Republic of Iraq

Ministry of Higher Education

and Scientific Research

University of Diyala

College of Science

Document Signing Using ESSO Algorithm

A Thesis

Submitted to the Computer Science Department\ College of Science\ University of Diyala

In a Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer.

By

Israa Nazeeh

Supervised by

Asst. Prof Jamal Mustafa Abbas

2020 A.D. 1442 AH.

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

﴿وَقُلِ الْحَمْدُ لِلَّهِ سَيُرِيكُمْ آيَاتِهِ فَتَعْرِفُونَهَا﴾

[سورة النمل الآية : 93]

Dedication

I dedicate my humble effort

To the light that illuminates me the path of success **…..** my dear father

To whom was her prayer the secret of my success**.. …**my dear mother

To those who were lighting the road for me and supporting me, to the true companions, who prove the deep meaning of friendship. **…..** my dear sisters

To whom I loved **…..**my dear family

To whom illuminated the way of science **…..** my dear teachers

With all my love and respect

Israa Nazeeh

2020

Acknowledgements

I would like to thank my supervisor Asst. Pro Dr.Jamal Mustafa Abbas for his sincere help and encouragement throughout my study and the writing of this thesis. I thank him for his beautiful attitude and continuous follow-up. This work would not have been possible without his support.

Abstract

Biometrics lack revocability and privacy while cryptography cannot detect the user's identity. By obtaining cryptographic keys using biometrics, one can achieve the properties such as revocability, assurance about user's identity, and privacy. In addition, the Multi-biometric systems alleviate a few of the problems observed in unimodal biometric systems. Besides improving matching performance and its can integrate information at various levels.

In this thesis presents Document Signing Using ESSO Algorithm, its aims to introduce a new technique to generate stream cipher key by using a multi – biometric identification system that consists of (sclera and palm) images and using the best coordinates is produced by an enhancement of shark smell optimization algorithm (SSO) based on 3d logistic chaotic map.

The stages of implementation the proposed system include feature extraction from sclera and palm biometric images of same personal using proposed sclera – identification system and palm –identification system, each system has different preprocessing techniques to preparing images to exacted features.

In addition , the scale-invariant feature transform (SIFT) algorithm in multibiometric identification system extract features from the sclera and palm biometric images and to get fast access to the important regions inside the sclera and palm biometric images. These features are used to find the optimal solution by using enhancement shark smell optimization algorithms(SSO) based on chaotic function.

The enhancements shark smell optimization algorithm (SSO)consists from three steps: 3d logistic map to generate set of random numbers to seed random parameters (R1,R2,R3) in SSO algorithm this step aims to enhance the

performance of SSO , the features that extracted from sclera and palm biometric images dropping on secret image to connected between sclera feature that represent (shark position) and palm feature that represents (fish position) this step aims to find set of optimal solution .

To generate stream cipher key, the proposing system presents new technique to generating variable and unpredictable stream key based on convert to binary the values of all optimal solution (fitness value, objective value, solution point coordinate (x,y)) .

The final stage in the proposed system is the document signature by using the MD5, the proposed system has the ability to generate a unique digital signature for each user.

The proposed system using the stream key in document signature to protect personal information in a completely safe manner.

The implementation the proposed system and results of Random Number Generation Tests (NIST) National Institute of Standards and Technology shown the proposed system has ability to generating stream key for multiply users that has several proprieties likes: unique, unpredictable, strong, and various length.

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

Abbreviations	Meaning
C#	C sharp
R1,R2	Constants
DB	Data Base
DOG	Difference of Gaussian
•	Eat
ESSO	Enhancements shark smell optimization
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
•	Fish
MM	Mathematical Morphology
μ	Mean Value
NIST	National Institute of Standards and Technology
ND	Number of decision
NP	Number of Population
—	Path
RGB	Red, green, blue
SIFT	Scale Invariant Feature Transform
⌑	Shark
SSO	Shark Smell Optimization
SURF	speeded up robust features
σ	Standard Deviation
SE	Structure Element
Xi	The random neighbor
3D	Three Dimension
T	Threshold
2D	Two Dimension
MD5	Message-digest algorithm

