ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

A MULTIBIOMETRIC CRYPTOSYSTEM FOR USER AUTHENTICATION

Ph.D. THESIS

Faezeh Sadat BABAMIR

Department of Electronics and Communication Engineering

Electronics Engineering Programme

MAY 2019

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE
ENGINEERING AND TECHNOLOGY

A MULTIBIOMETRIC CRYPTOSYSTEM FOR USER AUTHENTICATION

Ph.D. THESIS

Faezeh Sadat BABAMIR
(504132210)

Department of Electronics and Communication Engineering

Electronics Engineering Programme

Thesis Advisor: Associate Professor Dr. Mürvet KIRCI

MAY 2019

STANBUL TEKNK ÜNVERSTES ★ FEN BİLİMLERİ ENSTİTÜSÜ

KULLANICILARIN KİMLİK DOĞRULAMASI İÇİN ÇOKLU-BİYOMETRİLİ ŞİFRELEME SİSTEMİ

DOKTORA TEZİ

Faezeh Sadat BABAMIR
(504132210)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Associate Professor Dr. Mürvet KIRCI

MAYIS 2019

Faezeh Sadat BABAMIR, a Ph.D. student of ITU Graduate School of Science Engineering and Technology 504132210 successfully defended the thesis entitled "A MULTIBIOMETRIC CRYPTOSYSTEM FOR USER AUTHENTICATION", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Associate Professor Dr. Mürvet KIRCI** Istanbul Technical University	.....
Jury Members :	**Professor Dr. Ece Olcay GÜNEŞ** Istanbul Technical University	.....
	Associate Professor Dr. Ender Mete EKŞİOĞLU Istanbul Technical University	.....
	Assistant Professor Dr. Bülent BOLAT Yıldız Technical University	.....
	Assistant Professor Dr. Nihan KAHRAMAN Yıldız Technical University	.....

Date of Submission : **10 May 2019**
Date of Defense : **27 May 2019**

To my spouse and family,

FOREWORD

First and foremost, I want to thank my advisor Associate Prof. Dr. Mürvet KIRCI, who took over the supervision of my Ph.D. studies and steadily supported me. Her joy and enthusiasm for research lit up my path in its hour and made me regain passion for academic work.

Besides my supervisor, I would like to thank Prof. Dr. Ece Olcay GÜNEŞ and Assistant Prof. Dr. Bülent BOLAT, who kindly agreed to become my Ph.D. examiners. Their knowledge and experience were fundamental to set the quality bar of my research.

Looking back at these last four years, there are my family whom I owe acknowledgement. *My Father*, for our open exchange of opinions behind closed doors. He managed to give me a constant motivation for going forward. *My Mother*, for lending me their ears and guiding me to a better life; for her truthful support, encouragement and endless patient during the last half of my Ph.D. I can not thank you enough for what you did for me. And *My Spouse*, for his help, support and especially the countless hours spent together trying to gure out positive solutions to negative situations. Thank you for being part of my life.

May 2019 Faezeh Sadat BABAMIR

TABLE OF CONTENTS

Page

ABBREVIATIONS

PKI	**:** Public Key Infrastructure
PK	**:** Public Key
MSK	**:** Master Secret Key
SK	**:** Secret Key
HP	**:** Helper Parameter
HD	**:** Hamming Distance
TTP	**:** Trusted Third Party
RSA	**:** Rivest-Shamir-Adleman
EXP	**:** EXPonentiation
GM	**:** Group Mul in G
FAR	**:** False Acceptance Rate
FRR	**:** False Reject Rate
PI	**:** Pseudonymous Identifier
DLP	**:** Discrete Logarithm Problem
CRT	**:** Chinese Remainder Theorem
SHA	**:** Secure Hash Algorithm
DOS	**:** Denial-of-Service
WSN	**:** Wireless Sensor Network
ECC	**:** Elliptic Curve Cryptography
OTP	**:** One-Time Password
TMIS	**:** Telecare Medical Information System
MITM	**:** Man-In-The-Middle
MV	**:** Mask Vector
PCA	**:** Principle Component Analysis
ICA	**:** Independent Component Analysis

SYMBOLS

$\mathbf{X}, \mathbf{X}'$	**:** Feature vectors of identities ID and ID
$\mathbf{D_{ID}}$	**:** Digest of identity ID
$\mathbf{S_{ID}}$	**:** Semi-digest of identity ID
$\boldsymbol{r}, \boldsymbol{\lambda}$	**:** Random numbers
$\boldsymbol{\tau}$	**:** Threshold value
G	**:** Finite cyclic multiplicative group
PK	**:** Public Key set
SK	**:** Secret Key Set
derand	**:** De-randomizing parameter
M	**:** Mask vector of feature vector X
H(.)	**:** SHA-2 hash function
CPW	**:** Client PassWord
SPW	**:** Server PassWord
seed	**:** Seed of pusedo-random number function PR
SC	**:** Smart Card

LIST OF TABLES

Page

LIST OF FIGURES

Page

A MULTIBIOMETRIC CRYPTOSYSTEM FOR USER AUTHENTICATION

SUMMARY

Cryptography is the science and art of keeping information secret to unintended parties. But, how can we determine who is an intended party and who is not? Authentication is the branch of cryptography that aims at confirming the source of data or at proving the identity of a person. This Ph.D. thesis is a study of a different way to perform cryptographic biometric authentication of data and users.

Biometric authentication has been deployed over last few years and is progressing very fast. An automated authentication system operated through biometric data, creates a secure guarded port for access control. Moreover, it is a lock and capture mechanism for preserving critical data or controlling access of clients who wish to enter to the system. Authentication is the process of client identification by according the actual client's attributes with the expected (claimed) ones as well as the proof of the originality.

The main proposed contributions are contained in the *five papers* included in Appendix A.2 and cover the following research areas: (i) Biometric template security; (ii) Privacy; (iii) Mutual authentication; (iv) User's anonymity; (v) indistinguishability; and (vi) biometric authentication in Wireless Sensor Networks (WSNs).

We first propose a *basic* secure scheme including new concept called *(trait) digest* in which all individual's information perfectly are preserved but there are some deficiencies related to *privacy*. Afterwards, we propose a *randomized digest* based authentication method that preserves *privacy* of client's biometric templates and authenticates the client securely by generating non-deterministic semi-digest. It focuses on the improvement of the method for providing invulnerability against user anonymity and server masquerading attacks. We show that our improved scheme is secure against the attacks and prove its functionality features. The digest is a tuple that is used to verify the authentication of a client such that the original biometric plain cannot be decrypted from the protocol output. Therefore, nobody including authentication server can discover any information about the client biometric sample(s).

Our *secure template* based scheme enables a client to login into a system in which safeguarding critical data or/and controlling access are signified. A biometric based system legitimates users who are the owners of legal biometric information. To secure such a system we should protect all information belonging to legal individuals and preserve privacy of tracking action.

By the investigation of the biometric based authentication protocol we presented in terms of cryptanalysis criteria as well as some attacks, the proposed basic method was extended for the following issues:

1) Providing user *anonymity* against the authenticating party;

2) Protecting the passwords of mobile users against the off-line dictionary attack;

3) Making the protocol secure against the man-in-the-middle attack.

In addition, we incorporate an important function to enable clients for change or recovery of their passwords. To this end, every user should register using the third party during the registration phase.

Compared with related studies, we consider our improved scheme in terms of anonymity and mutual authentication using different metrics such as the time to perform one way hash computation cryptosystem.

The client authentication is a significant process in client server systems. Such a process is highly secure when a client may be authenticated according to a set of unique verifiable data, i.e., biometric traits. However, biometric based systems with the low-cost, dense biometric sensors, and power of fast processing need a method of automatic client recognition *indistinguishably* for the robust client authentication. Such a method faces three challenges: (1) the effective recognition of the biometric patterns in-putted to the system, (2) the provision of security to prevent the vulnerability of the system, and (3) the preparation of personal privacy. Many remote biometric authentication schemes have been developed to establish secure *mutual communication* between a client as device node and server over an untrusted channel. By employing a secure remote biometric based authentication protocol, a client that acts in a node and a server that contains sources can authenticate each other in secure and trust-able manner in different client-server based network including WSNs.

Through some practical scenarios, we consider different attacks from client, server, and network sides to intrude into the privacy. We mathematically and practically prove that our scheme is enough safe to resist against different attacks and protect legitimate individuals' information and privacy. Finally, we show our computation and memory efficiency compared with related studies.

KULLANICILARIN KİMLİK DOĞRULAMASI İÇİN ÇOKLU-BİYOMETRİLİ ŞİFRELEME SİSTEMİ

ÖZET

Şifreleme (Kriptografi), korunmak istenen bilginin sır olarak saklanmasını sağlayan bir bilim dalıdır. Burada temel sorun bu sırrı kimin çözebileceğini belirlemekle ilişkilidir. Kimlik doğrulama, bir kişinin kimliğini kanıtlarken veri kaynağının da doğrulanmasını sağlayan önemli bir kriptografi konusudur. Bu doktora tezinde, farklı yollarla kullanıcıların kriptografik ve biyometrik kimlik bilgilerinin doğrulamasını sağlayan bir sistem önerilmektedir. Biyometrik kimlik doğrulama uygulamaları son yıllarda hızla yeni alanlara doğru yayılmaktadır. Biyometrik verilerle işletilen bir otomatik kimlik doğrulama sistemi; erişim kontrolü için güvenli bir kapı oluşturur. Ayrıca bu kilit ve yakalama sistemi kritik verilerin korunması veya isteyen istemcinin erişiminin kontrol edilmesi için bir mekanizma oluşturur.

Kimlik doğrulama sayesinde gerçek istemciye ait olan özellikler ile sahte istemciye ait özellikler öznitelik belirleme ve sınıflandırma teknikleri ile ayrıştırılmaktadır. Böylece gerçek istemci büyük bir doğrulukla belirlenebilmektedir.

Bu tezde biyometrik şablon güvenliği, gizlilik, karşılıklı kimlik doğrulama, kullanıcıların anonimliği ve kablosuz sensör ağlarda biyometrik kimlik doğrulama konularında temel katkılar yapılmıştır.

Yapılan çalışmalarda tüm bireylerin mükemmel bir şekilde bilgilendirildiği temel bir güvenlik programı önerilmekle birlikte gizliliğin korunmasında bazı zayıf taraflar bulunmaktadır. Bu çalışmada ise gizliliği koruyan kimlik doğrulama yöntemine dayanan bir özet önerilmektedir. Bu özet, istemcilerin biyometrik şablonlarının gizliliğini koruyarak ve deterministik olmayan bir yarı özet üreterek istemciyi güvenli bir şekilde doğrular.

Bu yöntemde kullanıcı gizliliğine ve sunucu maskelenme saldırılarına karşı güvenlik açıklarını belirlemek ve kapatmak üzerine çalışılmıştır.

Geliştirdiğimiz planın saldırılara karşı güvenli olduğunu ve işlevsellik özelliklerini sağladığı kanıtlanmıştır. Bu çalışmada tanımlanan özet, kimlik doğrulamasını onaylamak için kullanılan sistemin bir parçasıdır. Bu özet sayesinde protokol çıktısından yararlanılarak şifre çözülemeyecek ve istemcinin biyometrik kimlik bilgilerine ulaşılamayacaktır.

Bu nedenle, istemcinin biyometrik örnekleri ile ilgili bilgiye, kimlik doğrulama sunucusu da dahil hiç kimse herhangi bir şekilde ulaşamaz, ancak güvenli şablon tabanlı programımız, istemcinin, kritik verilerinin korunduğu veya erişimin kontrol edildiği sisteme giriş yapmasını sağlar.

Biyometrik tabanlı sistem biyometrik bilgilerin sahibi olan kullanıcıların yasallaşmasını da sağlar. Güvenlik için böyle bir sistem tüzel kişilere ait tüm bilgileri ve izleme eyleminin gizliliğini de korumalıdır. Bu amaçla biyometrik tabanlı kimlik doğrulama protokolünün araştırılması kapsamında kriptanaliz kriterleri ve bazı saldırılar açısından, önerilen temel yöntem aşağıdaki sorunları çözmek için

genişletilmiştir:

1) Kimlik doğrulaması yapan tarafa karşı kullanıcı anonimliği sağlamak;
2) Mobil kullanıcıların şifrelerini offline sözlük saldırısına karşı korumak;
3) Protokolü, ortadaki adam saldırısına karşı güvenli hale getirmek.

Ek olarak, istemcilerin şifrelerinin değiştirilebilmesine veya kurtarılmasına izin veren önemli bir fonksiyon kullanılmaktadır. Bu amaçla, her kullanıcı kayıt aşamasında üçüncü bir grup kullanarak kayıt yaptırmalıdır. İlgili çalışmalarla karşılaştırıldığında; tek yönlü karma hesaplama şifreleme sistemi çalışma zamanı gibi farklı metrikler kullanılan, anonimlik ve karşılıklı doğrulamaya dayanarak geliştirdiğimiz şemayı göz önüne alıyoruz.
İstemci doğrulama, istemci sunucu sistemlerinde önemli bir işlemdir. Böyle bir işlem bir istemciye göre bir dizi kimlik doğrulaması benzersiz doğrulanabilir veriler, yani biyometrik özellikler ile yapıldığında son derece güvenlidir.
Ancak biyometrik tabanlı sistemler, sağlam istemci kimlik doğrulaması için; düşük maliyetli, hassas biyometrik sensörler içeren ve hızlı işlem gücüne sahip özellikte olmalıdır. Böyle bir yöntem üç zorlukla karşı karşıyadır:

1) sisteme girilen biyometrik imgenin etkin şekilde tanınması,
2) sistemin güvenlik açığını önlemek için yeterli güvenlik sağlanması ve
3) kişisel mahremiyetin korunması.

Birçok uzaktan biyometrik kimlik doğrulama şeması, cihaz düğüm noktası olarak konumlanan bir istemci ile güvenilmeyen bir kanal üzerinden haberleşen sunucu arasında sistemin karşılıklı ve güvenli iletişimini kurmak için geliştirilmiştir. Güvenli bir uzaktan biyometrik tabanlı kimlik doğrulama protokolü sayesinde, bir düğümde konumlanan bir istemci ile kaynaklar bulunduran sunucu, kablosuz sensör ağları de dahil olmak üzere farklı istemci-sunucu tabanlı ağlarda birbirlerini güvenli bir şekilde doğrulayabilir.
Bazı pratik senaryolar sayesinde, istemciden, sunucudan ve ağ tarafından gelebilecek mahremiyete müdahale etmesi olasılığı bulunan farklı saldırılar da göz önüne alınmıştır. Programımızın farklı saldırılara karşı direnmek, yasallığını korumak ve bireylerin bilgi gizliliği için yeterince güvenli olduğu matematiksel ve pratik olarak kanıtlanmıştır. Son olarak, ilgili çalışmalara göre hesaplama ve hafıza verimliliğimizin daha yüksek olduğu ortaya konmuştur.
Önerilen protokol, tersinir olmayan fonksiyonun kullanld güvenli bir protokoldür.
Hiç kimsenin girdiden çıktyla ilgili bilgileri kavrayamayacaı şekilde bir protokol oluşturulmutur. Bu şekilde, (şablon koruması) birçok saldırı önlenmi ve orijinal biyometrik özelliklere erişilmesi engellenmiştir.
Ek olarak, burada hedeflenen yöntem sayesinde bir istemcinin birkaç kişiye yetki vermek istediinde deterministik olmayan bu yöntem, doru çalışan bir protokol ile benzersiz bir özet üretecektir. Bu yüzden gizliliin, kullanıcının kimliine ve etkinliine tam olarak saygı gösterilmeyen saldırı durumlarda geliştirilen yöntem kullanıcı sistemdeki bilgilerini iptal edebilecek özelliktedir.
Ayrıca, kayıt sunucusu ve kimlik dorulama sunucusu olarak iki sunucu olduundan sırasıyla kullanıcıları kaydettirmek ve istemcileri yetkilendirmek için kullanılan

istemci güvenilir olmayan sunucuları (güvensiz bir a üzerinden) kimlik dorulaması için yetkilendirme verilmesi kritik biyometrik bilgilerin sızdırılmasına neden olacaktır. Bu tezde gelitirilen koruma yolları ile her müşteri için bir özet üretilerek tezde belirtilen tüm ataklara karşı güvenli hale getirilmiştir.

Tez aşaıdaki şekilde devam ediyor:

İkinci bölümde çalımamzı üç bölümde açıklıyoruz; öncelikle temel gereksinimler ve biyometrik sistem yapısı açıklanıyor, önerilen protokol veriliyor ve son olarak da kriptoanaliz işlemleri anlatılıyor.

Biyometrik sistem yapsnda veri toplama, özellik çıkarma modülü, eşleştirme modülü, çoklu biyometrik sistem tanıma, biyometrik şablon koruması, önerilen protokol de ise, temel önerilen protokol, tanımlar, temel önerilen protokol açıklaması, performansla ilgili özellikler, önerilen protokol- 1 ve 2, ayrıca önerilen protokol: kayıt algoritması, kimlik dorulama algoritması, biyometrik kimlik dorulama kontrol akıı gibi konulara yer verilmiştir.

Bölüm 3'te, uygulamalar yapılarak elde edilen sonuçları dikkate alınmıtır. Veri Kümeleri olarak CASIA-Iris-V1 ve UBIRIS ile çalışılmıştır. Çalımanın performansı ise dier çalışmalara göre verimlilik, hesaplama süresi, hassasiyet ve doruluk açısından tartışılmıştır.

Son olarak, 4. Bölümde, çıkarılan sonuçlar verilmiş ve gelecekte çözülebilecek problemler önerilmiştir.

1. INTRODUCTION

The biometric authentication is the science of specifying the identity of a user systematically, based on his/her physical or behavioural attributes or biometric traits. To identify a user, the biometric authentication method replaces the common method of user name and password, which is a primary method of authentication, with biometric traits; this leads to effectiveness of the systems that need high security. Nowadays, such systems increase throughout the world. Simple systems such as mobile phones and limited business applications and sensitive systems such as on-line transactions and e-payments are the typical systems that biometric traits are applied to. Remarkably, in the daily life, industry, military and security forces and law enforcement invest in developing and manufacturing facial, iris and voice recognition technologies; the biometrical authentication is used.

Security of a biometric template may be threaten by attacks. Thus if an individual's template is revealed without any protection, the individual's biometric attributes should not be used no longer for the authorization by the biometric system. Moreover, a fused template stored in the system memory, can reveal more accurate information about enrolled users. This is why nowadays multibiometric template protection is a serious challenge for researchers when they want to apply cryptographic methodologies to protect the templates stored in a biometric system.

Furthermore, if the system collects a multibiometric trait that is the fusion of two or more uni-modal biometric traits, it is expected that the system to be more reliable due to the presence of multiple independent traits including iris, fingerprint, etc. Such a system is able to withstand many threats successfully because of multibiometric nature.

Biometric based systems with the low-cost, multi biometric sensors, and power of fast processing need a method of automatic client recognition for the robust client authentication. Such a method faces three challenges: (1) the effective recognition of the biometric patterns inputted to the system, (2) the provision of security to prevent the vulnerability of the system, and (3) the preparation of personal privacy. Many

remote biometric authentication schemes have been developed to establish secure mutual communication between a client as device node and a server over an untrusted channel, i.e., a client (that acts in a node) and a server (that contains sources) can authenticate each other in secure and trustable manner.

In this thesis, for the first time, we proposed a multibiometric authentication protocol (using a number of traits) called digest based authentication system. It is a biometric authentication protocol taking a biometric template and generating a tuple to verify the authority of client where the decryption of the original biometric template from the protocol output may not be carried out. Therefore, nobody including authentication server can discover any information about the client biometric sample(s).

Moreover, our proposed protocol saves a print of individual biometric traits through a specific framework called digest, which is output of a deterministic one-way function. This framework supplies perfect security in public key cryptosystem framework without carrying out any encryption or decryption processes.

Furthermore, the proposed protocol is a decryption-less method where it compares just inputted encrypted template with ones stored in the database. Therefore, the FAR value is close to zero but in some cases, matched individuals are incorrectly rejected. Since, we aim to provide a high privacy level, we verified received bits using the corresponding ones stored in the database. This issue led to reject authorized individuals who send their code with high error rates.

The starting point for investigating different studies of biometric authentication systems is to define types of biometric based protocols. These protocols operate within privacy preserving schemes including biometric encryption based scheme, cancelable biometric based scheme, multi-modal and hybrid based schemes, and secure computation based scheme [1]. In this work, we deployed a cancelable biometric system that is based on storing functionally digested template data extracted from biometric feature traits of scanned biometric signals. This transformation can be performed through a non-invertible function that returns a quantity. Nobody can relate this quantity to the extracted original biometric signal [2]. In order to guarantee a high-level of security for a system, multi-modal schemes are deployed in which some biometric traits (e.g. fingerprint and iris signals) are used. Then, in the verification round, related obtained values are fused to match with its counterpart in database [2].

In [3] Rane et al proposed a biometric scheme for template protection. However, other mentioned concerns were not considered. Also, they briefly investigated possible attacks and their scheme performance. In [4], like [3], authors proposed a template protection scheme where details are not clear [1]. In [5], authors mentioned multibiometric recognition and multi-modal biometric. They reviewed and combined biometric fusion and biometric template protection concepts. However, no attacks or main concerns were considered. Bringer in [6] overviewed the secure function evaluation for the biometric identification. In addition, a number of tools related to authentication schemes including homomorphic encryption were considered, but just the first mentioned concern (template protection) of the four main concerns related to biometric based verification system were considered. In [7], authors focused on the forth mentioned concerns of biometric based system, i.e. "network security". They deployed a scheme that was resistant against the spoofing attack. Patel et al in [8] presented an overview on cancelable biometric systems and in [9], biometric feature preprocessing subject was considered. Authors in [10] designed a privacy-preserving scheme from biometric secret sharing and fuzzy extractors. In [11] and [12] secure computations were utilized.

The most recent work we studied is Bart et al [13] that introduced a multi-modal biometric authentication system for untrusted distributed environment. They utilized (min-max) normalization method to calculate evaluation score. In this study, security criteria including accuracy, privacy, etc. are analyzed. However, the proposed protocol is too time-consuming and computation and communication complexity effected on its accuracy.

Authors in [14] studied one of the most harmful attacks on a biometric system that is on the user's templates. They explained how such attacks could lead to grave vulnerabilities where a template can be replaced by an impostor's templates to achieve unlawful access to the system. They warned us against storing biometric template in the plaintext form and insisted on the necessity of fool-proof methodologies to secure storage of biometric templates; such methodologies are safeguard for both safety of the biometric system and that of the systems users.

