi nga pragu i imazhit energjitik. Për një imazh të dhënë frekuence F , me orientim të vijës papilare θ dhe me frekuencë të vijës papilare r , imazhi i energjisë E mund të gjenerohet me formulën (5.23) [99]:

$$E(x, y) = \log \left\{ \int_{\theta} \int_r |F(r, \theta)|^2 \right\} \quad (5.23)$$

Përmirësimi i cilësisë së imazhit është më i vështirë në mënyrë specifike, në zona me lakim të madh, afër qendrave dhe deltave të gjurmëve papilare që kanë me shumë se një drejtim dominant. Në mënyrë të veçantë gjerësia e ngushtë e brezit këndor shkakton karakteristika të rreme dhe shkëputje të vijës papilare në imazhin e rindërtuar.

Një matje koherente siguron dedektimin e saktë të pikave të dukshme [99]. Nëse konsiderojmë se $\theta(x, y)$ është orientimi i bllokut dhe madhësia e tij është $W \times W$, imazhi i matur i koherencës C merret nga ekuacioni (5.24):

$$C(x_0, y_0) = \frac{\sum_{i=0}^W |\cos(\theta(x_0, y_0) - \theta(x_i, y_i))|}{W \times W} \quad (5.24)$$

Koherenca është e lartë kur orientimi i bllokut qëndror $\theta(x_0, y_0)$ është i ngjashëm me secilin prej fqinjëve të tij $\theta(x_i, y_i)$. Në imazhin e gjurmës papilare, koherenca pritet të jetë shumë pranë zonave me lakime të mëdha. Kështu që matja e koherencës mund të përdoret për të përshtatur gjerësinë e brezit këndor të filtrit drejtues [99].

5.3.2.4 Përmirësimi i imazhit

Imazhi ndahet në dritare të mbivendosura, brenda të cilave imazhi është i qëndrueshëm dhe mund të modelohet afërsisht si sipërfaqe vale. Spektri Furie i kësaj zone të vogël analizohet dhe vlerësohen vlerat propabilistike të frekuencës dhe orientimit të vijës papilare. Në çdo dritare aplikohet filtri i taruar për frekuencën

radiale dhe sipas drejtimit të vijës papilare dominante. Filtri është i ndashëm në kënd dhe frekuencë dhe jepet me anë të ekuacioneve:

$$H(\rho, \theta) = H_\rho(\rho)H_\theta(\theta) \quad (5.25)$$

$$H_\rho(\rho) = \sqrt{\left[\frac{(\rho \rho_{BW})^{2n}}{(\rho \rho_{BW})^{2n} + (\rho^2 - \rho_0^2)^{2n}} \right]} \quad (5.26)$$

$$H_\theta(\theta) = \begin{cases} \cos^2 \left[\frac{\pi (\theta - \theta_C)}{2 \theta_{BW}} \right], & \text{nëse } |\theta| < \theta_{BW} \\ 0, & \text{ndryshe} \end{cases} \quad (5.27)$$

ku $H_\rho(\rho)$ është filtër brez-lejues Butterworth, me qendër të përcaktuar në ρ_0 dhe gjerësi brezi ρ_{BW} . ρ_0 është e derivuar nga imazhi i orientimit të brendshëm, ndërsa gjerësia ρ_{BW} është e zgjedhur të jetë invers proporcionale me matjen koherente të këndit. Filtri këndor $H_\theta(\theta)$ është një filtër i majave të ngritura kosinusoidale në rrafshin këndor me mbështetjen e θ_{WB} dhe qendër θ_C [99].

5.3.2.5 Rezultatet e matura

Rezultatet e marra nga përdorimi i teknikës dhe algoritmit të përmirësimit të gjurmës papilare me analiza STFT jepen në figurën 5-11, ku në (a) jepet imazhi origjinal i skanuar i gjurmës papilare, në (b) jepet imazhi i orientimit të vijave papilare, në (c) jepet imazhi nëbazë të energjisë së zonës, në (d) jepet imazhi i frekuencës së vijave papilare, në (e) jepet imazhi i matur me koherencë këndore, si dhe në (f) jepet imazhi përfundimtar i përmirësuar [99].

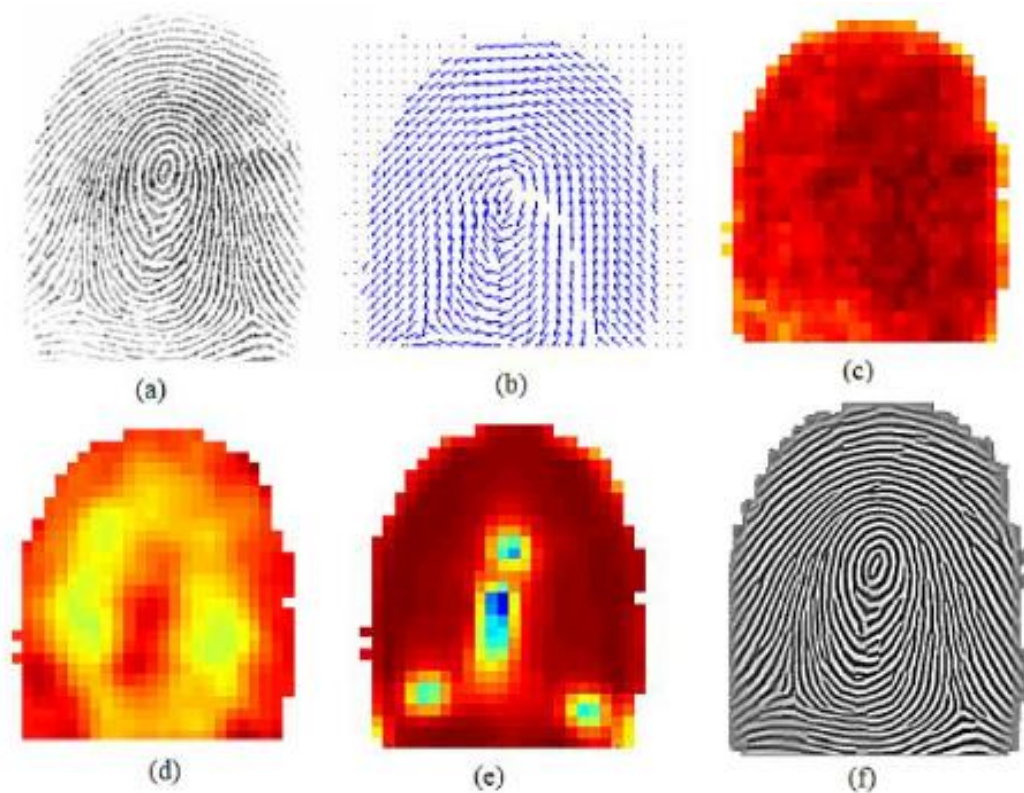


Figura 5-11. (a) Imazhi original i skanuar i gjurmës papilare; (b) Imazhi i orientuar; (c) Imazhi i filtruar në bazë të energjisë së zonave; (d) Imazhi pas filtrimit në frekuencë; (e) Imazhi i matur në koherencë këndore; (f) Imazhi përfundimtar i përmirësuar

Në figurën e mësipërme mund të vërehet se cilësia e rindërtimit nuk ndikohet madje edhe rreth pikave me lakim të madh të shenjuara nga prezenca e karakteristikave. Rezultatet e përmirësimit të imazheve disa gjurmëve papilare respektivisht imazhet 107 dhe 109 të bazës së të dhënave FVC2004 DB1, imazhet 101 dhe 104 të bazës së të dhënave FVC2004 DB4 që ilustrohen në figurën 5-12 dhe 5-13.

Nga ilustrimet mund të vërehet se përmirësimi rrit cilësinë e imazhit të strukturave të vijave papilare, edhe në zona me lakim të madh, pa shtuar asnjë element tjetër në imazh.

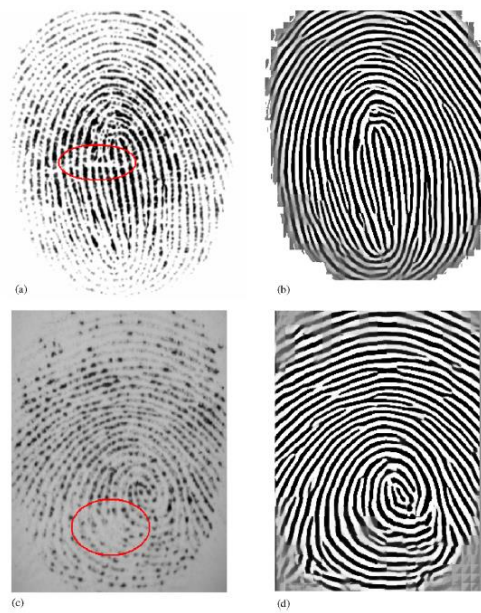


Figura 5-12. (a) dhe (b) Imazhi original i skanuar i gjurmës papilare dhe imazhi i përmirësuar (107 FVC2004DB1) ; (c) dhe (d) Imazhi original i skanuar i gjurmës papilare dhe imazhi i përmirësuar (109 FVC2004DB1)



Figura 5-13. (a) dhe (b) Imazhi original i skanuar i gjurmës papilare dhe imazhi i përmirësuar (101 FVC2004DB4) ; (c) dhe (d) Imazhi original i skanuar i gjurmës papilare dhe imazhi i përmirësuar (104 FVC2004DB4)

5.3.3 Teknika e përmirësimit në dy-etapa duke mësuar nga imazhi fillestar

Deri tani u prezantuan dy nga teknikat më të përdorura të përmirësimit të gjurmëve papilare, e para nëpërmjet përdorimit të filtrit njëdrejtimësh të Gabor, kernel në rrafshin e hapësirës [13] dhe e dyta nëpërmjet përdorimit të analizës STFT në fushën e frekuencës. Teknika e fundit analizon frekuencën e një blloku imazhi nëpërmjet analizës STFT dhe mat në të njëjtën kohë, orientimin lokal të vijës papilare. Kjo teknikë nuk është efiçente me imazhet me cilësi të ulët në hyrje, pasi nuk mund rikuperohen saktësisht të gjithë zonat e parikuperueshme të gjurmës papilare. Kjo pasi është e vështirë për të matur saktësisht disa parametra të filtrave nëpërmjet një analize të thjeshtë.

Kjo teknikë duhet të përmirësohet për të rritur cilësinë e imazhit në zonat e parikuperueshme të imazhit me cilësi të ulët. Në vitin 2013 nga J.Yang, N.Xiong dhe A.V.Vasilakos [102] u propozua skema e kontrollit dhe përmirësimit me dy-etapa, e cila realizon përmirësimin e imazhit në të dy rrafshet atë hapësinor dhe të frekuencës, duke mësuar nga imazhet fillestare siç tregohet në figurën 5-14. Kjo teknikë e re kontrolli dhe përmirësimi u zhvillua për të kapërcyer të metat e teknikave të mëparshme, në përmirësimin e imazheve të gjurmëve papilare me cilësi shumë të dobët, me të çara, me plagë, me lëkurë të thatë, me vija papilare të dobëta dhe kontrast të dobët ndërmjet vijave dhe brazdave papilare.

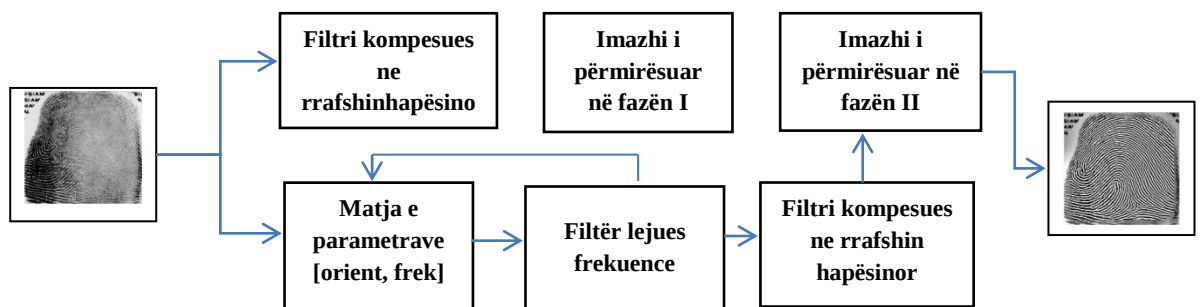


Figura 5-14. Bllokskema e përmirësimit me dy-etapa

Kjo teknikë së pari përmirëson imazhet në rrafshin e hapësirës me një filtër kompesues dhe më tej përmirëson imazhet në rrafshin e frekuencës. Parametrat (drejtimi i vijës papilare dhe frekuenca), për filtrat brezlejujes të frekuencës janë matur nga imazhi origjinal dhe imazhi i përmirësuar i etapës së parë.

5.3.3.1 Etapa e parë e përmirësimit - Filtri kompesues në rrafshin hapësinor

Në etapën e parë realizohet kompesimi i vijës papilare në rrafshin e hapësirës përgjatë vijave papilare. Në këtë etapë përmirësohen vijat papilare lokale të gjurmës papilare duke përdorur pixel-at fqinjë në një dritare të vogël me një maskë të ponderuar përgjatë orientimit të vijave papilare lokale. Kjo përmirëson vlerat e nivelit gri të pixel-ave të vijave papilare përgjatë orientimit të vijave papilare lokale, ndërsa zvogëlohen vlerat e nivelit gri të pixel-ave jo në vijat papilare. Në këtë mënyrë është e mundur që të lidhen vijat e ndërprera dhe të eliminohen njollat në imazhin e gjurmës papilare.

Ideja kryesore e përmirësimit e skemës së propozuar në etapën e parë është të matim orientimin lokal të paanshëm dhe të kompesojmë defektet e mundshme nga përdorimi i orientimit lokal. Kjo skemë e propozuar konsiston në tre etapa:

1. Normalizimi lokal;
2. Matja edrejtimitlokal;
3. Filtrimi kompesues i vijës papilare lokale.

5.3.3.1.1 Normalizimi i drejtimit lokal

Kjo etapë përdoret për të zvogëluar variancat lokale dhe për të standartizuar shpërndarjen e intensitetit në mënyrë që të masim në mënyrë të vazhdueshme orientimin lokal. Funksioni i përcaktimit të saktë të pixel-it nuk e ndryshon qartësinë e vijës papilare dhe strukturave të brazdës, por redukton variancat e vlerave të nivelit gri përgjatë tyre. Për çdo pixel(i,j) në një nënimazh, i cili merret nga ndarja së parie imazhit të gjurmës papilare në nënimazhe, imazhi i normalizuar përcaktohet në formulat (5.28) dhe (5.29)[102]:

$$norimg(i,j) = M_0 + coeff * [img(i,j) - M] \quad (5.28)$$

$$coeff = \frac{V_0}{V} \quad (5.29)$$

ku, $img(i,j)$ është vlera e nivelit gri të imazhit të gjurmës papilare në pixel(i,j), $norimg(i,j)$ është vlera e normalizuar në pixel (i,j), $coeff$ është amplifikuesi i shumëfishtë i imazhit të normalizur, M është mesatarja e nënimazhit dhe V është varianca e tij. M_0 dhe V_0 janë respektivisht vlerat e dëshiruara të mesatares dhe variancës[102].

5.3.3.1.2 Matja e orientimit lokal

Kjo etapë e skemës përcakton drejtimin dominant të vijave papilare në pjesë të ndryshme të imazhit të gjurmës papilare. Për këtë përdoren metoda e gradientit për matjen e orientimit dhe një metodë lëmimi për të korrigjuar orientimin me një dritare Gausiane.

Për një pjesë të blloqeve që nuk mbivendosen me madhësi $W \times W$, një orientim i vetëm caktohet dhe i korrespondon orientimit më të mundur dhe dominant të bllokut. Për çdo pixel në një bllok, një operator gradient i thjeshtë, i tillë si maska Sobel [106], aplikohet për të marrë vlerat e gradientit horizontal $G_x(u, v)$ dhe gradientit vertikal $G_y(u, v)$. Gradientët vertikalë dhe horizontalë të bllokut, psh G_{xx} dhe G_{xy} merren nga shtimi i të gradientëve të pixel të drejtimit korrespondues. Atëherë orientimi i bllokut $O(x, y)$ përcaktohet duke përdorur gradientët horizontal dhe vertikalë të bllokut të përcaktuar në formulat e mëposhtme [102]:

$$G_{xy} = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2G_x(u, v) G_y(u, v) \quad (5.30)$$

$$G_{xx} = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} G_x^2(u, v) G_y^2(u, v) \quad (5.31)$$

$$O(x, y) = \frac{1}{2} \tan^{-1} \left(\frac{G_{xy}}{G_{xx}} \right) \quad (5.32)$$

5.3.3.1.3 Filtri kompesues lokal

Me vlerat e matura të drejtimit, në etapën përfundimtare kompesohen defektet e vijës papilare duke përdorur një filtër të kompesimit të vijës papilare lokale me një dritare drejtkëndore të rrotulluar në mënyrë që të përcaktojmë orientimin lokal. Për çdo pixel(i,j), në imazhin e normalizuar, formula e llogaritjes për filtrin kompesues përcaktohet në formulat e mëposhtme [102]:

$$fltimg(i, j) = \frac{(\sum_{m=-(W-1)/2}^{(W-1)/2} norimg(i' j'))}{((W-1) \times \beta + \alpha) \times h} \quad (5.33)$$

$$i' = i + m \cos(O(i, j)) + n \sin(O(i, j)) \quad (5.34)$$

$$j' = j - m \cos(O(i, j)) + n \sin(O(i, j)) \quad (5.35)$$

ku fltimg(i,j) paraqet imazhin e filtruar me kompesim të vijës papilare, norimg(i,j) është imazhi lokal i normalizuar, $O(i, j)$ është imazhi i orientuar i vijës

papilare lokale dhe (i', j') janë koordinatat e pixel në akset e reja me një transformim relacional për të gjetur orientimin lokal të vijës papilare.

w dhe h janë gjerësia dhe gjatësia e dritareve të përmirësuar, respektivisht m dhe n janë numra të plotë dhe përcaktohen nga w dhe h .

α dhe β janë vlera konstante, që janë të përshtatura me kontrastin e vijave papilare dhe janë përcaktuar në mënyrë eksperimentale. Në ndryshim me funksionin e lëmimit, filtri i kompesimit përdor vlera konstante të ponderuara për të kontrolluar parametrat e kontrastit. Në figurën 5-15 tregohet dritarja $w \times h$ përgjatë orientimit lokal të bllokut [102].

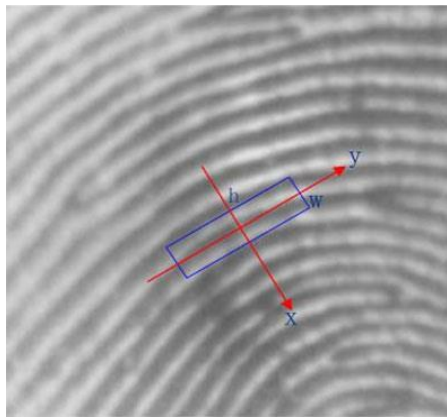


Figura 5.15. Dritarja përgjatë orientimit lokal të vijës papilare

5.3.3.2 Etapa e dytë e përmirësimit - Filtri lejues i frekuencës

Rezultati i filtrit të parë në rrafshin e hapësirës rrit kontrastin e vijës papilare në drejtim pingul me vijat papilare, proces i cili mund të mjeçgullojë edhe imazhin. Prandaj një përmirësim i etapës së dytë me një filtër brezlejues të taruar është propozuar të përmirësojë në mënyrë seriale imazhin. Filtrat brezlejues të frekuencës të përdorur janë të ndashëm, respektivisht në rrafshet e hapësirës dhe frekuencës. Parametrat e filtrit brezlejues mësohen nga të dy imazhi origjinal dhe imazhi i përmirësuar [102]. Filtrat brezlejues të frekuencës kanë treguar që janë efektiv për përmirësimin e imazhit të gjurmës papilare. Megjithatë këto metoda kanë të meta, të tilla si zgjedhja e parametrave të vështira dhe filtrimi jo-efektiv. Për të tejkaluar këto të meta, një skemë e përmirësuar është propozuar me një filtër brezlejues eksponencial. Duke përdorur koordinatat polare (ρ, φ) për të shprehur filtrat si një funksion i ndarë, filtrat brezlejues të frekuencës $H(\rho, \varphi)$ që përdoren janë të ndarë në rrafshet radiale dhe këndore, që tregohet në formulën (5.36):

$$H(\rho, \theta) = H_\rho(\rho)H_\theta(\theta) \quad (5.36)$$

$$H_\rho(\rho) = \frac{1}{\sqrt{2\pi}\rho_{BW}} \exp\left(-\frac{(\rho-\rho_c)^2}{2\rho_{BW}}\right) \quad (5.37)$$

$$H_\theta(\theta) = \begin{cases} \cos^2\left[\frac{\pi(\theta-\theta_c)}{2\theta_{BW}}\right], & \text{nëse } |\theta| < \theta_{BW} \\ 0, & \text{përndryshe} \end{cases} \quad (5.38)$$

Filtri radial $H_\rho(\rho)$ është një filtër brezlejues eksponencial me frekuencë qendrore që përcaktohet nga ρ_c dhe gjerësi ρ_{BW} , ku,

$$\rho_{BW} = \frac{C \times \rho_c - C}{\rho_c} \quad (5.39)$$

ku C është një konstante.

