العنوان:	مخطط يربط المفتاح بالقياسات الحيوية لحماية أنظمة المعلومات
المؤلف الرئيسي:	الشريفي، أبرار خلف
مؤلفين آخرين:	الموسوي، كاظم مهدي، الإبراهيمي، كاظم حسن(مشرف)
التاريخ الميلادي:	2016
موقع:	ذي قار
الصفحات:	1 - 87
رقم MD:	881149
نوع المحتوى:	رسائل جامعية
اللغة:	English
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة ذي قار
الكلية:	كلية التربية للعلوم الصرفة
الدولة:	العراق
قواعد المعلومات:	Dissertations
مواضيع:	أمن الشبكات، أمن المعلومات، أنظمة التشفير
رابط:	http://search.mandumah.com/Record/881149

Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Thi-Qar
College of Education for Pure Sciences
Department of Computer Science

A Biometric Key Binding Scheme for Information Systems Protection

A Thesis

Submitted to the council of the College of Education for Pure Sciences University of Thi-Qar as a Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

BY

Abrar Khalaf Al-Sharify

Supervised By

Prof. DR.
Kadhim Mahdi Al-Mousawi

Assist.Prof. DR.
Kadhim Hasen Al-Ibraheemi

October, 2016

Muharram, 1438

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

﴿ وَالرّاسِخُونَ فِي الْعِلْمِ يَقُولُونَ آمَنّا بِهِ كُلٌّ مِنْ عِنْدِ رَبِّنا ﴾

صدق الله العلي العظيم

سورة ال عمران ﴿الآية / ٧﴾

DEDICATION

To My Parents,

My sisters and

My brothers

Who support me whenever I needed their support, without them I was unable to accomplish this competitive phase of education.

ACKNOWLEDGMENTS

*Praise be to ((**Allah**)), lord of the ability and the mercy who has given me opportunities to complete my objectives and provide the means to achieve them.*

*My sincere gratitude and thanks go to my supervisors **Prof.Dr. Kadhim Mahdi Al-Mousawi** and **Assist.Prof.Dr. Kadhim Hasen Al-Ibraheemi** for giving me the opportunity to pursue this study under their guidance. Their support, advice and suggestions have opened new perspectives for my research.*

Deep thanks go for everyone who supported me in the Department of Computer Science in the College of Education for Pure Sciences and College of Science for Computer and Mathematics. Also I want to express my heartfelt gratitude and thanks to my family, and all my friends for their unconditional love , patience, support and for making many favors for me throughout this long journey. I could not accomplish this dream without them and forever grateful for all that they have done and still do.

Abrar

Abstract:

Cryptosystems becomes an increasingly important feature as the most reliable tool in network and information security. However, while there are many forms of cryptosystems exist today a weak link of all systems is the secure management of the cryptographic key. And as a result of the growing interest in biometrics a new field of research has emerged, which is called "biometric cryptosystems". Within biometric cryptosystems the advantages of biometric authentication are introduced to generic cryptographic key management systems to enhance security.

This work proposes a scheme to bind a cryptographic key with the face biometric by combining correlation filters based biometric recognition with a biometric key binding scheme with providing the variation tolerance, discrimination and security which are the most important requirements that apply to a cryptographic key retrieval using a biometric. In the proposed scheme the cryptographic key is generated independently of user's face image using Pseudo-Noise generator to produce a unique and long enough key (128 bits) for each user then this key is linked to the face image only through a secure block of data known as the *'protected record'*. The correct key will only be derived via the interaction of this *protected record* with the correct user's face image during a live authentication process. The resultant key may be used in a system as cryptographic key or as a personal identification number (PIN) to overcome the need to carry, store, or remember keys for cryptosystems or any other application that are used (PIN).

The proposed scheme performance has evaluated using FACE 94 facial database. The performance rate reached to 100% which is a perfect result for practical applications. The proposed scheme is implemented using (MATLAB 2008). It is executed for testing purpose on computer with processor of 1.80 GHZ dual core, i3 under Microsoft Windows 7 operating system.