Fu et al [15] proposed a multibiometric cryptosystem by combining some features with biometrics and cryptography. In fact, there are two levels of combining, at the

biometric and cryptographic levels. They used the Shannon entropy to afford security and evaluated their accuracy and efficiency in comparison with other systems.

Zhang et al [16] proposed an encryption and an authentication scheme called mSEAS. The scheme is based on the multibiometric data with the intention of considering the privacy. This multibiometric system provides very important and secured methodology for enhancing the security level of information technology. The traditional cryptosystem suffers from problems in key management and key privacy. The use of biometric templates removes such problems and provides faster procedure with low complexity for encryption of private messages. The private key is generated using two or more biometric factors. The Elliptic Curve Cryptography (ECC) is used as a cryptographic algorithm that provides key generation and encryption, decryption of messages, and authentication. In addition, it establishes the fuzzy extractor algorithm. By means of biometric string reader, the information is excerpted. This can be used in optimization of biometric authentication.

Mahalakshm et al [17] proposed a method for generating an one-time password using a multibiomtric cryptosystem where securing authentication is performed using multibiometric cryptosystems to exploit various traits of an individual. ECC technique is used to generate curve and key. For providing a secured authentication, this study incorporates the use of One-Time Password (OTP). The proposed system can be applied for financial based services. When a user provided his/her multibiometric traits, the images are resized and fused into a single image. A matrix is generated using fixed points from the fused image; the ECC and key is generated using a number of parameters. Also, the curve is overlapped with the fused image and then an (OTP) is generated.

Nagar et al [18] proposed the feature level fusion of multibiometric templates. For higher level security, the multiple traits of an individual are combined into a single secure sketch. Their proposed method contains three phases: (1) obtaining biometric characteristics and converting them to a binary string, (2) combining the obtained biometric traits and (3) securely sketching. They used fuzzy vault and fuzzy commitments algorithms for decoding where the former uses a Berlekamp-Massae algorithm and the latter deal with decoding based on the crossover probabilities.

Juels et al [19] proposed the fuzzy commitment scheme for authentication in biometric systems. This scheme is used in biometric data for error tolerance by converting the data into hash table and storing them in a server. This scheme deals with the leading problems in authentication of biometric systems.

Yau [20] addressed the classifier fusion which is the process of merging fingerprint and speech biometric decisions. They suggested constructing the various combinations of hyperbolic functions by a network model. The suggested hyperbolic function is to demonstrate the approximation capability. Finally, it is exercised to combining the fingerprint and speech identification and verification to generate the best results.

Veeramachaneni et al [21] proposed an adaptive multimodal biometric management algorithm for multimodal biometric. It is a developing approach towards applying to the biometric security for the sensor management. It is an adaptive method because, according to the users requirements, it is adapted in time. To use the best results and provide a suitable performance, it selects a fusion rule as well as uses the sensor operating points.

The starting point for validating different studies of biometric based remote authentication systems is considering their vulnerability against different attacks that show the level of secrecy of them. However, some protocols [22–34] operate within an anonymity preserving simple, hybrid-based, and secure computation based schemes.

In [22], Li et al proposed an authentication scheme for E-health care application and considered flaws of the security of Amins scheme [35] for E-health care systems. Amins user authentication scheme doesn't provide the intractability of the patients as the clients of the system. Furthermore, their scheme has some flaws in changing password and the initialization phase. In addition, their scheme lacks the detection mechanism for an unauthorized login initiated by an invalid password, and just because of this, their scheme is vulnerable to the DoS attack if the patient updates his/her password mistakenly. Li et al investigated these problems and proposed a health care based scheme and their scheme covers a good number of functionalities but it is vulnerable for various attacks.

In [23], Islam et al cryptanalyzed the scheme of Li et al [36] for the security loopholes of the smartcard-based remote user password authentication. Li et al's

scheme [36] is vulnerable against the lost/stolen smartcard attack, as known the session-specific temporary information attack and the insider attack. Islam et al investigated these problems and proposed an authentication protocols covering a low number of functionalities.

In [24], Byun et al proposed an authentication scheme based on the smartcard-password. They proved their scheme satisfies security of the session key and the identifier anonymity. Moreover, their protocol generated two long-term secret mechanism for protecting client's identity and setting key in mutual authentication. They claim the protocol guarantees the client's privacy where nobody except server knows which client is communicating with the authenticating server. However, their protocol faces problem when there are several clients in the system and several requests to authenticate. In addition, their scheme computation efficiency is not optimal compared with other similar studies.

In [25], Mishra et al presented an authentication scheme with a pre-smart card authentication that obtains anonymity for Telecare Medical Information System (TMIS). They claim the protocol is efficient in the login phase and the password change can be done without server assistance. Moreover, their scheme satisfies anonymity, client's privacy, mutual authentication and session key agreement. However, this protocol has low storage efficiency compared with similar works.

In [26], Giri et al improved the scheme in [25] to get a more secure and efficient scheme for TMIS. However, the scheme doesnt satisfy anonymity criterion and is vulnerable against many attacks including server masquerade attack.

In [27], Lu et al presented a biometric-based authentication scheme with three factors, which was specialized for multi-server systems. They claim their scheme fulfils perfect forward secrecy and prevents many attacks. This scheme has an average level resistance but the communication efficiency is low and is not suitable for implementation in some real-life applications.

In [28], Wazid et al proposed a provable secure and efficient three-factor remote user authentication scheme for TMIS. The proposed scheme prevents many attacks and its functionality coverage is at average. However, its computation and communication efficiencies are not compatible with other similar works.

In [29], Chuadhry et al proposed a multi-server authentication scheme where client is registered one time and then he/she can access to the services and data as many as she/he desires. In fact, they improved Lu et al's scheme [27] by presenting a biometric-based authentication scheme for multi-server environments, which has an acceptable resistance and the functionality coverage. However, they proposed an authentication scheme for biometric data while they did not focus on the security of the biometric data and the privacy of clients was not considered.

In [30], Cao et al proposed a multi-factor biometric authentication scheme consisting of slightly high computation efficiency. Moreover, their protocol withstand some attacks but cannot fulfill the perfect resistance and it has very low functionality coverage.

In [31], Wang et al presented a novel biometric-based multi-server authentication and key agreement, which is an improvement of Mishra et al's scheme [37]. Moreover, they added some authentication features including user revocation or re-registration and biometric information protection. However, their scheme is vulnerable against attacks: insider, server masquerade and user impersonation.

In impersonation attack, adversary can successfully assumes the identity of one of the legitimate users in a system or in a communications protocol. The goal of a perfect authentication protocol is to make negligible the probability that, for a given user U, any user C distinct from U, processes the protocol and playing the role of U, can cause server to complete and accept U's identity [31].

In [32], Khan et al proposed a TMIS based scheme to facilitate sharing electronic health records and medical documents over an insecure public channel. They utilized chaotic maps to provide anonymity and intractability along with computational efficiency. However, their scheme is not able to withstand perfectly against various well-known attacks including user-impersonation attack.

In [33], Lu et al cryptanalyzed and improved Arshad et al's scheme [38] to propose a biometric-based remote authentication scheme for TMISs. Moreover, they utilized the hash function and ECC nonce to satisfy some security features with improving the computational cost. Furthermore, their scheme has the good resistance, the good functionality coverage of security, and the good computation-communication-storage

efficiencies but not ideal, i.e. security attacks including smart card attack are not prevented.

In [34], Park et al improved Cao et al's scheme [30] by presenting a scheme that provides anonymity and perfect security functionalities. This multi-factor biometric authentication scheme also provides the dynamic ID mechanism and is resistance to attacks off-line ID guessing and server masquerading.

One of the common network attacks is the masquerade attack, where the attacker pretends to be some part of network which he is not. Clients on that network who wishes to authenticate, send their current logon credentials to this fake server [34].

In [36], Li et al proposed smartcard based remote user password authentication scheme that bears from smartcard attack and insider attack. In addition, the scheme has no provision for lost/stolen smartcard revocation with the same identity. In addition, the scheme has no feature for user revocation/re-registration. Since the scheme is based on authenticating smartcard and password, therefore off-line password guessing attack should be investigated. Moreover, many schemes including [38] fail to protect against off-line password guessing attack.

In [37], Mishra et al proposed a biometric-based multi-server authenticated key agreement in which specialized for multi-server environment. Mishra et al claimed that their scheme satisfied the user anonymity and all security attributes. However, the scheme is vulnerable against the masquerade attack, replay attack and DoS attack. Moreover, the scheme doesnt fulfill the perfect forward secrecy as well as the user revocation or re-registration. These features are satisfied in the most of existing authentication schemes.

Tan et al [39] studied a biometrics-based authentication scheme for medical information systems that operates over internet or mobile networks to provide health monitoring and other healthcare-related services for patients. They proposed that their scheme prevents many vulnerable attacks. Some months later, Yan et al [40] showed that Tan et al scheme is vulnerable against the DoS attack. They improved the scheme to prevent it from the mentioned attacks to obtain more secure protocol with higher performances. Later, the improved scheme by Yan et al was investigated by Mishra et al [41] for other common attacks in the context of the biometric authentication

cryptosystems. They claimed that the scheme of user-name/password login/change proposed by Yan et al. It is inefficient to verify the correctness of client's password such that the password change can cause the Denial of Service (DoS) attack. However, they did not consider the security and replay and MITM attacks. Moreover, their improved schemes suffer from the lack of perfect forward secrecy. These shortcomings were resolved in [42] by three-factor authenticated key agreement concept. Amin et al [35] and [43] presented two biometric authentication schemes: (1) in [35] they considered three attacks: (a) impersonation, (b) smart card theft, and (c) session key computation and then enhanced the three-factor-based authentication, (2) in [43] they proposed an anonymity preserving remote patient authentication scheme for healthcare applications. They investigated their scheme under BurrowsAbadiNeedham (BAN) logic and used different models to prove the security of their model.

Li et al [44] analysed the proposed scheme in [43] and found some lacks of security in terms of the patient feature where a password check mechanism leads to the system vulnerability to DoS attack. Moreover, they proposed that updating password wrongly by some patient makes the system vulnerable to DoS attack. They considered these faults and proposed a biometric authentication for E-healthcare that was investigated by [45]. Ali et al in [45] found vulnerabilities to attacks: identity and password guessing, privileged insider, user impersonation, and smart card theft. They use BAN logic and random oracle model to validate their scheme.

We selected schemes in [22–34] to compare results to our scheme in terms of security features (resistance), the functionality coverage, the computational efficiency, and the communication/storage efficiency in Section 3. Moreover, we investigated these schemes in detail and provided their runtime and storage consumption.

The proposed protocol is a secure protocol where non-invertible function in which no body can comprehend information about input by output. This way, this concern (template protection) was respected leading to counteracting the many attacks intended to access the original biometric traits. In addition, our scheme provides a non-deterministic method meaning that when a client wished to be authorized several times, the protocol would generate a unique tuple. This is why that the privacy of user's identity and activity is not perfectly respected, which may lead to the linkage attack. In this case, the user may revoke her/his information in the system.

Furthermore, since two servers as registration server and authentication server are utilized for enrolling users and authorizing clients respectively, clients can trust to the untrusted authorizing servers (through an unsafe network) to be authenticating within their critical biometric information. It means that a tuple for every client are generated remotely and then sent through an untrusted environment to the authentication server.

The thesis continues as followings. In Chapter 2, we explain our study in three parts to address requirements basically and in the two extended manner as well as its cryptanalysis, respectively. In Chapter 3, we consider the results obtained by applying our proposal on Datasets CASIA-Iris-V1 and UBIRIS and then discuss performance of our proposal compared to other studies in terms of efficiency, computation time, and precision and accuracy. Finally, in Chapter 4 we draw conclusions and propose future work.

2. THE PROPOSED METHOD

Considering Section 1, our scheme is proposed in three parts where in part 1 we propose our approach to satisfy the concerns basically. Then, in part 2 we extend the approach presented in part 1 to face the threats may occur yet. In part 3, we improve our approach by adding some new functions and smartcard concept to enhance the security and functionality of the protocol. Before sketching these parts, we should state some explanations. We published parts 1 and 2 in Papers A-E (listed at Appendix A.2).

2.1 Biometric System Configuration

A biometric system recognition contain some levels from capturing data to authorizing user. Figure 2.1 shows basic levels of a biometric system [46].

2.1.1 Data capturing

To record or read biometric traits, individuals raw information should be captured and converted to digital information [47].

2.1.2 Feature extraction module

To extract features from the captured biometric traits, usually one or more preprocessing modules are required; these modules is responsible for enhancing the quality of the captured information as well as detecting artefacts from the information. Preprocessing helps the feature extractor to pick up distinct salient information of biometric trait. In Figure 2.1 the “process” block shows the preprocessing operation. In this figure, the “template database” was considered for extracting and storing features. Feature extraction means the process of creating expressive and digital representations. this information is obtained from output of the “process” block and gathered in feature sets. Ideally, a feature set should be unique and the feature sets obtained from different samplings of one individual should be same; this means that operations such as rotation

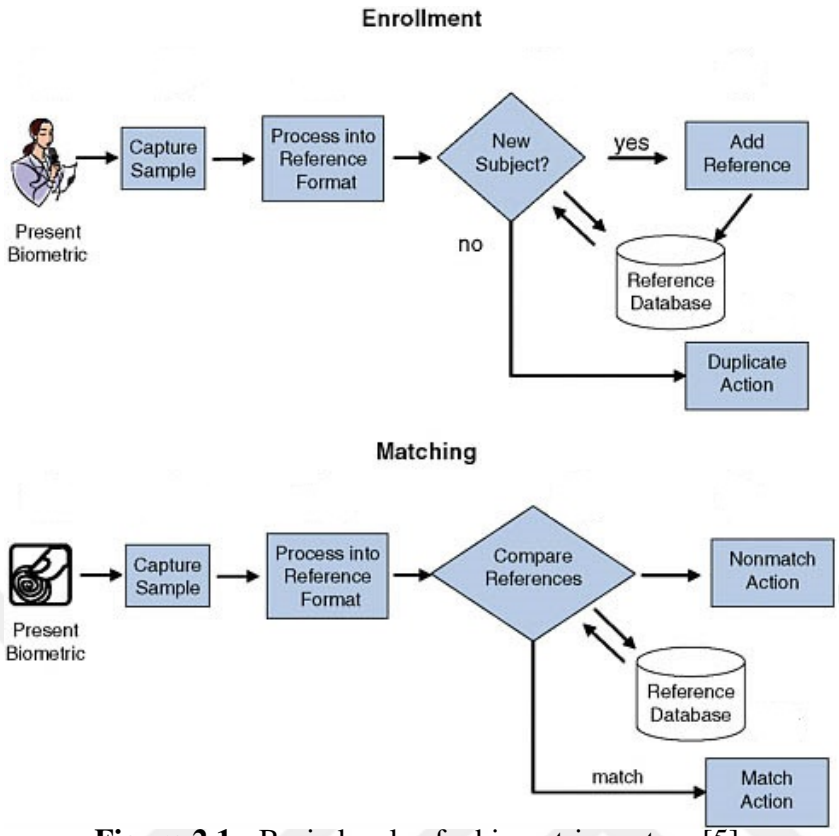

Figure 2.1 : Basic levels of a biometric system [5].

and artefacts should not effect on the quality and quantity of the feature sets. In the authentication process, feature sets are stored in the memory as main template [48].

2.1.3 Matching module

This module compares the feature set of a user with the enrolled individuals feature set that have been stored in the system memory. In fact, this module evaluates the similarity of feature set of a new user with the most similar set in the memory and assigns a score to the found set. This score forms a decision criterion for the next block; therefore, choosing an accurate matching algorithm is a principle stage [47,49].

2.2 Multibiometric System Recognition

The difference between a multibiometric and a uni-biometric system is the individual information *fusion*. The information fusion is a way to improve the accuracy of the matching step based on just template without referring to other techniques [50]. The process of fusion can be performed at the matching time or later. The matching and decision fusion levels are called biometric and cryptographic levels, respectively.

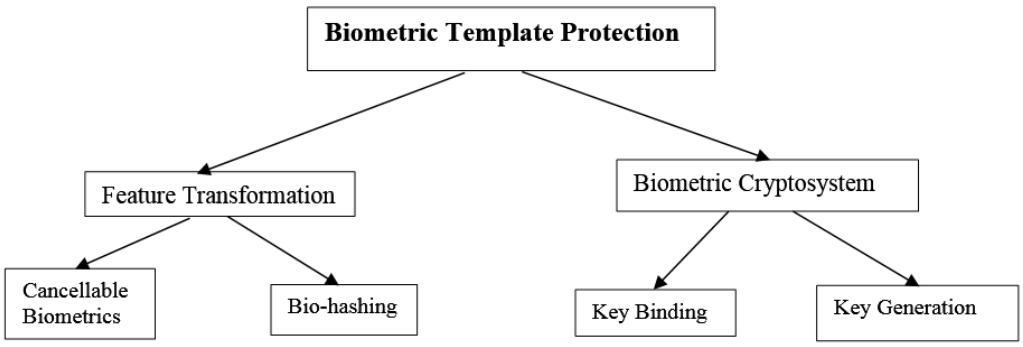

Figure 2.2 : Categorization of template protection methods [22].

2.2.1 Biometric template protection

To obtain a public acceptance level and user confidence, the reliability aspect of biometric authentication systems should be improved. As explained, there are many attacks in different stage of authentication. One of the very common attacks is "template attack in database" through which intruder pervades database to add a new template or modify or delete an existing template [51].

Traditional cryptographic systems cannot protect the personal biometric information as well but if every user creates individual password(s) as secret key(s), the system can provide more security with a protection layer for the user's information template. On the other hand, there is no need to decrypt an encrypted template of an enrolled person because the system can encrypt the user template with the users passwords and then comparing the results with enrolled persons encrypted template. Thus, there is no need to keep any password as well as the decryption process. A non-invertible cryptographic system doesnt need to store password because any password is so reliable [50, 52, 53].

Generally, two types of securities are provided by cryptosystems to protect a template: feature distortion (transformation) and Biometric cryptosystem (Figure 2.2) [47, 54].

- Using the "Feature Transformation", the system is able to create an encrypted template so that decrypting or restoring original information would be impossible. This transformation would be done so that original information shouldn't change. Therefore the transferring signals would be intentionally distorted. In the matching step, distortions is made based on user's biometric information for comparing with enrolled signals. Disadvantage of this system is that it needs to the a transforming key to make the same distortion on enrolled persons template and the user's one.

Thus, the key should be saved with the biometric template. There are two solution to face this problem: (a) Applying a non-invertible distortion so that an intruder can't obtain the original information if he/she found out the key and (b) Biometric salting. To use these two methods, we need so secure hashing functions or bio-hashing with low error rate [47, 54].

- The "Biometric Cryptosystem": (a) protects a template via new key generation and encryption techniques. (b) efforts to generate a strong data such as "helper data" to face copying, sharing and distributing templates. (c) drives a sketch from an enrolled biometric template and stores it as a function or new template instead of the original template in its memory. (d) performs the matching process indirectly and through restoring key. As we know, key has an essential role in such a system. The Biometric cryptosystems are a key binding system (which stores key through biometric template) or a key generation system (in which cryptographic key is obtained from biometric queries and helper data of biometric template) [51].

An automated authentication system operated through biometric data, creates a secure guarded port for the access control. Moreover, it is considered as a lock and a mechanism for preserving critical data or controlling access of clients who wish to enter to the system. In order to develop such a system, traits of users as legitimate matters are collected and stored in a secure database where used to authenticate the traits received from clients in the identification verification round [51].

A multibiometric system includes the concept of fusion by which we are able to improve the performance and accuracy of an identification system in search of a set of features in the space of features of the enrolled persons. Taking into account privacy of biometric, template security is not enough for a completely secure system. They are primary concerns (requirements) for a biometric authentication system that should be considered:

1. *Template protection:* The biometric trait of each user contains distinctive and personal characteristic data from which the biometric template is extracted. The protection of such template is a concern. To meet this concern, in the authentication process, server stores the template in its database. If the database is compromised by an enemy, the user's critical information can be revealed, that consequently might

imply the identification robbery of the client. In a secure biometric authentication scheme, the template is protected against some attacks.

2. *User's privacy:* in biometric based privacy preserving system, user's identity, biometric information and his/her activity should be preserved as far as possible. The leakage of any mentioned items leads to not preserving privacy. Moreover, if the system is cracked or the database is compromised, enemy can disclose user's identity and biometric information including habitats or medical information.

3. *Trust between user and server:* in order to implement a biometric authentication system, a user should send her biometric plains to the server to store his/her features in the database in a safe way. However, all servers may not be trustworthy for enrolment process, so a remote user cannot trust to any server to send her/his biometric information.

4. *Network security:* in addition to the untrusted server issue, insecure network is also capable of being intruded into by network attackers to compromise biometric information. Moreover, enemy may apply some attacks to grape biometric information being transmitted.

Disregarding any of these concerns leads to information leakage and vulnerability to attacks. A biometric based scheme should protect the privacy of biometric data as well as it should verify client accurately. Moreover, the scheme should authorize legitimated users and resist all attacks as possible as and deny all unauthorized accesses.

There are many proposed methods in biometric authentication for template protection. However, other mentioned concerns were not considered. Also, they briefly investigated possible attacks and their scheme performance. In some of studies, a template protection scheme where details are not clear. In a related study, authors mentioned multibiometric recognition and multi-modal biometric. They reviewed and combined biometric fusion and biometric template protection concepts. However, no attacks or main concerns were considered. In addition, a number of tools related to authentication schemes including homomorphic encryption were considered, but just the first mentioned concern "template protection" of the four main concerns related to biometric based verification system were considered. In a related study, authors

focused on the forth mentioned concerns of biometric based system, i.e. “network security. They deployed a scheme that was resistant against the network attack.

In one of the most recent work, a multi-modal biometric authentication system for untrusted distributed environment is introduced. They utilized (min-max) normalization method to calculate evaluation score. In this study, security criteria including accuracy, privacy, etc. are analysed. However, the proposed protocol is too time-consuming and computation and communication complexity effected on its accuracy.

Most studies on the biometric authentication provide security of client templates where details are not clear. However, the insufficient ability of these methods in the correction of errors causes insufficient accuracy in the matching process. Although to resolve such inability hash functions were proposed, they are not acceptable method in real world.

Some of matching protocols are secure techniques to address the authentication, but they are not able to provide both security and privacy of templates when the computations should be efficient. In a related study, applying of password and biometric technique at the same time and a combination of cryptography and steganography technique while communicating back to the user. Some secure authentication protocols uses mask vector methods, however none of them can provide acceptable security of templates or their computation complexities are inefficient to use in the real world.