5.3.3.2.1 Matja lokale e drejtimit me vetëmësim

Në këtë etapë të skemës përcaktohet drejtimi dominant i vijave papilare në pjesë të ndryshme të imazhit të gjurmës papilare duke mësuar nga imazhet. Matja e orientimit është e njëjtë me hapin e dytë në filtrimin e etapës së parë. Megjithatë, orientimi i ri $\theta(x, y)$ është saktësuar me imazhin e përmirësuar, pas përmirësimit të realizuar në etapën e parë[102]. Formula për llogaritjen e orientimit të ri $\theta(x, y)$ është si në (5.40):

$$\theta(x, y) = \begin{cases} \text{corr}_{\theta(x,y)}, & \text{nëse } |\text{corr}_{\theta(x,y)} - \text{orig}_{\theta(x,y)}| < t \\ \frac{\sum_{(i,j) \in W} \text{corr}_{\theta(x,y)}}{W \times W}, & \text{ndryshe} \end{cases} \quad (5.40)$$

ku $\text{orig}_{\theta(x,y)}$ është orientimi i një pixel-i në një imazh origjinal, $\text{corr}_{\theta(x,y)}$ është orientimi i pixel-i korrespondues në imazhin e përmirësuar, t është një vlerë prag dhe W është madhësia e dritares[102].

5.3.3.2.2 Matja e frekuencës lokale me vetëmësim

Kjo etapë e skemës përdoret për matjen e ndarjeve ndërmjet vijave papilare në zona të ndryshme të imazhit të gjurmës papilare. Frekuenca lokale matet duke aplikuar transformimin e shpejtë Furie (FFT) tek blloqet. Frekuenca e re balancon vlerën mesatare të fqinjët të tij nëse diferenca e tyre është më e madhe se një vlerë prag, ose ndryshe balancon frekuencën që merret në imazhin e përmirësuar. Frekuenca e përfutur përdoret gjithashtu për të projektuar filtrin radial[102]. Në mënyrë të ngjashme me ekuacionin (5.24), një imazh koherence përlogaritet që të masë koherencën ndërmjet bllokut qendror dhe fqinjët e tij[102].

5.3.3.2.3 Filtrimi brezlejes i frekuencës

Imazhi ndahet në nënimazhe të mbivendosura dhe transformimi i shpejtë Furie(FFT) të secilit nënimazh merret nga heqja e komponentit dc. Filtri radial $H_\rho(\rho)$ nga ekuacioni (5.36) aplikohet i ndjekur nga filtri këndor $H_\varphi(\varphi)$ nga (5.37). Blloku më pas filtrohet në rrafshin e frekuencës, p.sh:

$$H(\rho, \varphi) = H_\rho(\rho) \times H_\varphi(\varphi) = \pi r^2 \text{ si në (5.36).}$$

Imazhi i rikonstruktuar përftohet duke marrë inversin e transformimit të shpejtë Furie të $H(\rho, \varphi)$ [102]. Në figurën 5-16 tregohen shembuj të përmirësimit të imazhit të gjurmës papilare duke përdorur teknikën e përmirësimit me dy-etapa të imazhit të gjurmës papilare.

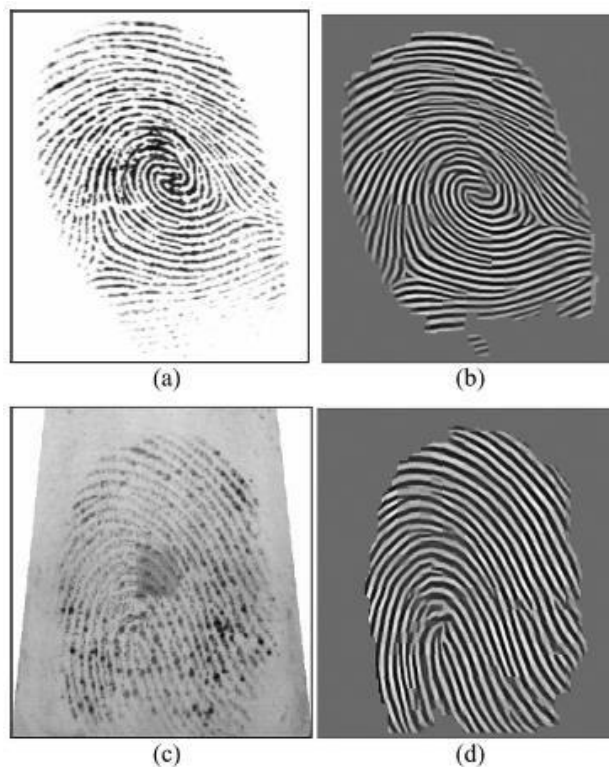


Figura 5-16 Rezultatet e skemës së përmirësimit me dy-etapa :(a) imazhi origjinal 109 FVC2004DB1; (b) imazhi i përmirësuar); (c) imazhi origjinal 104 FVC2004DB1; dhe (d) imazhi i përmirësuar).

5.4 Një krahasim i teknikave të analizuara

Objektivi i teknikave dhe algoritmeve të përmirësimit të imazhit të gjurmës papilare është të korrigjojë degradimin e imazhit të shkaktuara nga problemet e shfaqura në hyrje dhe rindërtimi i strukturës së gjurmës papilare me cilësinë më të lartë. Dihet që një imazh gjurmë papilare me zhurmë do të gjenerojë një informacion jo të vertetë. Siç u trajtua dhe më sipër, teknika e propozuar nga L.Hong [97], përdor filtrat brez-lejues të Gabor, të cilët janë taruar në frekuencë dhe orientim të vijës papilare për të hequr zhurmën e padëshiruar, po në të njëjtën kohë për të ruajtur strukturën e vërtetë të vijës apo brazdëspapilare.

Në këtë teknikë të gjitha veprimet kryhen në rrafshin e hapësirës, ndërkohë që filtrimi kontekstual realizohet në rrafshin Furie. Në anën tjetër, përpunimi me bllok të zgjedhur përdoret për të përfutur rezultatet e përmirësimit që sjellin rindërtimin e ndërprerjeve dhe të metave në kufinjtë e bllokut.

Ndërkohë që teknika e propozuar nga S.Chikkerur [99] bazohet në përmirësimin e imazhit nëpërmjet analizës STFT, të ndjekur nga filtrimi kontekstual duke përdorur filtrat e majave të ngritura kosinusoidale. Këto teknika janë të sukseshme në përmirësimin e imazhit në rastet e dëmtimit të lehtë dhe të moderuar të gjurmës papilare, por performanca e tyre ulët në kushte jo të favorshme të regjistrimit të imazhit [116].

Teknika e tretë e propozuar nga J.Yang[102], me anë të një skeme përmirësimi me dy-etapa dhe me vetëmësim nga imazhi fillestar, përmirëson dhe kapërcen kufizimet e teknikave të para të trajtuara në imazhe me cilësi të ulët me plasaritje, dëmtime, lëkure të thatë, kontrast të dobët të vijave apo brazdave papilare.

Kjo teknikë rezulton jo efiçente gjatë normalizimit lokal ku kërkohet lëmimi i imazhit të pixel-ave bazuar në pixel-at më të afërt. Përdorimi i kësaj teknike lëmimi në kushte ekstremisht jo të përshtatshme (psh. nën efektin e zhurmave të mëdha) degradon imazhin në mënyrë të ndjeshme.

5.5 Teknika e përmirësimit me piramidat e imazhit të Laplas-it

Qëllimi kryesor i një teknike apo algoritmi përmirësimi të gjurmës papilare është të korrigjojë degradimin e imazhit dhe të rindërtojë strukturën aktuale të gjurmës papilare në cilësinë më të mirë. Në teknikën e re të propozuar në vitin 2016, nga VENKATA[113], në mënyrë që të minimizohen të metat dhe kufizimet të pazgjidhura nga teknikat e mëparshme propozohet që në skemën me dy-etapa përmirësimi të propozuar nga J.Yang [102], të zëvendësohen dy proceset e kompesimit dhe normalizimit lokal të vijës papilare me zbërthimin dhe rindërtimin

me piramidat e imazhit të Laplas-it.

Përpunimi me shumë-rezolucione apo piramidat e imazhi tjanë përdorur gjerësisht dhe janë të njohura, në mënyrë të veçantë për kompresimin e imazhit, të propozuar për herë të parë në vitin 1983 [115] dhe përpunimin e imazhit mjekësor, të propozuar për herë të parë në vitin 2003) [117], por nuk janë përdorur për përmirësimin e imazheve të gjurmëve papilare. Piramida e Laplas-it ngjan me filtrimin brezlejues nërafshin e hapësirës.

Në këtë punim, imazhet e gjurmëve papilare janë zbërthyer duke përdorur zbërthimin me piramidën e Laplas-it (LPD-Laplacian Pyramids Decomposition) [115], duke qenë se i gjithë informacioni i duhur është përqëndruar në brezin e disa frekuencave.

5.5.1 Piramidat e imazhit të Laplas-it

Piramidat e imazhit në këtë punim janë përdorur me qëllim që të zbërthejnë imazhet në shkallë të shumëfishtë informacioni, e cila ndihmon në theksimin në mënyrë të saktë të tipareve për të cilat jemi të interesuar dhe eliminon zhurmën. Hapi i parë në kodimin me piramidat e imazhit të Laplasit është të filtrojmë me frekuencë të ulët imazhin origjinal g_0 për të përfutur imazhin g_1 , që është një version i reduktuar i g_0 , në mënyrë që në të njëjtën kohë, rezolucioni dhe densiteti i imazhit janë zvogëluar. Në mënyrë të ngjashme përfutojmë g_2 , si një version të reduktuar të g_1 dhe kështu me radhë. Filtrimi realizohet nga një procedurë ekuivalente me konvolucionin me një nga funksionet simetrike të peshës, lokale të familjes. Një anëtar i rëndësishëm i kësaj familje është i ngjashëm me shpërndarjen e probabilitetit sipas Gaus-it, e tillë që sekuenca e imazheve $g_0, g_1, \dots, g_n$ është quajtur piramida e Gaus-it. Një shembull i piramidave të Gaus-it jepet në figurën 5-17, ku pikat paraqesin pixel-at në secilën shtresë imazhi të piramidës.

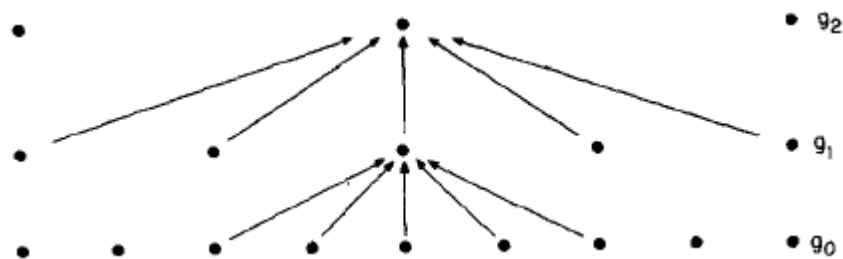


Figura 5-17. Piramida e Gaus-it

Metoda e zbërthimit në piramidat e imazhit njihet si funksioni i reduktimit [115]. Le të jetë 'g', imazhi origjinal me C kolona dh R rreshta dhe një funksion të peshës ekuivalente 'h', parametrat e të cilit (m,n) janë numra të plotë që radhiten

sipas madhësisë së imazhit. Imazhi i reduktuar g_l përfitohet nga funksioni i reduktimit i cili përcaktohet në formulën (5.41) :

$$g_l(i, j) = \sum_{m=-\frac{C}{2}}^{\frac{C}{2}} \sum_{n=-\frac{R}{2}}^{\frac{R}{2}} h_l(m, n) g_{l-1}(2i + m, 2j + n) \quad (5.41)$$

Ku l është numri i niveleve të piramidës $0 < l < n$, dhe (i, j) janë vlerat e pixel-it ku $0 \leq i < C$ dhe $0 \leq j < R$ [115]. Ekuacioni i mësipërm do të referohet në vazhdim si në ekuacionin (5.42):

$$g_l = REDUCE(g_{l-1}) \quad (5.42)$$

Metoda e rindërtimit është e njohur si funksioni i zmadhimit 'expand'[115]. Ky funksion është funksioni i kundërt i 'reduce'. Efekti i këtij funksioni është të zmadhojë një rreshtim të përmasave $(M+1) \times (N+1)$ në një rreshtim të përmasave $(2M+1) \times (2N+1)$ duke interpoluar vlerat e reja të nyjes ndërmjet vlerave të dhëna. Kjo do të zmadhojë rreshtimin g_l të piramidës së Gaus-it në mënyrë që të japë një rreshtim $g_{l,n}$, i cili është imazhi i zmadhuar [115].

$$g_{l,n}(i, j) = \sum_{m=-\frac{C}{2}}^{\frac{C}{2}} \sum_{n=-\frac{R}{2}}^{\frac{R}{2}} h_l(m, n) g_{l,n-1}\left(\frac{i-m}{2}, \frac{j-m}{2}\right) \quad (5.43)$$

Ekuacioni i mësipërm do të referohet në vazhdim si në ekuacionin (5.44):

$$g_{l,n} = EXPAND(g_{l,n-1}) \quad (5.44)$$

Në figurën 5-18 paraqiten gjashtë nivelet e para të piramidës së Gaus-it për imazhin "Lena". Imazhi original, në nivelin 0 matet me 257×257 pixel-a, dhe në nivelin 5 matet vetëm me 9×9 pixel-a [115].

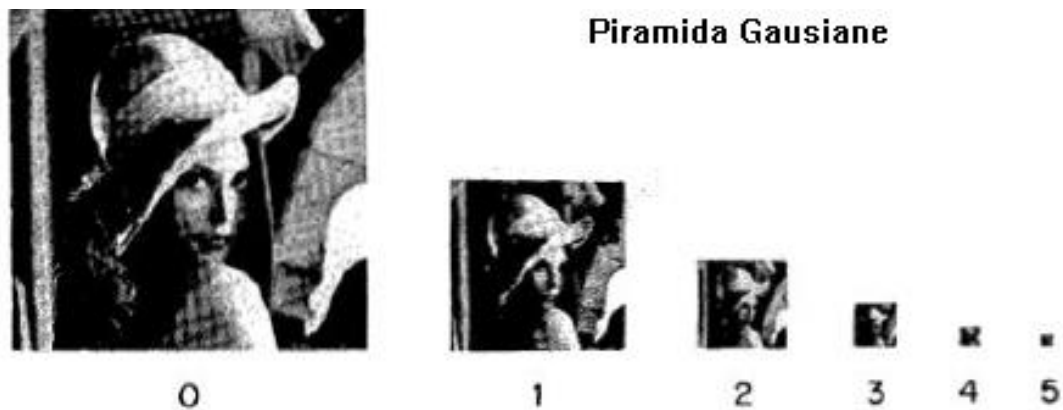


Figura5-18. Gjashtë nivelet e para të piramidës së Gaus-it për imazhin "Lena"

Në mënyrë që të përftojme paraqitjen me piramidat e imazhit sipas Laplas-it, imazhi i gabimit, i cili mbetet kur një imazh i zmadhuar g_1 zbritet nga imazhi g_0 , kodohet. Ky imazh bëhet niveli i fundit i piramidës së Laplas-it. Niveli tjetër gjenerohet nga kodimi në të njëjtën mënyrë i g_1 . Kështu që paraqitja me piramidën e Laplas-it mund të përcaktohet si sekuenca e imazhit të gabimeve $L_0, L_1, \dots, L_N$. Secili prej tyre është diferenca ndërmjet dy niveleve të piramidës së Gaus-it. Konsiderojmë 'l' nivelin e sekuençës së Laplas-it, ku $0 \leq l < N$. Imazhi i paraqitjes së Laplas-it në l jepet prej formulës (5.45) [115]:

$$L_l = g_l - \text{EXPAND}(g_{l+1}) \quad (5.45)$$

Imazhi i rindërtuar mund të përftohet nga zmadhimi dhe mbledhja e të gjithë niveleve të piramidës së Laplas-it:

$$g_l = L_l + \text{EXPAND}(g_{l+1}) \quad (5.46)$$

Në figurën 5-19 ilustrohen katër nivelet e para të piramidës së Gaus-it, në kolonën e parë dhe piramida e Laplas-it në kolonën e fundit për imazhin 'Lena'. Secili nivel i piramidës së Laplas-it është diferenca mes dy piramidave të Gaus-it [115] dhe mund të vihet re që imazhet e piramidës së Laplas-it theksojnë kufinj të objekteve në një imazh, të cilat janë karakteristika thelbësore për një imazh gjurme papilare.

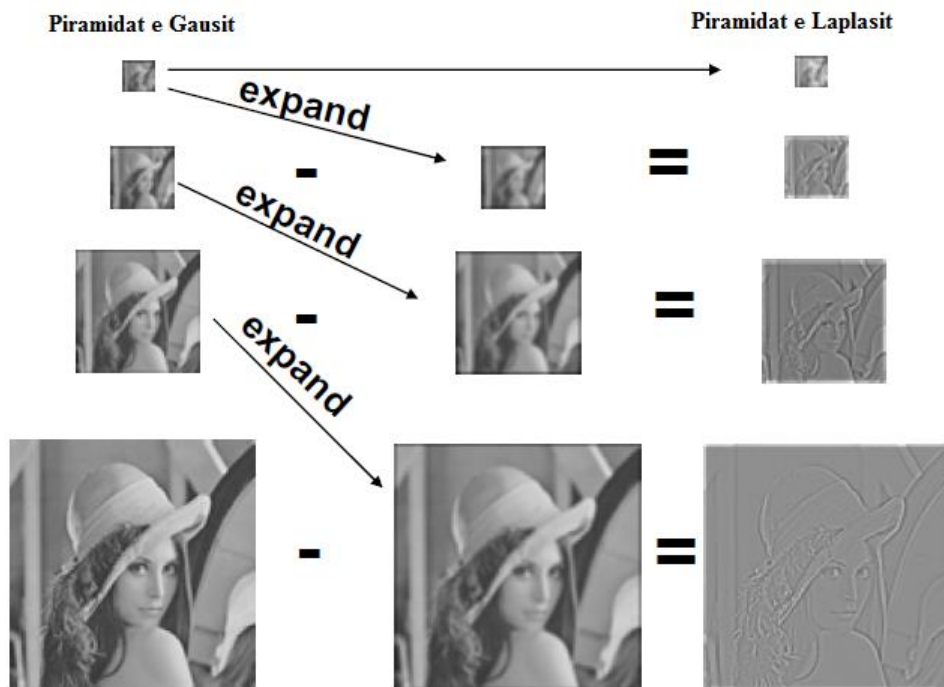


Figura 5-19. Katër nivelet e piramidës së Laplas-it për imazhin Lena"

5.5.2 Zbatimi i piramidave të imazhit të Laplas-it në skemën me dy-etapa

Përmirësimi që është propozuar është që në skemën e përmirësimit me dy-etapa [111] shtohet një hallkë shtesë përmirësimi, përpara komponentit të përmirësimit të etapës së parë. Në këtë etapë do të realizohet procesi i zbërthimit me piramida të Laplasit (LPD) në rrafshin e hapësirës në mënyrë që karakteristikat e vijës papilare do të dallohen nga zhurma dhe do të prodhojnë një përmirësim efektiv.

Duke qenë se karakteristikat më të rëndësishme të vijës papilare do të jenë prezente në nivelin e parë të piramidës së Laplas-it, imazhi fillestar do të shpërbëhet në dy nivele të piramidës së Laplas-it dhe secili prej niveleve L_0 dhe L_1 do të kalojë në skemën e përmirësimit me 2 etapa, më vete.

Në figurën 5-20 paraqitet bllokskema funksionale e propozuar për zbërthimin me piramidat e Laplas-it.