List of Symbols Table

Symbol	Meaning
+	Addition operation
+	Addition operation
Δ	Delta
/	Division operation
=	Equality sign
*	Multiplication operation
%	Percent sign
Σ	Sigma
√	Square root
-	Subtraction operation
∑	Summation
|X|	The absolute value
Θ	Theta

CHAPTER ONE

GENERAL INTRODUCTION

Chapter One

General Introduction

1.1 Overview

Network and computer security are highly dependent on the user's authentication. Now, token-based techniques (smartcards) and knowledge-based techniques (passwords) have been the major significant methods. Yet, such approaches have some security drawbacks. For instance, a password can be simply forgotten, stolen, and shared. Comparably, the smart-cards might be lost, stolen, shared, or duplicated. To circumvent such problems, some biometric authentication login approaches are applied [1].

The biometric verifications are referring to the person's automatic verification based on certain biometric features that are obtained from their behavior and/or physiological properties. A system of biometric verification has the ability of distinguish between imposters and authorized individuals in comparison to conventional systems which are using passwords or cards. About biometrics, and an individual might be identified on the basis of who they are instead of having an ID card or passwords [2].

Behavioral biometrics and physical biometrics are the two branches of biometrics. The latter includes face recognition, hand recognition, iris, fingerprints, and sclera. While the first one consists of key-stone and signatures. The biometrics, which are on the basis of ***physical behavior*** are of high importance, consisting of hand's geometrics, fingerprint's ridges, iris patterns, face's structure, voice as well as sclera vein patterns [3].

The biometric authentication system might be specified as multi-modal and uni-modal, basd on some biometric traits or applied modalities. The uni-modal biometric system is using one of the biometric characteristics of the individual to identify and verify identity, but the multi biometric system has ability to use two or more multiple biometric system characteristics to identify a person [4].

The multi-modal systems are better than of the other type (uni-modal systems), because of unacceptable false acceptance rates (FAR), and large false rejection rates (FRR). Yet, more information offer to the classifier increasing the recognition accuracy as well as decreasing the error rates, The identity proof has been strengthened as data, whereas it is obtained from various sources [5].

The biometric cryptosystems, including key binding, and the key generation systems are combining high security level. It is offered via cryptography in addition to the non-repudiation offered via biometric. The systems of key generation are producing stable cryptographic key which has been obtained from the biometric data. The systems of key binding are bound a cryptographic key that is randomly generated to biometric template [5].

Concerning the presented thesis, authentication and integrity are achieved by using (MD5-256) message-digest algorithm and the proposed cryptographic key generation algorithm based on the biometric features of users. Since two different biometric traits are obtained from the same user, different extraction techniques that best suit each of these is applied in this work. Sclera features are extracted using the sclera Identification System which is using different techniques to preprocessing sclera image of user and to determine strong features and their descriptions based on the Scale Invariant Feature Transform algorithm (SIFT). Also, palm features are extracted using palm Identification system, which is using different techniques to preprocessing palm image of same user and to determine strong features and their descriptions based on the Scale Invariant Feature Transform algorithm (SIFT). Following the feature extractions and their descriptions from of both proposed identification systems (sclera and palm), dropping these features on the secret image to combine between them, and using shark smell optimization based on the chaotic map to find a set of optimal solutions. In this work, the proposed algorithm for generation 128-bit cryptographic key is based on an optimal solution that is found by using the Shark Smell Optimization Algorithm (SSO) with chaotic maps to enhancement security architecture of the proposed system. Finally, the proposed document signature using message-digest algorithm (MD5-256) is to obtain high security and integrity of data.

1.2 Related Work

Many approaches are proposed in different studies to improve security data based on biometrics:

- ❖ In (2015), G. Radha, B. Suganyadevi, and C. Saranya, [6] have proposed a secure multi-modal biometrical system through the fusion of the Finger vein and eye vein images. In this fusion system, has taken under consideration eye veins as well as finger veins characteristics for the verifications, the user maybe authenticated by the recognition of the sclera veins with the use of a scale and rotation-invariant Y-shape descriptor based approach of feature extractions sufficiently removes the most unlikely match instances. The suggested model enhanced the system security as verified. It is possible to conduct the automatic authentication with state of the art approaches, such as the recognition of the sclera on the move and the scanner of the finger veins on the car steering.