In this thesis, we consider security features and functionalities, and processing costs of related studies (Paper E). There are seven types of attacks that are considered in this thesis: (1) replay, (2) password-off-line guessing, (3) insider, (4) server masquerade, (5) smart card, (6) user impersonation, (7) FAR, (8) Man-In-The-Middle (MITM), (9) linkage, and (10) hill-climbing attacks. In the most schemes in the literature, attacks 8-10 have not been considered (See Section 2.3.3.1).

We also overviewed literature and obtained six security functionalities (Paper E): (1) anonymity, (2) mutual authentication, (3) session key agreement, (4) perfect forward secrecy, (5) user revocation/re-registration, and (6) biometric information protection. Some overheads incurred in providing security by the schemes. They are the costs

considered for (1) Smart card Storage, (2) Communication, (3) Computation as well as the estimated time. For the storage requirement, we consider overhead arising from the messages that should be stored in user's smart card. For the communication overhead, we consider computation overheads in the registration, authentication, and total execution overhead. Considering these overheads, we claim that the proposed scheme provides more security and is applicable for real time applications.

2.3 The Proposed Protocol

Our proposed protocol, presented in three parts. In part one, we propose the fundamental of our protocol, i.e. digest based authentication. In part two, part one is extended for the problems unsolved in part one, consisting of information leakage and some attacks. Finally, in part three, the remaining unsolved problems deal with consisting of security features and improving functionality and performance. In addition to solving the problems, we proved our method by cryptanalysis formal method. In each part, we present the required definitions, related algorithm, its algorithm steps, and efficiency analysis.

2.3.1 The Basic proposed protocol

2.3.1.1 Definitions

Before presenting definition, we describe some concepts and the parameters used in definitions:

Mask Vector (MV): Suppose that X is a biometric feature vector of a client. A Feature extraction algorithm using vector X can produce a same length vector (called Mask Vector $M(X)$) with reliable and unreliable bits of original vector. It is a Boolean vector where values 0 and 1 denote unreliable and trustable bits respect to original vector, respectively. This vector can be used in matching process. Therefore, every biometric has a MV that averagely contains %15 until %25 unreliable bits.

Parameters: Let n and m be two large prime integers and $N = nm$. Then, for composite groups with order N, the hardness of the Discrete Logarithm Problem (DLP) indirectly is converted to that of factoring N. For a high security level (with selection of very large factors), factoring N is impossible. Disadvantage of this technique is that performing

group operation for large composite groups is slow leading to complicated operations. Moreover, the security degree of our system depends on hard DLP or problem of determining x from g^x mod N (an element of finite group G with a random generator g).

Let: 1- security parameter π means generating π bit prime p. 2- G is group of order p over an additive group and 3- g is one of random generators of G. Our system is based on a special generator to resist many attacks making the system faster. Such generator can produce a group with specific property, e.g. at first, the group order provides the homomorphic property for our protocol. The descriptions stated above are used in following definitions.

Definition 1. <*PK, SK*> = KeyGen(π):

Let G be a cyclic group with generator $g \in \mathbb{Z}_n$. If the security parameter be π, compute <G, g, n, m, N, s_1, s_2, α, β>$\leftarrow G(\pi)$, output

-the public key *PK*=<g, m, n, N, $u = s_1, \quad \alpha = \phi(m) >$,

-the secret key $SK =< \beta = \phi(n) >$,

-the system parameter is $SP =< s_2, n >$,

-the helper parameter $HP =< u, \quad \phi(N) >$ which is used to generate an individual digest in *authentication request time*.

Trapdoor in the verification process is $< \beta >$.

Definition 2. <$D(X)$> = Digest Generation (*PK, SK, X*):

To generate digest of original person (client) X at pre-authentication request time, using $< PK, SP, HP >$; Calculate $X \equiv a(\text{mod} m)$ from biometric vector (X) of original person and output $D(X) =< F(a) \bmod N >\in \mathbb{Z}_N$ to save in database. $F(a) = g^{(s_2 na)\phi(N)} \bmod N$ is a secure one-way function and $s_2 \in SP, n \in PK, \phi(N) \in HP$.

Definition 3. <$d(X')$> = Semi-digest Generation (*PK, X*):

Input semi-digest of new individual biometric vector *X'* to output $d(X') =< F(b') \bmod N >= g^{(X'-umb')\alpha} \bmod N \in \mathbb{Z}_N$ of $X' \equiv b'(\bmod n), < u, m >\in PK, \alpha \in HP$ at *authentication time*.

Definition 4. <K,M> = Homomorphic operation (I, J, mask(I), mask((J)):

In order to fuse two digests/semi-digests, the protocol homomorphicaly multiplies them to get one fused digest/semi-digest. moreover, all two corresponding bits of digests/semi-digests are multiplied in mod N. In order to fuse two mask vectors, all two corresponding bits of mask vectors are XOR. These operations are done within Equation 2.1 :

$$\begin{cases} K = I \times_h J \\ M = mask(I) \oplus mask(J) \end{cases} \tag{2.1}$$

Definition 5. <D> = Converting (d):

In order to compare two digests, the protocol utilizing SK, inputs a semi-digest and operates $D = (d)^{\beta}$ mod N.

Definition 6. <HD> = HD measuring (M,D,M',D'):

The protocol check HD of obtain individual semi digest with all one in database along with their mask vectors. Therefore, we have Equation 2.2:

$$HD\left(M,D,M',D'\right) = \frac{||\,(D \oplus D') \cdot M'.M||}{||M' \cdot M|} \tag{2.2}$$

Definition 7. < TRUE / FALSE > = Matching (HD):

Now the protocol compare obtained value to make final output Equation 2.3

$$Result = \begin{cases} \text{matched} & \text{HD} \leq \tau \\ \text{mismatched} & \text{O.W} \end{cases} \tag{2.3}$$

2.3.1.2 The Basic proposed protocol description

In this part, we propose a new concept in biometric authentication called *"digest"*. It saves a print of client biometric traits, which is output of a one-way function.

Furthermore, It allows one party, as client, to prove to another party (authentication server), that she is a legitimate individual, *without revealing to the authentication server what her original biometric data is*. The digest based authentication scheme, however, uses modular arithmetic and a secure one-way function to setup secure communication between the client and the authentication server.

Through applying the digest, we do not need to encrypt and decrypt biometric information, as well as we can utilize many efficient properties including homomorphic

and HD. Computing digest is fast and nobody can discover any primary biometric information using a digest.

An authentication system is modelled based on locations of: (1) storing the generated referenced of individual's biometric trait (or digest tuple), (2) fusing references, and (3) according (comparing) traits. Each of these locations may be the client side, or the server side. According to ISO 24745 [55], there may be several models based on these locations. Because of simplicity and being basic, we used the model where the locations of storing and accordance are the server side, i.e., the referenced digest is stored in the registration server database and the accordance is carried out by the authentication server. However, the fusion is performed both by the serve (for saving in the database system in the time of user's enrolment) and client (when user's traits should be authenticated). Note that: (1) the authentication server has access to the database and (2) we enjoy the fusion of references because of multi-modality of our approach.

Following, we describe the basic protocol algorithm in brief. Then, we explain every step in detail.

2.3.1.3 The Basic proposed protocol algorithm

In this section, we explain the basic proposed algorithm through Steps 1-8 which are included in two phases of *enrolment* and *authentication* in Figure 2.3. This figure includes two parts. Part A shows the general digest-based authentication and part B presents authentication process of a client with two traits.

The enrolment phase is processed through Steps 2-3 in off-line mode. The authentication phase that is the main part of authenticating system is done through Steps 3-8. In these phases, individual records multiple samples of his/her biometric, (Ex: *fp, iris*), Afterwards, from each sample, a feature vector, say X_i is obtained, and then user sends X_i, along with his/her identity, to the server.

Following, the system firstly feeds biometric vectors to the protocol (INPUT) and gets feedback of the protocol that is a result containing TRUE/FALSE value (OUTPUT). Following, we describe our protocol according to the definitions mentioned in Section 2.3.1.1.

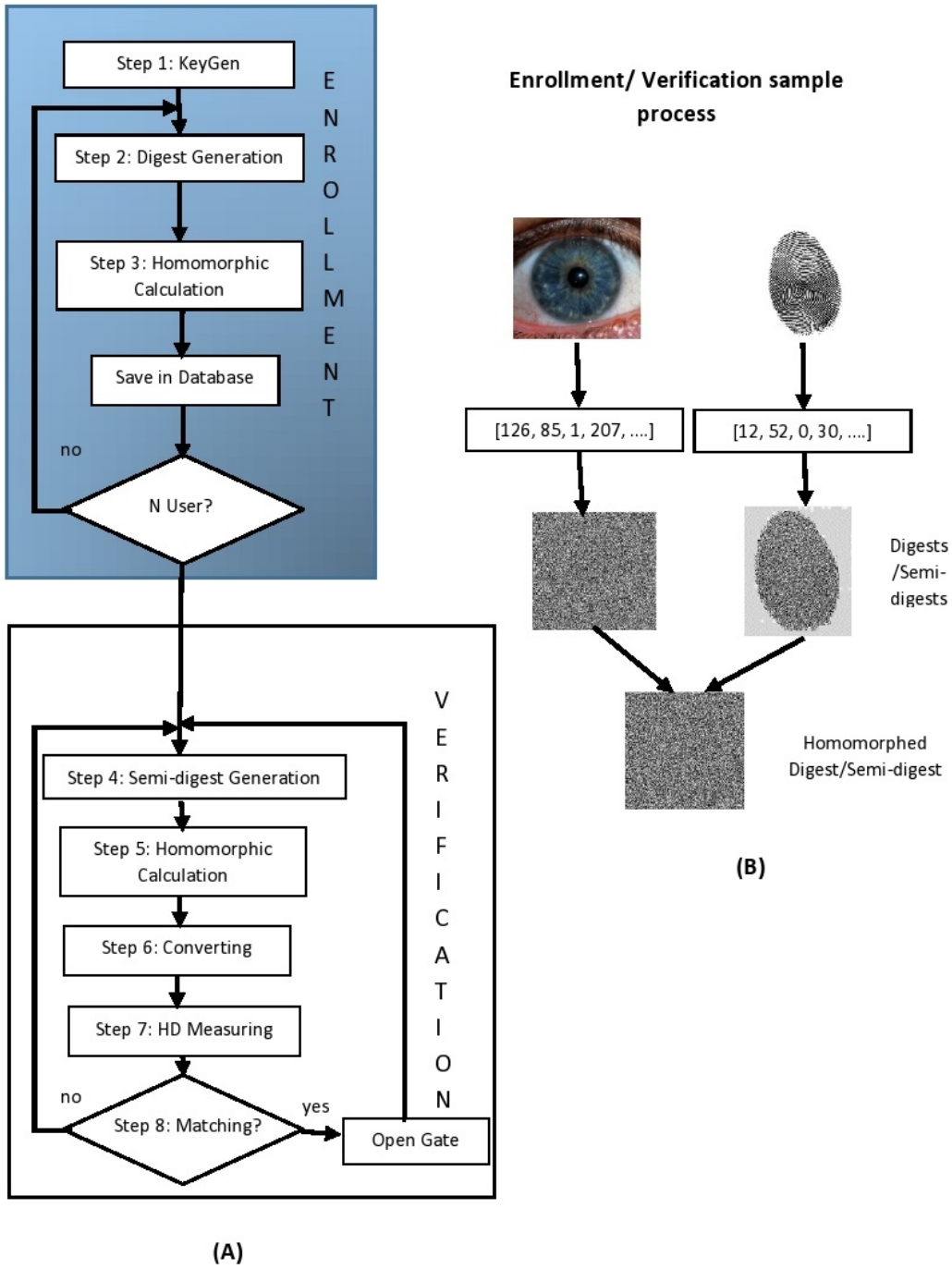

Figure 2.3 : Digest-based authentication flowchart (A), and client sample process (B).

Input: the client input's is biometric vector X, mask vector M, each $\in \{0,1\}^l$. The system has database of enrolled client digests and threshold τ .

Output: the system learns matching score of new individual and then notify individual about matching result.

The Protocol:

Step 1: System initializes: Set values of $< Pk, SK > \leftarrow$ KeyGen(π) (See Figure 2.3.A, step 1).

Enrolment (Off-line phase):

Step 2: $D_{clt}(X) =$ Digest Generation(PK, SK, X) $\therefore X \in$ {*fp, iris*} (See Definition 2, Section 2.3.1.1, Figure 2.3.A, Step 2).

Step 3: <D_{clt}, *M'*> = Homomorphic operation $(D_{clt}(fp), D_{clt}(Iris), mask_{clt}(fp), mask_{clt}(Iris))$: Equation 2.4 fuses D_{clt} of lris and fingerprint vectors of the client to output tuple < D_{clt}, *M'*>. The Equation 2.4 is explained in Definition 4, Section 2.3.1.1, Figure Figure 2.3.A, step 3.

$$\begin{cases} D_{clt} = D_{clt}(fp) \times_h D_{clt}(Iris) \\ M' = mask_{clt}(fp) \oplus mask_{clt}(Iris) \end{cases} \tag{2.4}$$

Tuple (D_{clt}, M) along with M will be save in database.

Authentication (On-line phase):

Step 4: d_{idv} = Semi-Digest generation (X'): The system process X' of client to get biometric vector X'.This function is explained in Definition 3 of Section 2.3.1.1, Figure 2.3.A, step 4.

Step 5: <d_{idv},M'> = Homomorphic operation $(d_{idv}(fp),\ d_{idv}(Iris)\ , mask_{idv}(fp),$ $mask_{idv}(Iris))$: the protocol obtains corresponding fused digest by calculating Equation 2.5, Figure 2.3.A, step 5.

$$\begin{cases} d_{idv} = d_{idv}(fp) \times_h d_{idv}(Iris) \\ M' = \text{mask}_{idv}(fp) \oplus \text{mask}_{idv}(Iris) \end{cases} \tag{2.5}$$

Step 6: D_{idv} = Semi-digest Converting (d_{idv}) : the protocol feeds semi-digest of client to convert it to corresponding digest by $D_{idv} = (d_{idv})^{\beta} \bmod N$, according to the Definition 5 of Section 2.3.1.1 Figure 2.3.A, step 6.

Step 7: <HD_{clt}> = HD measuring $(M, D_{clt}, M', D_{idv})$: The protocol feeds the input parameters to the HD algorithm of Definition 6 of Section 2.3.1.1 within Equation 2.6. Then HD value is obtained and will be passed to matching algorithm for decision Definition 5 of Section 2.3.1.1 Figure 2.3.A, step 7.

$$HD_{clt}\left(M, D_{clt}, M', D_{idv}\right) = \frac{||\left(D_{clt} \oplus D_{idv}\right) \cdot M'.M||}{||M' \cdot M|} \tag{2.6}$$

Step8: Matching (HD_{clt}): Applying matching algorithm (Definition 7 from Section 2.3.1.1), the client will be authorized (See Figure 2.3.A, step 8).

In Figure 2.3.B, after capturing the client's traits, the feature vector in form of numeric vectors are calculated. Then, their digests/semi-digests are obtained. In the next step, they are homomorphed to obtain one packet of data, called homomorphic digest/semi-digest.

Now, we explain Steps 1-8 in details:

We Firstly, system sets up our protocol by running KeyGen algorithm (Step 1). In this step, *PK* and *SK* as well as other system parameters will be initialized. Our protocol includes two phases: off-line and on-line. Moreover, clients and the server send messages in especial form to each other until the system identifies the original clients. To this end, every client should be registered through entering his/her biometric features using available instruments in the off-line phase. These instruments capture images and then process them to output vectors of *feature* and *mask* to cover errors as possible and send them to the enrolment algorithm. We utilize two biometric properties of Iris and fingerprint as biometric inputs of our presented algorithm. Hence, as first step of off-line phase, we capture this information. If it is not clear, system may gather some instances from one biometric property for the matching process to get the most accurate output, which will be achieved, by getting minimum HD measure. The minimum value is our criteria to compare with value of threshold τ.

After capturing the biometric information of every client and processing it to make biometric vector, our protocol should protect them in a safe way because any

Figure 2.4 : Six fingerprint samples (first raw) and their corresponding digests/semi-digests according to Algorithm 2.3.1.3 (second raw).

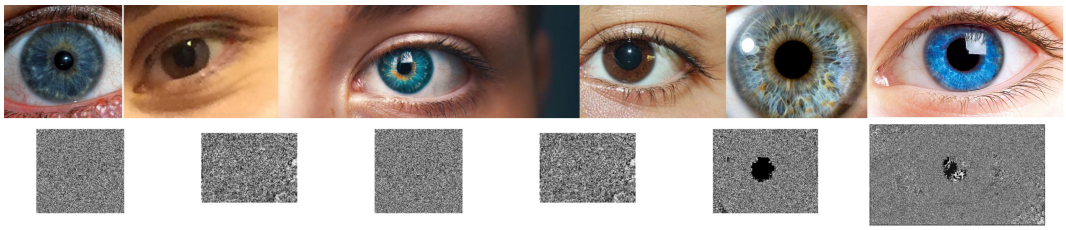

Figure 2.5 : Six Iris samples (first raw) and their corresponding digests/semi-digests according to Algorithm 2.3.1.3 (second raw).

information leakage causes damage to privacy of a client and makes the problem deeper. Since such kind of information is not reproducible, the biometric identification of a client may not be authorized again by any biometric authentication system. Moreover, the original information will not be trustable in any another authentication system.

Hence, our protocol does not save original information in database. Instead, our protocol keeps the information in cache for just some seconds in order to process it using mathematical one-way functions and convert it to different data with different formats and natures (Step 2). We name the final processed data *Digest*; Digests are values that nobody even system itself can identify the owner and the biometric property of the corresponding digest. Different digests of client will be fused with homomorphic operation (Step 3).

In other words, if an enemy captures our database and he/she cannot recover the original data of enrolled clients. Additionally, he/she cannot misused available digests, because at authentication request time or on-line mode, system accept just semi-digest data as input that needs one more processing step to output digest. This shows the high-level security of digests, which enables us to customize authentication process

even through the Internet. As mentioned before, our protocol may be customized for different applications.

For instance, for high-level security applications (e.g. army application), in enrolment step, we can obtain the password key associated with a client that is used in the digest processing step After generating all of fused digests, all of primary information is safely erased from the cache memory and the digest is transmitted to the system database. The database is set of all original digests whose owners and biometric properties are unknown.

Hereafter, if an individual wants to enter the system, the system will be able to identify him/her correctly as an authorized/unauthorized client.

In Figures 2.4 and 2.5, we show 6 fingerprints and irises as long as their corresponding digests/semi-digests. In some generated digests/semi-digests, there are patterns that show some information about samples (information leakage).

After completing the off-line phase and enrolling clients digests, the system runs on-line, i.e. it enters the authentication-request time phase of our protocol. An individual who request for authentication, enters his/her biometric information and the system captures it, process it to make fused semi-digest (Steps 4 and 5).

From now one, the proposed protocol starts comparing algorithms. It firstly combines semi-digest with the secret parameter of the system to generate the corresponding digest (Step 6). This digest will be compared with available digests in the database. This matching will be carried out using computation of the Hamming Distance measure of four parameters: (1) the stored digest, (2) its mask vector, (3) the new digest, and (4) its mask vector (Step 7). If the obtained HD is fewer than value of threshold , the client's identification has been matched (Step 8).

Note that, if there are some instances for a stored digest or if we have obtained some instances for a client through the instrumentation (for example, because of uncleanness), the matching process will compare all of instances pairwise to obtain the minimum HD. This value is compared with threshold value.

2.3.1.4 Performance considerations

Security Analysis:

We now consider proof of security; that is, nobody can violet privacy of an arbitrary client such that the verification algorithm accepts the validity of the forged digest. The security of privacy -preserving is based on the hardness of the DLP. More exactly, if adversary say **A** aims to duplicate or forge a semi-digest, it should break DLP.

Theorem: The proposed privacy preserving biometric authentication scheme is secure against adversary **A** in the random model if the DLP is hard in G.

Proof: We show that if **A** is capable of duplicating a non-valid semi-digest from original one, then on getting an DLP, instance g^a as challenge, the challenger **C** can use **A** to solve the DLP and get a. To do so, the adversary **A** outputs the biometric vector $X*$ which it intends to attack. **C** outputs a non-original but authorized digest $D*$ along with $M*$ as its mask vector, in which it HD. The main challenge in privacy-preserving is security and validation of digest of $X*$.

Digest generation Oracle: The adversary **A** queries Per-user digest generation oracle for biometric vector (*X, M*). The challenger **C** first queries $d_X(Iris)$ and/or $d_X(fp)$ for the challenge table. If so, it just retrieves corresponding d_X from the table. If X has not been queried for the *KeyGen* oracle before, **C** executes the simulation of the *KeyGen* and uses the corresponding *SK* to generate corresponding digest and add the value of d_X to the table.

Challenge:

Finally **A** outputs a new output including $< D_X^*, M^* >$ on biometric vector X*. **C** rewinds **A** to the point where it queries $< D_X * (\text{fp}), \quad D_X * \quad (\text{Ir}is) >$ and supplies a different value. **A** outputs another pair of digest $< D_{(2)X^*}, M_{(2)}^* >$. This is achieved by running the Turing machine again with the same random tape but with a different mask vector. **C** repeats and obtains $< D_{(3)}x^*, M_{(3)}^* >$. Note that $X*$ should be the same every time. We let a_1', a_2', and a_3' be the output of the modular operation oracle queried for the first, second, and third times. We now denote the discrete logarithm of $F(a_i')$ mod N, that is $g^{(s_2 n a')\phi(N)}$ mod $N = D(X')$. From the digest Equation 2.7, we have:

$$D_i^* = g^{(s_2 n a_i)\phi(N)} \bmod N \therefore X \equiv a_i (\bmod m); \quad i = 1,2,3 \tag{2.7}$$

C solves for these values from the above three linear independent equations and outputs $\phi(N)$ as the solution of the DLP.

Linkage attack: in this attack, adversary aims to track a legitimated client who registers in different biometric verification systems. Moreover, adversary monitors client's activity on-line and then using different helper data; she can compromise privacy of client. Our scheme is safe against this attack, because 1- in authentication request time, client sends helper data which is hard to obtain according to DLP, 2- every time, client sends different biometric digests where helper data is the same but random numbers are different. Therefore achieving biometric digest of a client cannot leak any information about biometric properties of that client.

Brute Force attack: this attach is an exhaustive search on all possible biometric traits. It requires massive amount of computation to crack scheme. In our scheme, we consider very large number for p and q so $N = n_I.n_2 = n_I.p \cdot q$ will be very large and hard to crack.

Efficiency Analysis:

The computation cost of our scheme on pre-authentication (off-line phase, $2EXP + 1GM$ See abbreviations) and authentication request time (on-line phase, $3EXP + 1GM$) is less than related studies, EXP and GM denote bilinear pairing evaluation and scalar multiplication, respectively.