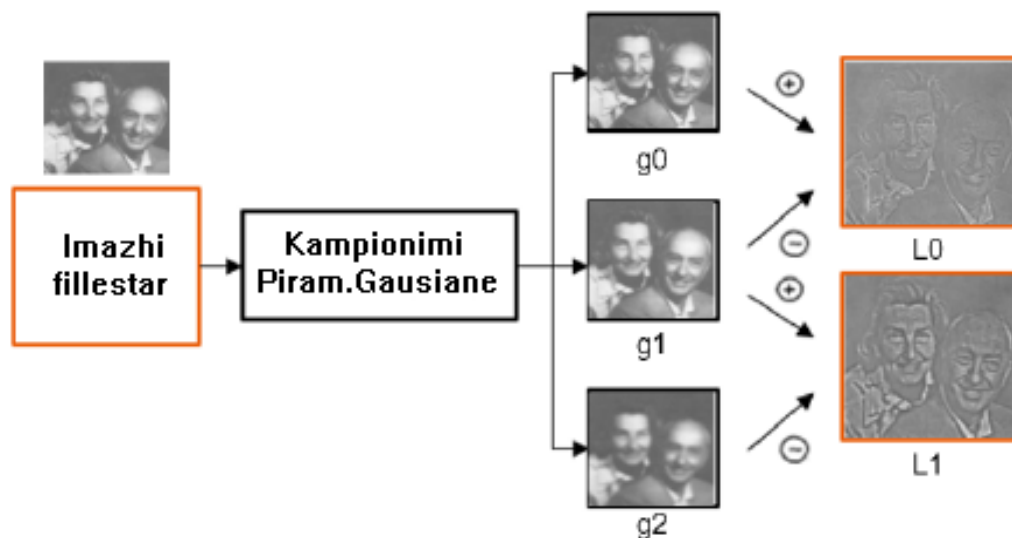


Figura 5-20. Bllokskema funksionale e propozuar për zbërthimin me piramidat e Laplas-it

Përmirësimi do të zbatohet tani si në një sistem me dy-nivele, ku përmirësimi i piramidës së Laplas-it L_0 do të theksojë kryesisht pixel-at me karakteristikat e vijës papilare, ndërsa përmirësimi i piramidës së Laplas-it L_1 kryesisht do të përbëhet nga pixel-a të padëshiruar.

Rindërtimi me piramidën e Laplas-it (LPR-Laplacian Pyramids Reconstructions) do të bëhet për të zmadhuar dhe mbledhur imazhet e përmirësuara të dy niveleve të piramidës së Laplas-it dhe për të përfutur imazhin përfundimtar, të përmirësuar të gjurmës papilare.

Në figurën 5-21 paraqitet bllokskema funksionale me shumë-etapa, me bazë LPD për përmirësimin e cilësisë së imazhit të gjurmës papilare.

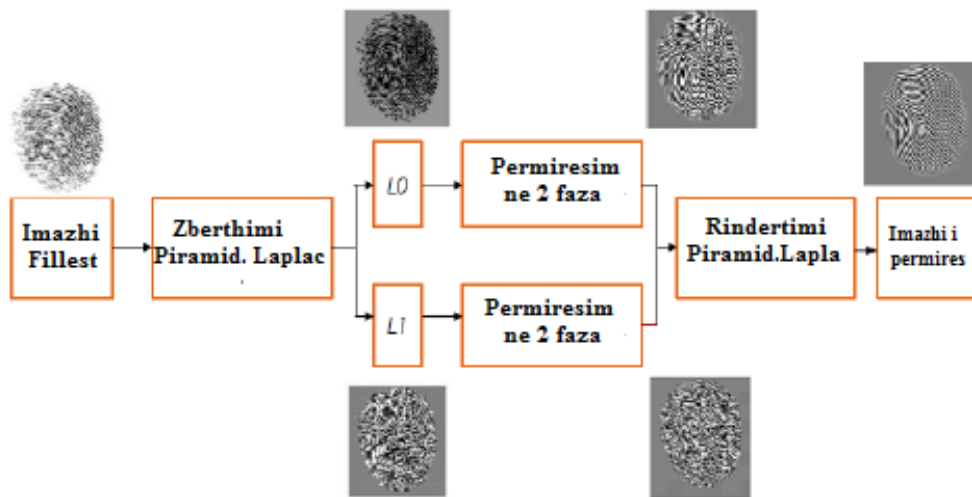


Figura 5-21. Bllokskema funksionale me shumë-etapa, me bazë LPD

5.5.3 Përmbledhje

Skemë e fundit e përmirësimit me shumë-etapa është propozuar të përdoret për përmirësimin e imazhit të gjurmës papilare duke përdorur zbërthimin me piramidën e Laplasit (LPD) dhe rindërtimin me piramidën e Laplasit e cila jep saktësi më të lartë të strukturës së vijave apo brazdave papilare të imazheve të gjurmëve papilare. Në mënyrë që të mbështesim procesin e ekstraktimit të karakteristikave duhet të ekstraktojmë sa më shumë karakteristika të jetë e mundur nga një imazh i një gjurme papilare.

Zbërthimi me piramidat e Laplas-it realizohet për të gjeneruar imazhet e diferencës së piramidës së Laplas-it L_i me anë të ekuacionit(5.45). Në mënyrë që të zvogëlojmë kohën e përpunimit, hallka LPD kufizohet në dy nivele, megjithëse përmirësimi do të ishte më i saktë nëse numri i niveleve të LPD-ve do të ishte më i madh.

Secili $L(i,j)$ mund të konsiderohet si një hyrje për ekuacionin (5.28), e cila jepet në hyrje të skemës së përmirësimit me dy-etapa [102]. Imazhi i përmirësuar i Laplas-it i secilit nivel $L'(i,j)$ përftohet nga IFFT e ekuacionit (5.36). Në përfundim, imazhi i plotë i gjurmës papilare i përmirësuar gjenerohet nga kryerja e procesit të rindërtimit me piramidat e Laplas-it (LPR) në sekuencën e imazheve L' duke përdorur ekuacionin (5.46).

Në mënyrë që të vlerësojmë dhe krahasojmë eficiencën e teknikave të propozuara, në kapitullin pasardhës imazhet e përmirësuara me skemën e përmirësimit me shumë-etapa bazuar në LPD-në do të krahasohen me imazhet e përmirësuara me skemat e tjera të vlerësuara. Krahasimi është realizuar duke përdorur krahasimin vizual, si dhe duke matur parametra të tillë si: raportet e minutiae (TMR dhe FMR) dhe kohën e përpunimit të imazheve në eksperimentet e realizuara në ambientin MATLAB.

KAPITULLI 6

Zbatime, eksperimente dhe interpretime për teknikat e përmirësimit

6.1 Ambienti i testimit

Për të krahasuar dhe vlerësuar efikasitetin e teknikave të përmirësimit të analizuar dhe vlerësuar janë përzgjedhur për testime, një grup të dhënash, imazhet e gjurmëve papilare të bazës së të dhënave publike të konkursit të verifikimit të gjurmëve papilare (Fingerprint Verification Competition)2004[110].

Në këtë konkurs pjesëmarrësit kanë testuar algoritmet e propozuara për të dy fazat e identifikimit atë të regjistrimit dhe të verifikimit. Në mënyrë që të vlerësojmë përmirësimin e realizuar nga teknikat e vlerësuara për përmirësimin e imazhit të gjurmëve papilare, ne duhet të eksperimentojmë me të dhëna gjurmësh papilare të cilësi të ulët ose të deformuara, ku përmirësimi i besueshëm bëhet një domosdoshmëri.

Eksperimentet u realizuan me imazhe të gjurmëve papilare të bazës së të dhënave publike FVC2004. Grupi i imazheve të përzgjedhura për eksperimentet, në bazën e të dhënave FVC2004 përbëhet nga 4 baza të dhënash, DB1, DB2, DB3 dhe DB4. Në bazat e të dhënave DB1 dhe DB2 imazhet e gjurmëve papilare u regjistruan me sensor optik, në bazën e të dhënave DB3 u regjistruan me një sensor termal dhe në bazën e të dhënave DB4 u regjistruan imazhe, që u gjeneruan artificialisht me Gjeneruesin Sintetik të Gjurmëve papilare (Synthetic Fingerprint Generator) (SFinGe)[125]. Në kohën e regjistrimit të këtyre imazheve të gjurmëve papilare, individëve iu kërkua që të ndryshojnë forcën e shtypjes të aplikuar në sensor dhe se gishtat e tyre u pluhurosën ose u lagën në mënyrë që të impononin kushte cilësie të ndryshme për imazhin gjatë regjistrimeve të ndryshme.

Kodet dhe programet ekzekutuar në një makinë me parametra të performancës si më poshtë:

- Sistemi i operimit Windows 7 Professional
- Procesori: Intel(R) CPU E3-1240 v5 @ 3.50 GHz 3.50 GHz
- Memorie e instaluar: 16.0 GB
- Tipi i sistemit: sistem operimi 64-bit

dhe duke përdorur instrumentin MATLAB R2013a, i cili përdor një gjuhë programimi të patentuar dhe shfrytëzon librarinë e tij për përpunimin e imazhit.

Programi “Fingerprint recognition v2.2” është përdorur për llogaritjen e minutiae-ve të vërteta [123] dhe parametrin EER, ndërkohë që për llogaritjen e numrit total të minutiae-

ve dhe raporteve TMR dhe FMR është përdorur kodi MATLAB “Fingerprint minutiae extraction”.

6.2 Krahassimi i metrikave dhe parametrave të cilësisë

Për eksperimentet dhe rezultatet eksperimentale janë përdorur metrika të ndryshme të cilësisë së gjurmëve papilare të tilla si inspektimi vizual, raporti i minutiae-ve TMR dhe FMR, EER, si dhe koha e përpunimit. Këto metrika u matën e u krahasuan për teknikat e ndryshme të përmirësimit të trajtuara në këtë punim. Të dhënat e përdorura për eksperimentet janë marrë nga baza e të dhënave standarte publike FVC2004.

6.3 Inspektimi Vizual

Në figurën 6-1 jepet një imazh original, i skanuar i gjurmës papilare DB1 105, nga baza e të dhënave FVC2004. Ky imazh i skanuar nuk është një rast ekstrem me degradim të imazhit, por në të ndodhen pika të ndryshme, ku kemi shtrembërim të vijës papilare.



Figura 6-1. Gjurmë papilare origjinale FVC2004DB1105



Figura 6-2. Imazh i përmirësuar me filtrimin Gabor

Në figurat 6-2, 6-3, 6-4 respektivisht jepen imazhet e përmirësuara nga përdorimi i filtrit Gabor të taruar, skema e përmirësimit me dy-etapa dhe skema e LPD me shumë-etapa.



Figura 6-3. Imazhi i përmirësuar në skemën me dy-etapa

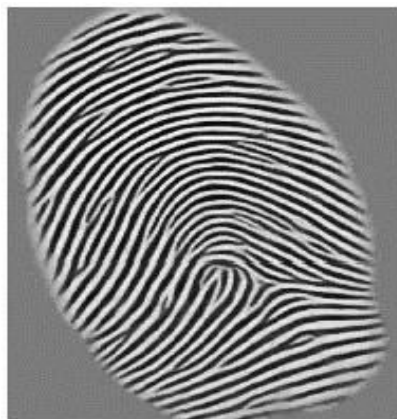


Figura 6-4. Imazhi i përmirësuar në skemën me shumë-etapa (LPD)

Siç shihet nga figurat 6-1, 6-2, 6-3 dhe 6-4, është e qartë që të gjitha teknikat e përmirësimit të përdorura janë të afta të rindërtojnë saktësisht strukturën vijë-brazdë të gjurmës papilare. Në veçanti pjesë të mjegulluara janë më të dukshme në figurat 6-2 dhe 6-3. Imazhi i përmirësuar në figurën 6-4 ka një strukturë më të qartë vijë-brazdë, pasi përpunimi LPD ka përmirësuar theksimin e karakteristikave dhe eliminimin e zhurmës.

Për të vlerësuar përmirësimin e imazhit në një rast ekstrem, me cilësi shumë të ulët është marrë imazhi i treguar si në figurën 6-5, në të cilin ka një përqindje të lartë të degradimit të imazhit. Në figurat respektivisht 6-6 dhe 6-7

jepen imazhet e marra nga përmirësimi me transformimin e shpejtë Furie dhe me skemën e përmirësimit me shumë-etapa (LPD). Nga inspektimi vizual është e dukshme që skema me shumë-etapa ka realizuar një rindërtim më të mirë të imazhit më cilësi të dobët të imazhit në hyrje, edhe në zona me karakteristika të degraduara.



Figura 6-5. Gjurmë papilare me cilësi shumë të ulët FVC2004DB1101



Figura 6-6. Përmirësim i imazhit bazuar në analizën STFT



Figura 6-7. Përmirësim i imazhit me skemën me shumë-etapa (LPD)

Për të vlerësuar përmirësimin e imazhit në një imazh gjurme me cilësi të mesme, është marrë imazhi i treguar në figurën 6-8, me dëmtime të shumta të strukturës së vijës papilare dhe një imazh tërësisht i mjegulluar. Në figurat respektivisht 6-9 dhe 6-10 janë imazhet e marra nga përmirësimi nga skema e përmirësuar LPD e nivelit 1 dhe nivelit 2[115]. Ndërsa figurat 6-11 dhe 6-12 janë respektivisht imazhet e përmirësuara me skemën me dy-etapa të imazheve në figurat 6-9 dhe 6-10.



Figura 6-8. Imazhi fillestar i gjurmës papilare 102 nga FVC2004DB1



Figura 6-9. Imazhi i piramidës së Laplas-it Nivel 1



Figura 6.10. Imazhi i piramidës së Laplas-it Niveli 2



Figura 6-11. Imazi i piramidës së Laplas-it Niveli 1 i përmirësuar



Figura 6-12. Imazhi i piramidës së Laplas-it Niveli 2 i përmirësuar

Figurat 6-13 dhe 6-14 janë imazhet e marra nga përmirësimi me transformimin e shpejtë Furie dhe me skemën me bazë LDP me shumë-etapa. Siç mund të vërehet edhe në figurë imazhi i përmirësuar në figurën 6-13, me transformimin e shpejtë Furie ka shtrembërime të vijave, të cilat janë më të dukshme

dhe që përkthehen gjatë ekstraktimit në minutiae të rreme. Vihet re përmirësimi i realizuar për të njëjtin imazh nga skema me shumë-etapa(LPD), në figurën 6-14, ku vërehet se imazhi i përmirësuar nga kjo skemë ka më pak shtrembërimë.

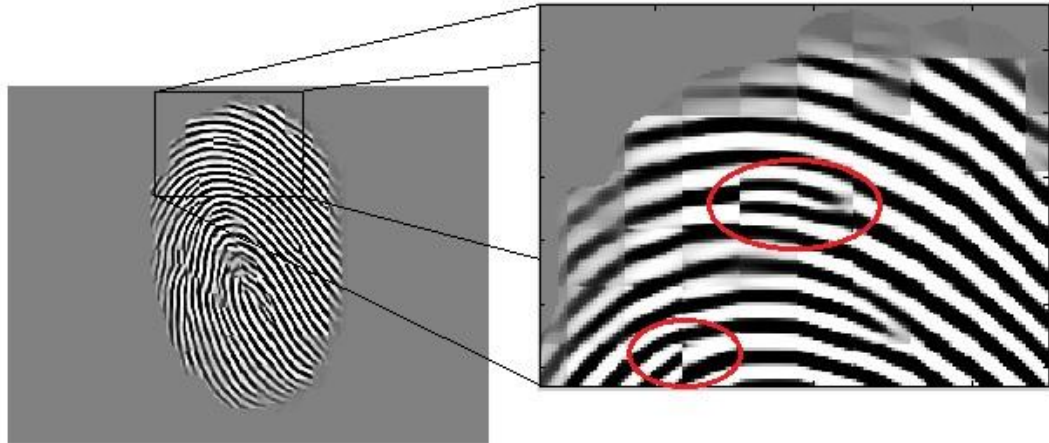


Figura 6-13. Imazhi përmirësuar me analizën STFT me shtrembërimë të theksuara

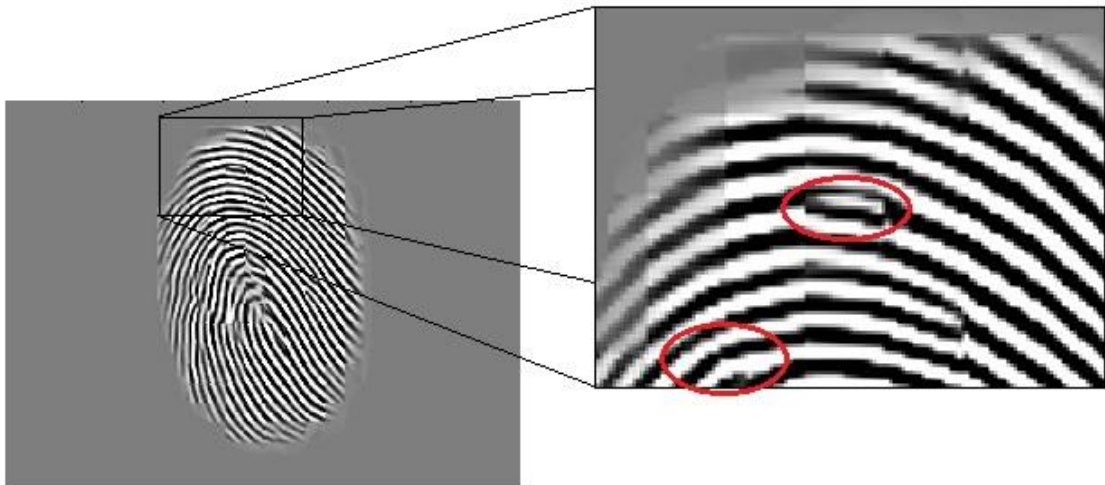


Figura 6-14. Imazhi përmirësuar me skemën me shumë-etapa (LPD), me më pak shtrembërimë

Në figurat 6-15, 6-16, 6-17, 6-18, 6-19, 6-20 ilustrohen rezultatet e marra nga procesi i përmirësimit të disa imazheve fillestare nga baza e të dhënave FVC2004 [110] me disa teknika përmirësimi si: përmirësimi me filtrin Gabor dhe skemën e përmirësimit me shumë-etapa(LPD). Në mënyrë më specifike në figurat 6-15 dhe 6-16 jepen imazhet fillestare 104 dhe 107 nga baza e të dhënave FVC2004 DB1 dhe imazhet e përmirësuara me teknikat e filtrimit Gabor dhe skemën e përmirësimit me shumë-etapa.

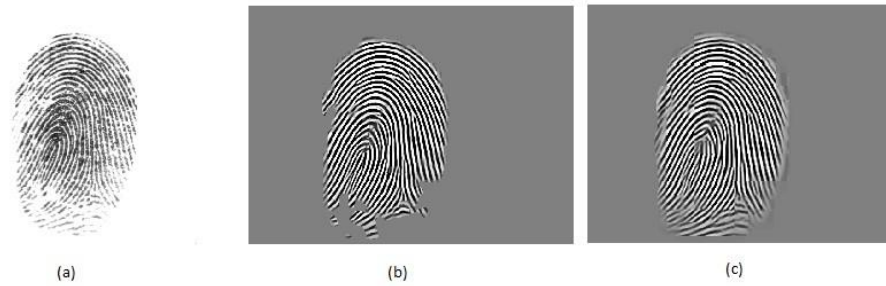


Figura 6-15. (a) Imazhi origjinal 104 FVC2004 DB1; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD).

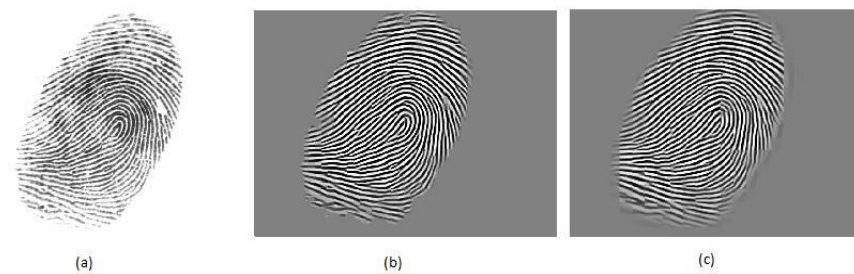


Figura 6-16. (a) Imazhi origjinal 107 FVC2004 DB1; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD)

Në figurat 6-17 dhe 6-18 jepen imazhet fillestare 101 dhe 104 nga baza e të dhënave FVC2004 DB2, si dhe imazhet e përmirësuara me teknikat e filtrimit Gabor dhe skemën e përmirësimit me shumë-etapa (LPD).



Figura 6-17. (a) Imazhi origjinal 101 nga FC2004 DB2; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD).



Figura 6-18. (a) Imazhi origjinal 104 FVC2004 DB2; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën e re me shumë-etapa (LPD)

Në figurat 6-19 dhe 6-20 jepen imazhet fillestare 104 dhe 105 nga baza e të dhënave FVC2004 DB3, si dhe imazhet e përmirësuara me teknikat e filtrimit Gabor dhe skemën e përmirësimit me shumë-etapa.