List of Content

Chapter 3. The Proposed Scheme

Chapter 4. Discussion of the Experimental Results

List of Tables

List of Abbreviations

Abbreviations	Description
PIN	personal identification number
ATM	Automated Teller Machine
BCs	Biometric Cryptosystems
pwd	password
hpwd	hardened password
ECC	Error Correction Coding
LDPC	low density parity check
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
SHA	Secure Hash Algorithm
NSA	National Security Agency
Hex	Hexa-Decimal system
1D	One dimension
2D	Two dimension
Maxval	Maximum value
Minval	Minimum value
CFs	Correlation Filters

Abbreviations	Description
FT	Fourier transform
DFT	discrete Fourier transform
FFT	Fast Fourier Transform
MACE	The Minimum Average Correlation Energy
PSR	Peak to sidelobe ratio
pdf	probability density function
PN	Pseudo - noise
LFSR	linear feedback shift register
FFs	Flip-Flops
XOR	the Exclusive-OR
AES	Advanced Encryption Standard
BKB	Biometric Key Binding
Id	Identification code
W	word
RC	round coefficients

Chapter One
General Introduction

1.1. Introduction

Taking into account today's ever-increasing demand on high security standards, in order to secure any kind of crucial information[1], this account comes with the fact that the numerical world is under a fast development which leads to generate facilities and threats. The recommended solutions are mostly the protection of information in all its states. The levels of protection appear a discrepancy from an application to another governmental, commercial or even cybercriminal [2]. The science of cryptography has become even more important as the most reliable tool in network and information security [1].

The fundamental idea of cryptography is to encipher a "secret" or message into an intermediate form, also called "cipher text" in which the original message exists in a hidden state. The same message can be transformed into many intermediate forms by using different ciphers chosen by a key called "cipher key". The original message can be retrieved accurately by reversing this process only using the correct decryption key. While current cryptographic algorithms provide high security, they suffer from some limitations not due to weaknesses in the algorithms themselves but due to the whole setup of the security system [3].

In cryptography, successful key management is critical to the security issues which consists of key generation, key storing, key updating and sharing [4]. Keys are very important in cryptography as if a key is lost the reliability of the algorithm is lost. All cryptographic algorithms require that the keys must be reasonably long and securely stored [5].

Randomly generated long cryptographic keys (of 128, 192 or 256 bits) are difficult to memorize and it would clearly not be feasible to require the user to enter the key each time it is required [6]. However, in generic cryptographic systems user authentication is still possession based. This means possession of a cryptographic key is a sufficient to authenticate a user. In the most cryptographic key management systems these keys are released by presenting a password (or PIN) − chosen by the user to the system [1]. This implies the security of the cryptographic key and hence the cipher system is now only as good as the used password. Due to practical problems of remembering various passwords, some users have the tendency to choose simple words, phrases, or easily remembered personal data obviously these methods pose potential security risks. Another concern is that the lack of direct connection between the passwords and the user. As passwords are not tied to a user, the system running the cryptographic algorithm is unable to distinguish between the authentic user and an attacker who fraudulently acquires the password of an authentic user [7]. Additionally, a physical token such as a smartcard can be lost or stolen [1].

The security of such cryptographic systems can be strengthened by introducing biometric would address some of the above mentioned shortcomings of cryptographic authentication systems as well as enhance the security [1, 7].

Biometrics is the science of measuring and analyzing human characteristics. There are certain human characteristics which are appropriate to be used in authentication systems. These comprise physiological and behavioral characteristics such as face, fingerprint, iris, hand geometry, voice, signature, keystroke etc.

Adequate devices are used to acquire each of these human characteristics. Afterward, information in terms of features is extracted. These features are then compared with the other features that have previously been stored in a so-called enrollment procedure, and a user is accepted or denied otherwise [1].

Table (1.1): Comparison of Various Biometric Technologies Based on the Perception of the Authors. High, Medium, and Low are Denoted by H, M, and L, respectively.

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Each biometric has its strengths and weaknesses. In other words, no biometric is "optimal". The match between specific biometrics and an application are determined by depending on the requirements of the application and the properties of the biometric characteristics. A brief comparison of some of the biometric identifiers based on seven factors is shown in Table (1.1). Universality (do all people have it ?), distinctiveness (can people be disinguished based on an identifier ?), permanence (how permanent is the identifier ?) and collectability (how can the identifier be captured and quantified ?) are characteristics of biometric identifiers. Performance (which includes speed and accuracy), acceptability (willingness of people for using it) and circumvention (foolproof) are attributes of biometric systems [8].

Due to the fact that the human characteristics tend to be very distinct (these cannot be lost or forgotten either) these seem to be suitable and sufficiently secure for the purpose of user authentication and requires the person being authenticated to be present at the time of the authentication (conniving users denying having shared the passwords). It is difficult to forge biometrics (it requires more time, experience, money, and access privileges) [1, 8].