2.3.2 The Proposed protocol-extension 1

In our extended model, we extended the definitions stated in Part 1, as follows:

2.3.2.1 Definition

Definition 1. KeyGen(π)

Input π to calculate $G(\pi)$ where $(G, g, n, m, N, v, \mu, \alpha, \beta, h = g^{\alpha}) \leftarrow G(\pi)$ and output:

-Public Key $PK =< N, g, h = g^{\alpha} >$: $\alpha \in \mathbb{Z}_Z$ randomly,

-Master Secret Key $MSK =< \alpha, derand >$, which is a *random* number and used for the authentication process at the authentication server side,

-$SK =< n, v >$ as the user's Secret Key is used to generate individual semi-digest in the authentication time at the client side,

-Helper Parameter $HP =< m, \mu >$ is used to generate an individual digest in the enrolment time.

We assume that public key N is large enough for factoring; therefore, extracting SK from PK is impossible. In order to de-randomize the expression that is received by the authenticating server, the server multiplies the received expression by the *derand* parameter from Equation 2.8. Moreover, *derand* cancels the effect of ephemeral key from semi-digest value.

$$derand = \left(h^{tN} \bmod N\right)^{-1} \bmod N \tag{2.8}$$

Where is the number of biometric samples (or feature vectors), which in our protocol, i.e., fingerprint and iris. where t is the number of biometric samples (or feature vectors), which t = *2* in our protocol, i.e., fingerprint and iris.

Definition 2. <d_i> = Digest Generation (PK, HP, X, ID): in order to generate digest of biometric feature vector (client) consider:
-Biometric feature vector is a k-bit vector $X_{i,j}$
-Calculation of $X_{i,j} \equiv a_{i,j}(\bmod m)$ from plain-biometric vector bits of $X_{i,j}$
-Calculation of $l_{i,j} = \left[\left(X_{i,j} - \mu a_{ij}\right)\right] \bmod N$
-Calculation of $d_{ID}\left(X_{ij}\right) =< F\left(l_{i,j}\right) \bmod N >= h^{l_{i,j}} \bmod N \in \mathbb{Z}_N$
Tuple $d_i =< d_{ID}\left(X_i\right), \mathrm{mask}\left(X_i'\right), g^{ID} \bmod N >$ is the output.

Definition 3. <$D_{ID}(X)$> = Fusing-Digest-Homomorphic operation (PK, d_1, d_2): In our protocol, corresponding fused digest tuple D_{ID} is generated and saved in the system database. Using the homomorphic property, we fused digest of k-bit fingerprint and iris vectors. In addition, associated mask vectors are fused in one k-bit mask vector M that covers bits possibly with error, which was obtained by a scanning instrument in the capturing time. Here, our one-way function is $F(x)$, which ensures most of our security. The protocol calculates corresponding fused digest $d_{ID}\left(X_{1,2}\right)$ in Equation 2.9.

$$\begin{aligned} &d_{ID}\left(X_{i,j}\right) = \left[d_{ID}\left(X_{1j}\right) \cdot d_{ID}\left(X_{2j}\right) \bmod N\right] \\ &M_{i,j} = \mathrm{mask}_{ID}\left(X_{1,j}\right) \oplus \mathrm{mas}\,k_{ID}\left(X_{2,j}\right) \\ &D_{ID}(X) = \left(d_{ID}(X), M, g^{ID} \bmod N\right) \end{aligned} \tag{2.9}$$

where tuple D_{ID} is saved in the system database. We note that our protocol is homomorphic in the multiplication, at the server and client sides.

Using the homomorphic property, we fuse two digests of k-bit vectors $d_{ID}(X)$ to make vector D_{ID}. In addition, their mask vectors are fused in one k-bit mask vector M that covers bits possibly with errors, which has been obtained at the capturing time by a scanning instrument.

Definition 4. $<s_i>$ = Semi-Digest generation (PK, SK, X', ID'): client inputs new individual biometric vector X' that includes k bits: $X'_{i,j} \therefore i \in \{fp, \text{iris}\} = \{1,2\}, j \in \{1 \ldots k\}$ and then:

-Chooses ephemeral keys $r_i, \lambda_i \in \left(\frac{\mathbb{Z}}{(N-1)\mathbb{Z}}\right) \therefore r_i + \lambda_i \bmod N = 0$ at random for every feature vector;
-$g^{\lambda} = \prod_{i=1}^{t} \left(g^{\lambda_i} \bmod N\right)$;
-For every bit of vector X'_i with k bit, we have: $X'_{ij} \equiv b'_{ij} (\bmod n)$;
-$y_{ij} = \left[\left(vmb'_{ij}\right) + r_i\right] \bmod (N-1)\ sd_{ID'}\left(X'_{ij}\right) =< F\left(y_{ij}\right) \bmod N \geq h^{y_{ij} \bmod N}$
Make $s_i =< sd_{ID'}(X'_i), \text{mask}(X'_i), g^{ID\prime} \bmod N, g^{\lambda} \bmod N >$ as output. Ephemeral key r_i is a random number that is newly generated for every biometric feature vector bit.

Definition 5. $<S_{ID'}>$ = Fusing-SemiDigest-Homomorphic operation (PK, s_1, s_2): In our protocol, first the corresponding fused semi-digest $S_{ID'}$ is calculated at the client side as Equation 2.10.

$$\begin{aligned} sd_{ID'}\left(X'_{i,j}\right) &= sd_{ID'}\left(X'_{1,j}\right) \cdot sd_{ID'}\left(X'_{2,j}\right) \\ M'_{i,j} &= \text{mask}\left(X'_{1,j}\right) \oplus \text{mask}\left(X'_{2,j}\right) \end{aligned} \tag{2.10}$$

Then, Tuple $S_{ID'} = \left(sd_{ID'}(X'), M', g^{ID\prime} \bmod N, g^{\lambda} \bmod N\right)$ is sent to the authentication server.

Definition 6. $<D_{ID'}(X')>$ = Converting $(PK, S_{ID'})$: The authentication server converts $\left(sd_{ID,}(X'), M', g^{ID\prime} \bmod N, g^{\lambda} \bmod N\right)$ into fused digest $D_{ID'}(X')$ within Equation 2.3.2.1:

$$\left[sd_{ID,}(X') \cdot \left(g^{\lambda}\right)^{\alpha}. \text{derand}\right] \bmod N =$$
$$\left[\prod_i h_i^{\left(X'_i - vb'\right) + r_i} \cdot g^{\lambda_i \alpha}.\text{derand}\right] \bmod N = \prod_i h^{\left(X'_i - vb'\right) + r_i} \cdot g^{\lambda_i \alpha}. \text{derand} \bmod N =$$
$$\left[\prod_i h^{\left(X'_i - vb'_i\right)}.h^{tN} \cdot \left[\left(h^{tN} \bmod N\right)^{-1}\right]\right] \bmod N = \prod_i h^{\left(X' - vb'_i\right)} \bmod N =$$
$$\prod_i h^{\left(\mu na'_i\right)} \bmod N = D_{ID'}(X') \bmod N \ (2.11)$$

Definition 7. HD measuring: This algorithm operates similar to HD measuring algorithm explained in Definition 6 of Section 2.3.1.1.

Definition 8. Matching: This algorithm also is the same as Definition of Section 2.3.1.1.

2.3.2.2 The Proposed protocol description

We explain, Steps 2-8 of our basic protocol adapted to extended remote authentication system, in two cases: (1) enrolment for registering individuals (Steps 2-3) and (2) their authentication (Steps 4-8) (Step 1 is the same as Section 2.3.1.3). In this section, we have a glance at cases (1) and (2) that are improvement of basic protocol. Afterwards, we discuss them through Figure 2.6 for enrolment and Figure 2.7 for authentication where *improvements* are highlighted in red color.

Algorithm 2.3.2.3 gives a step-by-step description of the enrolment process. Note that the information that is passed from the enrolment server to the authentication server are just the users digest tuple, public key, the helper parameters, and a threshold value. To enroll a user, we utilize registration server as TTP that operates separately from authentication server. This server accesses all user's plain information. In previous version of the protocol, we had one server that made enrolment as well as authentication(highlighted in Figure 2.6). If user did not trust to authentication server, she could not able to send her biometric information to the server and so authentication process could not be perfectly done. Figure 2.6 shows enrollment process consisting of three levels, User, Registration server, and Database. The user level is responsible for: (1) capturing user's plain information using scanning equipment, (2) extracting features from the information, and (3) feeding the extracted features to Registration server (box 1 in Figure 2.6).

2.3.2.3 The Proposed protocol: enrolment algorithm

Firstly, the user provides her/his biometric features vector through feature extractor in box 1 in Figure 2.6.

Step 2: Digest Generation: The registration server collects X_i and uses the other system parameters to compute authentication digest $d_{ID}(X_i)$ along with its mask vector. (See

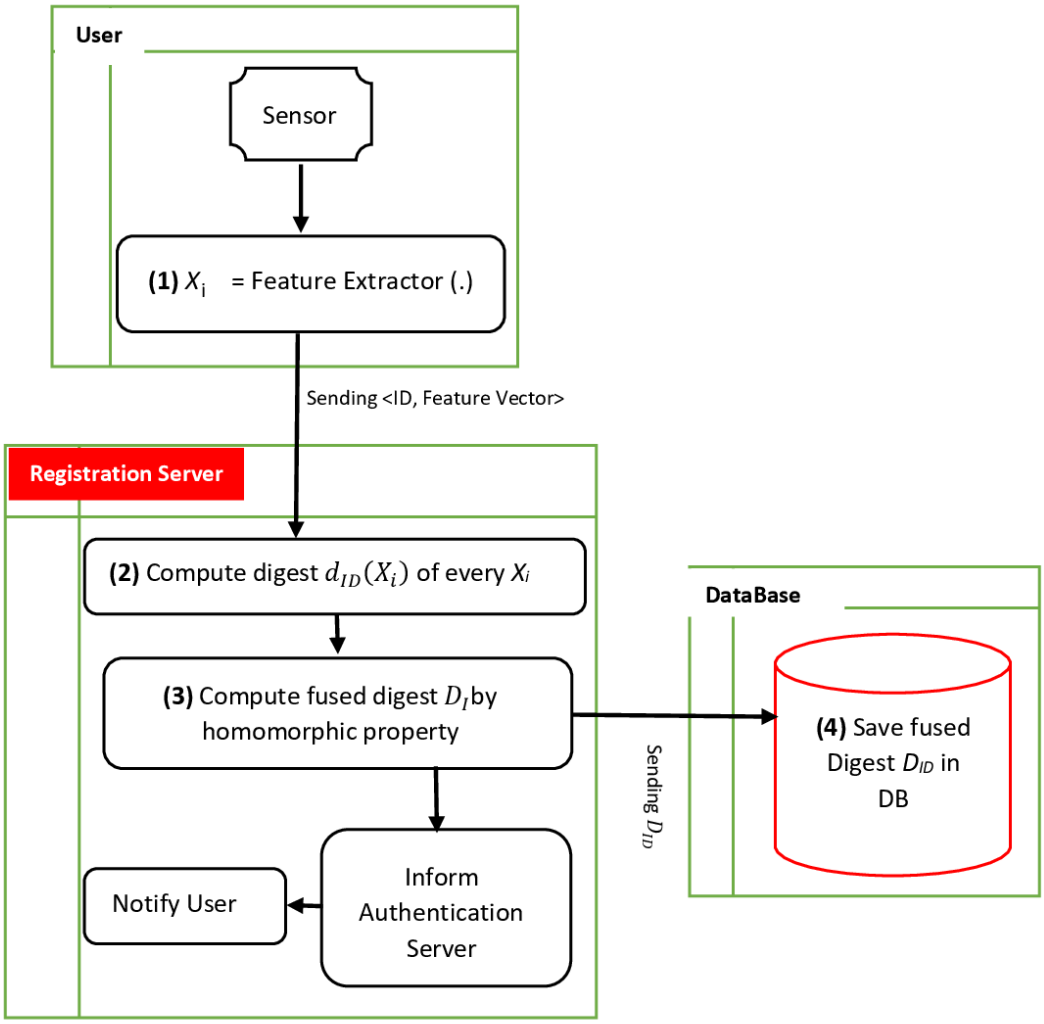

Figure 2.6 : Enrolment process (Paper C).

Definition 2 of Section 2.3.2.1). moreover, Using system parameters, the registration server computes digest of any biometric feature vector (box 2 in Figure 2.6),

Step 3: Homomorphic operation: The server calculates fused digest D_{ID} using the homomorphic property including the fused digest of every trait vector, the fused mask vector, and the locked user's identity with format $D_{ID} = \left(d_{ID}(X), M, g^{ID} \bmod N\right)$ (See Definition 3 of Section 2.3.2.1) for all legitimated users (box 3 in Figure 2.6). Then the tuple calculated above will be saved in the database (box 4 in Figure 2.6),

The user and the server are noticed about success now. Hereafter, user will directly contact with authentication server for verification.

2.3.2.4 The Proposed protocol: authentication algorithm

Assume the registration server (TTP) gives access authority to the authentication server for accessing the copies of the authorized fused biometric digests in database as well as helper parameters. These digests are calculated during the enrolment phase by the trusted registration server that trains for the users and for authentication server in the verification process. The trained parameter is locked and sent to the authentication server, and the ready notification is sent back to the client. is sent during KeyGen(π) process at the initialization time.

During the authentication process, the client's biometric signals are inputted to the feature extraction module. The obtained multi-feature bit vectors will be fed to the semi-digest generator module, as well as the system public key parameters.

Figure 2.7 shows the authentication process in the improved digest based authentication protocol, where the sensor unit records client biometric signals to feed to the feature extraction module. Client generates feature vector, $X'_{i,j} \therefore i \in \{1,2\}, j \in \{1,\ldots,k\}$ from test data for samples of fingerprint and iris, where t is the number of samples with k bits (box 1 in Figure 2.7),

Step 4: Semi-Digest Generation: In order to generate digest of every feature vector, client generates random number, $r_i \in \mathbb{Z}_N$ and $\lambda_i \in \mathbb{Z}_N$ such that, $(r_i + \lambda_i) \bmod N = 0$ (box 2 in Figure 2.7; highlighted in red).

Therefore, one is able to generate different semi-digest every time through a truly random generated number as ephemeral key. This prevents the attacker from matching

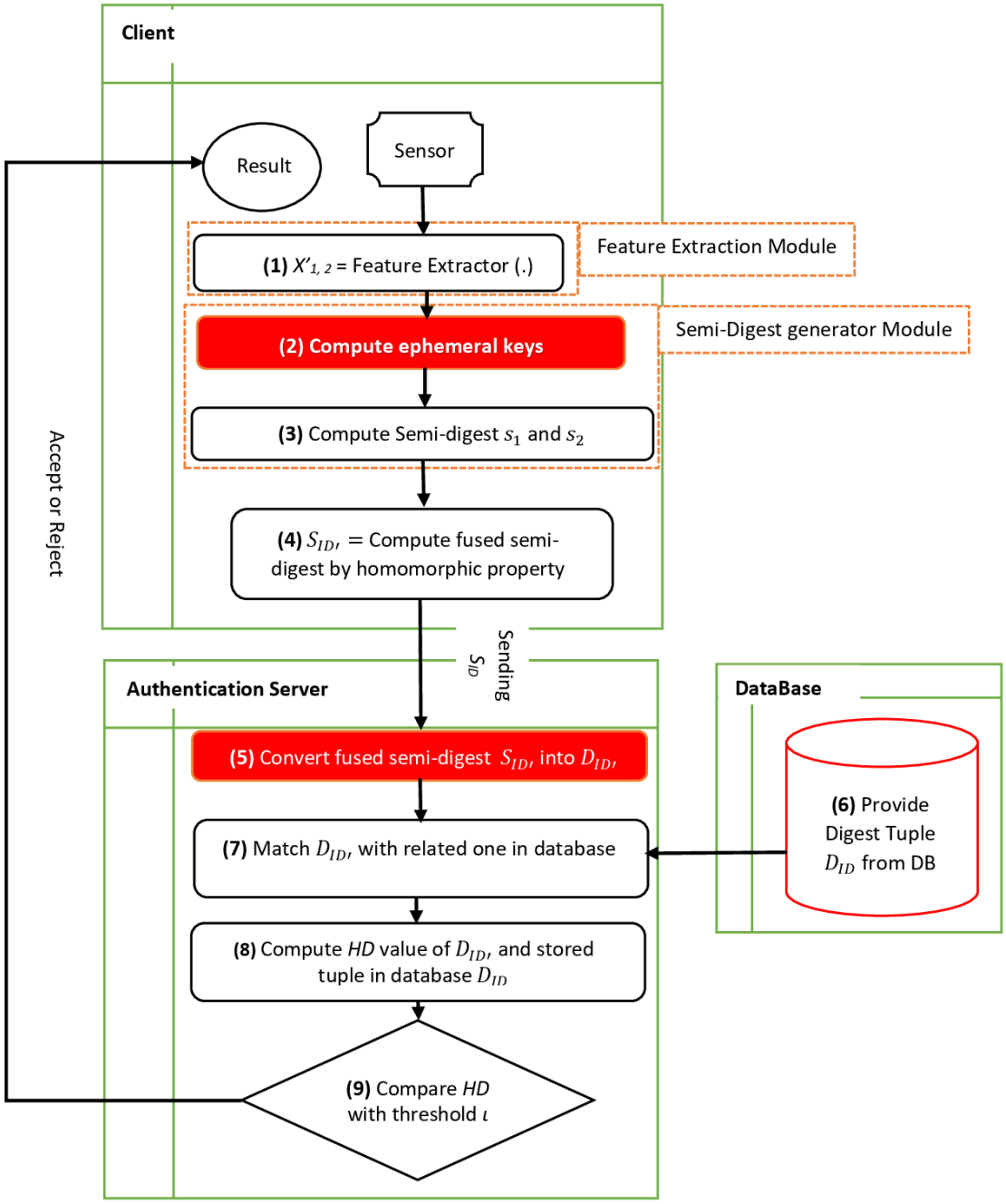

Figure 2.7 : Authentication process (Paper C).

the captured data belonging to one client who sends her semi-digest tuple several times with same biometrics and ID.

Furthermore,The privacy of our system is based on the ability of the client to generate ephemeral keys. We, thus, assume that the server can access to a truly random number generator (PRNG). Values are generated using PRNG while ensuring that the equations in this algorithm holds.

After generating ephemeral keys, the client computes b'_j as X'_j module n, Each feature X'_i is converted to semi-digest $sd_{ID}(X'_i)$ (box 3 in Figure 2.7). (See Definition 4 of Section 2.3.2.1).

Step 5: Homomorhic operation: Client computes fused semi-digest $S_{ID'} = \left(sd_{ID'}(X'), M', g^{ID} \bmod N, \prod g^{\lambda} \bmod N\right)$, by Homomorphic propert, in this tuple, fused mask vector is $M' = \text{mask}(X'_1) \oplus \text{mask}(X'_2)$. This tuple is sent to server (box 4 in Figure 2.7). (See Definition 5 of Section 2.3.2.1),

Step 6: Converting: Server computes $D_{ID'}(X') = \left[sd_{ID'}(X) \cdot \left(g^{\lambda}\right)^{\alpha}. \text{ derand }] \bmod N\right.$ as digest of X' (box 5 in Figure2.7; highlighted in red). (See Definition 6 of Section 2.3.2.1),

Step 7: HD measuring: Server matches lock of ID' of $S_{ID'}$ with related one and then calculates Hamming distance of obtained tuple using the counterpart stored in the database, (boxes 6, 7 and 8 in Figure 2.7). (See Definition 7 of Section 2.3.2.1),

Step 8: Matching: Server matches calculated HD to threshold value to decide on the ID authorization (box 9 in Figure 2.7). (See Definition 8 of Section 2.3.2.1), Client will be notified about the decision.

Note that nobody including authenticating server and the client are able to extract original traits from generated semi-digests (and digests). Moreover, to authorize the legality of the client, the authenticating server directly matches the stored tuple to the calculated semi-digest and does not reveal more information about identity of the client; therefore, it preserves the confidentiality of the system and secrecy of information as well as the client privacy. If an adversary compromises the system including data store, he/she cannot threat security of the system.

For simplicity, we initially assume that both enrolling and authenticating schemes accept feature vector X (or X') of length k as input. *In implementation phase,*

Figure 2.8 : Six fingerprint samples (first raw) and their corresponding *randomized* semi-digests according to Algorithm 2.3.2.4 (second raw).

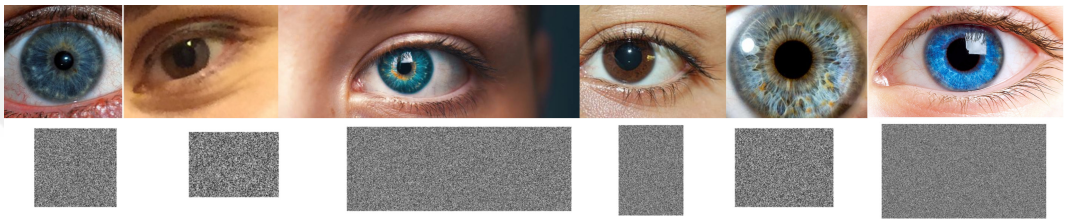

Figure 2.9 : Six Iris samples (first raw) and their corresponding *randomized* semi-digests according to Algorithm 2.3.2.4 (second raw)

Every biometric feature vector can be represented as a fixed length vector with k bits. Furthermore, we verify our work with two biometric traits $((X_{i,j} \therefore i \in \{1 =$ fingerprint, $2 =$ Iris$\}, j \in \{1 \ldots k\})$, *that are* X_{1j} *to* X_{2j}. Since our flexible protocol is a multibiometric authentication, no matter how many trait types, we utilize for implementation. Figures 2.8 and 2.9 show generated semi-digests of six fingerprint and Iris samples with randomized property. Compared with Figures 2.4 and 2.5, information leakage is solved. Moreover, there is no pattern between pixels of a generated semi-digest.

Since, we generates a randomized digest or semi-digest in which a truly random generated ephemeral key is used therefore, if some client sends her/his semi-digests several times, different tuples will be sent to the authentication server and thus an attacker will not able to extract any information from semi-digest as well as she/he will not able to discover the client's identity. Moreover, the attacker will not able to comprehend the semi-digests are sent by a single client.

A client is able to send a valid but different random semi-digest with locked ID in every verification request round. A locked ID is a combination of the client ID and a parameter, which maybe time or a random number according to the client desire. If this

tuple in leaked (for example in transmitting time), attacker will not able to comprehend any information about the user's identity or biometric data leading to client's perfect privacy. For the simplicity, in the presented protocol, we do not affect the time stamp or random number parameter. However, if client wishes, she/he can generate a different locked ID upon every verification round, by utilizing these parameters.