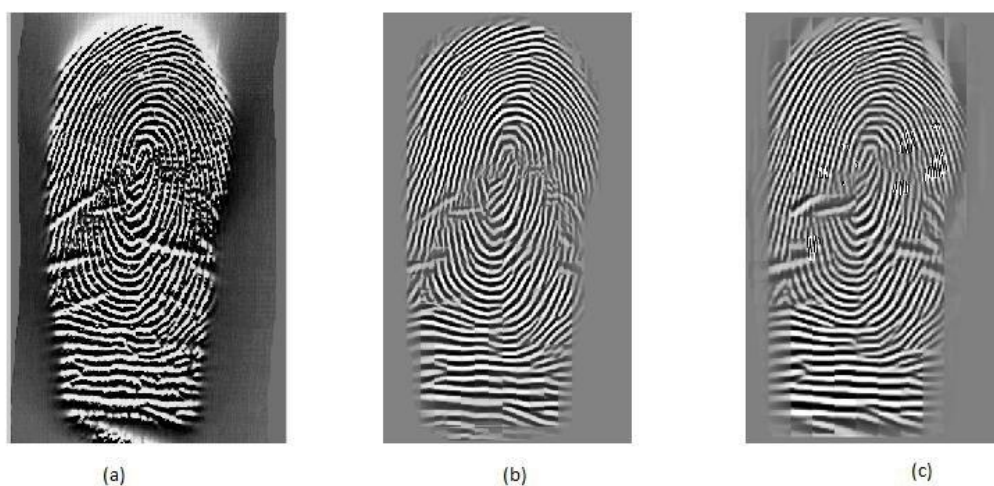


Figura 6-20. (a) Imazhi origjinal 104 FVC2004 DB3; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD)



Figura 6-21. (a) Imazhi original 105 FVC2004 DB3; (b) Përmirësimi me filtrin e Gabor; (c) Përmirësimi me skemën me shumë-etapa (LPD)

Inspektimi visual i rezultateve me imazhet e përmirësuara të bazës së të dhënave FVC2004 provon që të tre teknikat e përmirësimit të imazhit të përdorura, si dhe skema e përmirësimit me shumë-etapa dhe bazuar në LPD kanë pasur performancë të mirë në rindërtimin e zonave me cilësi shumë të dobët të imazheve të gjurmëve papilare.

Megjithatë, vihet re se skema me shumë-etapa e bazuar në LPD është më efiçente për përmirësimin e imazhit me cilësi të dobët dhe të degraduar, si dhe saktësisë së vijave papilare.

Në figurën 6-22 tregohen rezultatet krahasuese për në imazh gjurme papilare me cilësi të ulët. Ndërsa efekti i algoritmit të përmirësimit mund të dallohet në mënyrë vizuale, objekti përfundimtar i procesit të përmirësimit është të rrisë saktësinë e sistemit të identifikimit.

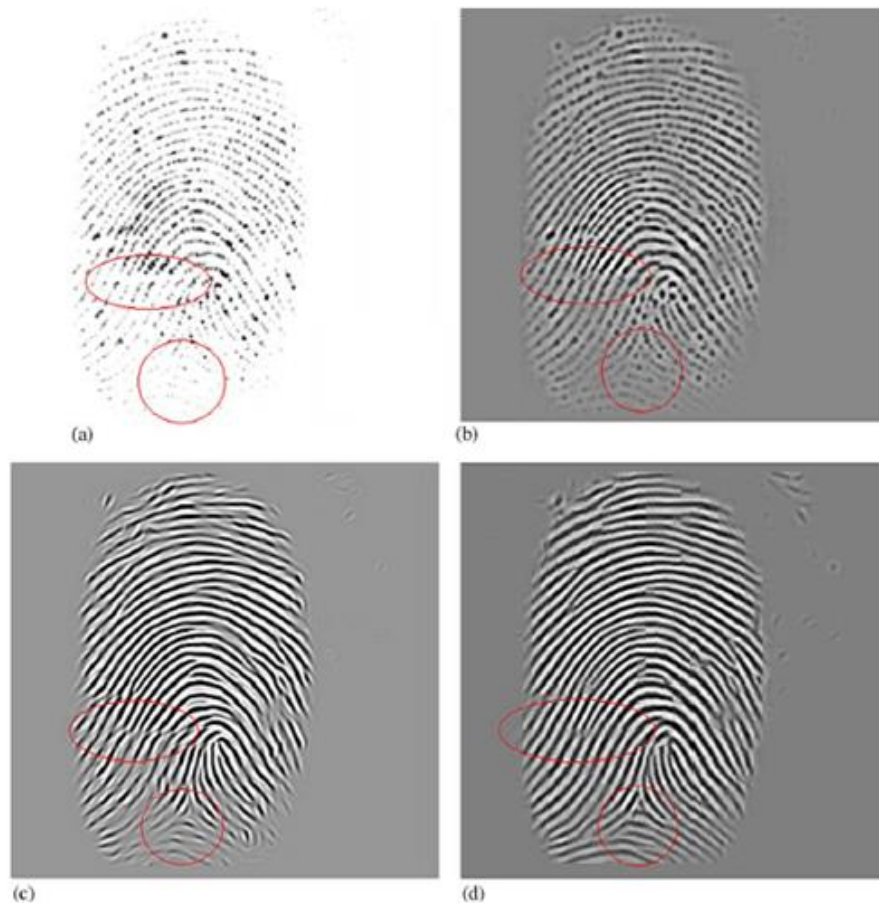


Figura 6-22. (a) Imazhi original 103 FVC2004 DB3; (b) Përmirësimi me analizën STFT; (c) Përmirësimi me skemën me dy-etapa; (d) Përmirësimi me skemën me shumë-etapa (LPD).

Në figurën 6-23 paraqiten minutiae-t që ekstrahohen nga imazhi original 103 FVC2004 DB3 dhe nga imazhet e përmirësuara duke përdorur teknikat [197], [99] [102] dhe skemën e propozuar të fundit. Duke krahasuar imazhin original me imazhet e përmirësuara, mund të vihen re që mungojnë disa minutiae (të vijëzuara me të kuqe), që janë dedektuar me sukses në imazhet e përmirësuara. Në figurën 6-23(b) paraqiten minutiae-t e ekstraktuara nga imazhi i përmirësuar me skemën [99], ku vërehet që mungojnë disa struktura të vijës papilare në kufirin e gjurmës papilare dhe minutiae-t në këto zona nuk mund të dedektohen.

Në figurën 6-23(c) e cila tregon imazhin e përmirësuar me skemën me analizë STFT, në minutiae-t e ekstraktuara, mund të vërehet që ajo përmban disa minutia të rreme jashtë gjurmëve papilare për shkak të disa karakteristikave të rreme të prodhuara nga kjo teknikë. Skema me shumë-etapa (LPD) rezulton të jetë më efikase, pasi jep rezultatin më të mirë në lidhje me minutiae-t e ekstraktuara, siç dhe ilustruhet në figurën 6-20 (d). Kjo skemë dedekton shumë më pak minutiae të rreme në krahasim me rezultatet e arritura me skemat e mëparshme të përmirësimit.

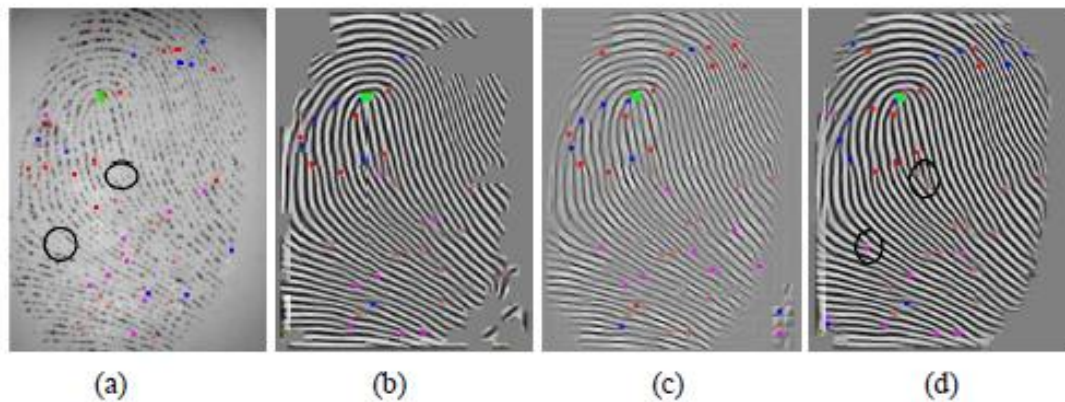


Figura 6-23. Minutia-t e ekstraktuara në katër imazhe gjurme papilare (a) Imazhi original; (b) Imazhi përmirësuar me filtrin Gabor; (c) Imazhi i përmirësuar me analizën STFT; (d) Imazhi i përmirësuar me skemën me shumë-etapa (LPD)

Në figurën 6-24 ilustruhet rezultati i procesit pas përmirësimit të binarizimit dhe qartësimit të imazhit [1], në mënyrë që të ekstrahohen minutiae-at nga imazhet e gjurmëve papilare. Në figurën 6-24 (a) ilustruhet binarizimi dhe qartësimi i imazhit original 101 FVC2004 DB2, në të cilin mund të vërehen pika të ndryshme të rreme. Në figurën 6-24 (b) ilustruhet binarizimi dhe qartësimi i imazhit të përmirësuar 101 FVC2004 DB2 me teknikën e L.Hong, që bazohet në filtrimin Gabor, në të cilin disa pika të rreme mund të vërehen ende. Në figurën 6.24 (c) ilustruhet binarizimi dhe qartësimi i imazhit të përmirësuar 101 FVC2004 DB2 me teknikën e skemës e re të përmirësimit me shumë-etapa (LPD), në të cilin shumë pak pika të rreme mund të shihen dhe në përgjithësi është arritur saktësia e vijës papilare.

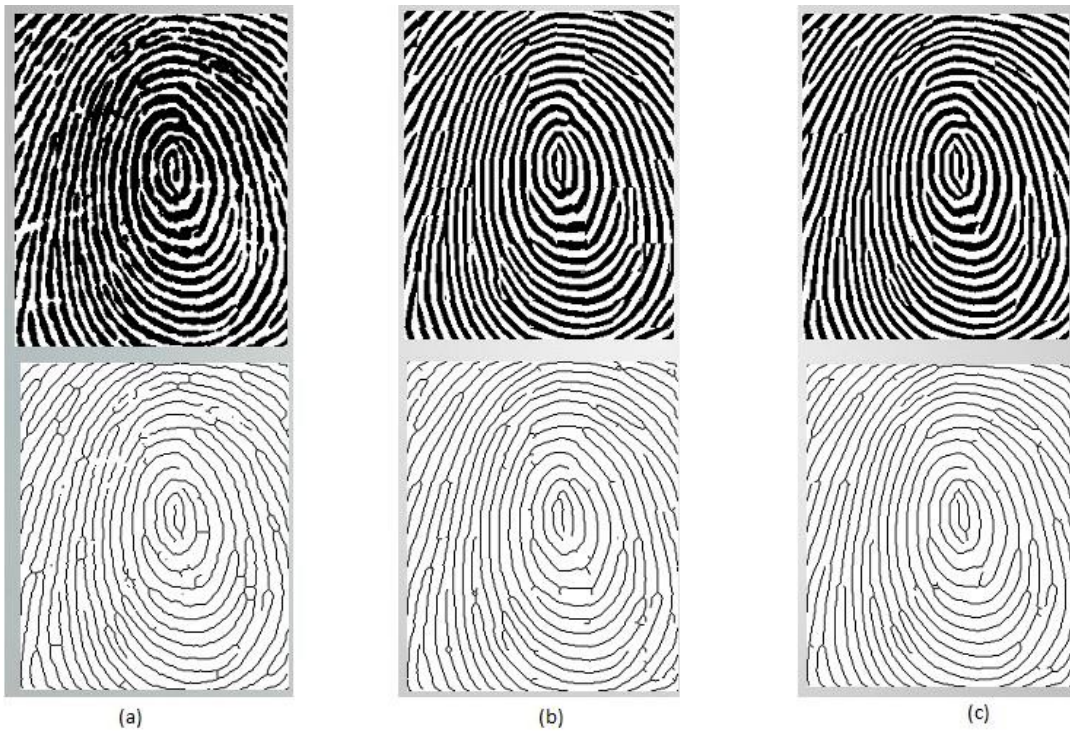


Figura 6-24. Veprimi i qartësisë në (a) imazhin original 101FVC2004DB2; (b) përmirësimi i skemës me teknikën e filtrimit Gabor; (c) skema e përmirësimit me shumë-etapa (LPD)

Në figurën 6-25 tregohen minutiae-t e ekstraktuar nga imazhet e qartësuara të vëzhguara në figurën 6.24.

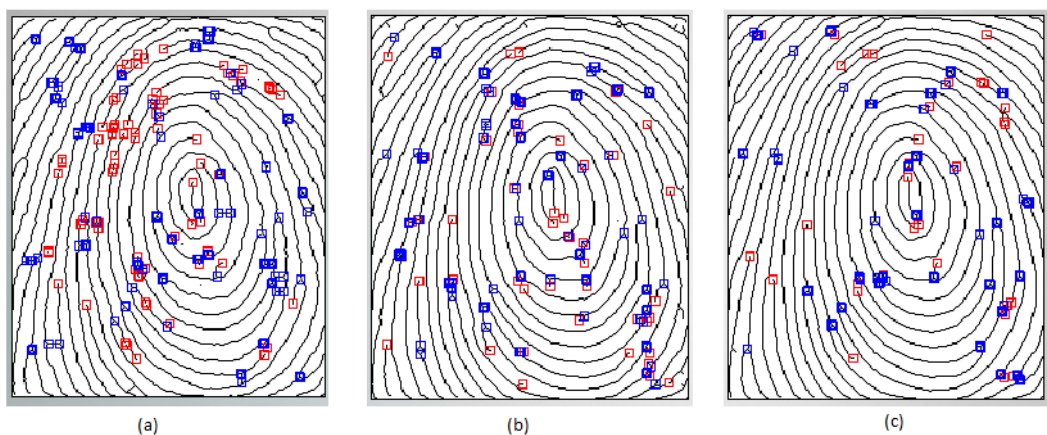


Figura 6-25. Minutia-t e ekstraktuar nga imazhi i qartësuar (a) imazhi original 101 FVC2004 DB2; (b) përmirësimi i skemës me teknikën e filtrimit Gabor; (c) skema e përmirësimit me shumë-etapa (LPD)

6.4 Parametra të matur

Teknika e përmirësimit me skemën me shumë-etapa me bazë LPD do të zbatohet dhe do të krahasohet me skemat e tjera të përmirësimit të trajtuara në punim.

Parametrat e mëposhtëm janë përcaktuar dhe përdorur për krahasimin e performancës së teknikave të përmirësimit[119]:

1. Minutiae të vërteta: një minutiae e dedektuar;
2. Minutiae e rreme: një minutiae që nuk përputhet me minutiae e vërtetë, e cila konsiderohet e rreme dhe që matet me diferencën e minutia-ve në total të dedektuara me numrin e minutiae-ve të vërteta të dedektuara.

Këto parametra janë përdorur më tej për të përcaktuar raportin e minutiae-ve të vërteta (TMR) dhe raportin e minutiae-ve të rreme (FMR), që llogariten më anë të formulave të mëposhtme [102]:

$$TMR\% = \frac{Minutiae_{vert}}{Minutiae_{tot}} * 100 \% \quad (6.1)$$

$$FMR\% = \frac{Minutiae_{rrem}}{Minutiae_{tot}} * 100 \% \quad (6.2)$$

Parametri EER (%) [100] është matur për vlerësimin e shkallës së gabimit të barabartë, ku EER është shkalla e gabimit që paraqet pikën ku FNMR dhe FMR janë të njëjtë. Parametri siç e kemi cituar edhe më lart në punim FMR njihet me termin FAR dhe FNMR njihet edhe si FRR.

Në vijim janë realizuar eksperimente dhe simulime për imazhe më cilësi të ndryshme gjurmësh papilare.

Pas procesit të binarizimit dhe qartësimit [78], imazhi i qartësuar përdoret nga kompjuteri për të përlogaritur minutiae-t e ekstraktuara nga imazhi i gjurmës papilare, ashtu siç ilustron në figurën 6-25.

Figurat 6-26, 6-27 dhe 6-28 tregojnë minutiae-t e ekstraktuara respektivisht nga imazhet 104 FVC2004DB1; 101 FVC2004DB2; dhe 105 FVC2004DB3. Në këtë figurë (a), (b) dhe (c) tregojnë ekstraktimin e minutiae-ve nga imazhi original, nga imazhi i përmirësuar me filtrin Gabor [96], dhe imazhi i përmirësuar me skemën me shumë etapa (LPD).

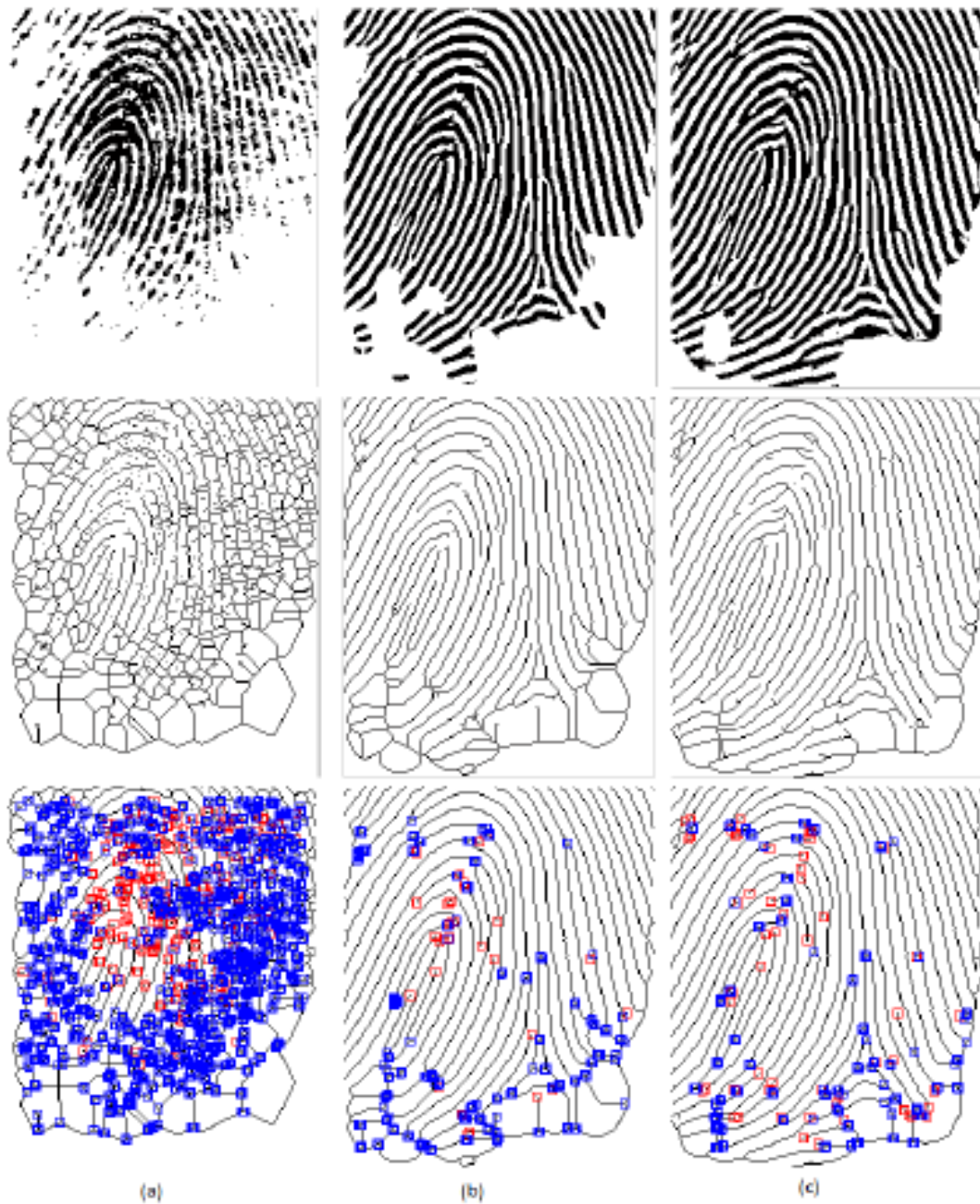


Figura 6-26. Minutiae të nxjerra nga (a) imazhi original 103 FVC2004DB1, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)

