CERTIFICATE

It is certified that the work contained in the thesis titled DESIGN AND IMPLEMENTATION OF PRIVACY PRESERVING SECURE SCHEMES FOR BIOMETRIC TEMPLATES by DEBANJAN SADHYA has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

It is further certified that the student has fulfilled all the requirements of Comprehensive Examination, Candidacy and SOTA for the award of Ph.D. Degree.

Dr. Sanjay Kumar Singh

Department of Computer Science and Engineering

Indian Institute of Technology (Banaras Hindu University)

सह प्रोफेसर / Associate Professor
संगणक अभियांत्रिकी विभाग / Department of Computer Engg.
भारतीय प्रौद्योगिकी संस्थान / Indian Institute of Technology
(बनारस हिन्दू यूनिवर्सिटी) / (Banaras Hindu University)
वाराणसी / Varanasi

DECLARATION BY THE CANDIDATE

I, DEBANJAN SADHYA certify that the work embodied in this thesis is my own bona fide work and carried out by me under the supervision of DR. S. K. SINGH from JULY-2013 to NOV-2016, at the DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, Indian Institute of Technology (BHU), Varanasi. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, *etc.*, reported in journals, books, magazines, reports dissertations, theses, *etc.*, or available at websites and included them in this thesis and cited as my own work.

Date: 26/11/2016
Place: Varanasi

Debanjan Sadhya
Signature of the Student
(Debanjan Sadhya)

CERTIFICATE BY THE SUPERVISOR

It is certified that the above statement made by the student is correct to the best of my knowledge.

Dr. S. K. Singh
Department of Computer Science and Engineering
Indian Institute of Technology (BHU), Varanasi

सह प्रोफेसर / Associate Professor
Department of Computer Engg.
Technology
Banaras Hindu University)

25-11-16

Signature of Head of Department
(Prof. K.K. Shukla)

आचार्य व विभागाध्यक्ष
Professor & Head

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: Design and Implementation of Privacy Preserving Secure Schemes for Biometric Templates.

Name of the Student: Debanjan Sadhya.

Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University) Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the DOCTOR OF PHILOSOPHY.

Date: 26/11/2016

Place: Varanasi

Debanjan Sadhya
Signature of the Student

(Debanjan Sadhya)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute's copyright notice are indicated.

ACKNOWLEDGEMENTS

The hardest arithmetic to master is that which enables us to count our blessings - Eric Hoffer

I would like to take this opportunity for expressing my deep sense of gratitude to everyone who helped me directly or indirectly during my thesis work. First of all, I would like to thank my supervisor, Dr. Sanjay Kumar Singh, for being a great mentor and adviser. His constant support, encouragement and critics worked as a source of motivation and inspiration behind the successful completion of this work. It has truly been a great privilege while working with him in these years. I am highly obliged to all the faculty members of the Department of Computer Science and Engineering, IIT(BHU), for their wholehearted support. I express my sincere thanks to Professor K. K. Shukla, Professor A. K. Tripathi, Professor R. B. Mishra, Dr. B. Biswas and Dr. Neeraj Sharma (School of Biomedical Engineering, IIT(BHU)) for providing their continuous support to me. I express my profound appreciation to the Director, Registrars, Deans, Heads, and office staff of the Indian Institute of Technology (BHU), Varanasi. My time spent at this institution would never be complete without the company and assistance of my fellow researchers. I would like to convey special thanks to Miss. Bodhi Chakraborty, Mr. Ali Imam Abidi, Mr. Durgesh Singh, Mr. Sumit Jaiswal and Mr. Anshu Sharan Singh for their continuous moral and academic support. I extend my special thanks to the non-teaching

staff in the department, especially Dr. R. P. Meena, Mr. Shashikant Singh, Mr. Rajendra Kumar, Mr. Kanhaiya Lal and Mr. Bharat Pandey for their consistent support. Lastly, I want to thank my mother Smt. Trishna Sadhya, my father Dr. Sudipta Kumar Sadhya and my sister Mrs. Saswati Sadhya for guiding me through the journey of life. They showed me the strength of resilience in the face of failures and the ability to bounce back from such situations.

- Debanjan Sadhya

Contents

List of Figures

List of Tables

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
$\|\|$	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

PREFACE

Biometrics based authentication systems have garnered widespread popularity due to their various advantages over contemporary token based systems. The core of a typical biometric framework consists of a database wherein the biometric data of the registered users get stored. This database can either be stored locally (e.g. in smart cards), or in a centralized manner (e.g. servers). From a security point of view, the risks associated with such databases are alarmingly high. Theoretically, they can be subjected to a wide variety of external attacks by an adversary, thereby compromising both the security and privacy aspects of the users. Some primary examples of these user predicaments include unauthorized access, privacy breach and even identity theft in the worst case. Considering the fact that biometric entries are mostly invariant with time, (i.e. they cannot be re-issued like passwords on being compromised) the stakes for protecting these unique entries become much higher.

Researches in the area of biometric template security were initiated for enforcing effective countermeasures against biometric security threats. These semi-cryptographic techniques can be broadly classified into two categories based on their functioning methodologies- *Biometric Cryptosystems* (or Biometric Encryption in some literature) and *Cancelable Biometrics*. Biometric cryptosystem based security schemes essentially associate a random key with the biometric values, thereby generating a secured token (referred to as Helper Data). This auxiliary piece of information is

stored in the database and subsequently used for facilitating during matching. On the other hand, cancelable biometric techniques function on the idea of protecting a biometric template via transforming it in a different domain (based on a distortion parameter derived from a key). An important feature of these schemes is that a fresh protected template can be generated on demand by altering/issuing a new key.

A major problem with the current biometric template protection schemes is simultaneous fulfillment of various security goals along-with providing acceptable recognition accuracy rates. On an abstract level, these two properties are complementary. Even the essential security requirements such as *irreversibility*, *unlinkability*, *information leakage* and *privacy preservation* are not always concurrently realized. Importantly, both theoretical and empirical analysis of these properties are required for proving that any particular scheme complies with these requirements. This thesis is dedicated towards the development of secure biometric models which target to solve these issues. Attempts have been made to provide the aforementioned security and privacy notions, while not degrading the performance of the overall recognition system. In this thesis, secure frameworks based on the biometric modalities of fingerprint, iris and soft biometric have been proposed. In addition to maintaining acceptable recognition rates, these frameworks have been both formally and empirically analyzed for the fulfillment of the aforementioned security properties.

Biometric data are implicitly associated with some properties such as *intra-class variations* and *spatial variability*. This poses a significant problem while designing proper biometric template protection schemes since these factors heavily affect

the performance parameters. To manage such issues, the proposed security frameworks in this thesis contain an ensemble of individual modules like *pre-alignment* and *quantization*. These functioning blocks mitigate the inherent 'errors' associated with biometric data, thereby facilitating the construction of a consistent framework. Another objective of this thesis is to successfully incorporate cryptographic ideas into the domain of biometric recognition. Although difficult due to the nature of biometric data, security notions such as *cryptographic hash functions*, *perfect secrecy* and *differential privacy* have been successfully integrated into the developed frameworks. This procedure not only enabled in constructing robust models but also facilitated in rigorously proving the security properties with tight computational bounds.