2.3.2.5 Performance considerations

In this section, we investigate our system resistance against the different attacks occurred from the outside including the impersonate attack by a malicious client or through an insecure network as a connection bridge between a client and the server. Such an attack leads to disclosure user's biometric data, illegal access, and/or deny the access when a user wish to log in. Here, we assess the system security through the amount of information that an attacker can extract from the transferred information or client/server actions that produce information. Privacy of the user is a part of user's information should be preserved securely.

ISO 24745 requirement In the following, we consider the cases stated in ISO 24745 in our proposal.

-Protected template structure: In our proposal, the Registration Server or (TTP) generates the digest of biometric traits as a pseudonymous identifier, which is the output of the one-way function. Using different auxiliary data, a user is able to create new digest, therefore our model is renewable/revocable. Furthermore, a user is able to generate a new semi-digest in the authentication time, using the user's Secret Key (SK), which is the auxiliary data.

-Security requirement: Since all of the biometric templates stored in the database are digested by a one-way DLP based function and the server has been saved just output of this function (digest tuple), cracking digest tuple is as hard as solving the discrete logarithm problem. This property guarantees the confidentiality of our protocol. On the other hand, data integrity can be achieved by replicating or transferring data into second place like the second database, which should be remain intact and unaltered between updates. Since the biometric digest can be altered by a system through different parameter, TTP can periodically update database leading to the data integrity. In addition, since in our system, semi-digests (or randomized digests) are transferred

through a public network, it is inherently impossible to extract original biometric template belonging to the same identity or it is renewable.

-*Privacy requirement:* Data references or digests are outputs of one-way function *F(x)*. This function ensures the irreversibility of a digest that satisfies the first property of privacy. On the other hand, there is no link between randomized digests (semi-digests) value; therefore, an adversary cannot distinguishes references from each other. This is considered as the unlinkability property. In addition, all users are registered in such a way both identity ID and biometric templates are locked. This property satisfies the confidentiality of user within the pseudonymous identifier.

-*Server requirement:* As stated in Section 2.3.1.1, we used the model where the store and accordance locations are the server side. To this end, we separated the enrolment session from the authentication process where a Registration Server or TTP included for the enrolment. The responsibility of TTP is generating keys and enrolling users within the their biometric traits. Having enrolled, TTP notifies the user (who trusts completely to TTP). A system database is considered to save output of enrolment process or output of digest generation algorithm within users biometric traits. Also, an authentication server is included for identifying a client who wishes to access to the system; this is done by collaborating the server with TTP. The authentication server may be untrustworthy.

In the enrolment session, a user should send his/her biometric traits to the TTP; then, the generated digest tuple is saved in the system database by TTP. Afterwards, whenever a client (who does not trust to the authentication server) wants to log into the system, she/he should send her/his semi-digest of biometric traits to be authenticated by the authentication server. This server tries to find and compare the received and converted semi-digest of the clients biometric traits with the corresponding data in the system database if there exist.

Most of the systems that act as an authentication gate between client and server provide little privacy for users/clients. Therefore, the trust between user and the server is a subject to more importance. A system with complete security that preserves privacy perfectly satisfies the mentioned concern. Following, we consider the system security consisting of the server security and client security.

System security

Security of our digest based authentication system is based on preserving the user's biometric information and actions. Therefore, we take a close look at all scenarios that may lead to user's information leakage. Firstly, we consider the client security with two possible attacks: (1) passive and (2) brute force. Then, we investigate the server security against two template attacks: (1) the Template access attack and (2) the multiple semi-digest attack. We discuss the security level of authentication server with the presence of an attacker in the: (1) client side, (2) server side.

- Client security:

  -Security against the passive attack: Attacker is passive and observes the outputs of semi-digest generation function and homomrphic function during fusing semi-digest generation of S_i. In such a situation, the attacker tries to extract necessary information from obtained equations. The first output is $s_i =< sd_{ID'}(X_i'), M', g^{ID} \bmod N, g^{\lambda_i} \bmod N >$ where:

  (1) $Sd_{ID'}\left(X_{i,j}'\right)$: The semi-digested value of biometric feature bit vector $X_{i,j}'$. Here, $sd_{ID'}\left(X_{i,j}'\right)$, semi-digest value of every bit of the feature vector is calculated but $b_{i,j}'$ and r_i are unknown. Moreover, there are semi-digest equations with k+1 unknown variables,

  (2) M_i discloses no information about original biometric feature,

  (3) Locked $(1D')$ also is separate from original biometric feature,

  (4) Ephemeral keys r_iS and λ_iS, are truly random numbers and attacker cannot learn any information about them from $g^{\lambda} \bmod N$.

  In order to discover original data, i.e. X', attacker should consider t linear congruences over $k+1$ variables $b_1, b_2, \ldots .,b_k$, and r namely, $Sd_{ID'}\left(X_{i,j}'\right) = h^{\left(\omega m b_{i,j}'\right)+r_i \bmod N} \therefore j \in \{1,\ldots k\}\ i \in \{1,\ldots t\}$.

  where t is the number of biometric traits and k is the size of the trait. Suppose that the attacker discloses some information about $sd_{ID'}\left(X_{i,j}'\right)$ (See Definition 3, Section 2.3.1.1). However, gaining access to original biometric vector X' (or b' is as hard as cracking the DLP algorithm.

  If, by any chance, specific variables $b_{i,j}'$ and r_i are suspected to be disclosed, it is impossible to recover the original biometric from semi-digest s_i, as it requires

$|\mathscr{S}|^{k+1}$ authentication trials ($|S|$ is domain of s_i. Moreover, the client could create another semi-digest by renewing ephemeral key or asking administrator to change system parameter n. We now show that the amount of effort required for doing this, is at least as much as randomly guessing the original biometric, and hence no additional information is revealed in principle.

Without losing the totality, let that n of $N = nm$ is too big such that $X \leq n \rightarrow X$ mod $n = X$. In addition, attacker just is able to see the output of operations in the computer memory. Thus, $y_i = r_i + \sum_{j=1}^{k} vmx_{ij}, i \in \{1,\ldots,t\}$ for t biometric feature vectors. Here, we have t congruences over $k+1$ variables. Now we show that solving this congruence for attacker is impossible; so, she should guess randomly X at least to obtain original biometric data.

Let that $|x| \subset |y| \subset |u|$ where X and U are domains of X_{ij} and r_i, respectively. We know that every set of t linear congruences reduces brute force attack complexity by $O(|y|^t)$. Thus, we estimate that attacker needs $O\left(|y|^{k+1-t}\right)$ to solve t congruences over $k+1$ variables of y_i.

As mentioned, we input a $k+1$ -bit biometric trait vector that all its bits have independent values. Therefore, the number of efforts to disclose original biometric vector X is $\mathscr{O}\left(|X|^{k+1}\right)$. We convert a biometric vector X to the corresponding semi-digest including y_i. Therefore, the domain of X is transformed to the domain of y with $\mathscr{O}\left(|y|^{k+1-t}\right)$. Moreover, we have: $|X|^{k+1} \leq |y|^{k+1-t}$.

Therefore, we have: $(k+1)\ln(|x|) \leq (k+1-\ t)\ln(|y|) \rightarrow \ln(|x|) \leq \frac{k+1-t}{k+1}\ln(|y|) \rightarrow \frac{\ln(|x|D}{\ln(|y|)} \leq \frac{k+1-t}{k+1} \rightarrow \frac{\ln(|x|)}{\ln(|y|)} \leq 1 - \frac{t}{k+1}$

If $y_i = r_i + \sum_j vmx_{ij} \overset{v=m_n^{-1}}{\longrightarrow} |y| \approx |\mathscr{R}| + \left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| \times \left|\frac{\mathbb{Z}}{m\mathbb{Z}}\right| \times |X| = |\mathbb{Z}_P^*| + \left|\frac{\mathbb{Z}_N}{n\mathbb{Z}}\right| \times \left|\frac{\mathbb{Z}_N}{m\mathbb{Z}}\right| \times |\mathscr{X}| = |\mathbb{Z}_N^*| + |\mathscr{X}|^2 \geq |\mathscr{X}|^2$, therefore, we have: $|y| \geq |x|^2 \rightarrow \frac{\ln(|x|)}{\ln(|y|)} \leq \frac{\ln(|x|)}{\ln\left(|x|^2\right)} \leq 1 - \frac{t}{k+1} \rightarrow \frac{1}{2} \leq 1 - \frac{t}{k+1} \rightarrow t \leq \frac{k+1}{2}$.

As mentioned, t or the number of congruences is at least one for $k = 1 \rightarrow \frac{k+1}{2} = 1 = t$. However, it always should be kept at least to satisfy more security. In this way, the domain of ephemeral key $\mathbb{Z}_{N-1}^*$ should be increased for complete security.

-Security against brute force attack: In this attack, the attacker tries to crack the system from a remote machine by trying all statuses. The complexity of brute force attack is equal to the guessing randomly all possible plain states biometric vector

say X is n bit biometric vector. The domain of guessing all cases is $\mathscr{O}(|X|^n)$ where $\forall \mathscr{X} \in \mathbb{Z}_N$. Therefore, the attacker should apply $\mathscr{O}(N^n)$ times on average to get success.

Totally, we show that the server is secure against all types of attacks and no illegal person can misuse the system parameters to get any information about registered users.

- Server security: We consider two possible attacks against the server and analyse system reactions

  -Template protection concern (Template access attack): An attacker can access the templates stored in the server database. In such a situation, since all stored biometric templates of the database have been digested by a one-way DLP based function and the server has been saved just output of this function (digest tuple), cracking such a digest tuple is as hard as solving the discrete logarithm problem. In addition, since our protocol is non-deterministic, the Brute force attack definitely is impossible, even for limited-range data.

  -Multiple semi-digest attack: The attacker receives several semi-digest tuples of one client who wishes to be authorized in the system. In this case, the attacker tries to infer value of X or value of y_i (as states in following equations) from multiple linear congruences. Every time that a client wishes to send his/her semi-digest to the server, he/she should scan his/her biometric traits. Then he/she submits the captured signals as well as related mask vectors (that are slightly are different from each other) to the protocol for creating the semi-digest tuple. Since these signals contain noise, they are not the same. These changes will be inserted in the outputted semi-digest, i.e $y_i = r_i + \sum_{j=1}^{k} vmx_{ij}, j \in \{1 \ldots t\}$ Therefore, for each tuple, the attacker should: (1) estimate the clients are the same, (2) estimate submitted semi-digests belong to the same traits where error values are not the same, and (3) calculate value y_i by considering the noise value (for instance, $y_i + error$).

  The attacker can utilize the gained additional information to solve t congruences in k+1 variables. This idea may come to mind that the attacker can create additional equations to solve main variables. Therefore, we show that the number of variables will be increased in every authentication (for every tuple) such that the attacker

is not able to specify value of any variable, considering biometric trait vector X_i affected by noise. Furthermore, domain of Y_i is increased as indicated within Equation 2.12.

$$\begin{array}{l} Y_i = r_i + \sum_{j=1}^{k} vm\left(x_{ij} + \varepsilon_{ij}\right) = r_i + \sum_{j=1}^{k} vm\varepsilon_{ij} + \\ \sum_{j=1}^{k} vmx_{ij} = y_i + \sum_{j=1}^{k} vm\varepsilon_{ij}, \text{ where } i \in \{1,\ldots,t\} \end{array} \tag{2.12}$$

Therefore, Y is scaled up to $|Y| = |y| + |x|.|E|$ Accordingly, the additional information is inadequate to solve $k+1$ variables with domain $|\mathscr{X}|.|E|$, and does not solve all available equations to extract all variables.

In addition, for preserving complete privacy, we need to respect $|y|^t \leq |X|^{k+1}$. We showed that $|y| = \mathbb{Z}_N^*| + |X|^2 \geq |X|^2$. Therefore, we have $|x|^{2t} \leq |x|^{k+1} \xrightarrow{\ln} \ln|\mathscr{X}|^{2t} \leq \ln|X|^{k+1} \rightarrow 2t \leq k+1 \rightarrow t \leq \frac{k+1}{2}$. This inequality is true when condition $k \geq 1$ holds. Hence for any choice of t biometric traits, the attacker is not able to solve congruences in order to weaken the privacy security.

We come to conclusion that in spite of providing malicious server, privacy of client and template security will be preserved.

Privacy concern: Privacy is the user/client's critical information that would not be disclosed in authentication processing. Such information includes user/client's data and her/his activities tracking. In the following, we consider these issues and discuss them.

-Personal information privacy preservation: As proved in previous section, our digest based authentication system keeps critical information securely by transforming them to inconceivable data. Therefore, the user/client does not need to have a concern about her/his critical data.

-Track privacy preservation: As proved in previous section, every time that client wishes to be authorized, she/he can avoid to be viewed by sending random based digests to the server. Since all these digest tuples are irrelevant to each other, no one from outside of the system is able to follow up the client among all the clients. In addition, by locking up the user/client's identity, the authentication server has no authenticity to track the clients who request to log in to the system.

Trust preservation between user and server: Since all users at first should register their information in the registration server that is a kind of TTP, during authentication,

the client and the server need not to trust each other. In fact, no original critical information is disclosed in the network and thus the authentication server, as an untrusted server along with insecure network can carry out safely the authentication duty.

Network requirement: A network attacker observes the insecure network traffic and snoops up user's biometric information. Thus, the protocol should preserve the confidentiality of data such that the attacker would not be able to pick up any information even client identity. To this end, the protocol should generate very different and secure tuples every time for client so that the attacker cannot: (1) extract any information from the grabbed tuples and (2) match the two tuples to figure out any additional information. Since, our protocol has the unlinkability property [1], the attacker is not able to choose two tuples of one client between several uncorrelated tuples.

Furthermore, in the linkage attack, an adversary aims to track a legitimated client who wants to register in different biometric verification systems. Moreover, by monitoring the client's activity online through a public unsafe network and using different helper data, the adversary can compromise privacy of client. Our scheme is safe against such attacks because in the authentication request time, the client sends: (1) data tuple (h) which is hard to break according to DLP and (2) different biometric semi-digests containing same biometric traits and different random ephemeral keys. Therefore, obtaining biometric semi-digest of a client may not lead to leaking any information about the biometric properties of the client.

In addition, our scheme is resistant to many attacks including the replay attack. Moreover, by applying the time stamp, the network attacker is not able to threaten our system using the replay attack.

2.3.3 The Proposal cryptanalysis and extension 2

In this section, we firstly define secure hash function. However we utilized all definitions stated in Section 2.3.2.1. Next, we cryptanalyse our proposal presented in part 2 and then, add a hash function for improving the scheme's security and functionality (extension-2). To this end, we assume that an adversary **A**, has

capabilities to carry out different attacks that decreases the functionality level of the system. Considering these issues (that are explained as follows), various disadvantages are appeared.

2.3.3.1 Cryptanalysis

Adversary Capabilities

we assume that an adversary, say **A**, has the following capabilities:

-**A** eavesdrops all the communications between the client device and server one over a *public* channel. However, the clients send their biometric data and other information for registration through a *safe* channel,

-**A** is able to intercept, insert, delete, or modify any message transmitted via a *public* channel in authentication time,

-**A** can modify, delete, and resend the eavesdropped messages,

-**A** can be presented in the system as a malicious client or an foreigner part of the system,

-**A** can extract the sensitive stored information in a lost or stolen smart card by examining the power consumption.

Attacks

There are ten popular attacks in the literature, which we deal with them in this thesis [14–16, 53, 54]:

Replay attack: It is category of network attack where an attacker eavesdrops data transmission. The attacker fraudulently obtains it to make delay or repeating for malicious goals. In other words, a replay attack is an attack on the security protocol using replays of data transmission from a different sender into the intended into receiving system, thereby fooling the participants into believing they have successfully completed the data transmission [53].

Insider attack: An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access [54].

Password-offline guessing attack: It is an attack to recover one or more passwords from a password storage file that has been recovered from a target system [14].

Server masquerade attack: It includes any attempt by an enemy that uses a forged identity to gain unofficial access to a security system. The enemy who is someone within the organization or by an outsider from a public network; generally performs by using either stolen passwords or log-on, locating gaps in programs, or finding a way around the authentication process [15].

Smart card (loss) attack: That is, if an unauthorized person obtains the smart card, he/she can guess the correct password to masquerade as a legitimate user to login the system. The attack is caused by the smart card outputs fixed message for the same inputs [16].

User impersonation attack: An attack in which an adversary fooling the participants into believing to own the identity of one of the legitimate parties in the system or in a communication protocol [54].

FAR Attack: This attack occurs when two different data as inputs of the given algorithm returns same/very similar outputs consisting of characteristic signal (called collision). Therefore, if an adversary accesses to the large biometric data input and output domains, he/she can find collisions to get fraudulently the authorization [17].

Man-In-The-Middle (MITM) attack: This attack happens when a communication between two systems is intercepted by an outside entity. In fact, it is a kind of active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection [18].

Linkage attack: in this attack, an adversary aims to track an individual who registers in different verification systems. Moreover, by monitoring individual's activity online and using different data, the adversary can compromise privacy of client [19].

Hill climbing attack: in this attack, an adversary monitors similarity degree between received encrypted data to obtain some information to regenerate original data [20]. Attacks 8-10 are just considered in our research.

Functionalities

An important issue in biometric authentication schemes supporting functionalities. We overviewed literature and obtained six security functionalities [22–24]:

Anonymity: a system with anonymous property allows all entities to send messages to each other without revealing their identity. Conceptually, anonymity is aimed at hiding who performs some action, whereas full privacy requires additionally hiding what actions are being performed [21, 34].

Mutual authentication: is a process in which both entities in a communications link authenticate each other. In a network environment, the client authenticates the server and vice-versa. In this way, network users can be assured that they are doing exclusively with legitimate entities and servers can be certain that all would-be users are attempting to gain access for legitimate purposes [33].

Session key agreement: is an encryption/decryption key agreement that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers [32].

Perfect forward secrecy: gives assurances the session keys will not be compromised even if the private key of the server is compromised [31].

user revocation/re-registration: when (encrypted) data breaches is happen or the users password is compromised, the user can easily revoke that stolen password by creating a new one [30].

biometric information protection is not only simultaneously provides biometric and cryptography authentication but also during the authentication process protects the biometric data through cryptographic protocol [29].

Disadvantages

No Mutual Authentication Functionality: The scheme lacks mutual authentication. In the authentication round, the client calculates corresponding her/his S_{ID} and sends it to the authentication server for verification. We know that **A** has total control on the public channel and therefore he/she can grasps S_{ID}, which contains the client's identity and locked ID. However, Ad cannot obtain the original biometric templates but he/she can misuse the S_{ID}. Using the scheme, the client is not able to authorize the server as legitimate authentication server but he/she can be authorized by the server as follow.

-Process: According to the Algorithms 2.3.2.4, the client submits her/his semi-digest $S_{ID} =< sd_{ID}(X'), g^{ID} \bmod N, g^{\lambda} \bmod N >$ to the authentication server via a public channel.

Not that, the server and **A** cannot extract the neither original biometric templates nor ID from S_{ID} because it is impossible that one can computationally derive X and ID from *F(X)* and *F(ID)*, respectively.

-Problem: Since the server is used to check the validity of client X in the authentication phase and the client does not receive any information for authenticating the server, the client cannot verify the authority of the server and therefore *mutual authentication* is not provided. Moreover, this means that it is vulnerable to the following attacks. Therefore, the generation method in the authentication round must be revised.

Replay attack: The registered client's semi-digest S_{ID} may be grasped by an **A** who is eavesdropping on the network when the client sends his/her S_{ID} through an insecure channel. After capturing S_{ID} by an **A**, as the client, sends the S_{ID} and connects to the server. When the server asks for the identity correctness, the **A** sends the clients S_{ID} of the last session. Afterwards, the server accepts the request and **A** grants the system access. Since the S_{ID} is registered as an authorized client, **A** can login to the system and access to the resources whenever he/she wants. The following shows that the scheme is vulnerable to replay attack:

-Process: To being authorized by the system, a client, say X, scans his/her biometric information and derive its templates. Then X calculates the corresponding S_{ID} and sends it through an insecure channel to the server,

-Problem:

1: **A** captures the S_{ID} that is transmitting over the channel,

2: **A** sends the captured tuple to the server for authentication many times and uses the system while the server cannot discover such issue.

In the replay attack, **A** obtains S_{ID} of an authorized biometric template. However, **A** cannot obtain any information about the client of S_{ID} i.e. **A** just know that this S_{ID} belongs to legitimate client. Moreover, we have clearly demonstrated in Algorithm 2.3.3.1 where an attacker is able to get S_{ID} belonging to unknown ID of a user.

Algorithm Replay-attack

1. **Input**: The values of Public Key $PK =< g, N, n, v, h = g^{\alpha} >$ and $S_{ID} =< sd_{ID}(X'), g^{ID} \bmod N, g^{\lambda} \bmod N >$, which may belong to a legitimate client.

2. **Output**: Authentication whenever an **A** wants.

3. **A** eavesdrops the network and captures $S_{ID} =< sd_{ID}(X'), g^{ID} \bmod N, g^{\lambda} \bmod N >$, which belongs to a client,

4. **A** waits for capturing the response message from the server that contains acceptance or rejection of the authentication,

5. **if** (accepted) **then**

6. **A** stores the tuple of ID and he/she knows that this tuple belongs to a legitimate client, **A** cannot comprehend any information about identity ID and the original biometric template.

7. **else**

8. Repeats steps 3-5 for obtaining the legitimate tuple

9. **end if**

Server Masquerading attack:
Since client X is not able to authorize the server and just sends some information to the server, X cannot distinguish between the server and the **A**.
-Process: The S_{ID} that X believes that is sent to the server, can be sent to the **A** attempting to masquerade as the legal server.

-Problem: **A** who has received the authorized tuple can send a valid, sends acknowledgement message to X, which the message has been captured right before this communication. The following shows that the scheme is vulnerable to server masquerading attack:

Algorithm Server Masquerading attack

1. **A** captures an authentication request from a client through an insecure network.

2. **A** sends back a message containing "accepted" to the client. This message is captured from the previous authentication rounds when the server was active for authenticating and issued this message to the legitimate client,

3. **A** can intercept S_{ID} over the communication channel,

4. **A** can misuses the received data and/or continue to authorize other users to collect tuple,

5. **A** can masquerade as a legitimate sever who can fool any legal client.

Since client X does not receive any authenticating information e.g. the server password, etc. X is not able to comprehend the connection to a malicious server. Therefore, the **A** can continue keeping up the masquerade as a legal server. Algorithm 2.3.3.1 shows this process systematically in detail.

2.3.3.2 Biometric authentication control flow

In this section we present control flow of activities in an authentication system in Figure 2.10. Indeed, it is a biometric-based development for the resources that facilities the use of which should be regulated in mobile networks through the access control mechanism. We presented the basic digest concept in our previous works [1], which is improved in this section to protect the attacks stated previously. The second extension considers more firm security assumption that is needed for smart appliances.