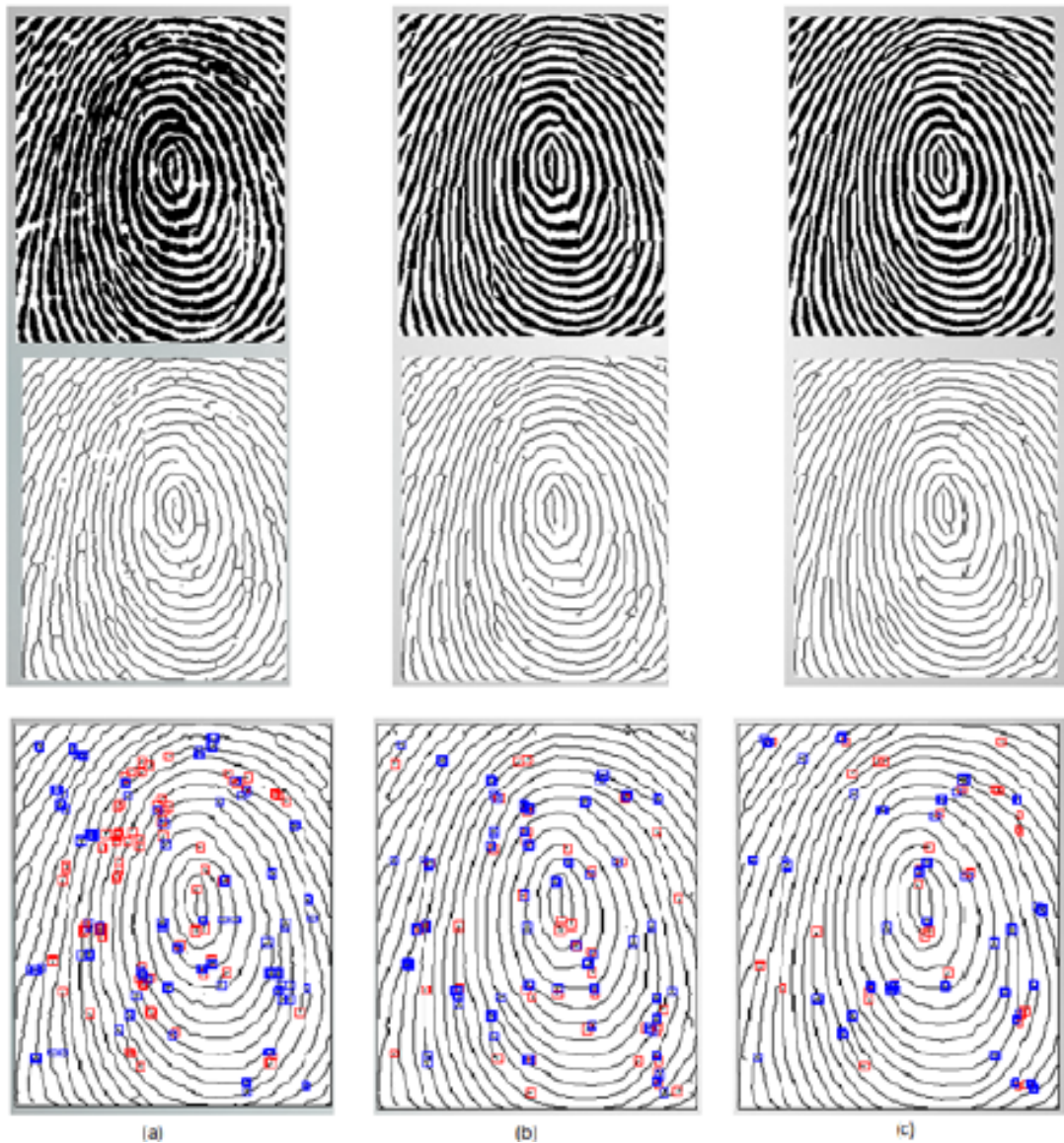


Figura 6-27. Minutiae të nxjerra nga (a) imazhi origjinal 105 FVC2004DB2, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)

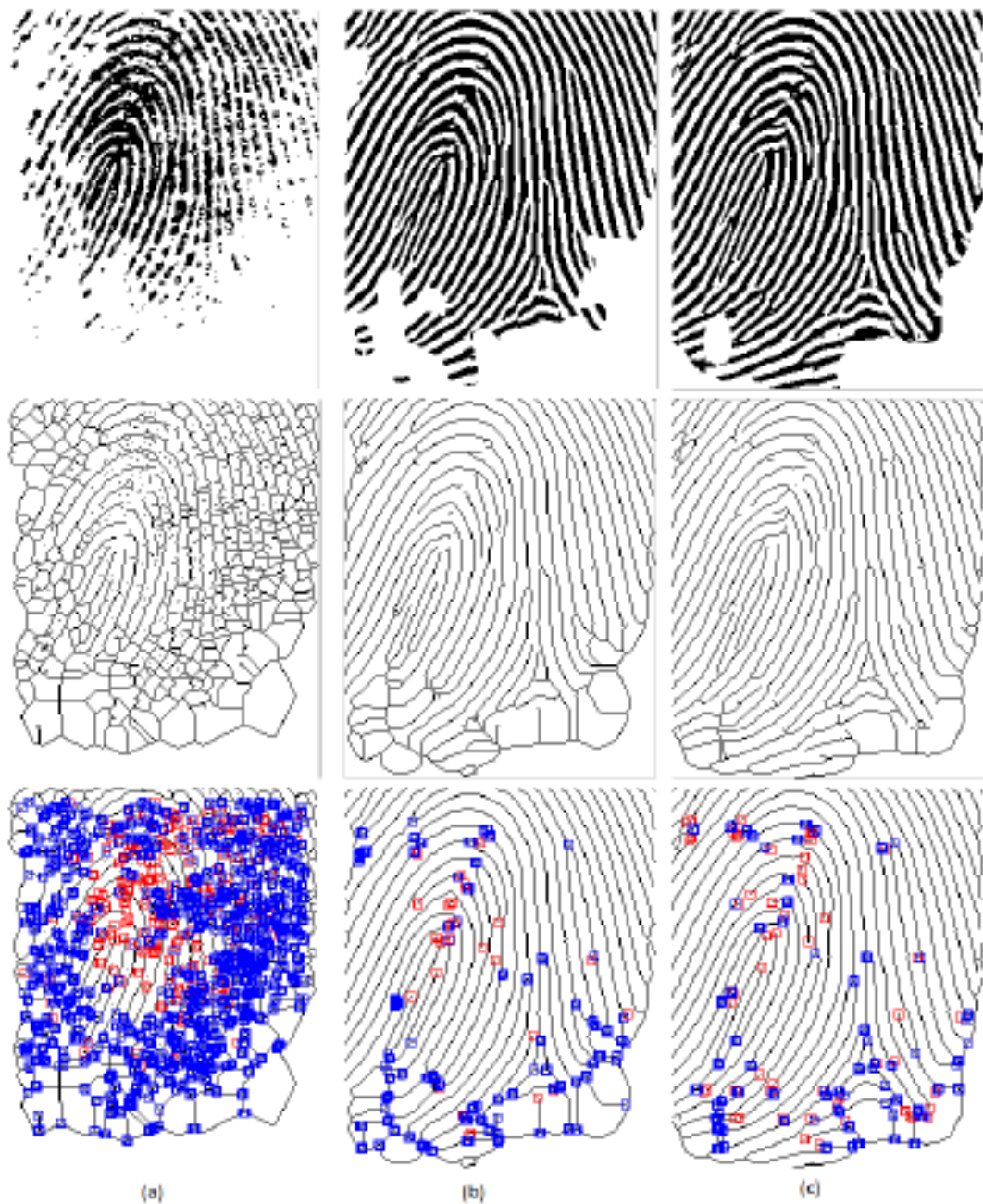


Figure 6-28. Minutiae të nxjerra nga (a) imazhi original 102 FVC2004DB3, (b) imazhi i përmirësuar me filtër Gabor, (c) imazhi i përmirësuar me skemën me shumë-etapa (LPD)

Në tabelën 6-1 paraqiten respektivisht numri i minutia-ve të dedektuara nga imazhet 103 FVC2004DB1, 105 FVC2004DB2 dhe 102 FVC2004DB3. Në tabelën 6-2 paraqitet numri i minutiae-ve të rreme të llogaritura për tre imazhet e vlerësuara të bazës së të dhënave FVC2004: 103 FVC2004DB1, 105 FVC2004DB2 dhe 102 FVC2004DB3.

Tabela 6-1 Llogaritja e minutiae të dedektuara për imazhe të bazës së të dhënave

Baza e të dhënave FVC2004	Imazhi (Nr.Minutiae të vërteta)	Imazhi original (Nr.Minut)	Imazhi i përmirësuar me F.Gabor (Nr.Minut)	Imazhi i përmirësuar me analizën STFT (Nr.Minut)	Imazhi i përmirësuar me skemën me 2-etapa me vetëmësim (Nr.Minut)	Imazhi i përmirësuar me skemën me shumë-etapa me bazë LPD (Nr.Minut)
Imazhi 103 FVC2004DB1	119	1212	183	182	177	169
Imazhi 105 FVC2004DB2	101	356	148	143	136	130
Imazhi 102 FVC2004DB3	107	278	146	141	136	131

FVC2004

Tabela 6-2 Numri i minutiae-vetë rreme të dedektuara në imazh

Baza e të dhënave FVC2004	Imazhi origjinal	Imazhi i përmirësuar me F.Gabor	Imazhi i përmirësuar me analizën STFT	Imazhi i përmirësuar me skemën me 2-etapa me vetëmësim	Imazhi i përmirësuar me skemën me shumë-etapa me bazë LPD
103 FVC2004 DB1	1093	64	63	58	50
105 FVC2004 DB2	255	47	42	35	29
102 FVC2004 DB3	171	39	34	29	24

Ndërkohë në tabelën 6-3 paraqitet krahasimi i raporteve të minutiae-ve të vërteta dhe të rreme të dedektuara, si dhe dhe mesatarja e tyre, duke përdorur formulat (5.47) dhe (5.48).

Tabela 6-3 Tabela e krahasimit të raporteve të minutiae TMR, FMR dhe mesatarja e tyre

Baza e të dhënave FVC2004	Imazhi origjinal (Vlerat %)		Imazhi i përmirësuar me F.Gabor (Vlerat %)		Imazhi i përmirësuar me analizën STFT (Vlerat %)		Imazhi i përmirësuar me skemën me 2-etapa me vetëmësim (Vlerat %)		Imazhi i përmirësuar me skemën me shumë-etapa (Vlerat %)	
	<i>TMR</i>	<i>FMR</i>	<i>TMR</i>	<i>FMR</i>	<i>TMR</i>	<i>FMR</i>	<i>TMR</i>	<i>FMR</i>	<i>TMR</i>	<i>FMR</i>
103 FVC2004 DB1	9.8	90.2	65.1	34.9	65.4	34.6	67.3	32.7	71.5	29.5
105 FVC2004 DB2	28.4	71.6	68.2	31.8	70.6	29.4	74.3	25.7	77.7	22.3
102 FVC2004 DB3	38.5	61.5	73.3	26.7	75.9	24.1	78.7	21.3	81.7	18.3
<i>Mesatare</i>	25.6	74.4	68.9	31.1	70.6	29.4	73.4	26.6	76.6	23.4

Nga vlerësimi dhe krahasimi i vlerave të matura për teknikat e përmirësimit, konstatojmë që skema me shumë-etapa me bazë LPD krahasuar me skemën e Filtrit Gabor ka përmirësimin më të ndjeshëm prej 6 - 8 %, ndërsa me teknikën me analizë STFT është në vlerat 5 -7 %, ndërsa me teknikën me 2-etapa me vetëmësim është në vlerën 3 - 4 %.

Krahasimi i raporteve të minutiae-ve të llogaritura për imazhet në përmirësim TMR, FMR, si dhe mesatarja e tyre ilustrohen dhe me grafikët e ndërtuar në figurën 6-29.



Figura 6-29 Krahasimi i raporteve të minutiae TMR, FMR dhe mesatarja e tyre

Në tabelën 6-4 paraqitet vlerësimi i parametrut EER për përmirësimin e katër imazheve të ndryshme nga baza e të dhënave FVC2004 me anë të teknikave të përmirësimit të trajtuara në punim. Krahasimi i rezultateve dhe shkallës së përmirësimit të parametrut EER (%) për imazhet e përmirësuara ilustrohen dhe me grafikët e ndërtuar në figurën 6.30. Sa më shumë t'i afrohet EER 0% aq më e mirë është performanca e njohjes biometrike të sistemit të identifikimit me imazhin e përmirësuar.

Tabela 6.4 Rezultatet dhe shkalla e përmirësimit të parametrut EER (%)

FVC 2004		106 DB1_A FVC2004	101 DB2_A FVC2004	107 DB3_A FVC2004	103 DB4_A FVC2004
Imazhi origjinal	EER(%)	32,50	35,31	15,00	13,05
Imazhi i përmirësuar me F.Gabor	EER(%)	22,27	20,24	10,90	9,39
Imazhi i përmirësuar me analizën STFT	EER(%)	20,96	18,43	9,00	8,14
Imazhi i përmirësuar me skemën me 2-etapa me vetëmësim përmirësuar me skemën me 2-etapa	EER(%)	10,89	9,65	5,48	4,67
mazhi i përmirësuar me skemën me shumë-etapa me bazë LPD	EER (%)	7,23	6,83	4.12	3.25

Nga krahasimi i vlerave të matura të EER-së për imazhet e përmirësuara me teknikat e trajtuara në punim vërehet se skema me shumë etapa me bazë LPD, është më efiçente (EER më e vogël se të gjitha skemat e tjera të përmirësimit).

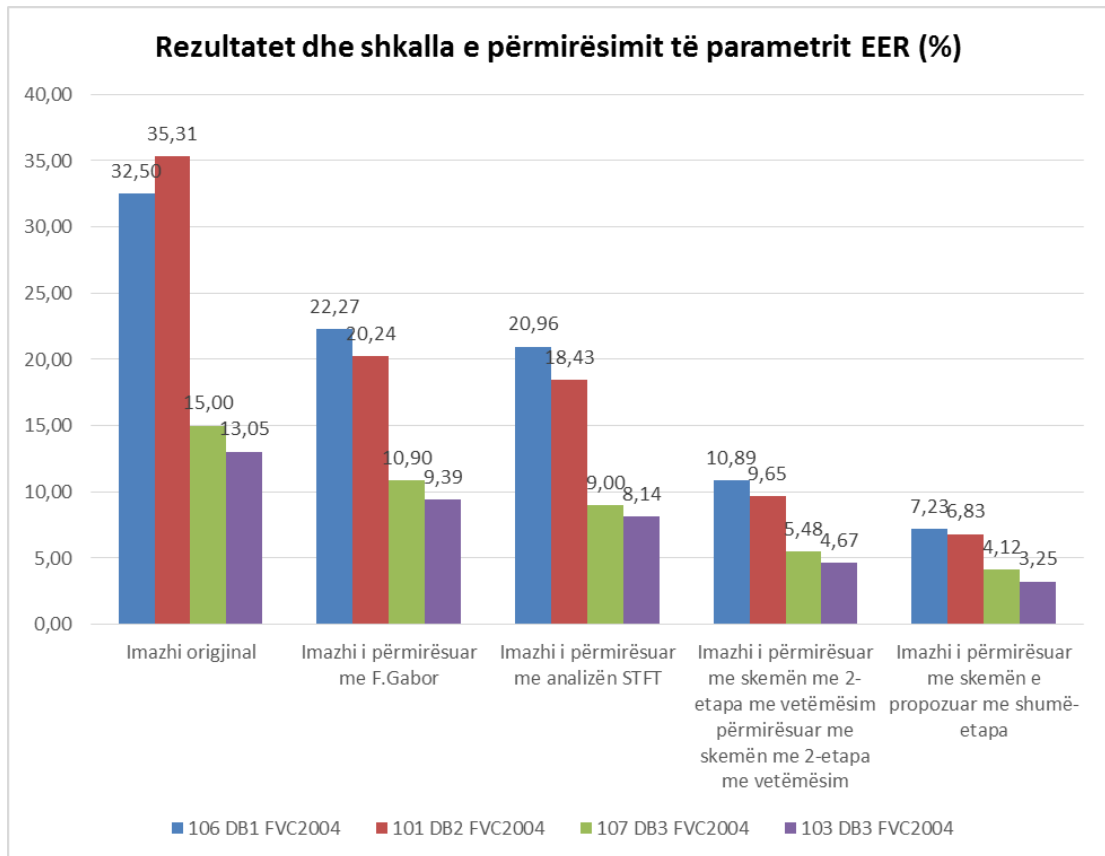


Figura 6.30. Krahasimi i rezultateve dhe shkallës së përmirësimit të parametrit EER(%)

Në tabelën 6-5 paraqiten vlerat e matura për kohën e nevojshme për leximin e imazhit në hyrje, përmirësimin e imazhit dhe ekstraktin e karakteristikave nga imazhi. Për imazhin origjinal koha e nevojshme për përpunim është ajo e leximit të imazhit në hyrje. Gjithashtu vërejmë se koha e nevojshme për përpunimin në skemën me shumë-etapa me bazë LPD është afro 1.5 -2.5 herë më e madhe se koha e matur me teknikat e tjera të përmirësimit.

Tabela 6-5 Koha e përpunimit të imazheve sipas teknikave të përmirësimit

Imazhet nga baza e të dhënave FVC 2004	Koha e përpunimit për Imazhin origjinal (sekonda)	Koha e përpunimit për Imazhin e përmirësuar me F.Gabor (sekonda)	Koha e përpunimit për Imazhin e përmirësuar me analizën STFT (sekonda)	Koha e përpunimit për Imazhin e përmirësuar me skemën me 2-etapa me vetëmësim (sekonda)	Koha e përpunimit për Imazhin e përmirësuar me skemën me shumë-etapa (sekonda)
103 FVC2004 DB1	0.9486	1.0789	1.0528	1.5026	2.9138
105 FVC2004 DB2	0.6637	0.9407	0.9378	1.3589	2.8239
102 FVC2004 DB3	0.7372	1.0124	1.0093	1.4587	2.8958
106 FVC2004 DB1	0.9235	1.0531	1.0425	1.4571	2.9654
101 FVC2004 DB2	0.7254	1.005	0.9974	1.4124	2.3254
107 FVC2004 DB3	0.8269	1.0324	1.2671	1.6853	2.8426
Koha mesatare e përpunimit	0.8042	1.0204	1.0512	1.4792	2.7945

Rezultatet e matura për kohën e përpunimit dhe krahasimi i tyre janë ilustruar dhe në grafikun e figurës 6-31.

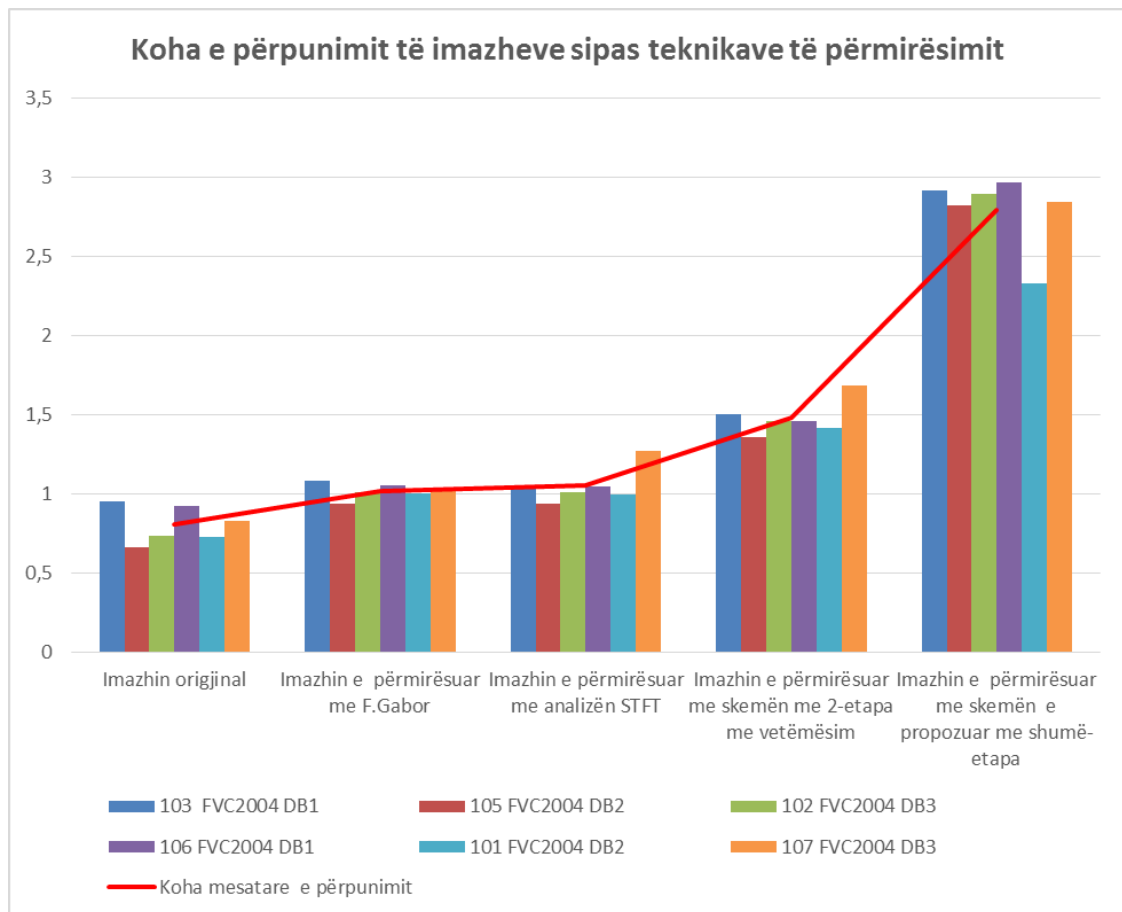


Figura 6-31. Grafiku i kohës mesatare për leximin, përpunimin e përmirësimit dhe ekstraktit të karakteristikave të imazheve

Në përfundim konstatohet se dyfishimi i kohës së përpunimit të procesit të përmirësimit të imazhit në skemën me shumë-etapa (LPD) ndikohet dhe rritet nga numri i shtuar i hallkave të përmirësimit në skemën me shumë-etapa me bazë LPD.

