Contents

Certificate iii

Declaration by the Candidate v

Copyright Transfer Certificate vii

Acknowledgements ix

Contents xi

List of Figures xv

List of Tables xvii

Abbreviations xix

Symbols xxi

Preface xxiii

1 Introduction 1
- 1.1 Historical Background 1
- 1.2 Biometric Traits 4
- 1.3 Biometric System Features 6
  - 1.3.1 System Modules 6
  - 1.3.2 Operation Modes 7
- 1.4 Application Domains 9
- 1.5 Performance Measures 10
  - 1.5.1 Score Distributions 11
  - 1.5.2 System Errors 12

1.6 Attacks on Biometric Systems 16

1.6.1 Threat Agent 16

1.6.2 Attack Model 17

1.6.3 Adversary Attacks 19

1.7 Objectives of the Thesis 23

1.8 Contributions 26

1.9 Thesis Organization 28

2 Background and Literature Survey **31**

2.1 Biometric Security Schemes 31

2.2 Biometric Cryptosystem 33

2.2.1 Fuzzy Commitment 35

2.2.2 Fuzzy Vault 38

2.3 Cancelable Biometrics 49

2.3.1 Fingerprint Based Schemes 50

2.3.2 Iris Based Schemes 55

3 Fingerprint Template Protection **59**

3.1 Introduction 59

3.2 Motivation 62

3.3 Model Development 63

3.3.1 System Modules 63

3.3.2 Database Size 72

3.3.3 Matching Complexity 73

3.4 Theoretical Security Analysis 74

3.4.1 Template Inversion 74

3.4.2 Cross-linking/Diversity 76

3.4.3 Stolen Token Attacks 77

3.5 Experiments and Results 80

3.5.1 Data Acquisition and Performance Metrics 80

3.5.2 Framework Analysis 82

3.5.3 Evaluation on Security Criteria 89

3.6 Conclusion 92

4 Iris Template Security **95**

4.1 Introduction 95

4.2 Motivation and Overview 97

4.3 Model Development 99

4.3.1 Modified Bloom filters 99

4.3.2 Proposed Modification 101

4.3.3 Comparison 103

4.3.4 Key Management 105

4.4 Theoretical Security Analysis 106
4.4.1 Additional Notations 107
4.4.2 Observations 108
4.4.3 Unlinkability 109
4.4.4 Irreversibility 110
4.4.5 Information Leakage 111
4.5 Experiments and Results 115
4.5.1 Data Acquisition 115
4.5.2 Framework Analysis 118
4.6 Conclusion 123

5 Soft Biometrics and Privacy **129**
5.1 Introduction 129
5.1.1 Applications of Soft Biometrics 131
5.1.2 The Privacy Paradigm 135
5.2 Motivation and Overview 137
5.3 Important Observations 143
5.3.1 Soft Biometric vs. Micro Databases 143
5.3.2 Generic Soft Biometric Database Schema 144
5.3.3 Attribute Based Correlation - Practical Instances 146
5.4 Model Construction 148
5.4.1 Assumptions 148
5.4.2 Categories of Privacy Loss 149
5.4.3 Micro Database Model 150
5.4.4 Soft Biometric Database Model 152
5.4.5 Auxiliary Background Information 154
5.5 Quantified Privacy Levels 155
5.6 Background Requisites 161
5.6.1 Underlying Soft Biometrics Fusion Framework 161
5.6.2 Differential Privacy Foundations 165
5.7 Framework Development 168
5.7.1 Query Based Biometric System (QBBS) 168
5.7.2 Permissible Queries 171
5.7.3 Global Sensitivity (Δf) Computation 173
5.7.4 QBBS Based Privacy Preserving Framework 175
5.7.5 Composability 180
5.7.6 Additional Advantages 181
5.8 Theoretical Security Analysis 182
5.9 Results and Analysis 186
5.9.1 Database 187
5.9.2 Framework Analysis 189
5.10 Conclusion 205

6 Conclusion and Future Scope of This Thesis **207**

6.1 Concluding Remarks 207

6.2 Future Scope of This Thesis 211

A List of Publications **215**

Bibliography **217**

List of Figures

1.1 Various measurements taken under the Bertillonage system. 2
1.2 Variation of a child's fingerprints over time 3
1.3 Different working modes of a biometric system. 9
1.4 Intra-sample variations for biometric features. 11
1.5 Score distribution for a real matching algorithm. 13
1.6 FMR and FNMR function distributions. 14
1.7 Demonstration of a ROC curve. 15
1.8 The biometric system attack model. 18
1.9 Various forms of infrastructure based attacks. 21

2.1 Classification of biometric template protection schemes. 32
2.2 Key binding based biometric cryptosystem framework. 34
2.3 The fuzzy commitment framework. 36
2.4 The fuzzy vault framework. 40
2.5 The BioHashing scheme [97]. 51

3.1 Discriminating patterns of a fingerprint. 60
3.2 Fingerprint alignment. 64
3.3 Quantization of fingerprint minutiae points. 67
3.4 Proposed biometric template security framework. 72
3.5 Sample fingerprint images from the FVC databases 81
3.6 Genuine-impostor distributions under the plain verification scenario. . 85
3.7 Genuine-impostor distributions under the stolen token scenario. . . . 87
3.8 EER for the FVC databases under the stolen token scenario 88
3.9 ROC curves for FVC 2002 under the stolen token scenario 88
3.10 ROC curves for FVC 2004 under the stolen token scenario 89
3.11 Genuine,impostor and pseudo-impostor distributions under the plain verification scenario 91