According to Figure 2.10, the client has a smart card included with hashed password and ID. To gain access, he/she inserts the smart-card in the card reader to feed his ID and hashed password. Additionally, he/she enters his password that will be hashed separately on the client side. These obtained data including, hash of new entered password as well as the data that is available on his/her smart card (i.e. the hashed password and ID) will be sent through the network to the authentication server. We assume that the card reader and the smart card are physically vulnerable; therefore, the system needs to make use of a safe cryptographic hash function to protect this communication. According to [56], the authentication protocol, is based on a variant of the Secure Sockets Layer (SSL) authentication protocol.

According to Figure 2.10, the system contains components: (1) client, (2) the smart card that is personalized for each client, (3) the authentication server and (4) the biometry sensor. The data stored on the card includes the card identifier, the misuse counter, and hash value of the identification password shared with the authentication server. To prevent the MITM attack by which an attacker tries to get permission by sending a forged biometric sample (like artificial finger) many times, by a forged

or stolen smart card. Furthermore, a misuse counter is located on the card leading to disabling the card if it gets a zero value (which has been set by a value > 0). The authentication server checks the identity of the client against the hash value of password. The biometric authentication is gotten started with the sending of the authentication request message to the server. Smart card also verifies the authentication server using the signals received from the card reader slot that belongs to the server. The authentication request contains the client ID, the stored hash of the password and the hash of the new entered password. If hash values are gotten matched, then client ID will be searched in the database for authorizing (i.e., a registered user). If so, the reference digest will be fetched and client will be asked to send the semi-digest of his/her biometric data. Through the biometry sensor, the client will extract: (1) the biometric template and (2) its feature vector to generate the corresponding semi-digest. This semi-digest as well as the positive signal issued by authorized server will trigger the server to convert semi-digest to the corresponding digest. The server will calculate the HD value with reference digest and the new calculated digest will be used for decision on the legitimation of the client.

2.3.3.3 The Proposed protocol description

We present the improvement in four phases: enrollment, and authentication, and password change. The used notations were explained in abbreviations section. Now, we deal with the phases.

Client registration phase (Enrollment): In this phase, a new client is registered in the TTP server via a secure channel to obtain the smartcard SC. Afterwards, the client can access remotely to the authentication server with the help of SC for utilizing protected resources. In following, Steps 1-3 shows the registration as Figure 2.11.

Steps 1-3: The client C chooses password CPW , identity ID and registers $< h_1 = H(ID||CPW), ID >$ in the TTP server via a secure channel.

Steps 4-7: TTP obtains tuple $< h_1, ID >$ and stores $< h_1$,Locked$(ID) >$ as *reference tuple* in database, first and then selects a password (SPW) and seeded pseudo-random number function PR_i and then sends tuple $< h_2$, seed, SeverID,Lock $(ID) >$ where $h_2 = H(h_1 \| SPW), h_3 = H(h_2 \| PR_i)$ to C. Now, TTP issues the smartcard SC including the values$\{h_l, h_2, seed, Locked(ID), PK\}$ and sends it to client C via the same channel.

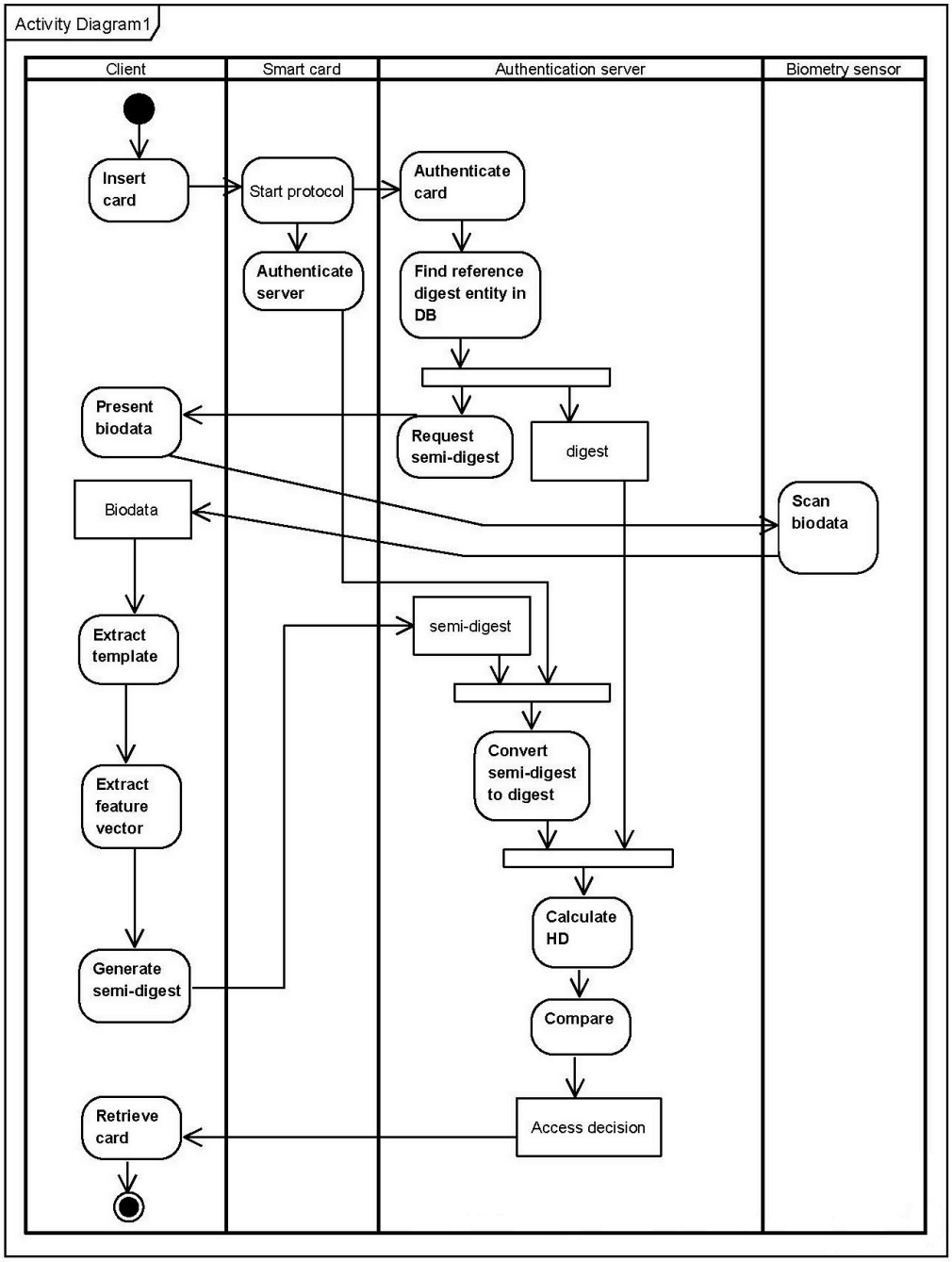

Figure 2.10 : Activity diagram of a digest-based authentication system

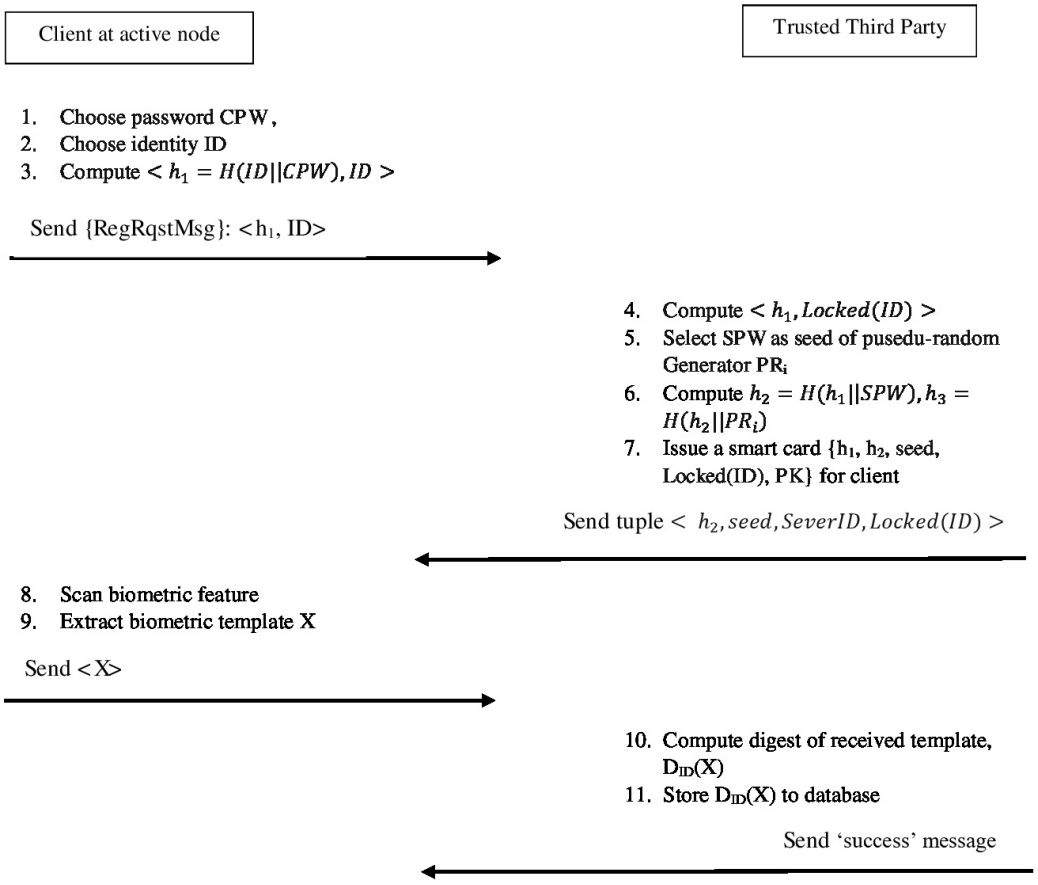

Figure 2.11 : Enrollment phase flow

Steps 8-11: Client C obtains SC from TTP and then sends her/his biometric feature vector via a secure channel. Then, TTP calculates the digest of biometric feature vector as follows. Afterwards, TTP stores calculated and stores it on database.

In this phase, client C is authenticated by the authentication server (hereafter, we call it server) to access to the resources. For the authentication, C inserts his/her card to the card reader where the slot authorizes the card and its owner by asking CPW. It also, calculates hash function value h_1 and compares it with the corresponding value stored in the card. In case of matching up, authentication request message $< h_1$, Locked (ID), TimeStamp $(T) >$ is constructed and sent to the server. The server determines whether $\frac{\text{TimeStamp}(T_C)}{\text{Timestamp}(T_{Now})} \leq \Delta T$ and it rejects the client if not met; otherwise, it checks the rest of this tuple against the stored reference tuple in its database. In case of matching up, it sends back message $< h_3, ServerID >$ to the the card reader presenting C. Then, the card reader checks $< h_3 = H\left(h_2 \| PR_i\right), SeverID >$ against the received data; in case of matching up, it sends message O.K. to the server. In this

way, the mutual-authentication is performed. At the next step, the server requests the client's *non-deterministic* semi-digest for the authentication. The authentication process is started by scanning client biometric and extracting template data and then the matching process in Figure 2.12.

Password Change Phase

In this phase, the password is changed freely by the client. To do this, (1) the client is authorized, (2) new password CPW is chosen by hime/her, (3) tuple $< h_1' = H(ID||CPW')$,Locked$(ID) >$, is constructed and sent to the server, (4) the old password is replaced with CPW' by the server, (5) $h_2' = H(h_1'||SPW)$ is calculated and sent to the card reader by the server, and (6) h_2' replaces old one. Afterward, card reader will use $h_3' = H(h_2'||PR_i)$ (See Figure 2.12) for mutual authentication process.

2.3.3.4 Performance considerations

Resolving User Anonymity: This issue is resolved through coding the client's ID. The authentication server stores the registered client's IDs in the locked form. In the registration phase, TTP checks the availability of a unique ID in locked form. Also, in the authentication time, ID is locked and transmitted over the network in an encrypted form. In this case, the improved protocol is secure against client privacy threats.

Resolving Mutual authentication: This issue is resolved through a hash function where both client and server can authenticate each other through a password management system as follows. At first, client X sends the output value of a hash function fed by an identity number and password $h_1 = H(ID||CPW)$. Then, the authentication server checks the value. If it is matched with corresponding locked ID, it sends the tuple $< h_2, seed, SeverID, Lock(ID) >$ where $h_2 = H(h_1||SPW)$, $h_3 = H(h_2||PR_i)$ to X. X checks the received value against the corresponding one stored on the card. This way, a client device and the authentication server achieve the mutual authentication and both of them can be sure that they are legitimate.

Resolving Confidentiality: The confidentiality of the digest and semi-digest could not be broken by any attacker. In most cases, the communication in the mobile network is done over the open air where uncountable messages are exchanged; this is an attractive situation for attackers. We suppose that an attacker can easily capture semi-digests while transferring over the network. However, an attacker cannot extract

Client at active node

Authentication Server

1. Activate node by entering password CPW to the node,
2. Compute tuple $TimeStamp(t) = g^t mod\ N$
3. Recove values h_1 and Locked(ID) from the card

Send {AuthRqstMsg}: <h_1, Locked(ID), TimeStamp(T)>

→

4. Check whether $\frac{TimeStamp(T_c)}{TimeStamp(T_{Now})} \leq \Delta T$
5. If No, ignor the message and terminate.
6. If Yes, check < h_1, Locked(ID)> to DB.
7. If it doesn't match, terminate
8. Otherwise, calculate

$$h_2 = H(h_1 || SPW),$$
$$h_3 = H(h_2 || PR_i):$$

Send tuple $< h_3, ServerID >$

←

9. Recover h_2 and PR_i information from card.
10. Check whether tuple $<h_3, ServerID>$ matches
11. If No, terminate,
12. Otherwise scans the biometric feature and extract their template and mask vector as X' and M'.
13. Compute S_{ID} = Semi-Digest(PK, X', M', ID)

Send S_{ID}= $<sd_{ID}(X'), Locked(ID), g^{\lambda} mod\ N, M', TimeStamp(T_c)>$

→

14. Check whether $\frac{TimeStamp(T_c)}{TimeStamp(T_{Now})} \leq \Delta T$
15. If No, ignor the message and terminate.
16. If Yes, compute digest of the client by computing $D_{ID}(X')$=Converting(S_{ID})
17. Extract digest (D) and mask vector from DB correponding to the same Locked(ID')
18. Compute HD value

$$HD\big(M, D_{ID}(X), M', D_{ID}(X')\big)$$

19. If $HD \leq \tau$, Then Matched = TRUE, otherwise Matched = FALSE.

Send {Matched}

←

Figure 2.12 : Authentication phase flow

any valuable information via the open air messages. This way, we can provide an adequate confidentiality for the semi-digest messages.

Providing Forward secrecy: Suppose that the servers secret password SPW is compromised, the identity ID is still unknown to the adversary. Therefore, h_1 is kept secret and semi-digest and ID remain secure. Thus by compromising SPW, the adversary cannot compute the previous the original biometric template.

Resistance to Insider attack: This attack is performed by an insider ad who is familiar with system routine, and has an authorized system access. In this attack, **A** attempts to extract the private information such as password and biometrics of client. In our improved scheme, ad cannot retrieve the password CPW or biometrics template X from $h_1 = H(ID\|CPW), ID >$ because CPW is not stored in the database or SC. Moreover, as stated in our previous work in [1], the biometric template is converted to the corresponding digest/semi-digest where deriving the original biometric is impossible. Thus, our scheme is resistant to the *insider* attack.

Resolving Replay attack: Our proposed protocol is resistant to replay attacks, because the semi-digest S_1 is timestamped and *nonce*-based (a nonce is an arbitrary number that is used just once in a communication). They are validated by checking the freshness of timestamps. Suppose that an attacker intercepts semi-digest S_1 and attempts to access the mobile networks by replaying the same semi-digest (S_1). The attempt by the attacker for verification of this authentication fails due to the expiration of the verification time (i.e., $\frac{\text{TimeStamp}(T_c)}{\text{Timestamp}(T_{Now})} > \Delta T$). In the same way, if the attacker intercepts semi-digests S_2 or S_2 and attempts to replay one of them, the verification request will fail because the verification time is expired again. Moreover, the nonce will show that the semi-digest has already been used. Hence, our protocol is secure against replaying messages.

MITM attack: An attacker may attempt for a MITM attack by modifying the authentication messages S_1 and S_2. Nevertheless, this malicious attempt will not work, as the false values S_1 and S_2 will not be verified by the authentication server and the client nodes. Thus, MITM attacks are not applicable to our protocol.

Offline-password guessing attack: The password and ID guessing attacks are not feasible for our proposed system because they lack the client's biometric information. Moreover, in the authentication phase, password and ID are not transmitted through network; instead, they are hashed which is difficult for guessing.

Securely change/update password: The proposed protocol helps users to discover/change their forgotten/get hacked password at any time. The password change facility provides robustness of the proposed improved protocol in comparison with a static password-based protocol.

User masquerading attack: Adversary is required to compute a valid request message including, $S_{ID}\left(sd_{ID}\left(X'\right), \text{Locked}(ID), g^{\lambda} \text{mod } N\right.$, Timestamp (T_c) to impersonate a legal user at the first step. At the second step, adversary should attempt for sending the valid stamped semi-digest. However, semi-digest is dynamic in every session; therefore, the message may not be seen by the adversary repeatedly. Moreover, an adversary cannot generate a valid dynamic semi-digest because he/she cannot discover TimeStamp (T_c).

Server masquerading attack: To masquerade as a legal server, adversary must compute message $h_2 = H\left(h_1 \| SPW\right), h_3 = H\left(h_2 \| PR_i\right)$. The improved proposed protocol is resistant to such an attack. Moreover, an adversary could not apply replay the h_2 captured in a previous session because PR_i is renewed in every round. Therefore, our proposed scheme is secure against this attack because we use pseudo random number PR_i and therefore S_2 becomes fresh in each round.

False Acceptance Rate (FAR) Attack: This attack occurs when two different biometrical templates X and X as inputs of the given algorithm returns same/very similar outputs consisting of characteristic signal (called collision). Therefore, if an adversary accesses to the large biometric data input and output domains, he/she can find collisions to get fraudulently the authorization. Here, we show if condition $\beta = \phi(m) > \forall X$ is met, the collision will never occur.

Claim: in our scheme, if $\phi(m) > \forall X$, then it will be FAR resistance.

Proof by contradiction: assume that and there is a collision meaning that there are authorized traits X and unauthorized trait X where X and X have very similar characteristic signal and therefore they get authentication in the scheme, i.e. the system receives same biometric semi-digests from two different clients. According, we have formally can proved it (See Figure A.1). In all possible cases, either $X = X'$ or < 0 or $X' < m - 1$, , that are in contradiction with claim. Therefore, according to the contradictions, our claim holds.

Linkage attack: in this attack, an adversary aims to track a legitimated client who registers in different biometric verification systems. Moreover, by monitoring client's

activity online and using different helper data, the adversary can compromise privacy of client. Our scheme is safe against this attack, because (1) in the authentication request time, client sends helper data which is hard to obtain according to DLP and (2) client sends different biometric digests with same helper data and different random numbers. Therefore obtaining biometric digest of a client cannot lead to leaking any information about biometric properties of the client.

Hill climbing attack: in this attack, an adversary monitors similarity degree between received biometric traits and their saved counterpart helper data to obtain some information to regenerate original biometric traits. In our scheme, we consider time stamp and pseudo random number to generate different semi-digests in every round.

3. CAPABILITY ANALYSIS

3.1 The Basic Proposed Protocol

In this section, we compare our scheme with those of Kulkarni et al [57] and Upmanyu [58] with regard to the computation and time costs. Note that to the best of our knowledge, no work on digest identification is applied in biometric authentication. Since authentication request time is very important in any verification system, comparison on on-line phase is presented.

Tables 3.1 and 3.2 list the computation cost of the schemes on pre-authentication and authentication request time (off-line and on-line phases). e and EXP denote bilinear pairing evaluation and modular exponentiation operation in additive group, respectively. SM, GM and A are Scalar Multiplication, Group Multiplication and Addition in additive groups respectively.

According to Table 3.3, The scheme of Upmanyu [58] has the highest computation cost, because of the bilinear pairing which is a very costly operation. The main advantage of our proposal is that there is no need to carry out pairing on either the user or the receiver side. The time costs of bilinear pairing and multiplication calculated by Oliveira et al [59] are 5.45 and 0.00402 seconds, respectively, using the binary field and MIRACL library [60]. Ghassan et al. [61] were able to compute the modular exponentiation in 0.00748 seconds implemented by squaring technique.

Upmanys [58] used especial hardware to reduce the computation complexity, but they used the RSA operations 5 times, so their cost exceeded to minutes. The digest concept improved efficiency of the encryption and decryption operation in cost and time as well as it is safe enough to customize for any application.

3.2 The Proposed Protocol-Extension 1

The environment Setup: We used a PC with 512 GB hard disk, Intel Core i5-7400 processor running on Windows 64-bit at 3.0 GHz with 16 GB of main memory. The

Table 3.1 : Comparison of digest generation/encryption a computation times.

Scheme	EXP	SM	GM	A	RSA	TOTAL
[62]	0	1	2	n + 1	4	2EXP+2SM
[13]	2	2	0	0	0	SM+2GM+(n+1)A+4RSA
Ours	2	0	1	0	0	2EXP+1GM

Table 3.2 : Comparison of authentication/decryption computation time.

Scheme	EXP	SM	GM	e	RSA	TOTAL
[62]	0	3n	0	0	1	3(n+1)RSA
[13]	0	2	2	5	0	5e+2SM+2GM
Ours	3	0	1	0	0	3EXP+1GM

Table 3.3 : Comparison of total time cost in second.

Scheme	Time cost
[62]	240 (4 min)
[13]	58
Ours	0.04544

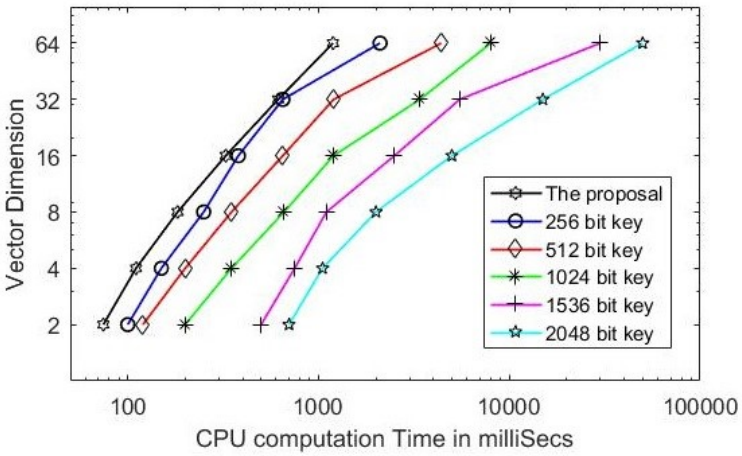

Figure 3.1 : Computation time versus vector dimension for our proposed method and RSA based methods.

client and authentication server are run as separate and synchronous processes where the client waits for processing his/her request by the server. We consider the scenarios presented in Section 2. Since, we considered the client, server, and TTP on one machine, the network latency was not considered. We used a template with size of 256 bits for our analysis.