KAPITULLI 7

Përfundime dhe Objektiva

7.1 Përfundime të punimit

Në këtë punim, është realizuar:

- ***Në pjesën e parë***, është trajtuar analiza e metodave të avancuara të kontrollit për identifikimin dixhital, që mbulon çështjet teknike dhe të sigurisë me platformat, algoritmet, mekanizmat e sigurisë, sensorët dhe në mënyrë të veçantë ndërveprimin me teknologjitë e tjera.

Ndërkaq, janë dhënë dhe problemet dhe kufizimet e teknikave të trajtuara, në mënyrë më specifike:

- Analiza dhe vlerësimi i zgjidhjes më të frytshme, me teknikat e avancuara të kontrollit, për realizimin e identifikimit dixhital të saktë dhe të besueshëm të individëve;*
- Duke u nisur dhe nga eksperiencia modeste në këtë fushë, fokusi parësor i trajtimit në punim u orientua drejt sistemit kriptobiometrik të identifikimit dixhital, parametrat e performancës, vlerësimi i tyre, si dhe evidentimi i faktorëve që shqetësojnë më së shumti këto sisteme, ku më kryesoret janë:*
 - Saktësia (FMR/FNMR) e sistemit;
 - Mbrojtja e template-it biometrik;
 - Dedektimi i kërcënimeve të paraqitura.
- Ndërveprimi i sistemeve biometrike me kartat inteligjente dhe teknikën kriptografike, standartet, rekomandimet dhe vlerësimet ndërkombëtare të arritjeve në këtë fushë, duke marrë në studim në veçanti dhe vlerësuar disa raste studimore të zbatimit të zgjidhjes së integruar të teknologjive të avancuara të identifikimit dixhital me kartë inteligjente:*
 - Zgjidhja MoC me kartën inteligjente;
 - Identifikimi dixhital nëpërmjet Infrastrukturës së Çelësit publik (pasaporta elektronike)
 - shërbimet elektronike me përdorimin e kartës inteligjente (MoC) dhe Infrastrukturës së Çelësit Publik.

- **Në pjesën e dytë**, orientimi është fokusuar në analizën e teknikave të avancuara të përmirësimit të imazhit të gjurmës papilare, kjo pasi gjurmët papilare janë identifikuesit më të saktë universalë dhe unik në mes gjithë biometrive. Detyrat kryesore të kontrollit automatik në një sistem identifikimi më bazë gjurmën papilare janë :

- Ekstraktimi i saktë i karakteristikave të gjurmëve papilare;
- Krahasimi i gjurmëve papilare me anë të karakteristikave të ekstraktuara në mënyrë që të gjejme ngjashmërinë (përputhshmërinë) ndërmjet gjurmëve papilare të krahasuara.

Në lidhje me këto janë trajtuar dhe pohohen këto përfundime:

- a. Realizimi me saktësi i këtyre detyrave të sistemit varen tërësisht në cilësinë e imazhit të gjurmës papilare. Përmirësimi i imazhit të gjurmës papilare është teknika më e përdorur për të rritur saktësinë e ekstraktimit të karakteristikave dhe performancën e krahasimit në një sistem identifikimi me gjurmë papilare. Prania e vijave papilare të dëmtuara, njollave, rrudhave dhe vijat papilare jo të vërteta në imazhin e gjurmës papilare e bëjnë detyrën e përmirësimit një problem të vështirë.*
 - b. Shumë metoda janë propozuar nga studiues të ndryshëm për të tejkaluar këto vështirësi në mënyrë që të përmirësojmë cilësinë e imazheve të gjurmëve papilare. Mirëpo, këto skema përmirësimi kanë hasur një kompleksitet të shtuar në përmirësimin e imazheve të gjurmëve papilare, duke qenë se këto skema mbështeten në llogaritjen e karakteristikave kryesore (orientimi i vijës papilare, frekuenca e vijës papilare, etj). Në anën tjetër koha e llogaritjes ndikohet negativisht për shkak të nevojës për llogaritje të saktë të këtyre karakteristikave kryesore. Për më tepër, shumica e teknikave të përmirësimit përdorin teknikën e përpunimit të bllokut të imazhit dhe për këtë arsye cilësia e imazhit të gjurmës papilare vuan nga efekti i 'bllokut'.*
 - c. Ky punim ka pasur në fokus parësor studimin e teknikave të automatizuara të përmirësimit të imazhit të gjurmës papilare dhe vlerësimin në mënyrë specifike të teknikës më të frytshme ndërmjet katër të pranuar. Kjo, për faktin që, këto skema përmirësimi, jo vetëm të zgjidhin problemet e ngritura nga nevoja për vlerësim të saktë të karakteristikave kryesore të gjurmëve papilare, por edhe të trajtojnë në mënyrën efektive problemet e shfaqura nga përpunimi në bllok i imazheve të gjurmëve papilare.*
- **Në pjesën e tretë**, në mënyrë që të vlerësojmë arritjet dhe rendimentin e skemave të përmirësimit të analizuara, eksperimentet u realizuan me imazhe me cilësi të

ndryshme të gjurmëve papilare të bazës së të dhënave publike FVC2004. Me anë të parametrave të matur gjatë eksperimenteve(TMR, FMR, EER, etj) arrihet në përfundimin se të gjitha skemat e përmirësimit të zbatuara kanë një ndikim në rritjen e performancës së njohjes të teknikës së krahasimit të bazuar në minutiae, në përqindje më të lartë skema me shumë-etapa, e bazuar në LPD. Kështu:

- a. *Një përmirësim i dukshëm i kësaj skeme përmirësimi në krahasim me skemat e përmirësimit të vlerësuar është shmangia e zhurmës në nivel të lartë dhe përcaktimi i kufijve me saktësi me të madhe për karakteristikat e nivelit 1 dhe 2 të gjurmës papilare me cilësi të mesme dhe të ulët imazhi;*
- b. *Një mangësi e kësaj skeme që duhet zgjidhur në të ardhmen është koha më e madhe e përpunimit të imazhit, në krahasim me skemat e tjera të përmirësimit, kjo për shkak të shtimit të disa hallkave në skemën e përmirësimit.*

7.2 Objektiva për të ardhmen

Në vijim të punës së kryer, vëzhgimeve teorike, simulimeve dhe eksperimenteve, dhe veçanërisht praktikës së fituar nga aplikimet e ndryshme në kohë reale, kam arritur të evidentoj disa objektiva për punën në të ardhmen:

- *Në skemën me shumë-etapa që bazohet në piramidat e Laplas-it (LPD/LPR), të optimizojmë filtrin lejues për të përmirësuar etapën e dytë të skemës, e cila është një filtër në rrafshin e frekuencës;*
- *Në të ardhmen ne mund të përdorim një gjuhë programimi më të frytshme, në mënyrë që të përmirësojmë kohën e përpunimit të imazheve;*
- *Së fundmi, studiues të ndryshëm po shqyrtojnë identifikimin dhe ekstraktimin e karakteristikave të imazheve të gjurmëve papilare shumë sfiduese si gjurmët papilare latente, imazhi i të cilave në shumicën e rasteve përbëhet nga pjesë gjurmësh papilare të dobëta, në mes të një sfondi të strukturuar dhe të zhurmshëm. Parapërpunimi është i domosdoshëm për të segmentuar në mënyrë efektive zonën e gjurmës papilare nga sfondi dhe gjithashtu për të përmirësuar cilësinë e veçorive të dëmtuara të vijës/brazdës papilare. Skema me shumë-etapa e bazuar në LPD mund të përmirësohet për tu konsideruar si një fazë parapërpunimi për përmirësimin e imazheve të gjurmëve papilare latente. Në këtë drejtim mund të vazhdojë edhe ky punim të thellohet.*

LITERATURA

- [1] Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, may 2015
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- [2] Cristina Alcaraz and Sherali Zeadally. Critical control system protection in the 21st century: Threats and solutions. 2013.
- [3] Eric D Knapp and Raj Samani. Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure. Newnes, 2013.
- [4] Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A Frincke. Smart-grid security issues. Security & Privacy, IEEE, 8(1):81–85, 2010.
- [5] Ernst A. Hartmann, Marc Bovenschulte, ‘Skills Needs Analysis for “Industry 4.0” Based on Roadmaps for Smart Systems’, Institute for Innovation and Technology, Berlin, Germany, 2015
- [6] Public Interest Energy Research (PIER) Program INTERIM PROJECT REPORT: ‘Smart Grid Cyber Security potential threats, vulnerabilities and risks’, May 2012
- [7] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo , ‘Cyber-Physical Systems Security – A Survey’, 17February 2017.
- [8] A.K.Jain, S.Pankanti, S.Prabhakar, L.Hong, and A.Ross. Biometrics: ‘A grand challenge’. International Conference on Pattern Recognition (ICPR), 2:935–942, 2004.
- [9] J. Mahier, M.Pasquet, C.Rosenberger, and F.Cuozzo. Biometric authentication.
- [10] Encyclopedia of Information Science and Technology, pages 346–354, 2008.
- [11] ISO/IEC 19795-1. Information technology–biometric performance testing and reporting – part 1: Principles and framework, 2006.
- [12] G.Zhang and Y.Wang. Asymmetry-based quality assessment of face images. In Proceedings of the 5th International Symposium on Advances in Visual Computing (ISVC), volume 5876, pages 499–508, 2009.
- [13] N.Poh, J.V.Kittler and T.Bourlai. Quality-based score normalization with device qualitative information for multimodal biometric fusion. IEEE Transactions on Systems, Man, and Cybernetics, 40:539–554, 2010.
- [14] N.K.Ratha, J. H.Connell, and R.M.Bolle. An analysis of minutiae matching strength. In Audio- and Video-Based Biometric Person Authentication, pages 223–228, 2001.
- [15] T.V.der Putte and J.Keuning. Biometrical fingerprint recognition: Don’t get your fingers burned. In proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications, volume 31, pages 289–306, 2000.
- [16] D.Maltoni, D.Maio, A. K.Jain, and S.Prabhakar. Handbook of Fingerprint Recognition. Springer-Verlag, 2003.
- [17] U.Uludag and A.K.Jain. Attacks on biometric systems: A case study in fingerprints. In Proc.SPIE-EI 2004, Security, Segnography and Watermarking of Multimedia Contents VI, volume 5306, pages 622–633.
- [18] N.Poh, T.Bourlai, and J.Kittler. A multimodal biometric test bed for quality-dependent, cost-sensitive and client-specific score-level fusion algorithms. Pattern Recognition, pages 1094–1105, 2010.
- [19] ISO/IEC 29794-1. Biometric quality framework standard, first ed. jtc1/sc37/working group 3, 2006.
- [20] P.Grother and E.Tabassi. Performance of biometric quality measures. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29:531–543, 2007.
- [21] F.Alonso-Fernandez, J.Fierrez, J.Ortega-Garcia, J.Gonzalez-Rodriguez, H.Fronthaler, K.Kollreider and J.Bigun. A comparative study of fingerprint image-quality estimation methods. IEEE Transactions on Information Forensics and Security, 2:734–743, 2007.
- [22] L.Shen, A.C. Kot and W.M.Koo. Quality measures of fingerprint images. In Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pages 266–271, 2001.
- [23] Y.Chen, S.C.Dass and A.K.Jain. Fingerprint quality indices for predicting authentication performance. In 5th International Conference Audio- and Video-Based Biometric Person Authentication (AVBPA), volume 3546, pages 160–170, 2005.
- [24] S.Lee, C.Lee, and J.Kim. Model-based quality estimation of fingerprint images. In IAPR/IEEE International Conference on Biometrics (ICB’06), pages 229–235, 2006.
- [25] M E.Tabassi and C.L.Wilson. A novel approach to fingerprint image quality. In International Conference on Image Processing (ICIP), pages 37–40, 2005.
- [26] V Q. He, Z.A.Sun, T.N. Tan and Y.Zou. A hierarchical model for the evaluation of biometric sample quality. In International Conference on Pattern Recognition (ICPR), pages 1–4, 2008.
- [27] X.F. Gao, S.Z. Li, R. Liu, and P.R. Zhang. Standardization of face image sample quality. In International Conference on Biometrics (ICB’07), pages 242–251, 2007.
- [28] J.Sang, Z. Lei, and S.Z. Li. Face image quality evaluation for ISO/IEC standards 19794-5 and 29794-5. In Proceedings of the Third International Conference on Advances in Biometrics (ICB), pages 229–238, 2009. Real-time
- [29] ISO 13407:1999. Human centred design process for interactive systems, 1999.

-
- [30] M. El Abed, R.Giot, B.Hemery, C.Charrier and C.Rosenberger. A SVM-based model for the evaluation of biometric sample quality.In IEEE International Workshop on Computational Intelligence in Biometrics and Identity Management, pages 115–122, 2011.
 - [31] James P. Egan. Signal detection theory and ROC-analysis. by Academic Press, New York, 1975.
 - [32] BIOSECURE. Biosecure Multimodal Biometric Database. <http://www.biosecure.info/>, 2008.
 - [33] A. Mayoue, B. Dorizzi, L. Allano, G. Chollet, J. Hennebert, D. Petrovska-Delacr  taz and F. Verdet. Guide o biometric reference systems and performance evaluation, chapter The BioSecure multimodal evaluation campaign 2007 (BMEC'2007), pages 327–372. 2009..
 - [34] P.J.Phillips, P.J.Flynn, J.R.Beveridge, W.T.Scruggs, A.J.O'Toole, D.S.Bolme, K.W.Bowyer, B.A.Draper, G.H.Givens, Y.M.Lui, H.Sahibzada,J.A.Scallan,and S.Weimer.Overview of the multiple biometrics grand challenge. In International Conference on Biometrics (ICB'09), pages 705 – 714, 2009.
 - [35] S.Smith. Humans in the loop: Human computer interaction and security. IEEE Security & Privacy, 3:75–79, 2003.
 - [36] ORC. Public Attitudes Toward the Uses of Biometric Identification Technologiesby Government and the Private Sector. Technical report, Opinion Research Corporation International (ORC), 2002.
 - [37] M.Theofanos, B.Stanton, S.Orandi, R.Micheals, and N.F.Zhang. Usability testing of ten - print fingerprint capture.Technical report, National Institute of Standards and Technology (NIST),2007.
 - [38] M.Theofanos, B.Stanton, C.Sheppard, R.Micheals, N.Zhang, J.Wydler, L.Nadel, and W.Rubin.Usability testing of height and angles of ten-print fingerprint capture. Technical report, National Institute of Standards and Technology (NIST), 2008
 - [39] ISO/IEC 24745:2011
<https://www.iso.org/standard/52946.html>
 - [40] M. El Abed, R. Giot, B. Hemery, and C. Rosenberger. Evaluation of biometric systems: A study of users' acceptance and satisfaction. Inderscience International Journal of Biometrics, pages 1–26, 2011.
 - [41] L. Coventry, A. De Angeli, and G. Johnson. Honest it's me! self service verification. In The ACM Conference on Human Factors in Computing Systems (CHI), pages 1–4, 2003.
 - [42] S.J.Elliott, S. A. Massie, and M. J. Sutton. The perception of biometric technology: A survey Automatic Identification Advanced Technologies, pages 259–264, 2007.
 - [43] A. P. Pons and P. Polak. Understanding user perspectives on biometric technology.Communications of the Association for Computing Machinery (ACM), 51(9):115–118, 2008.
 - [44] M.El Abed, R.Giot, B.Hemery, and C.Rosenberger. A study of users' acceptance and satisfaction of biometric systems. In International Carnahan Conference on Security Technology (ICCST), pages 170–178, 2010.
 - [45] ISO/IEC FCD 19792. Information technology – security techniques – security evaluation of biometrics, 2008.
 - [46] Common criteria for information technology security evaluation. Technical report, 1999.
 - [47] C.Dimitriadis and D.Polemi. Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems. In international conference on biometric authentication (ICB), volume 3072, pages 724–730, 2004.
 - [48] O. Henniger, D.Scheuermann, and T. Kniess. On security evaluation of fingerprint recognition systems. In International Biometric Performance Testing Conference (IBPC), pages 1–10, 2010
 - [49] M. El Abed, P.Lacharme, and C.Rosenberger. Security evabio:An analysis tool for the security evaluation of biometric authentication systems. In the 5th IAPR/IEEE International Conference on Biometrics (ICB), pages 1–6, 2012.
 - [50] A.Ross, K. Nandakumar, , and A.K. Jain. Handbook of Multibiometrics. Springer, 2006.
 - [51] A.Azzini, S.Marrara, R.Sassi, and F.Scotti. A fuzzy approach to multimodal biometric authentication. In Knowledge-Based Intelligent Information and Engineering Systems, number 8, pages 801–808, 2007.
 - [52] A.K.Jain, K.Nandakumar, and A.Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008:1–17, 2007.
 - [53] A.Juels and M.Wattenberg. A fuzzy commitment scheme. In ACM Conference on Computer and Communication Security, pages 28–36, 1999.
 - [54] A. Juels and M. Sudan. A fuzzy vault scheme. In IEEE International Symposium on Information Theory, pages 237–257, 2001.
 - [55] R. Belguechi, C. Rosenberger, and S.A. Aoudia. Biohashing for securing minutia template.In Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10), pages 1168–1171, 2010.
 - [56] J. Lee, L. Goldman, and T. Ebrahimi. A new analysis method for paired comparison and its application to 3d quality assessment. In Proceedings of the 19th ACM International Conference on Multimedia, pages 1281– 1284, 2011.
 - [57] ANSI INCITS 378.Information technology - Finger Minutiae Format for Data Inter- change, 2004.
 - [58] Claude Barral and Serge Vaudenay. A protection scheme for moc-enabled smart cards.IEEE - Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research, 2006.
 - [59] Bir Bhanu and Xuejun Tan. Fingerprint indexing based on novel features of minutiae triplets. IEEE Trans.Pattern Anal. Mach. Intell., 25(5):616–622, 2003.
 - [60] HAO FENG , A Cryptosystem With Private Key Generation From Dynamic Properties of Human Hand Signature , 2002
 - [61] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni. Fingerprint image reconstruction from standard templates.IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9):1489–1503, 2007.
-

-
- [62] D. Cooper, H.Dang, P.Lee, W.MacGregor, and K. Mehta. Secure biometric match-on- card feasibility report - nistir 7452. Technical report, National Institute of Standards and Technology, 2007.
 - [63] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory,22: 644–654, 1976.
 - [64] P. Grother and W. Salamon. Performance of fingerprint match-on-card algorithms evaluation plan- nistir 7485. Technical report, National Institute of Standards and Technology, 2007.
 - [65] P. Grother and et al. Performance of fingerprint match-on-card algorithms - nistir 7477.Technical report, National Institute of Standards and Technology, 2008, 2009.
 - [66] P. Grother and et al. Performance and interoperability 378 fingerprint template – nistir 7296. Technical report, National Institute of Standards and Technology, 2006.
 - [67] ICAO. Annex 1 - Use of Contactless Integrated Circuits. Technical report, May 2004. Available at <http://www.icao.int/mrtd/download/documents/Annexs.pdf>.
 - [68] ICAO. Biometrics deployment for Machine Readable Travel Documents.Technical report, May 2004. Available at <http://www.icao.int/mrtd/download/documents>.
 - [69] ICAO.PKI for Machine Readable Travel Documents offering ICC read-only access.Technical report, Oct. 2004. Available at <http://www.icao.int/mrtd/download/documents/TR-PKI>
 - [70] A. Menezes, P. Van Oorschot, and S. Vanstone. Handbook of Applied Cryptography.The CRC Press series on discrete mathematics and its applications. CRC-Press, 1997.
 - [71] Douglas Stinson. Cryptography - Theory and Practice - 2nd edition. Chapman & Hall / CRC, 2002.
 - [72] Serge Vaudenay. A Classical Introduction to Cryptography: Applications for Communications Security.Springer, 2005.
 - [73] Home Page of NIST: <https://www.nist.gov/>
 - [74] A. K.Jain, A. A.Ros, and K.NandaKumar, “Introduction to Biometrics”, Springer, 2011.
 - [75] S. C. Lee, “An Introduction to Identity Management”, SANS Institute, March 2003
 - [76] Article by V.Matys and Z.Riha on ‘Biometric Authentication – Security and Usability’: http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf
 - [77] A. K.Jain, A.Ross, and S.Pankanti, “Biometrics: A tool for information security,” IEEE Trans. Info.Forensics Security, vol. 1, no. 2, pp. 125–143, June 2006.
 - [78] Article on the Overview of Biometrics.
<http://www.biometrics.gov/Documents/BioOverview.pdf>
 - [79] Article on the future of Biometrics.
<http://www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification/>
 - [80] Article on types of Biometrics
<http://www.tns.com/biometrics.asp>.
 - [81] D. Kumar and Y. Ryu, “A Brief Introduction of Biometrics and Fingerprint Payment Technology,” International Journal of Advanced Science and Technology, vol. 4, pp. 25–37, March 2009.
 - [82] Nagar A, Nandakumar K, Jain A: A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recogn Lett 2010, 31:733-741.
 - [83] Dodis Y, Ostrovsky R, Reyzin L, Smith A: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data. Proc Eurocrypt 2004, 2004:523-540, (LNCS: 3027).
 - [84] Juels A, Wattenberg M: A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security 1999, 28-36.
 - [85] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: Biometric encryption using image processing. Proc SPIE, Optical Security and Counterfeit Deterrence Techniques II 1998, 3314:178-188.
 - [86] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV: Biometric encryption, ICSA Guide to Cryptography. 1999.
 - [87] Hao F, Anderson R, Daugman J: Combining cryptography with biometrics effectively. IEEE Trans Comput 2006, 55(9):1081-1088.
 - [88] Zhang L, Sun Z, Tan T, Hu S: Robust biometric key extraction based on iris cryptosystem. Proc of the 3rd Int Conf on Biometrics 2009 (ICB'09) 2009, 1060-1070, LNCS: 5558.
 - [89] Teoh A, Kim J: Secure biometric template protection in fuzzy commitment scheme. IEICE Electron Express 2007, 4(23):724-730.
 - [90] Nandakumar K: A fingerprint cryptosystem based on minutiae phase spectrum. Proc of IEEE Workshop on Information Forensics and Security (WIFS) 2010
 - [91] Clancy TC, Kiyavash N, Lin DJ: Secure smartcard-based fingerprint authentication. Proc ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop 2003, 45-52.
 - [92] Li P, Yang X, Cao K, Tao X, Wang R, Tian J: An alignment free fingerprint cryptosystem based on fuzzy vault scheme. J Netw Comput Appl 2010, 33:207-220.
 - [93] Nagar A, Nandakumar K, Jain AK: Securing fingerprint template: Fuzzy vault with minutiae descriptors. Int Conf on Pattern Recognition (ICPR'08). IEEE 2008, 1-4.
 - [94] Dutta S., Kar A., Mahanti N.C., Chatterji B.N. (2008) Network Security Using Biometric and Cryptography. In: Blanc-Talon J., Bourennane S., Philips W., Popescu D., Scheunders P. (eds) Advanced Concepts for Intelligent Vision Systems. ACIVS 2008. Lecture Notes in Computer Science, vol 5259. Springer, Berlin, Heidelberg
-