- In (2016), Sujata Kataria and Ashok K. Goel [7] proposed a new multi-biometric system based on fingerprint and signature. The signature uses SIFT (Scale-invariant Feature Transform) and fingerprint uses minutia extraction. The researchers propose using two different datasets. In the fingerprint, the dataset is made up of 10 images. A signature dataset is made up of 10 images.
- In (2017), K. Tamilsevan, et al. [8] suggested a hybrid method of utilizing the palm and finger veins for designing a biometrical system. The suggested system method was performed the simultaneous acquisition of palm and finger vein database. Also, it had resulted in the combination of those 2 pieces of evidence with the use of a hybrid method of comparison for increasing system's sensitivity, and accuracy at the same time as decreasing time harmfulness, and complexity to the user.
- In (2018), M. Madhivhanan and R. Ravi [9] proposed a new hybrid technique in multi- biometrics, which are fingerprint and sclera. The whole process was implemented in the FPGA SOC. The dataset has consisted of 50 fingerprint images and 50 sclera images. Another

dataset has contained 10 fingerprint images, and sclera images of the same finger and the same eye from 6 different users.

- In (2018), Roh, et al. [10] have introduced an approach with recurrent neural network (RNN) and convolutional neural network (CNN) for the generation of the cryptographic keys from the biometrics of the face. CNN has been utilized for the extraction of feature vector from the images of the face, and the RNN results in key generation from feature vectors. In the procedure of the registration, RNN is trained in an iterative manner.
- In (2019), Jaswal et al. [11] are presented a new method for a multi-modal biometric system that has been suggested. The feature-level fusion of geometry, palm print, and hand shape features were carried out. The much-unrelated characteristics have been chosen from a fused set of features. This work achieved results that are matched with other formal art systems.
- In (2019), Pager et al. [12] have been focused on generating cryptographic keys according to the fusion method of the finger-prints reducing other conventional crypto-systems' complexity. The biometrical characteristics such as the finger-prints are permanent during the life-span of the person. In this study, a finger-print key generation approach has been presented, it is robust and utilized to encrypt and decrypt in the elliptic curve approach of cryptography The experimentation has been carried out on the available data-set. The obtained results have shown the significance concerning efficiency, producing a strong key of cryptography.

1.3 Problems statement

Biometric is the measure of behavioral and physiological features for the individual, commonly utilized biometric features for identification or verification, but it is at the same time can be employed as a key for various security applications. However, the unimodal biometric system is suffering from noise, interclass variations, non-universality attacks, so to overcome these attacks, the multimodal biometrics system is joining of two or more modalities biometrics. Among various biometric properties like as, fingerprint, face, voice, area, etc., hybrid techniques represent combinations of two biometric-identification systems (sclera and palm) based on Shark Smell Optimization (SSO) with chaotic maps to overcome many difficulties in individual biometrics .the sclera and palm print biometrics can provide a higher level of security because of its inherent robustness.

1.4 Aims of thesis

The aim of the thesis is to build a strong identity system based on a hybrid technique by using proposed Sclera and Palm identification systems, where each identification system has different techniques to extract features for each user). Enhancement shark smell optimization (ESSO) algorithms based on the 3-dimension logistic chaotic map to enhance the performance of SSO algorithms to generate a stream cipher key. It is used for many purposes and make the system more secure and authentication.

1.5 Layouts of Thesis

The thesis has been organized into five chapters., as follow:

Chapter One: This chapter includes the basic introduction, aim of the thesis, related work, and the layout of the thesis.

Chapter Two: This chapter includes theoretical background and discusses the algorithms that we use.

Chapter three: This chapter illustrated all tools and algorithms used in the design and implementation of proposed document signature based on hybrid identification techniques (sclera and palm–identification system).

Chapter Four: This chapter presents the tests and results.

Chapter Five: This chapter offers conclusions and suggestions for future work.