Dataset selection [63, 64]: The CASIA-IrisV1 dataset. This dataset was provided for the recognition applications that need subject-ageing related effects for fingerprint. The data was collected for 49 different individuals in 2009 and 2013, with a time span of 4 years between the old and new fingerprints for the individuals. The fingerprints were obtained using different sensors such as optical and capacitive off-the-shelf fingerprint scanners. While in 2009 one sensory type was used, in 2013, three different sensory types were used. Each record contains fields: (1) A = Number of Acquisition Session, (2) I = User ID, (3) R = Sensor ID, (4) F = FingerID (1: Left Index Finger, 2: Left Middle Finger, 6: Right Index Finger, 7: Right Middle Finger), (5) X = Image Index, (6) Z = Session. Dataset 2009 contains 1 acquisition session, 49 subjects, 20 images per subject, left and right index and middle finger for each subject (in total 4 different fingers and 5 imprints for each finger), in total 980 images with 1000 classes and resolution 640*480. Similarly, dataset 2013 contains, in total, 1960 images. The UBIRIS dataset contains 1877 images from 241 subjects, which was obtained in 2004 in two distinct sessions.

Consideration of Efficiency: The asymptotic complexity of our protocol depends

on the modular exponentiation order. However, in real cases, factors, such as the cryptological primitives and the execution environment play a role in the complexity. A multiplication requires an execution round, whereas a comparison requires fixed execution rounds [65]. Moreover, we have reduced the number of multiplications that are needed for a xed standard template size. Also, we measured the average execution time for the amount of multiplications and the necessary comparisons. We have used mostly the modular exponentiation to generate digest of individual traits. Moreover, we used mathematical operations such as multiplication, addition, and XOR, and modular exponentiation. Therefore, most memory and computational CPU times are consumed by modular exponentiation. To optimize this operation we have used modular - pow, which introduced in Applied cryptography [66]. In this method, we convert exponent x in g^{x_i} into Equation 3.1.

$$x_i = \sum_{i=0}^{z-1} a_i 2^i \rightarrow \prod_{i=0}^{z-1} g^{x_i} = \prod_{i=0}^{z-1} \left(g^{2^i}\right)^{a_i} \text{ where } z \text{ is the number of } x, a_j \text{ , is coefficient} \tag{3.1}$$

The running time of this method is $O(\log \text{ exponent}) = O(\log x)$. Other operations, i.e. the multiplications, additions, and comparisons used by our protocol, are linear operation and have negligible cost [67, 68].

Consideration of computation time: Figure 3.1 shows our proposed method compared with RSA based biometric authentication methods [13, 68–71] in terms of CPU computational time versus the vector dimension. The average CPU time of 35.6×10^{-3} seconds was used for multiplications and modular exponentiation and 2.5×10^{-3} of inequality tests were applied in average [69]. It is obvious when the template vector size increases, the CPU computation time increases but the level of security is improved.

Since, the digest generation in our proposed method is similar to template encryption in the RSA based biometric authentication methods, we compare our propose method to these methods. In contrast with these methods that require decryption for matching received encrypted template with stored templates in database, we do not need to de-digest (processing to obtain original data) any generated digests and we match received digest with stored digests in database. Therefore, the authentication time of our method is significantly less than the other methods.

The Consideration of precision and accuracy: Table 3.4 shows the modalities and techniques used by related methods [72–79] and our proposed method and Table 3.5 shows the experimental results obtained using these methods in terms of FAR/FRR (False Accept Rate/False Reject Rate), Precision and Accuracy.

Table 3.4 : The used modalities and techniques in schemes.

Scheme	Applied Technique	Modality	Remarks
[72]	Different Classifier	ear, face, thermal face	Multi-Classifier
[73]	Fuzzy Vault	fp, face and iris	-
[74]	Token based Scrambling	face & fp	1-Sensor Scenario
[75]	Fuzzy Commitment	fp	1-Sensor Scenario
[76]	Fuzzy Commitment	3D face & 3D face	1-Sensor Scenario
[77]	Fuzzy Commitment	fp & face	-
[78, 79]	Fuzzy Vault	fp & iris	-
Ours	Non-Inverting Transformation	iris, fp	Decrypt-less Optimization

Table 3.5 : Experimental results of approaches for multibiometric template protection schemes.

Scheme	FAR/FRR	Precision	Accuracy
[72]	0.00068 / 0.029	0.9993	0.9852
[73]	0.010 / 0.0	0.9901	0.9950
[74]	~0.150 EER	0.8500	0.8500
[75]	0.0556 / 0.01	0.9468	0.9672
[76]	~ 0.025 EER	0.9750	0.9750
[77]	0.92 / 0.001	0.5206	0.5395
[78, 79]	0.018 / 0.01	0.9821	0.9860
Ours	0.0 / 0.01	1.0000	0.9950

False Reject Rate (FRR) is the percentage of rejected valid entities. In this case, the system incorrectly rejects the individuals who have registered in database. Moreover, it cannot match the inputted pattern of individual with its registered template. Equal Error Rate (EER) is the rates at which both accept and reject errors are equal. A system with lower EER, demonstrates more accuracy [5]. Precision and Accuracy of a method are computed as the following Equations 3.2 and 3.3 [80] where TPR=1-FRR and TNR=1-FAR. Rates TPR and TNR indicate True Positive (Accept) Rate and True Negative (Reject) Rate, respectively.

$$Precision = \frac{TPR}{TPR + FRR} \tag{3.2}$$

$$Accuracy = \frac{TPR + TNR}{TPR + TNR + FAR + FRR} \tag{3.3}$$

A recent work [72] reported results of multibiometric methods with four different classifiers. It presented tables that show four different classifiers considering authentication levels and obtained a good result of FAR/FRR = 0.00068 / 0.029.

Authors in [73] improved an embedding algorithm, for projecting a binary set to a point set, which obtained the best result for multibiometric fuzzy vault scheme by considering fingerprint, face, and iris modalities; they successfully reduced FRR to zero.

In [74], authors proposed a multibiometric protocol for template protection based on fingerprint and face modalities. They fused the biometric feature sets employing

decision level fusion technique. They reported score 0.150 for ERR. This score is slightly high and shows the un-trustable system. In [75], authors utilized the iris code as part of a multibiometric system and believed that this kind of treat provides a uniform distribution of error probabilities. In order to correct the code, they executed error correction codes that are a combination of the most reliable bits. However, its FAR score was 0.0556, which is a high value.

In [76], authors applied two different feature extraction algorithms for 3D face data. In order to obtain FAR/FRR results, they compared the number of errors corrected by the error correction method, which led to ERR of 0.025. In [5], authors claimed that they have obtained the best results for fusion algorithms at feature level.

In [77], the rst multibiometric cryptosystem has been presented based on the fuzzy commitment scheme where binary fingerprint and face features are combined. It measures suitable FAR/FRR values showing a trustable system for the authentication.

In [78], authors show that the combination of biometric modalities increases the accuracy level and therefore security will perfectly be provided. They reported score 0.018 for FRR at a FAR of 0.01.

In [79], authors combined PCA (Principle Component Analysis) and ICA (Independent Component Analysis) coefcients to achieve cancelable biometric system. The FAR and FRR scores of [78] and [80] are close to each other.

In our proposed method, a decryption-less method was presented where we compared just inputted encrypted template with ones stored in the database. Therefore, the FAR value is close to zero but in some cases, matched individuals are incorrectly rejected. Since, we aim to provide a high privacy level, we verified received bits using the corresponding ones stored in the database. This issue led to reject authorized individuals who send their code with high error rates.

3.3 The Proposed Protocol-Extension 2

3.3.1 Security feature inclusion

One of the important issues considered in the literature is that how many security features are supported by a security scheme. We overviewed the literature and obtained the security features supported by 13 schemes (Table 3.6). As the table shows, the

Table 3.6 : The resistances provided by schemes.

Scheme	R1	R2	R3	R4	R5	R6	R7
[22]	+	-	+	-	-	-	NA
[23]	+	-	+	+	+	+	NA
[24]	-	-	-	+	+	+	NA
[25]	+	+	+	+	+	+	NA
[26]	+	+	+	-	-	+	-
[27]	+	+	+	+	+	+	-
[28]	+	+	+	+	+	+	+
[29]	+	+	+	+	+	-	+
[30]	+	+	NA	+	NA	+	NA
[31]	+	+	-	-	+	-	+
[32]	+	+	+	NA	+	-	NA
[33]	+	+	+	NA	-	+	-
[34]	+	-	NA	+	NA	+	NA
Ours	+	+	+	+	+	+	+

schemes proposed in [28, 31, 34] are vulnerable to the server masquerading attack. The ones that stated in [24, 26, 34] are not able to withstand the insider attack. However, our proposed protocol is secured against various security attacks: replay, MITM, offline-password guessing, user and server masquerading, FAR, linkage, and hill climbing. Moreover, user anonymity, mutual authentication and confidentiality are securely provided. Therefore, our scheme is protected against various security attacks. Table 3.6 shows the resistance to the attacks, indicated by R1 to R7 supported by various biometric-based authentication schemes. They were extracted based on what has been stated in the schemes references. Notations '+'/ '-'/ 'NA' denote providing/not providing/not considering the resistance by the schemes, respectively. Notations R1-R7 denote the scheme resistance to attacks: (1) replay, (2) password-offline guessing, (3) insider, (4) server masquerade, (5) smartcard, (6) user impersonation, and (7) FAR, respectively. As indicated by Table 3.6, our scheme is more secure and achieves all resistances. Schemes [23, 25, 27–29] provide five or six resistances of seven resistances. Considering not including MITM attack, linkage attack and hill-climbing attack in the most schemes of [22–34] but including in ours, we don't mention these attacks in Table 3.6.

Another important issue is that how many security functionalities are considered by the schemes. We overviewed literature and obtained the security functionalities

Table 3.7 : The functionalities provided by the schemes.

Scheme	F1	F2	F3	F4	F5	F6
[22]	+	+	+	+	+	+
[23]	-	+	-	+	-	NA
[24]	+	+	+	+	NA	NA
[25]	+	+	+	+	-	NA
[26]	-	+	+	-	NA	NA
[27]	+	+	-	+	-	NA
[28]	+	+	+	-	-	-
[29]	-	+	-	+	NA	NA
[30]	+	+	+	+	+	NA
[31]	+	+	+	+	+	+
[32]	+	+	+	+	-	NA
[33]	+	+	+	+	-	-
[34]	+	-	-	NA	-	NA
Ours	+	+	+	+	+	+

provided by the schemes (Table 3.7). Functionalities F1-F6 denote (1) anonymity, (2) mutual authentication, (3) session key agreement, (4) perfect forward secrecy, (5) user revocation/re-registration, and (6) biometric information protection, respectively. According to this table, we tried to provide all the functionalities and the schemes proposed in [22, 24, 30–32] provide a good number of functionalities.

Table 3.8 shows the computation cost and the estimated time of our scheme and other schemes stated in [22–34]. Notations C1, C2, and C3 denote computation overhead in the registration phase, computation overhead in the authentication phase, and total execution overhead, respectively. According to Table 3.8, schemes [22, 27, 29, 31, 33, 34] and ours have lower computational costs than others. However, According to Table 3.6, schemes [23, 25, 27–29] and ours were almost resistance to various attacks and according to Table 3.7, schemes [22, 24, 30–32] had good functionality properties. Considering these three tables, totally schemes [27, 29] and ours have low computational costs and are almost secure but [36, 38] don't cover all expected functionalities. On the other hand, schemes [22, 31] and ours have low computational costs and the coverage of a good number of functionalities but [22, 31] are not enough safe. Totally, our scheme is safe and enjoys providing a good number of functionalities and low computational cost in compare with similar schemes.

Table 3.8 : Total Computation Time in msec.

Scheme	C1	C2	C3	Total
[22]	$5\mathrm{T}_h$	$11\mathrm{T}_h + 11T_M$	$16\mathrm{T}_h + 1T_M$	4.548
[23]	$2\mathrm{T}_h + 2T_M$	$4\mathrm{T}_h + 4T_M$	$6\mathrm{T}_h + 6T_M$	6.588
[24]	$3\mathrm{T}_h + 2T_M + 1T_S$	$4\mathrm{T}_h + 7T_M + 1T_S$	$7\mathrm{T}_h + 9T_M + 2T_S$	10.342
[25]	$3\mathrm{T}_h + 2T_M$	$6\mathrm{T}_h + 6T_M$	$9\mathrm{T}_h + 8T_M$	9.014
[26]	$3\mathrm{T}_h$	$6\mathrm{T}_h + 1T_M$	$9\mathrm{T}_h + 2T_M$	3.806
[27]	$1\mathrm{T}_{AS} + 7T_h$	$1\mathrm{T}_{AS} + 5T_h$	$2\mathrm{T}_{AS} + 12T_h$	3.92
[28]	$7\mathrm{T}_h + 1T_M$	$7\mathrm{T}_h + 2T_S + 2T_M$	$14\mathrm{T}_h + 3T_M + 2T_S$	6.744
[29]	$1\mathrm{T}_{AS} + 7T_h$	$1\mathrm{T}_{AS} + 5T_h$	$2\mathrm{T}_{AS} + 12T_h$	3.82
[30]	$13\mathrm{T}_h$	$12\mathrm{T}_h$	$25\mathrm{T}_h$	5.75
[31]	$4\mathrm{T}_h$	$11\mathrm{T}_h$	$15\mathrm{T}_h$	3.45
[32]	$7\mathrm{T}_h + 3T_S$	$3\mathrm{T}_h + 3T_S$	$10\mathrm{T}_h + 6T_S$	5.06
[33]	$3\mathrm{T}_h$	$11\mathrm{T}_h + 4T_S$	$14\mathrm{T}_h + 2T_S$	4.14
[34]	$11\mathrm{T}_h$	$7\mathrm{T}_h$	$18\mathrm{T}_h$	4.14
Ours	$3\mathrm{T}_h + 2T_M$	$2\mathrm{T}_h + 2T_M$	$53\mathrm{T}_h + 4T_M$	4.622

Table 3.9 : The communication overhead and storage requirement comparison in bytes.

Scheme	S1	S2	ST	SS
[22]	28	100	128	100
[23]	92	124	216	68
[24]	60	130	190	168
[25]	70	202	272	304
[26]	168	32	200	200
[27]	40	60	100	60
[28]	92	128	220	124
[29]	140	180	320	120
[30]	272	40	312	64
[31]	102	80	182	100
[32]	62	40	102	100
[33]	62	62	124	100
[34]	120	80	200	100
Ours	88	90	178	86

Table 3.9 represents the communication overhead and the storage requirement of schemes in byte where S1, S2, ST, and SS denote communication overhead during registration phase, communication overhead during authentication phase, total communication overhead, and SS storage requirement, respectively. Altogether, in terms of the computation cost, our scheme is more appropriate for practical applications for remote distributed networks.

According to Table 3.9, the smartcard storage cost of our proposed scheme is less than that of schemes [22, 24–26, 28, 29, 31–34] and slightly higher than the protocols [23, 27, 30]. However, the scheme proposed in [30] has neither an acceptable number of functionalities nor enough security. On the other hand, schemes [23, 27] don't cover a suitable number of functionality. As a result, the proposed scheme provides more security and is applicable for real time applications. Figure fig:ch3-2 visually shows a comparison of the schemes according to Tables 3.6, 3.7, 3.8, 3.9.

The first aim of designing a client-based biometric authentication protocol is to provide security for a client-server system through an authentication server in order to control the access of clients to server and neutralize various attacks. Moreover, resistance to attacks is the basic goal of every authentication system. After the resistance, other factors should also be considered. Now, we deal with the coverage indicated by Figure 3.2 in percent.

Based on Figure 3.2, the schemes proposed in [25,27,28] and ours satisfy at least %80 security against the attacks mentioned in Table 3.6. On the other hand, the schemes proposed in [31, 33-34, 36-37, 39-42] and ours, satisfy at least %50 of functionalities. Also, the schemes proposed in [22, 26, 27, 29, 31, 32, 34] and ours satisfy at least %40 computation efficiency. For communication and storage efficiency, the schemes proposed in [22,24,27,31–33] and ours satisfy at least %40. The schemes proposed in [25,27–29] have the resistance higher than %70. However, the scheme proposed in [25] has computation, communication and storage efficiency lower that %20. The scheme proposed in [28] has computation and communication efficiency lower that %40 and the scheme proposed in [29] has the communication efficiency lower than %20. Therefore, our proposal and scheme in [27] have acceptable levels for implementing and applying in various applications. According to Table 3.9, the smartcard storage cost of our proposed scheme is less than that of schemes [22,24–26,28,29,31–34] and slightly higher than the protocols [23,27,30]. However, the scheme proposed in [30] has neither an acceptable number of functionalities nor enough security. On the other hand, schemes [23,27] don't cover a suitable number of functionality. As a result, the proposed scheme provides more security and is applicable for real time applications. Figure 3.2 visually shows a comparison of the schemes according to Tables 3.6, 3.7, 3.8, 3.9.

The first aim of designing a client-based biometric authentication protocol is to provide security for a client-server system through an authentication server in order to control the access of clients to server and neutralize various attacks. Moreover, "resistance to attacks" is the basic goal of every authentication system. After the resistance, other factors should also be considered. Now, we deal with the coverage indicated by Figure 3.2 in percent.

Based on Figure 3.2, the schemes proposed in [25, 27, 28] and ours satisfy at lease %80 security against the attacks mentioned in Table 2. On the other hand, the schemes proposed in [22, 24, 25, 27, 28, 30–33] and ours, satisfy at least %50 of functionalities. Also, the schemes proposed in [22,26,27,29,31–34] and ours satisfy at least %40 computation efficiency. For communication and storage efficiency, the schemes proposed in [22,24,27,31–33] and ours satisfy at least %40.

The schemes proposed in [25,27–29] have the resistance higher than %70. However,

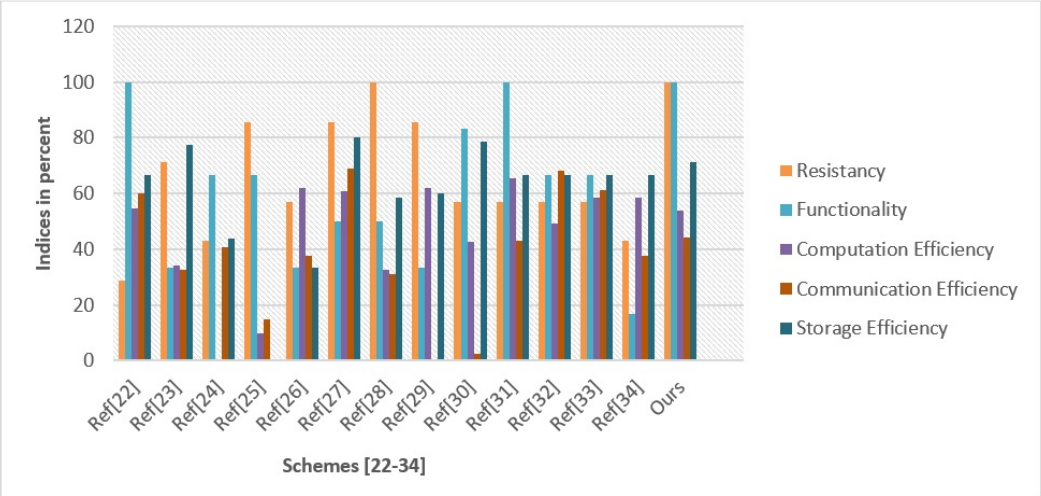

Figure 3.2 : Computation time versus vector dimension for our proposed method and RSA based methods.

the scheme proposed in [25] has computation, communication and storage efficiency lower that %20. The scheme proposed in [28] has computation and communication efficiency lower that %40 and the scheme proposed in [29] has the communication efficiency lower than %20. Therefore, our proposal and scheme in [27] have acceptable levels for implementing and applying in various applications.

4. CONCLUSION AND FUTURE WORK

In this thesis, we presented a secure digest based multi-biometric authentication protocol in an untrusted network. The protocol is applicable for client server systems over an untrusted public network because in such systems. In a client-server system that works through an unsecured public network, the attack resistance and costs are basic concerns.This protocol satisfied all mentioned criteria including privacy preserving and functionality coverage. Our protocol is dynamic such that it is easy to adjust parameters and traits through input of the system. It also is enough fast compared with similar studies. The limitation is that by increasing the number of templates, the computation complexity may effect on the overall. Our future work is: (1) to explore different classifiers to decrease the matching time and (2) the extension of the protocol to evaluate efficient identification so that to be secure and fast by considering different classifiers.

Our primary focus was on vulnerability to *replay* and *server masquerading* attacks; afterwards, we extended our study to support the *anonymity* and *mutual authentication*. Our current work could withstand these attack as well as was resistance to password guess, which is done by the off-line dictionary and man-in-the-middle attacks. Moreover, it provided various functionalities including anonymity and securely changing password. Options of single registration, password change, recording error and noisy bits, strong resistance against various attacks, and functionality coverage are basic advantages of our scheme. In our primary work, we designed a scheme including the single registration, and recording error and noisy bits. In our extended work, we improved the scheme by augmenting the feature of the secure and simple password change and various functionalities. Moreover, we strengthen the scheme by withstanding various attacks. In a client-server based-system with the single registration feature, a client is not need to enrol more than one time. Then, the client can access to the services and data when she/he wishes to be intractable and anonymous. In our extended scheme of digest based authentication system, we provided the simple password change property. Moreover, the client was able to

change his/her password securely without interference of the server. Furthermore, having checked by his/her smartcard, a client is allowed for the password modification. On the other hand, in an authentication system, communication and computation overheads are important considerations in the overall evaluation of a scheme for implementing in a client-server based system. The communication/storage costs can be improved to get optimum level. Our extension of the protocol considered to act in an efficient way for minimum computation cost so that the client could connect to the server with optimum communication energy. Compared with related studies, we respected a suitable cost in our improved scheme using hash functions and modular exponentiations for the authentication, which is performed majorly in the client side. For the feature work, we aim to extend our scheme for multi-server applications such that a client with the single registration can send an authentication request to more than one server where every server operates separately. Moreover, a client could make a connection to the servers and utilizes their services anonymously and intractability.