-
- [95] Arakala A: Secure and private fingerprint-based authentication. Bull Aust Math Soc 2009, 80:347-349
 - [96] L. Hong, A.K. Jain, S. Pankanti, and R. Bolle, "Fingerprint Enhancement," Proc.First IEEE WACV, pp. 202- 207, Sarasota, Fla.,1996.
 - [97] L. Hong, Y. Wan, and A.K. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation".IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789, Aug. 1998.
 - [98] K.R.Rao, D.N.Kim and J.J.Hwang, "Fast Fourier transform: Algorithms and applications", Heidelberg,Germany: Springer 2010.
 - [99] S.Chikkerur, A.N.Cartwright, and V.Govindaraju,"Fingerprint enhancement using STFT analysis", IEEE Transactions on Pattern Recognition, vol. 40, no. 1, pp. 198–211, Jan. 2007.
 - [100] K.G.Darpanis, "Gabor Filters", York University, April 2007.
 - [101] A Jagadeesan, T.Thillaikkarasi and Dr.K.Duraiswamy. Article:Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature. International Journal of Computer Applications 2(6):16–26, June 2010
 - [102] J.Yang, N. Xiong, and A. V. Vasilakos, "Two-stage enhancement scheme for low- quality fingerprint images by learning from the images", IEEE transactions on Human-Machine Systems, vol. 43, no. 2, pp. 235-248, Mar.2013.
 - [103] A Jagadeesan A & R.M.Madhumathi (2015), "EER Analysis of MultimodalBiometric Identification System" Proceedings of International Journal of Research in Electronics (IJRE) Vol. 02, Issue 02, PP: 07-12
 - [104] Fabian Monrose, Michael K. Reiter, Q. (Peter) Li , Susanne Wetzel. Cryptographic Key Generation From Voice. In Proceedings of the IEEE Conference on Security and Privacy, Oakland, CA. May, 2001
 - [105] A. K. Jain, "Fundamentals of Digital Image Processing", Englewood Cliffs, NJ: Prentice Hall, 1989.
 - [106] R.C. Gonzalez and R.E. Woods, "Digital Image Processing", 3rd edition, Prentice Hall, 2007.
 - [107] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Trans. Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.
 - [108] D.K. Misra, S.P. Tripathi and D. Misra, "A Review Report on Fingerprint Image Enhancement Techniques". International Journal of Emerging Trends & Technology in Computer Science, vol. 2, no. 2, pp. 224-230,April 2013.
 - [109] S.Greenberg, M.Aladjem, D.Kogan, and I.Dimitrov, "Fingerprint image enhancement using filtering techniques", ICPR, Vol. 3, pp. 326–329, Sep. 2000.
 - [110] Fingerprint Verification Competition database:
<http://bias.csr.unibo.it/fvc2004/download.asp>
 - [111] Article on Gabor filter: http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/TRAPP1/filter.html
 - [112] MS thesis paper by S.Chakraborty on 'Fingerprint enhancement by directional filtering'.
http://www.uta.edu/faculty/kr Rao/dip/Courses/EE5359/Shreya_Paper_v6.pdf
 - [113] MS thesis paper by R.V.VENKATA on 'Multistage Enhancement Scheme for low quality fingerprint images'
<http://www.cs.toronto.edu/~jepson/csc320/notes/pyramids.pdf>
 - [114] R.C. Gonzalez, R.E. Woods and S.L. Eddins, "Digital Image Processing Using MATLAB", 2nd edition, McGraw Hill Education, 2010.
 - [115] P.J. Burt and E.H. Adelson, "The Laplacian Pyramid as a Compact Image Code",IEEE Transactions on Communications, vol. 31, no. 4, pp. 532-540, Apr. 1983.
 - [116] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of fingerprint recognition". Springer, 2003.
 - [117] H. F. D. Kunz, K. Eck, and T. Aach, "A Nonlinear Multi-Resolution Gradient-Adaptive Filter for Medical Images", In SPIE Medical Imaging, volume 5032, pages 732–742, May 2003.
 - [118] A. Jepson, "Notes on Image Pyramids to attenuate noise":
 - [119] <http://www.cs.toronto.edu/~jepson/csc320/notes/pyramids.pdf>
 - [120] H. Fronthaler, K. Kollreider, and J. Bigun, "Local features for enhancement and minutiae extraction in fingerprints," IEEE Trans. Image Process., vol. 17, no. 3, pp. 354–363, Mar. 2008.
 - [121] P.K. Shimna and B. Neethu, "Fingerprint Image Enhancement Using STFT Analysis", IOSR Journal of Electronics and Communication Engineering, vol. 10, Issue 2, pp. 61-68, Apr. 2015.
 - [122] Z. Shi and V. Govindaraju, "A chaincode based scheme for fingerprint feature extraction," IEEE Transactions on Pattern Recognition, vol. 27, no. 5, pp. 462–468, Apr. 2006.
 - [123] Matlab: <http://www.mathworks.com/downloads/>
 - [124] Fingerprint Recognition v2.2 software
<http://www.codeproject.com/Articles/97590/A-Framework-in-C-for-Fingerprint-Verification>
 - [125] Fingerprint minutiae extraction code by N.S. Athi:http://www.mathworks.com/matlabcentral/fileexchange/31926-fingerprint-minutiae-extraction/content/Fingerprint_Minutiae_Extraction/Minutiae_Extraction.m
 - [126] O. Marques, "Practical Image and Video Processing Using MATLAB",1st Edition, Wiley-IEEE Press, 2011.
 - [127] Multimedia processing course website: <http://www.uta.edu/faculty/kr Rao/dip/>
 - [128] Visual studio: <http://www.dreamspark.com>
 - [129] Miranda HARIZAJ, Petrika MARANGO,"Preventing identity fraud by using biometric control system security mechanisms", The International Journal of Science, Innovation and New Technology, Vol.1.No.14, ISSN 2223-2257
 - [130] Miranda HARIZAJ "Building and implementing an robust Digital Identity System", Pavaresia Scientific Journal, Volume 2 No.2(3), 2016, ISSN 2304-2664;
 - [131] Miranda HARIZAJ " Enhancing Security and Privacy of Biometric Systems", IJCSMS (International Journal of Computer Science & Management Studies) Vol. 32, Issue 01, ISSN (Online): 231–5268.
 - [132] Miranda HARIZAJ, Mirela BOGDANI, "Albania ID card usage next indoor challenge for providing e- Government Services in line with EU-Standards" Scientific International Conference, Faculty of Economy, University of
-

- Tirana,” Economic and social challenges 2011, globalization and sustainable development”, 9-10 December 2011, Tirana, Albania, ISBN-978-99956-95-26-2
- [133] Miranda HARIZAJ, "An proposal for enhancing security in smart cards using biometric technology", Konferenca e 3-te Nderkombetare "Sfidat e transformimit te Shoqerise Shqiptare drejt Standarteve te Bashkimit European", 9 Dhjetor 2016, ISSN-2520-0399
- [134] ISO/IEC 7816-4:2013
<https://www.iso.org/standard/54550.html>

SHTOJCA

Kode në MATLAB

Ekstraktimi i minutiae-ve të gjurmëve papilare

```
%Program for Fingerprint Minutiae Extraction
%
%Author : Athi Narayanan S
%Senior Research Associate
%http://sites.google.com/site/athisnarayanan/
%s_athi1983@yahoo.co.in
%
%Program Description
%This program extracts the ridges and bifurcation from a fingerprint
image

%Read Input Image
binary_image=im2bw(imread('input_1.tif'));

%Small region is taken to show output clear
binary_image = binary_image(120:400,20:250);
figure;imshow(binary_image);title('Input image');

%Thinning
thin_image=~bwmorph(binary_image,'thin',Inf);
figure;imshow(thin_image);title('Thinned Image');

%Minutiae extraction
s=size(thin_image);
N=3;%window size
n=(N-1)/2;
r=s(1)+2*n;
c=s(2)+2*n;
double temp(r,c);
temp=zeros(r,c);bifurcation=zeros(r,c);ridge=zeros(r,c);
temp((n+1):(end-n),(n+1):(end-n))=thin_image(:,:);
outImg=zeros(r,c,3);%For Display
outImg(:,:,1) = temp .* 255;
outImg(:,:,2) = temp .* 255;
outImg(:,:,3) = temp .* 255;
for x=(n+1+10):(s(1)+n-10)
    for y=(n+1+10):(s(2)+n-10)
        e=1;
        for k=x-n:x+n
            f=1;
            for l=y-n:y+n
```

```
        mat(e,f)=temp(k,l);
        f=f+1;
    end
    e=e+1;
end;
if(mat(2,2)==0)
    ridge(x,y)=sum(sum(~mat));
    bifurcation(x,y)=sum(sum(~mat));
end
end;
end;

% RIDGE END FINDING
[ridge_x ridge_y]=find(ridge==2);
len=length(ridge_x);
%For Display
for i=1:len
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),2:3)=0;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;

    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),1)=255;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
end

%BIFURCATION FINDING
[bifurcation_x bifurcation_y]=find(bifurcation==4);
len=length(bifurcation_x);
%For Display
for i=1:len
    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),1:2)=0;
    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),1:2)=0;

    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),3)=255;
    outImg((bifurcation_x(i)-
3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-
3):(bifurcation_y(i)+3),3)=255;
end
figure;imshow(outImg);title('Minutiae');
```

Korrelacioni duke përdorur FFT

```
% work: calculate the max correlation
% parameters: basic image and a template image
% output: max correlation between the basic and template image

function maxCorrelation=correlationFFT(bIm,tIm)

tIm = rot90(tIm,2);
if (size(bIm,2) >= size(tIm,2))
    ComWidth = size(bIm,2);
else
    ComWidth = size(tIm,2);
end;

if (size(bIm,1) >= size(tIm,1))
    ComHeight = size(bIm,1);
else
    ComHeight = size(tIm,1);
end;

M = sym(log2(ComWidth));
N = sym(log2(ComHeight));
if (frac(M)~=0)
    M = ceil(M);
    ComWidth = int8(2^M);
end;
if (frac(N)~=0)
    N = ceil(N);
    ComHeight = int8(2^N);
end;

bIm(ComHeight,ComWidth) = 0;
tIm(ComHeight,ComWidth) = 0;

FbIm = fft2(bIm);
FtIm = fft2(tIm);
FResult = FbIm.*FtIm;
corrlIm = ifft2(FResult);

maxCorrelation = max(corrlIm(:))/sqrt(sum(bIm(:))*sum(tIm(:)));
```

Përmirësimi i imazheve gri

```
% DIP assignment - 5
% Question - 3
% Name - Sanyam Sharma
```



```
% Roll No. - 200101072
%
clear;
img_name = input('Enter the image name (grayscale) :','s');
img = imread(img_name);
size_img = size(img);

%Adaptive histogram equaliztion
global_res = histeq(img);
res_image = img;
threshold = 20;

% for ..... Adaptive Histogram Equalization .....

for i = 2:size_img(1)-1
    for j = 2:size_img(2)-1
        deviation = std(double(img(i-1:i+1,j-1:j+1)));
        if abs(double(img(i,j)) - double(deviation)) > threshold
            res_image(i,j) = global_res(i,j);
        end
    end
end

fprintf('\n saving image to pics/img_adpHist.jpg \n');
imwrite(res_image,'pics/img_adpHist.jpg','jpg');

% for ..... Homomorphic Filtering .....

img_fft = fft2(log(double(img) + 1 ));

size_img = size(img_fft);

lpf = [1 1 1;1 1 1;1 1 1]/9;
hpf = [-1 -1 -1;-1 8 -1;-1 -1 -1]/9;
lpf_fft = fft2 ( lpf , size_img ( 1 ) , size_img ( 2 ) );
result_fft = img_fft .* lpf_fft;
result_img = exp ( ifft2(result_fft) ) ;

fprintf ( '\n saving image to pics/img_homomorphic.jpg \n' );
imwrite ( uint8(real ( result_img )) ,
'pics/img_homomorphic.jpg' , 'jpg' );

% for ..... Adaptive Contrast Enhancement .....

res_image = img;
constant = 1.5;
for i = 2:size_img(1)-1
    for j = 2:size_img(2)-1
        deviation = std(double(img(i-1:i+1,j-1:j+1)));
```

```
        if abs(double(img(i,j)) - double(deviation)) >
threshold
            res_image(i,j) = double(img(i,j)) * constant ;
        end
    end
end
fprintf('\n saving image to pics/img_adpContrast.jpg \n');
imwrite(res_image,'pics/img_adpContrast.jpg','jpg');
```

Edge detection of greylevel image

```
function func_ant_colony_image_edge_detection
%
%
% This is a demo program of image edge detection using ant colony,
based on
% the paper, "An Ant Colony Optimization Algorithm For Image Edge
% Detection," IEEE Congress on Evolutionary Computation (CEC), pp.
751-756, Hongkong,
% Jun. 2008.
%
%
%
% Input:
% gray image with a square size
%
% Output:
% four edge map images, which are obtained by the method using four
functions,
% respectively.
%
% image loading
filename = 'camera128';

img = double(imread([filename '.bmp']))./255;
[nrow, ncol] = size(img);

%visiblity function initialization, see equation (4)

for nMethod = 1:4;
    %Four kernel functions used in the paper, see equations (7)-(10)
    %E: exponential; F: flat; G: gaussian; S:Sine; T:Turkey; W:Wave
    fprintf('Welcome to demo program of image edge detection using
ant colony.\nPlease wait.....\n');

    v = zeros(size(img));
    v_norm = 0;
    for rr =1:nrow
        for cc=1:ncol
            %defination of clique
```

```
temp1 = [rr-2 cc-1; rr-2 cc+1; rr-1 cc-2; rr-1 cc-1; rr-1  
cc; rr-1 cc+1; rr-1 cc+2; rr cc-1];  
temp2 = [rr+2 cc+1; rr+2 cc-1; rr+1 cc+2; rr+1 cc+1; rr+1  
cc; rr+1 cc-1; rr+1 cc-2; rr cc+1];  
  
temp0 = find(temp1(:,1)>=1 & temp1(:,1)<=nrow &  
temp1(:,2)>=1 & temp1(:,2)<=ncol & temp2(:,1)>=1 & temp2(:,1)<=nrow &  
temp2(:,2)>=1 & temp2(:,2)<=ncol);  
  
temp11 = temp1(temp0, :);  
temp22 = temp2(temp0, :);  
  
temp00 = zeros(size(temp11,1));  
for kk = 1:size(temp11,1)  
    temp00(kk) = abs(img(temp11(kk,1), temp11(kk,2)) -  
img(temp22(kk,1), temp22(kk,2)));  
end  
  
if size(temp11,1) == 0  
    v(rr, cc) = 0;  
    v_norm = v_norm + v(rr, cc);  
else  
    lambda = 10;  
    switch nMethod  
  
        case 1%'F'  
            temp00 = lambda .* temp00;  
  
        case 2%'Q'  
            temp00 = lambda .* temp00.^2;  
  
        case 3%'S'  
            temp00 = sin(pi .* temp00./2./lambda);  
  
        case 4%'W'  
            temp00 =  
sin(pi.*temp00./lambda).*pi.*temp00./lambda;  
            end  
  
        v(rr, cc) = sum(sum(temp00.^2));  
        v_norm = v_norm + v(rr, cc);  
    end  
end  
end  
  
v = v./v_norm; %do normalization  
v = v.*100;  
% pheromone function initialization  
p = 0.0001 .* ones(size(img));  
  
%paramete setting, see Section IV in CEC paper  
alpha = 1; %equation (4)
```

```
beta = 0.1;      %equation (4)
rho = 0.1;      %equation (11)
phi = 0.05;     %equation (12), i.e., (9) in IEEE-CIM-06

ant_total_num = round(sqrt(nrow*ncol));

ant_pos_idx = zeros(ant_total_num, 2); % record the location of
ant

% initialize the positions of ants

rand('state', sum(clock));
temp = rand(ant_total_num, 2);
ant_pos_idx(:,1) = round(1 + (nrow-1) * temp(:,1)); %row index
ant_pos_idx(:,2) = round(1 + (ncol-1) * temp(:,2)); %column index

search_clique_mode = '8'; %Figure 1

% define the memory length, the positions in ant's memory are
% non-admissible positions for the next movement

if nrow*ncol == 128*128
    A = 40;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
elseif nrow*ncol == 256*256
    A = 30;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
elseif nrow*ncol == 512*512
    A = 20;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
end

% record the positions in ant's memory, convert 2D position-index
(row, col) into
% 1D position-index
ant_memory = zeros(ant_total_num, memory_length);

% System setup
if nrow*ncol == 128*128
    total_step_num = 300; % the numbe of iterations?
elseif nrow*ncol == 256*256
    total_step_num = 900;
elseif nrow*ncol == 512*512
    total_step_num = 1500;
end

total_iteration_num = 3;
```

```
for iteration_idx = 1: total_iteration_num

    %record the positions where ant have reached in the last
    'memory_length' iterations
    delta_p = zeros(nrow, ncol);

    for step_idx = 1: total_step_num

        delta_p_current = zeros(nrow, ncol);

        for ant_idx = 1:ant_total_num

            ant_current_row_idx = ant_pos_idx(ant_idx,1);
            ant_current_col_idx = ant_pos_idx(ant_idx,2);

            % find the neighborhood of current position
            if search_clique_mode == '4'
                rr = ant_current_row_idx;
                cc = ant_current_col_idx;
                ant_search_range_temp = [rr-1 cc; rr cc+1; rr+1
cc; rr cc-1];
            elseif search_clique_mode == '8'
                rr = ant_current_row_idx;
                cc = ant_current_col_idx;
                ant_search_range_temp = [rr-1 cc-1; rr-1 cc; rr-1
cc+1; rr cc-1; rr cc+1; rr+1 cc-1; rr+1 cc; rr+1 cc+1];
            end

            %remove the positions our of the image's range
            temp = find(ant_search_range_temp(:,1)>=1 &
ant_search_range_temp(:,1)<=nrow & ant_search_range_temp(:,2)>=1 &
ant_search_range_temp(:,2)<=ncol);
            ant_search_range = ant_search_range_temp(temp, :);

            %calculate the transit prob. to the neighborhood of
            current

            %position
            ant_transit_prob_v =
zeros(size(ant_search_range,1),1);
            ant_transit_prob_p =
zeros(size(ant_search_range,1),1);

            for kk = 1:size(ant_search_range,1)

                temp = (ant_search_range(kk,1)-1)*ncol +
ant_search_range(kk,2);

                if length(find(ant_memory(ant_idx,')==temp))==0
%not in ant's memory

                    ant_transit_prob_v(kk) =
v(ant_search_range(kk,1), ant_search_range(kk,2));
```

```
        ant_transit_prob_p(kk) =  
p(ant_search_range(kk,1), ant_search_range(kk,2));  
        else %in ant's memory  
            ant_transit_prob_v(kk) = 0;  
            ant_transit_prob_p(kk) = 0;  
        end  
    end  
  
    % if all neighborhood are in memory, then the  
    permissible search range is RE-calculated.  
    if (sum(sum(ant_transit_prob_v))==0) |  
    (sum(sum(ant_transit_prob_p))==0)  
        for kk = 1:size(ant_search_range,1)  
            temp = (ant_search_range(kk,1)-1)*ncol +  
ant_search_range(kk,2);  
            ant_transit_prob_v(kk) =  
v(ant_search_range(kk,1), ant_search_range(kk,2));  
            ant_transit_prob_p(kk) =  
p(ant_search_range(kk,1), ant_search_range(kk,2));  
        end  
    end  
  
    ant_transit_prob = (ant_transit_prob_v.^alpha) .*  
(ant_transit_prob_p.^beta) ./ (sum(sum((ant_transit_prob_v.^alpha) .*  
(ant_transit_prob_p.^beta))));  
  
    % generate a random number to determine the next  
position.  
    rand('state', sum(100*clock));  
    temp = find(cumsum(ant_transit_prob)>=rand(1), 1);  
  
    ant_next_row_idx = ant_search_range(temp,1);  
    ant_next_col_idx = ant_search_range(temp,2);  
  
    if length(ant_next_row_idx) == 0  
        ant_next_row_idx = ant_current_row_idx;  
        ant_next_col_idx = ant_current_col_idx;  
    end  
  
    ant_pos_idx(ant_idx,1) = ant_next_row_idx;  
    ant_pos_idx(ant_idx,2) = ant_next_col_idx;  
  
    %record the delta_p_current  
    delta_p_current(ant_pos_idx(ant_idx,1),  
ant_pos_idx(ant_idx,2)) = 1;  
  
    % record the new position into ant's memory  
    if step_idx <= memory_length  
  
        ant_memory(ant_idx,step_idx) =  
(ant_pos_idx(ant_idx,1)-1)*ncol + ant_pos_idx(ant_idx,2);
```

```

elseif step_idx > memory_length
    ant_memory(ant_idx,:) =
circshift(ant_memory(ant_idx,:),[0 -1]);
    ant_memory(ant_idx,end) =
(ant_pos_idx(ant_idx,1)-1)*ncol + ant_pos_idx(ant_idx,2);

end

%update the pheromone function (10) in IEEE-CIM-06
p = ((1-rho).*p +
rho.*delta_p_current.*v).*(delta_p_current + p.*(abs(1-
delta_p_current)));

end % end of ant_idx

% update the pheromone function see equation (9) in IEEE-
CIM-06

delta_p = (delta_p + (delta_p_current>0))>0;

p = (1-phi).*p; %equation (9) in IEEE-CIM-06

end % end of step_idx

end % end of iteration_idx

% generate edge map matrix
% It uses pheromone function to determine edge?

T = func_separate_two_class(p); %eq. (13)-(21), Calculate the
threshold to separate the edge map into two class

fprintf('Done!\n');
imwrite(uint8(abs((p>=T).*255-255)), gray(256), [filename
'_edge_aco_' num2str(nMethod) '.bmp'], 'bmp');

end % end of nMethod

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Inner Function
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

function level = func_separate_two_class(I)
% ISODATA Compute global image threshold using iterative isodata
method.
% LEVEL = ISODATA(I) computes a global threshold (LEVEL) that can
be
% used to convert an intensity image to a binary image with IM2BW.
LEVEL
% is a normalized intensity value that lies in the range [0, 1].