One could imagine to withdraw money from an Automated Teller Machine (ATM) by presenting a face to an adequate camera to provide secure authentication instead of inserting a four – digit PIN. This would be a prime example for combining biometrics with cryptography in key management systems.

A new field of research has been established to combine biometrics with cryptography which goes by the name of 'Biometric Cryptosystems'.

Biometric cryptosystems combine biometrics and cryptography to benefit from the strengths of both fields. In such systems, while cryptography provides high security levels, biometrics brings in nonrepudiation and removes the need to remember passwords or to carry tokens and hence provides solutions to many of the cryptography problems and may replace the traditional authentication component of cryptosystems [1].

Biometric cryptosystems present various methods that securely generate a cryptographic key from a biometric or link a cryptographic key with the user's biometric template and stored in the database in such a way that the key cannot be retrieved without a successful biometric authentication [9].

1.2. Problem statement

One of the most important issues when design a biometric cryptosystem is that biometric authentication systems come with their own challenges due to drastic acquisition variations in the representation of a biometric identifier and the imperfect nature of biometric features extraction and matching algorithms with the fact features collected during biometric authentication and stored features can vary from session to session. This variation can occur for a number of reasons including different environments according to lighting, emotional state or physical changes like facial hair, glasses, etc. Cryptography, on the other hand, requires that keys be exactly right.

Storing biometric data is different than storing other kinds of data, data like fingerprints, facial recognition data, retinal scan information, etc. are the elements stored. Furthermore, biometric data has to be stored in databases in a secure way which is rarely the case.

There have been a number of attempts to bridge the gap between the fuzziness of biometrics and the accuracy of cryptography by deriving biometric keys from facial characteristics [10], the human voice [11],fingerprints [12,13], and iris [1] . These attempts proposed that data derived from the biometric are used directly as a cryptographic key. However, there are two main problems with these methods as follow; Firstly, as a result of changes in the biometric images due to environmental and physiological factors and hence the biometric template is not consistent enough to use as a cryptographic key. Secondly, if the cryptographic key is compromised, thus the use of that particular biometric is irrevocably lost. In such systems where periodic updating of the cryptographic key is required, this is undesired in the practical cryptosystems. Moreover, most of these attempts have suffered from an excessive False Rejection Rate usually more than 20%, which is unacceptable for practical applications [14].

Social acceptance is an important criterion to the success of biometric technology. The fear of potential misuse of biometric data may make the people reluctant to use systems that depend on it. Generally, iris has a high discrimination with a low acceptance while a face is the most acceptable, it is the least discrimination. So, the question if there exist more efficient schemes handle space problem remains open.

1.3. Related work

There have been a number of research efforts aimed at addressing the issues related to integration of biometrics into cryptosystems.

Soutar *et al.* [15, 16] proposed a biometric-key scheme based on fingerprints. They extracted phase information from the fingerprint images using a Fourier transform. Instead of generating a key directly from biometrics, a pre-defined key is linked with the user’s fingerprint images at the time of enrollment by forming a phase - random phase product. This product can be unlocked during authentication by another genuine biometric sample then the key is retrieved. The disadvantage of this proposed scheme is that the performance measurements and test results are renounced.

Monrose *et al,* they proposed two new schemes to make passwords more secure. In the first scheme [17] they combine keystroke biometric with passwords, their technique was inspired by a password "salting" where a user’s password (pwd) is salted by prepending it with 8-bits random number (the "salt ") the resultant of this proposed scheme is a hardened password (hpwd). A weakness of this work is that the lengths (15 bits) of generated keys are usually too short, Thus making them only marginally more secure. They made some minor modifications to their original scheme, applied it to voice biometrics in [18, 19] and were eventually able to generate cryptographic keys of up to 60 bits, is still quite low for most security applications.

Goh *et al* [10] they adopted the biometric key approach used by Soutar et al [15, 16]. Eigen-projections are extracted from the face image as features, each of which is then mixed with a random string and quantized into a single bit. A binary key is formed by concatenating these bits. The primary limitation with this scheme is the amount of security, which is not on par with the present day encryption algorithms like AES-128 by extracting a short (80-bit) key. This approach is beginning to the parameters needed for a practical system.