REFERENCES

[1] **Kirci, M. and Babamir, F.S.** (2017). A Digest-based Method for Efficiency Improvement of Security in Biomterical Cryptography Authentication, *21th IEEE Conference on Computer Science and Software Engineering*, pp.30–35.

[2] **Ratha, N.K.**, **Connell, J.H. and Bolle, R.M.** (2001). Enhancing Security And Privacy In Biometrics-Based Authentication Systems, *IBM System journal*, *40*(3), 614–634.

[3] **Rane, S.**, **Wang, Y.**, **Draper, S.C. and P., I.** (2013). Secure biometrics: Concepts, authentication architectures and challenges, *IEEE Signal Process. Magazine*, *30*(5), 51–64.

[4] **Nandakumar, K. and Jain, A.K.** (2015). Time Series Analysis, Forecasting and Control, *IEEE Signal Process. Magazine*, *32*(5), 88–100.

[5] **Rathgeb, C. and Busch, C.**, (2012). Multi-Biometric Template Protection: Issues and Challenges. Rijeka, Croatia, InTech Open Access, pp.30–37.

[6] **Bringer, J.**, **Chabanne, H. and Patey, A.** (2013). Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends, *IEEE Signal Process Magazine*, *30*(2), 42–52.

[7] **Hadid, A.**, **Evans, N.**, **Marcel, S. and Fierrez, J.** (2015). Biometrics systems under spoong attack: An evaluation methodology and lessons learners, *IEEE Signal Process Magazine*, *32*(5), 20–30.

[8] **Patel, V.M.**, **Ratha, N.K. and Chellappa, R.** (2015). Cancelable biometrics: A review, *IEEE Signal Process. Magazine*, *32*(5), 54–65.

[9] **Lim, A.**, **Teoh, A.B. and Kim, J.** (2015). Biometric feature-type transformation: Making templates compatible for secret protection, *IEEE Signal Process. Magazine*, *32*(5), 77–87.

[10] **Wu, X.**, **Wang, K. and Zhang, D.** (2008). A cryptosystem based on palmprint feature, *In Proceeding of 19th International Conference on Pattern Recognition*, Hanscomb Air Force Base, MA, pp.1–4.

[11] **Nandakumar, K.** (2010). A fingerprint cryptosystem based on minutiae phase spectrum, *In Proceeding of IEEE Workshop Information Forensics Security*, pp.1–6.

[12] **Van der Veen, M.**, **Kevenaar, T.**, **Schrijen, G.J.**, **Akkermans, T.H. and Zuo, F.** (2006). Face biometrics with renewable templates, *In Proceeding of SPIE*, pp.205–216.

[13] **Angeliki Toli, C.**, **Aly, A. and Preneel, B.** (2018). Privacy-Preserving Multibiometric Authentication in Cloud with Untrusted Database Providers, *IACR Cryptology ePrint Archive*, *359*, 56–68.

[14] **Brindha, V.E.** (2012). Biometric Template Security using Dorsal Hand Vein Fuzzy Vault, *Journal of Biometrics*, *5*(1), 76–80.

[15] **Fu, B. and Yang, S.X.** (2009). Multibiometric cryptosystem: Model structure and performance analysis, *IEEE Transactions on Information Forensics Security*, *4*(4), 867–882.

[16] **Zhang, M. and Yang, B.** (2011). Multibiometric based secure encryption and authentication scheme with fuzzy extractor, *International Journal of Network Security*, *12*(1), 50–57.

[17] **Mahalakshmi, U.I. and Shankar Sriram, V.S.** (2013). An ECC Based Multibiometric System for Enhancing Security, *INDJST Conference*, volume 6, pp.10–15.

[18] **Nagar, A. and Nandhakumar, K.** (2012). Multibiometric Cryptosystem Based On Feature Level Fusion, *IEEE Transaction on Information Forensics and Security*, *7*(1), 255–268.

[19] **Juels, A. and Wattenberg, M.** (1999). A fuzzy commitment scheme, *Proceedings of the Sixth ACM Conference On Computer and Communications Security*, pp.28–36.

[20] **Yau, W.** (2004). Combination of hyperbolic functions for multimodal biometrics data fusion, *IEEE Transaction on System, Man, Cybernetics*, *34*(2), 1196–1209.

[21] **Veeramachaneni, K. and Osadciw, L.A.** (2000). An adaptive multimodal biometric management algorithm, *IEEE Transactions on systems, Man, and Cybernetics-Part C: Applications and Reviews*, *35*(3), 344–356.

[22] **Li, X.**, **Niu, J.**, **Karuppiah, M.**, **Kumari, S. and Wu, F.** (2016). Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications, *Journal of Medical Systems*, *40*(12), 268–270.

[23] **Islam, S.** (2016). Design and analysis of an improved smartcard-based remote user password authentication scheme, *International Journal of Communication Systems*, *29*(11), 1708–1719.

[24] **Byun, J.** (2015). Privacy preserving smartcard-based authentication system with provable security, *Security Communication Network Journal*, *8*(17), 3028–3044.

[25] **Mishra, R. and Barnwal, A.** (2015). A privacy preserving secure and efficient authentication scheme for telecare medical information systems, *Journal of Medical Systems*, *39*(5), 1–10.

[26] **Giri, D.**, **Maitra, T.**, **Amin, R. and Srivastava, P.** (2015). An efficient and robust rsa-based remote user authentication for telecare medical information systems, *Journal of Medical Systems*, *39*(1), 1–9.

[27] **Lu, Y.**, **Li, L.**, **Peng, H. and Yang, Y.** (2015). A biometrics and smart cards-based authentication scheme for multi-server environments, *Security Communication Network*, *3*(3), 70–75.

[28] **Wazid, M.**, **Das, A.**, **Kumari, S.**, **Li, X. and Wu, F.** (2016). Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for tmis, *Security Communication Network*, *9*(13), 1983–2001.

[29] **Chaudhr, S.**, **Naqvi, H.**, **Farash, M.**, **Shon, T. and Sher, M.** (2015). An Improved and robust biometrics- based three factor authentication scheme for multiserver environents, *The Journal of Supercomputing*, *10*(2), 1–7.

[30] **Cao, L. and Ge, W.** (2015). Analysis and improvement of a multi-factor biometric authentication scheme, *Security Communication Network*, *8*(4), 617–625.

[31] **Mishra, R. and Barnwal, A.** (2015). A privacy preserving secure and efficient authentication scheme for telecare medical information systems, *Journal of Medical Systems*, *39*(1), 1–9.

[32] **Khan, I.**, **Chaudhry, S.**, **Sher, M.**, **Khan, J. and Khan, M.** (2016). An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data, *The Journal of Supercomputing*, *11*(3), 1–19.

[33] **Yanrong, L.**, **Lixiang, L.**, **Haipeng, P. and Yixian, Y.** (2015). An Enhanced Biometric-based Authentication Scheme for Telecare Medicine Information Systems using Elliptic Curve Cryptosystem, *Journal of Medical Systems*, *39*(32).

[34] **YoHan, P.**, **KiSung, P.**, **KyungKeun, L.**, **Hwangjun, S. and YoungHo, P.** (2017). Security analysis and enhancements of an improved multi-factor biometric authentication scheme, *International Journal of Distributed Sensor Networks*, *13*(8), 100–110.

[35] **Amin, R. and Biswas, G.** (2015). A secure three-factor user authentication and key agreement protocol for tmis with user anonymity, *Journal of Medical Systems*, *39*(8), 78–100.

[36] **Li, X.**, **Niu, J.**, **Khan, M.K. and Liao, J.** (2013). An enhanced smartcard based remote user password authentication scheme, *Journal of Network and Computer Applications*, *36*, 1365–1371.

[37] **Mishra, D.**, **Das, A. and Mukhopadhyay, S.** (2014). A secure user anonymity-preserving biometric-based multiserver authenticated key agreement scheme using smart cards. Expert Systems with Applications Cryptanalysis and Improvement of an Authenticated Key Agreement Scheme, *PLOS*, *41*(18), 129–8143.

[38] **Arshad, H. and Nikooghadam, M.** (2014). Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems, *Journal of Medical Systems*, *38*(12), 1–12.

[39] **Tan, Z.** (2013). An efficient biometrics-based authentication scheme for telecaremedicine information systems, *Journal of Network*, *2*(3), 200–204.

[40] **Yan, X. and Li, W.** (2013). A secure biometrics-based authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, *5*(37), 1–6.

[41] **Mishra, D.**, **Mukhopadhyay, S.**, **Chaturvedi, A.**, **Kumari, S. and Khan, M.** (2014). Cryptanalysis and improvement of yan et al.'s biometricbased authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, *38*(6), 1105–1115.

[42] **Zhang, L.**, **Zhu, S. and Tang, S.** (2017). Privacy protection for telecare medicine information systems using a chaotic map-based three factor authenticated key agreement scheme, *IEEE Journal of Biomedical Health Information*, *21*(2), 465–475.

[43] **Amin, R.**, **Islam, S.**, **Biswas, G.**, **Khan, M. and Li, X.** (2015). Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems, *Journal of Medical Systems*, *39*(11), 140–150.

[44] **Li, X.**, **Niu, J.**, **Karuppiah, M.**, **Kumari, S. and Wu, F.** (2016). Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications, *Journal of Medical Systems*, *40*(12), 268–280.

[45] **Ali, R. and Kumar pal, A.** Cryptanalysis and Biometric-Based Enhancement of a Remote User Authentication Scheme for E-Healthcare System, *Arabian Journal for Science and Engineering*, 1–16.

[46] **Emad, T.K. and Norrozila, S.** (2015). Multibiometric systems and template security survey, *Journal of Scientific Research and Development*, *2*(14), 8–46.

[47] **Mwema, J.**, **Kimwele, M. and Kimani, S.** (2015). A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates, *International Journal of Computer Trends and Technology (IJCTT)*, *1*(20), 12–18.

[48] **Jisha Nair, B. and Ranjitha Kumari, S.** (2015). A Review On Biometric Cryptosystems, *International Journal Of Latest Trends In Engineering And Technology*, *6*(1), 15–25.

[49] **Kashyap, B. and Satao, K.J.** (2015). A Review on Multi-Biometric Cryptosystem for Information Security, *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(5), 17–23.

[50] **Dodis, Y.**, **Ostrovsky, R.**, **Reyzin, L. and Smith, A.** (2008). Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, *SIAM Journal of Computer*, *38*(1), 97–139.

[51] **Gobi, M. and Kannan, D.** (2015). A secured public key cryptosystem for biometric encryption, *IJCSNS International Journal of Computer Science and Network Security*, *15*(1), 49–57.

[52] **Lee, D.**, **Hussain, S.**, **Roussos, G. and Y., Z.** (2010). Wireless Pervasive Communnication, *ditorial: special issue on security and multimodality in pervasive environments.*, *55*(1), 1–4.

[53] **Rathgeb, C.**, **Uhl, A. and Wild, P.** (2011). Reliability-Balanced Feature Level Fusion For Fuzzy Commitment Scheme., *In Proceeding of 2011 International Joint Conference on Biometrics*, pp.1–7.

[54] **Nemanja, M.**, **Borislav, o.**, **Jelena, G. and Komlen, L.** (2015). *An Approach to Robust Biometric Key Generation System Design*, volume 8, 43-60.

[55] Biometric Information Protection Standard. ISO 24745.

[56] **Jurjens, J.** (2015). Code Security Analysis of a Biometric Authentication System Using Automated Theorem Provers, *In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC '05). The IEEE Computer Society*, pp.138–149.

[57] **Kulkarni, R. and Namboodiri, A.** (2013). Secure hamming distance based biometric authentication, *International Conference on Biometrics (ICB)*, pp.1–6.

[58] **Upmanyu, M.** (2010). Blind authentication: a secure cryptobiometric verification protocol, *Information Forensics and Security, IEEE Transactions on*, *5*(2), 255–268.

[59] **Oliveira, L.**, **Scott, M.**, **Lopez, J. and Dahab, R.** (2008). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, *5th Int. Conf. Networked Sensing Systems (INSS)*, pp.173–180.

[60] MIRACL Big Integer Library, http://www.shamus.ie/2009.

[61] **Karame, G.O. and Capkun, S.** (2010). Low-cost client puzzle based on modular exponentiation, *ESORICS 2015th European Symposium on Research in Computer Security*, pp.20–22.

[62] **Aly, A.** (2015). Network Flow Problems with Secure Multiparty Computation, *Ph.D. thesis*, Universitt'e Catholique de Louvain.

[63] CASIA Dataset, CASIA-IrisV1 Interval database. http://biometrics.idealtest.org/ dbDetailForUser.do/id=1.

[64] IIT Delhi iris database, http://www4.comp.polyu.edu.hk/ csajaykr/IITD/Database-Iris.htm.

[65] **Ben, M.**, **Goldwasser, S. and Wigderson, A.** (1998). Completeness theorems for non-cryptographic fault-tolerant distributed computation, *STOC-ACM*, *3*(2), 69–75.

[66] **Scneier, B.** (1996). *Applied cryptography, protocols, algorithms, and source code in C*, volume 2, John Wiley Sons.

[67] **Bogetoft, P.**, **Christensen, D.L.**, **Damgard, I.**, **Geisler, M.**, **Jakobsen, T.**, **Krigaard, M.**, **Nielsen, J.D.**, **Nielsen, J.B.**, **Nielsen, K.**, **Pagter, J.**, **Schwartzbach, M. and Toft, T.** (2009). *Secure multiparty computation goes live*, volume 3, Financial Cryptography.

[68] **Vincenzo Conti, S.V.** (2012). Fingerprint Traits and RSA Algorithm Fusion Technique, *Sixth International Conference on Complex, Intelligent, and Software Intensive Systems*, pp.351–356.

[69] **Upmanyu, M.**, **Namboodiri, A.**, **Srinathan, K. and Jawahar, C.** (2010). Blined authentication: a secure crypto-biometric verification protocol, *IEEE Transaction on information forensics and security*, *10*(2), 10–16.

[70] **Jagadiswary, D. and Saraswady, D.** (2016). Biometric Authentication using Fused Multimodal Biometric, *International Conference on Computational Modeling and Security (CMS 2016)*, pp.109–116.

[71] **Shahnawaz Nasir, M. and Kuppuswamy Perumal, P.** (2013). Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm, *International Journal of Innovative Research in Computer and Communication Engineering*, 8, pp.32–37.

[72] **Bayram, K.S. and Bolat, B.** (2018). Multibiometric identification by using ear, face, and thermal face, *EURASIP Journal on Image and Video Processing*, *1*(32), 89–99.

[73] **Nagar, A.**, **Nandakumar, K. and K., J.A.** (2012). Multibiometric cryptosystems based on feature level fusion, *IEEE Transactions on Information Forensics and Security*, *7*(1), 255–268.

[74] **Yang, B.**, **Busch, C.**, **de Groot, K.**, **Xu, H. and J., V.R.N.** (2012). Performance evaluation of fusing protected ngerprint minutiae templates on the decision level, *Sensor-Journal, Special Issue: Hand-Based Biometrics Sensors and Systems*, *2012*(12), 5246–5272.

[75] **Rathgeb, A.**, **Uhl, A. and P., W.** (2011). Reliability-balanced feature level fusion for fuzzy commitment scheme, *In Proc. of the Int. Joint Conf. on Biometrics (IJCBŠ11)*, pp.1–7.

[76] **Kelkboom, E.J.C.**, **Zhou, X.**, **Breebaart, J.**, **Veldhuis, R.N.S. and C., B.** (2009). Multi-algorithm fusion with template protection, *In Proc. of the 3rd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTASŠ09)*, pp.1–7.

[77] **Sutcu, Y.**, **Li, Q. and N., M.** (2007). Secure biometric templates from ngerprint-face features, *In IEEE Conf. on Computer Vision and Pattern Recognition, CVPR Š07*, pp.1–6.

[78] **Nandakumar, K. and Jain, A.K.** (2008). Multibiometric template security using fuzzy vault, *In IEEE 2nd Int. Conf. on Biometrics: Theory, Applications, and Systems, BTAS Š08*, pp.126–129.

[79] **Jeong, M.Y.**, **Lee, C.**, **Kim, J.**, **Choi, J.Y.**, **Toh, K.A. and Kim, J.** (2006). Changeable biometrics for appearance based face recognition, *In Proc. of Biometric Consortium Conf., 2006 Biometrics Symposium*, pp.1–5.

[80] **Elahi, A. and Babamir, S.M.** (2018). Identification of essential proteins based on a new combination of topological and biological features in weighted proteinŰprotein interaction networks, *IET Systems Biology*, *12*(6), 247–257.

APPENDICES

APPENDIX A.1 : Contradiction proof
APPENDIX A.2 : List of Publications

APPENDIX A.1

$$sd \bmod N = sd' \bmod N \rightarrow h^{y} \bmod N = h^{y'} \bmod N \rightarrow h^{[(vb)+r]} \bmod N = h^{\left[\left(vb'\right)+r'\right]} \bmod N \overset{Converting\ Process}{\rightarrow}$$

$$\left[h^{[(vb)+r]}.\left(g^{\lambda}\right)^{\alpha}.derand\right] \bmod N = \left[h^{[(vb')+r']}.\left(g^{\lambda'}\right)^{\alpha}.derand\right] \bmod N \rightarrow$$

$$\left[h^{[(vb)+r]}.(h)^{\lambda}.derand\right] \bmod N = \left[h^{[(vb')+r']}.(h)^{\lambda'}.derand\right] \bmod N \rightarrow$$

$$\left[h^{[(vb)+r+\lambda]}.(h^{tN} \bmod N)^{-1} \bmod N\right] \bmod N = \left[h^{[(vb')+r'+\lambda']}.(h^{tN} \bmod N)^{-1} \bmod N\right] \bmod N \rightarrow$$

$$h^{vb} \bmod N = h^{vb'} \bmod N \rightarrow g^{\alpha vb} \bmod N = g^{\alpha vb'} \bmod N \overset{Euler\ totient\ function}{\rightarrow}$$

$$\beta \left| (\alpha vb - \alpha vb') \overset{(\alpha,\beta)=1}{\rightarrow} \beta \right| v(b-b') \rightarrow v(b-b') = \beta c \therefore c \in \mathbb{Z}_N^* \rightarrow$$

$$vb - vb' = \beta c \therefore c \in \mathbb{Z}_N^* \rightarrow X - \mu a = X' - \mu a' \bmod \beta \rightarrow$$

$$X = X' + \mu(a' - a) \bmod \beta \rightarrow X = X' - \mu a'' \bmod \beta \overset{\beta<n}{\rightarrow} a'' \bmod \beta = [(a' \bmod n) - (a \bmod n)] \bmod \beta$$

$$\overset{\mu>0, a''\geq 0}{\rightarrow} \begin{cases} a'' = 0 \rightarrow X = X' \bmod \beta, \quad \forall X < \beta \rightarrow X = X' & \times\text{(Contrad with assumption)} \\ a > 0 \rightarrow X = X' + \mu a'' \bmod \beta \rightarrow X = X' + \mu a'' - k\beta & (*) \end{cases}$$

$$\rightarrow \begin{cases} k > 0 \overset{(m<n)}{\rightarrow} -\beta > -n \rightarrow -k\beta > -kn > -n, \mu a'' + X' > n, X < (n - kn) \rightarrow X < 0 & \times\text{(Contrad. with assum.)} \\ k = 0 \rightarrow X = X' + \mu a \overset{\mu = nn_m^{-1} > n}{\rightarrow} X' + \mu a > n > \beta, X > \beta & \times\text{(Contrad. with assum.)} \\ k < 0 \rightarrow -k\beta > \beta \overset{X' + \mu a'' \geq 0}{\rightarrow} X > \beta & \times\text{(Contrad with assum.)} \end{cases}$$

Figure A.1 : Proof of contradiction claim, Section 2.3.3.4

APPENDIX A.2

List of Publications

This Ph.D. thesis comprises a collection of five scientific articles devoted to user authentication in different settings. The settings considered in this thesis are: biometric based authentication (Paper A, Paper C, Paper D), and authentication cryptosystem for WSNs and Client-Server based systems (Paper B, Paper E). The aforementioned articles are published at the following venues:

Paper A: Mürvet KIRCI, Faezeh S. BABAMIR, "A Digest-based Method for Efficiency Improvement of Security in Biomterical Cryptography Authentication", 21th Conference on Computer Science and Software Engineerin, 2017.

Paper B: Faezeh S. BABAMIR, Mürvet KIRCI, "An Energy Efficient Biometric Authentication Protocol in Wireless Sensor Networks", Book chapter of Wireless Mesh Networks-Security, Architectures and Protocols, InTech publication, 2018.

Paper C: Faezeh S. BABAMIR, Mürvet KIRCI, "A Trustable, Accurate and Fast Multi-Biometric Cryptosystem for User Authentication", IEEE Access, 2019 (under review).

Paper D: Faezeh S. BABAMIR, Mürvet KIRCI, "Improvement of Indistinguishable Authentication Scheme for Biometric verification", 16th International ISC conference on Information Security and Cryptography, ISCISC2019.

Paper E: Faezeh S. BABAMIR, Mürvet KIRCI, "Dynamic Digest Based Authentication for Client-Server systems using Biometric Verification", Future Generation Computer Systems Journal, 2019 (Accepted for publication).

CURRICULUM VITAE

Name Surname: Faezeh Sadat BABAMIR

IRAN, 03/ 09/ 1986

E-Mail: babamir@itu.edu.tr, babamir@gmail.com

EDUCATION:

- **B.Sc.:** 2009, Shahid Bahonar University, Mathematic and Computer Science Faculty, Computer Science Department
- **M.Sc.:** 2012, Shahid Beheshti University of Tehran, Mathematic and Computer Science Faculty, Computer Science Department

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2011-2013 Top RA Reward: Research institute for Information and Communication Technology (IRAN Telecommunication).
- 2012 Best Speaker Awards: 5th Conference on Algebraic Combinatorics and Graph Theory.
- 2011-2012 Teacher Assistantship, Research Assistantship: Shahid Beheshti University of Tehran University

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Babamir F. S.**, eslami Z., 2012. data security in unattended wireless sensor networks through signcryption. *KSII transactions on internet and information systems*, 6(11), pp. 2940-2955.
- **Babamir F. S.**, norouzi, A., 2014. achieving key privacy and invisibility for unattended wireless sensor networks in healthcare, *The computer journal, oxford journal,* 57(4), pp. 624-635.
- Norouzi, A., **Babamir F. S.**, halim zaim, A. 2013. an interactive genetic algorithm for mobile sensor networks, *studies in informatics and control,* 22(2), pp. 213-218.