```

```
% This iterative technique for choosing a threshold was developed
by Ridler and Calvard .
% The histogram is initially segmented into two parts using a
starting threshold value such as  $0 = 2B-1$ ,
% half the maximum dynamic range.
% The sample mean (mf,0) of the gray values associated with the
foreground pixels and the sample mean (mb,0)
% of the gray values associated with the background pixels are
computed. A new threshold value 1 is now computed
% as the average of these two sample means. The process is
repeated, based upon the new threshold,
% until the threshold value does not change any more.
%
% Reference :T.W. Ridler, S. Calvard, Picture thresholding using an
iterative selection method,
% IEEE Trans. System, Man and Cybernetics, SMC-8 (1978)
630-632.

% Convert all N-D arrays into a single column. Convert to uint8 for
% fastest histogram computation.

I = I(:);

% STEP 1: Compute mean intensity of image from histogram, set
T=mean(I)
[counts, N]=hist(I,256);
i=1;
mu=cumsum(counts);
T(i)=(sum(N.*counts))/mu(end);

% STEP 2: compute Mean above T (MAT) and Mean below T (MBT) using T
from
% step 1
mu2=cumsum(counts(N<=T(i)));
MBT=sum(N(N<=T(i)).*counts(N<=T(i)))/mu2(end);

mu3=cumsum(counts(N>T(i)));
MAT=sum(N(N>T(i)).*counts(N>T(i)))/mu3(end);
i=i+1;
T(i)=(MAT+MBT)/2;

% STEP 3 to n: repeat step 2 if T(i)~=T(i-1)
Threshold=T(i);
while abs(T(i)-T(i-1))>=1
    mu2=cumsum(counts(N<=T(i)));
    MBT=sum(N(N<=T(i)).*counts(N<=T(i)))/mu2(end);

    mu3=cumsum(counts(N>T(i)));
    MAT=sum(N(N>T(i)).*counts(N>T(i)))/mu3(end);

    i=i+1;
    T(i)=(MAT+MBT)/2;
```



```
    Threshold=T(i);  
end  
  
% Normalize the threshold to the range [i, 1].  
level = Threshold;
```

Edge detection of greylevel image

```
function func_ant_colony_image_edge_detection  
%  
%  
% This is a demo program of image edge detection using ant colony,  
based on  
% the paper, "An Ant Colony Optimization Algorithm For Image Edge  
% Detection," IEEE Congress on Evolutionary Computation (CEC), pp.  
751-756, Hongkong,  
% Jun. 2008.  
%  
%  
%  
% Input:  
% gray image with a square size  
%  
% Output:  
% four edge map images, which are obtained by the method using four  
functions,  
% respectively.  
%  
  
% image loading  
filename = 'camera128';  
  
img = double(imread([filename '.bmp']))./255;  
[nrow, ncol] = size(img);  
  
%visiblity function initialization, see equation (4)  
  
for nMethod = 1:4;  
    %Four kernel functions used in the paper, see equations (7)-(10)  
    %E: exponential; F: flat; G: gaussian; S:Sine; T:Turkey; W:Wave  
  
    fprintf('Welcome to demo program of image edge detection using  
ant colony.\nPlease wait.....\n');  
  
    v = zeros(size(img));  
    v_norm = 0;  
    for rr =1:nrow  
        for cc=1:ncol  
            %defination of clique
```

```
temp1 = [rr-2 cc-1; rr-2 cc+1; rr-1 cc-2; rr-1 cc-1; rr-1  
cc; rr-1 cc+1; rr-1 cc+2; rr cc-1];  
temp2 = [rr+2 cc+1; rr+2 cc-1; rr+1 cc+2; rr+1 cc+1; rr+1  
cc; rr+1 cc-1; rr+1 cc-2; rr cc+1];  
  
temp0 = find(temp1(:,1)>=1 & temp1(:,1)<=nrow &  
temp1(:,2)>=1 & temp1(:,2)<=ncol & temp2(:,1)>=1 & temp2(:,1)<=nrow &  
temp2(:,2)>=1 & temp2(:,2)<=ncol);  
  
temp11 = temp1(temp0, :);  
temp22 = temp2(temp0, :);  
  
temp00 = zeros(size(temp11,1));  
for kk = 1:size(temp11,1)  
    temp00(kk) = abs(img(temp11(kk,1), temp11(kk,2)) -  
img(temp22(kk,1), temp22(kk,2)));  
end  
  
if size(temp11,1) == 0  
    v(rr, cc) = 0;  
    v_norm = v_norm + v(rr, cc);  
else  
    lambda = 10;  
    switch nMethod  
  
        case 1%'F'  
            temp00 = lambda .* temp00;  
  
        case 2%'Q'  
            temp00 = lambda .* temp00.^2;  
  
        case 3%'S'  
            temp00 = sin(pi .* temp00./2./lambda);  
  
        case 4%'W'  
            temp00 =  
sin(pi.*temp00./lambda).*pi.*temp00./lambda;  
            end  
  
        v(rr, cc) = sum(sum(temp00.^2));  
        v_norm = v_norm + v(rr, cc);  
    end  
end  
end  
  
v = v./v_norm; %do normalization  
  
v = v.*100;  
% pheromone function initialization  
p = 0.0001 .* ones(size(img));
```

```
%parameter setting, see Section IV in CEC paper
alpha = 1;          %equation (4)
beta = 0.1;         %equation (4)
rho = 0.1;          %equation (11)
phi = 0.05;         %equation (12), i.e., (9) in IEEE-CIM-06

ant_total_num = round(sqrt(nrow*ncol));

ant_pos_idx = zeros(ant_total_num, 2); % record the location of
ant

% initialize the positions of ants

rand('state', sum(clock));
temp = rand(ant_total_num, 2);
ant_pos_idx(:,1) = round(1 + (nrow-1) * temp(:,1)); %row index
ant_pos_idx(:,2) = round(1 + (ncol-1) * temp(:,2)); %column index

search_clique_mode = '8'; %Figure 1

% define the memory length, the positions in ant's memory are
% non-admissible positions for the next movement

if nrow*ncol == 128*128
    A = 40;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
elseif nrow*ncol == 256*256
    A = 30;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
elseif nrow*ncol == 512*512
    A = 20;
    memory_length = round(rand(1).*(1.15*A-0.85*A)+0.85*A); %
memory length
end

% record the positions in ant's memory, convert 2D position-index
(row, col) into
% 1D position-index
ant_memory = zeros(ant_total_num, memory_length);

% System setup
if nrow*ncol == 128*128
    total_step_num = 300; % the numbe of iterations?
elseif nrow*ncol == 256*256
    total_step_num = 900;
elseif nrow*ncol == 512*512
    total_step_num = 1500;
end
```

```
total_iteration_num = 3;

for iteration_idx = 1: total_iteration_num

    %record the positions where ant have reached in the last
    'memory_length' iterations
    delta_p = zeros(nrow, ncol);

    for step_idx = 1: total_step_num

        delta_p_current = zeros(nrow, ncol);

        for ant_idx = 1:ant_total_num

            ant_current_row_idx = ant_pos_idx(ant_idx,1);
            ant_current_col_idx = ant_pos_idx(ant_idx,2);

            % find the neighborhood of current position
            if search_clique_mode == '4'
                rr = ant_current_row_idx;
                cc = ant_current_col_idx;
                ant_search_range_temp = [rr-1 cc; rr cc+1; rr+1
cc; rr cc-1];
            elseif search_clique_mode == '8'
                rr = ant_current_row_idx;
                cc = ant_current_col_idx;
                ant_search_range_temp = [rr-1 cc-1; rr-1 cc; rr-1
cc+1; rr cc-1; rr cc+1; rr+1 cc-1; rr+1 cc; rr+1 cc+1];
            end

            %remove the positions our of the image's range
            temp = find(ant_search_range_temp(:,1)>=1 &
ant_search_range_temp(:,1)<=nrow & ant_search_range_temp(:,2)>=1 &
ant_search_range_temp(:,2)<=ncol);
            ant_search_range = ant_search_range_temp(temp, :);

            %calculate the transit prob. to the neighborhood of
            current

            %position
            ant_transit_prob_v =
zeros(size(ant_search_range,1),1);
            ant_transit_prob_p =
zeros(size(ant_search_range,1),1);

            for kk = 1:size(ant_search_range,1)

                temp = (ant_search_range(kk,1)-1)*ncol +
ant_search_range(kk,2);
```

```
        if length(find(ant_memory(ant_idx,:) == temp)) == 0
%not in ant's memory
            ant_transit_prob_v(kk) =
v(ant_search_range(kk,1), ant_search_range(kk,2));
            ant_transit_prob_p(kk) =
p(ant_search_range(kk,1), ant_search_range(kk,2));
        else %in ant's memory
            ant_transit_prob_v(kk) = 0;
            ant_transit_prob_p(kk) = 0;
        end
    end

    % if all neighborhood are in memory, then the
    permissible search range is RE-calculated.
    if (sum(sum(ant_transit_prob_v)) == 0) |
    (sum(sum(ant_transit_prob_p)) == 0)
        for kk = 1:size(ant_search_range,1)
            temp = (ant_search_range(kk,1)-1)*ncol +
ant_search_range(kk,2);
            ant_transit_prob_v(kk) =
v(ant_search_range(kk,1), ant_search_range(kk,2));
            ant_transit_prob_p(kk) =
p(ant_search_range(kk,1), ant_search_range(kk,2));
        end
    end

    ant_transit_prob = (ant_transit_prob_v.^alpha) .*
(ant_transit_prob_p.^beta) ./ (sum(sum((ant_transit_prob_v.^alpha) .*
(ant_transit_prob_p.^beta))));

    % generate a random number to determine the next
    position.

    rand('state', sum(100*clock));
    temp = find(cumsum(ant_transit_prob) >= rand(1), 1);

    ant_next_row_idx = ant_search_range(temp,1);
    ant_next_col_idx = ant_search_range(temp,2);

    if length(ant_next_row_idx) == 0
        ant_next_row_idx = ant_current_row_idx;
        ant_next_col_idx = ant_current_col_idx;
    end

    ant_pos_idx(ant_idx,1) = ant_next_row_idx;
    ant_pos_idx(ant_idx,2) = ant_next_col_idx;

    %record the delta_p_current
    delta_p_current(ant_pos_idx(ant_idx,1),
ant_pos_idx(ant_idx,2)) = 1;

    % record the new position into ant's memory
    if step_idx <= memory_length
```

```

        ant_memory(ant_idx,step_idx) =
        (ant_pos_idx(ant_idx,1)-1)*ncol + ant_pos_idx(ant_idx,2);

        elseif step_idx > memory_length
            ant_memory(ant_idx,:) =
            circshift(ant_memory(ant_idx,:),[0 -1]);
            ant_memory(ant_idx,end) =
            (ant_pos_idx(ant_idx,1)-1)*ncol + ant_pos_idx(ant_idx,2);

        end

        %update the pheromone function (10) in IEEE-CIM-06
        p = ((1-rho).*p +
        rho.*delta_p_current.*v).*(delta_p_current + p.*(abs(1-
        delta_p_current)));

        end % end of ant_idx

        % update the pheromone function see equation (9) in IEEE-
CIM-06

        delta_p = (delta_p + (delta_p_current>0))>0;

        p = (1-phi).*p; %equation (9) in IEEE-CIM-06

    end % end of step_idx

end % end of iteration_idx

% generate edge map matrix
% It uses pheromone function to determine edge?

T = func_seperate_two_class(p); %eq. (13)-(21), Calculate the
threshold to seperate the edge map into two class

fprintf('Done!\n');
imwrite(uint8(abs((p>=T).*255-255)), gray(256), [filename
'_edge_aco_' num2str(nMethod) '.bmp'], 'bmp');

end % end of nMethod

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Inner Function
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

function level = func_seperate_two_class(I)
% ISODATA Compute global image threshold using iterative isodata
method.
% LEVEL = ISODATA(I) computes a global threshold (LEVEL) that can
be

```

```
% used to convert an intensity image to a binary image with IM2BW.
LEVEL
% is a normalized intensity value that lies in the range [0, 1].
% This iterative technique for choosing a threshold was developed
by Ridler and Calvard .
% The histogram is initially segmented into two parts using a
starting threshold value such as  $0 = 2B-1$ ,
% half the maximum dynamic range.
% The sample mean (mf,0) of the gray values associated with the
foreground pixels and the sample mean (mb,0)
% of the gray values associated with the background pixels are
computed. A new threshold value 1 is now computed
% as the average of these two sample means. The process is
repeated, based upon the new threshold,
% until the threshold value does not change any more.
%
% Reference :T.W. Ridler, S. Calvard, Picture thresholding using an
iterative selection method,
% IEEE Trans. System, Man and Cybernetics, SMC-8 (1978)
630-632.

% Convert all N-D arrays into a single column. Convert to uint8 for
% fastest histogram computation.

I = I(:);

% STEP 1: Compute mean intensity of image from histogram, set
T=mean(I)
[counts, N]=hist(I,256);
i=1;
mu=cumsum(counts);
T(i)=(sum(N.*counts))/mu(end);

% STEP 2: compute Mean above T (MAT) and Mean below T (MBT) using T
from
% step 1
mu2=cumsum(counts(N<=T(i)));
MBT=sum(N(N<=T(i)).*counts(N<=T(i)))/mu2(end);

mu3=cumsum(counts(N>T(i)));
MAT=sum(N(N>T(i)).*counts(N>T(i)))/mu3(end);
i=i+1;
T(i)=(MAT+MBT)/2;

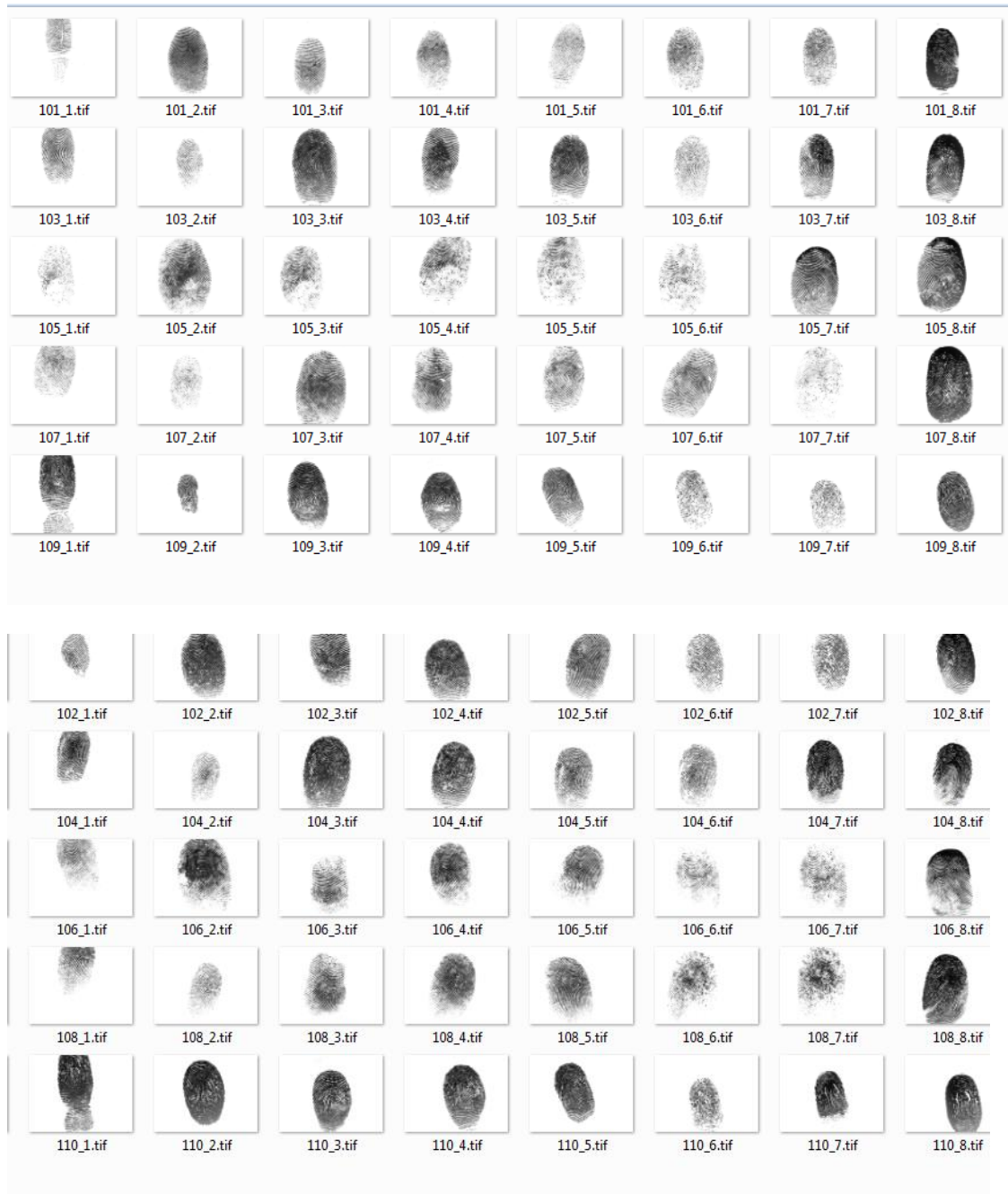
% STEP 3 to n: repeat step 2 if T(i)~=T(i-1)
Threshold=T(i);
while abs(T(i)-T(i-1))>=1
    mu2=cumsum(counts(N<=T(i)));
    MBT=sum(N(N<=T(i)).*counts(N<=T(i)))/mu2(end);

    mu3=cumsum(counts(N>T(i)));
    MAT=sum(N(N>T(i)).*counts(N>T(i)))/mu3(end);
```

```
i=i+1;  
T(i)=(MAT+MBT)/2;  
Threshold=T(i);  
end  
  
% Normalize the threshold to the range [i, 1].  
level = Threshold;
```


Baza e të dhënave publike FVC2004

Baza e të dhënave 1



Baza e të dhënave 2



Baza e të dhënave 3



Baza e të dhënave 4