4.1 Generic outline of a Bloom filter. 100
4.2 Modified Bloom filter based biometric template protection scheme. . . 104
4.3 Various stages of feature extraction from iris images. 117
4.4 ROC curves of the original iris systems 119

4.5 ROC curves for systems implementing the feature extraction algorithm of Masek [19]. . . . 125
4.6 ROC curves for systems implementing the feature extraction algorithm of Ma et.al [20]. . . . 126
4.7 Scores comparison before and after encoding following feature extraction method of Masek [19] . . . 127
4.8 Scores comparison before and after encoding following feature extraction method of Ma et. al [20] . . . 128

5.1 The soft biometric database schema. . . . 145
5.2 Enrollment process in the Bayesian decision theoretic framework. . . 162
5.3 Verification process in the Bayesian decision theoretic framework. . . 164
5.4 Basic structure of a QBBS . . . 169
5.5 Proposed privacy preserving QBBS . . . 176
5.6 Performance comparison of biometric systems based on primary traits. 192
5.7 Performance comparison of biometric systems based on fingerprint . . 195
5.8 Performance comparison of biometric systems based on face . . . 196
5.9 Performance comparison of biometric systems based on fingerprint and face . . . 196
5.10 Effects of noise on Deviation . . . 198
5.11 Effects of noise on Distortion . . . 199
5.12 Effects of noise on utility for fingerprint based QBBS. . . . 201
5.13 Effects of noise on utility for face based QBBS. . . . 203
5.14 Effects of noise on utility for fingerprint and face based QBBS 204

List of Tables

1.1 Comparison of various biometric trait in terms of the essential required properties. 5

3.1 Techniques for recovering fingerprint image from stored minutia points. 61
3.2 Parameters of FVC databases for stolen key based attack scenario (considering $n_\phi = 1$) 79
3.3 Tuning of quantization levels for obtaining optimum performance (same key scenario). 83
3.4 EERs for FVC databases under the plain verification scenario. 84
3.5 Performance comparison via EER(%) for various fingerprint based template protection schemes under the stolen token scenario. 89
3.6 Average matching scores for FVC databases under the *diversity* protocol. 92

4.1 GAR's (in %) at FAR = 0.01% for different system configurations using feature extraction technique of Masek [19] 120
4.2 GAR's (in %) at FAR = 0.01% for different system configurations using feature extraction technique of Ma et.al [20] 121

5.1 Soft biometric traits and their associated properties 130
5.2 Attributes used in soft biometrics databases. 147
5.3 Attributes of external micro databases. 147
5.4 Variation of a values for Primary traits. 191
5.5 Variation of a values for all traits. 194

Abbreviations

BC	Biometric Cryptosystem
BFS	Boosting Feature Selection
COA	Ciphertext Only Attack
CRC	Cyclic Redundancy Check
DT	Decision Threshold
EER	Equal Error Rate
FAR	False Accept Rate
FMR	False Matching Rate
FNMR	False Non Matching Rate
FRR	False Reject Rate
FTC	Failure To Capture
FTE	Failure To Enroll
IPC	Iris Pseudo Code
MSE	Mean Square Error
OFFC	Orientation Field Flow Curves
PCA	Principal Component Analysis
PPDP	Privacy Preserving Data Publishing
PRNG	Pseudo Random Number Generator
QBBS	Query Based Biometric System
ROC	Receiver Operating Characteristic
RP	Random Projection
SHA	Secure Hash Algorithm

Symbols

$E(.)$	expectation operator
$\oplus$	XOR operation
U	set of biometric system users
x	x-coordinate of fingerprint minutiae
y	y-coordinate of fingerprint minutiae
θ	angle associated with fingerprint minutiae
x'	shifted x-coordinate of fingerprint minutiae
y'	shifted y-coordinate of fingerprint minutiae
θ'	angle associated with fingerprint minutiae
H	height of an image/feature matrix
W	width of an image/feature matrix
ϕ	hexagonal grid points
δ	equidistant spacing between grid points
$\vert\vert$	concatenation operation
$\mathcal{H}(.)$	cryptographic hash function
$h(.)$	simple hash function
$J(.,.)$	Jaccard similarity co-efficient
HD	hamming distance
w	size of an iris codeword
l	block size of an iris feature matrix
$\mathcal{S}$	feature space
$\mathcal{B}$	set of Bloom filters (iris)

$\mathcal{K}$	key matrix (iris)
$\mathcal{T}$	transformed template matrix (iris)
$\mathbb{B}$	Bloom filter feature vector (iris)
X_B	random variable denoting $\mathbb{B}$
$\mathbb{K}$	key feature vector (iris)
X_K	random variable denoting $\mathbb{K}$
$\mathbb{T}$	transformed template vector (iris)
X_T	random variable denoting $\mathbb{T}$
$H(.)$	information theoretic entropy
$H_\infty(.)$	minimum entropy
e	privacy
X_e	random variable denoting privacy
$\mathcal{K}_{prv}$	set of private attributes
X_{prv}	random variable representing private attributes
$\mathcal{K}_{pub}$	set of public attributes
X_{pub}	random variable representing public attributes
Z	side information
X	set of primary biometric traits
Y	set of soft biometric traits
ϵ	privacy controlling parameter
Δf	global sensitivity
N	noise added to QBBS responses
n	number of soft biometric traits
m	number of query/responses for each soft trait