Another approach combines biometrics with cryptography has been the use of Error Correction Coding (ECC) to reduce the natural variability in biometrics. Hao *et al*. [20] use Hadamard and Reed Solomon codes for iris recognition ,while Sutcu *et al* [21, 22] use low density parity check (LDPC) codes on the fingerprints. David Zhang et al [23] proposed an approach based on iris features. A quantified 256-dimension textural feature vector is firstly extracted from the preprocessed iris images using a set of 2-D Gabor filters. At the same time, an (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Most of existing approaches in this direction are mainly based on iris and fingerprint. This is because iris and fingerprint features are more stable and can be easily incorporated with (ECC). Another concern that these approaches require to store error-correcting bits in the database and this could lead to some leakage of information about the user’s biometric data.

Naresh *et al* [3] proposed an approach to combine a designed multi – peak correlation filter based biometric recognition with a biometric key-binding scheme. The encryption key for each user in the scheme is formed by selecting a number of peaks and the locations of these peaks in the output correlation plane which are then concatenated as a user's key. The peak locations for the designing filter are chosen such that there is at least 3 pixels separation between adjacent peaks. This approach demonstrated its effectiveness in the recognition performance and security.

1.4. Aim of thesis

The aim of the thesis is to propose a biometric cryptosystem based on face as one of the most acceptance human characteristics to provide a mechanism capable of linking and retrieving a (128-bit) digital key in conjunction with the face biometric which can be used as a method for secure key management of cryptographic keys to complement existing cipher systems. The resultant key may be used in a system as an cryptographic key, or as a Personal Identification Number (PIN).

Finally, the aim is to obtain a false rejection rate good enough for real use using a face biometric.

1.5. Organization of the thesis

Beside chapter one, the remaining parts of this thesis consists of four chapters as follows: the basics concepts on the biometric and cryptography which have used in the proposed scheme in chapter two. The details of the proposed biometric key binding scheme as a biometric cryptosystem , their stages and steps are described in chapter three. In chapter four, the performance of the proposed scheme and the experimental results is discussed. Finally in chapter five, the conclusions of the proposed scheme are summarized and some suggestions for future work to enhance the presented scheme.

Chapter Two
Theory Background

2.1 Introduction

This chapter is devoted to explore the need of the theoretical background to establish a proposed scheme. In the sense of thesis context, biometric cryptosystem means the combining of biometric and cryptography. This chapter explains the components in both biometric and cryptography which will be integrated to design the proposed scheme.

2.2 Biometrics

A biometric is defined as a unique, measurable biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. Nowadays, biometric technologies are typically used to analyze human characteristics for security purposes. Security applications (especially cryptographic systems) need certain private information to authenticate a person's privilege. In the science of biometrics, this private information is replaced by personal information filtered out of human characteristics. These human characteristics are acquired with adequate devices, analyzed and distinct features are extracted. In a so-called enrollment process a user registers with the system by presenting biometric data to it. The system generates a so-called biometric template for the user and stores it in a database. At the time of authentication, another biometric input is acquired, processed and compared with the previously stored template in the matching process. This kind of authentication provides considerable advantages over simple password-based authentication. As a consequence of this, biometric is combined with cryptography to enhance security [1].

2.3 Merging Biometrics and Cryptography

Cryptography is a very important field in the science of computer security. Many cryptographic algorithms are available for securing any type of information. For all traditional algorithms the security depends on the secrecy of the secret or private key when a person deploys a symmetric or asymmetric system, respectively. The person chooses a password that is used to encrypt the cryptographic key and this key is then stored in a database (these keys are long and random and thus hard to remember). In order to retrieve the key back, the person enters the password which will then be used to decrypt the key. This means the authentication in such a cryptographic system is possession-based. The possession of the decrypting key ensures that the user is legitimate. This is one security leakage in generic cryptographic systems which can be avoided by introducing biometric authentication.

In general, there are two different types of cryptographic systems can be distinguished, namely symmetric systems, where all participants of the secret communication share the same secret key, and asymmetric (public key) systems, where pairs of a private key and a publicly available key are used to encrypt and decrypt secret information. While systems of the first category are typically designed for efficient cipher systems, the second type is used mainly in digital signatures to securely exchange secret session keys. In either category it is required to protect the private keys from unauthorized access[24]. As cryptographically strong keys are rather large, it is certainly not appropriate to let users memorize their personal keys. As a consequence of these digital keys are typically stored on smart cards or in databases and retrieved through password-based authentication as mentioned previously. Since the password is not directly tied to a person, the system is unable to differentiate between an authorized user and an attacker. Additionally, the security of the