وزارة التعليم العالي والبحث العلمي

جامعة ديالى

كلية العلوم

Multi-level security model based on retina and chaotic system

A Dissertation
Submitted to the Department of Computer Science\ College of Sciences\ University of Diyala in a Partial Fulfillment of the Requirements for the Degree of Master in Computer Science

By

Murooj Amer Taha

Supervised By

Dr. Taha MH. Hassan
Assistant Professor

Naji M. Sahib
Professor

2019AC 1440AH

Chapter one

General Introduction

1.1 Overview

With the growth of the Internet and its use in various dimensions, organizations and institutions have faced invasion with new issues related to information security and computer networks in a way that technology information industry and communication are seeking for security solutions for these networks and a secure network must be protected against intentional and unintentional attack and have a good response time, availability or high readiness, reliability or high reputation, integrity and be flawless and provide scalability as well as accurate information [1].

One of the issues discussed in information security is the exchange of information through the cover media, so that, different methods such as cryptography, steganography, coding, etc…, have been used [2]. Cryptography is a field of computer science and mathematics that focuses on techniques for secure communication between two parties while a third-party is present[3]. Classical cryptography provided secrecy for information sent over channels where eavesdropping and message interception was possible. Modern cryptography protects data transmitted over high-speed electronic lines or stored in computer systems[4]. The cryptography methods used are private key cryptography (symmetric) and public key cryptography (asymmetric). In Symmetric keys encryption or secret key encryption, a single key is used for the purpose of encryption and decryption. In asymmetric cryptography two keys are used: public key for encryption and private key for decryption. Public key is known to all whereas private key is known only to the user [5] .

Secret key cryptography schemes are generally classified as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing . A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block [6].

On the other hand steganography is the embedding of messages within an innocuous cover work in a way which cannot be detected by anyone without access to the appropriate steganographic key [2]. True random number generator (TRNG) generate random numbers by using the real physical sources which cannot be controlled and predicted. They are used to generate keys for the security systems. All the biometrics can be used as the non- deterministic source of TRNG[7]. So a unique key can be generated directly from the biometric information of the user namely retina biometric[8]. Chaotic functions are a very useful building block for many distinct cryptographic structures. Their deterministic and aperiodic properties enable a clean and elegant analysis of the cryptosystems. The security of such schemes relies on the parameters and initial conditions of the chaotic systems but not related to the computational bounds or stiffness[9].

The cryptography and steganography TRNG keys based on Retina image with chaotic map (or with aromatic sequence) are new techniques. These techniques are adopted in this thesis in order to build complete secure system.

1.2 Problem Statement

The need to protect information with different level of sensitivity led to the definition of a new design approach called Multilevel Security (MLS). The Multilevel Security problem itself is characterized by design secure system with unpredictable, random, and robust keys to protect secret data from access by un authorized users. This system has two different security models; they are cryptography and steganography. The cryptography model depend on retina images and chaotic map while steganography model depend on retina images and arithmetic sequence to generate keys.

1.3 Literature Review

In this section, some of previous studies which are related to the proposed system in this thesis will be shown as the following:

1. In (2010). V.V. Satyanrayanarayana Tallapragada, and E.G. Rajan [10] developed a novel security mechanism for high security networks by combining IRIS biometric techniques with cryptographic and steganographic mechanisms. Classification and recognition showed that the system had minimum false acceptance rate (0.83%). Considering that the password of the users and the data in the smart cards were unique, the probability of false acceptance is further minimized.
2. In (2012). Xingyuan.W et.al [11] produced a true random number generator (TRNG)through using mouse movement and one dimensional chaotic map. They utilized the x-coordinate of the mouse movement to be the length of an iteration segment of our TRNs and the y-coordinate to be the initial value of this iteration segment. And, when it iterated, they perturbed the parameter with the real value produced by the TRNG itself. The result TRNG passed all the NIST statistical tests successfully. The algorithm was suitable to produce true random numbers TRNs on universal personal computers PCs.
3. In (2013). Tajuddin.M, and C. Nandini [12] proposed a novel method that provide secure way to generate the key using retina biometric technique since retina is unique and reduces the probability of duplicates. an algorithm was introduced that directly generated the unique key from the human biometric information such as retinal blood vessels and was not stored in the database. The approach did not create redundant end points in addition to being more complex in nature to crack or to guess the cryptographic key. The method however limits to key generation and can be further explored from the number of bifurcation points, degree of bifurcation point and the number eye land present in the retina images.
4. In (2014), Gerguri S et.al [13] presented a possible approach towards random number generation using biometrics, with

fingerprints as the biometrics of choice. The method provided on-demand session key generation capabilities, typically for symmetric key generation, and to authenticate the user in the process. Analysis of the proposed method was not a straightforward task. The number of entropy-contributing factors was high, and it was difficult to precisely establish the effect they have on the produced binary sequences. Furthermore, behavioral factors were largely dependent on each other, and so the calculated entropies cannot simply been added together.

5. In (2015). Zhao.T et.al [14] proposed an image encryption system with fingerprint used as a secret key based on the phase retrieval algorithm and RSA public key algorithm. The encryption keys included the fingerprint and the public key of RSA algorithm, while the decryption keys are the fingerprint and the private key of RSA algorithm. The simulation results show the validity of the encryption scheme and the high robustness against attacks based on the phase retrieval technique.
6. In (2015). Barman.S et.al [15] used fingerprint based cryptographic key for encryption and decryption algorithms. Fingerprint features were extracted from fingerprint image. The features were processed to derive cryptographic key and the key is used for message encryption. The key is regenerated from a fresh sample (or instance) of same fingerprint at the time of decryption of message. The generated key can be revoke if required and the key does not reveal exact information about fingerprint features as the key non-invertible. The key is secured as the key is generated from fingerprint with the help of a random sequence. The key does not leak any information about the original fingerprint image.
7. In (2016). Ali M. Meligy et.al [16] suggested a novel methodology for securing digital images which utilizes two types of chaotic systems (Logistic map and Tent map). The suggested scheme switched between the two chaotic systems based on cipher-image information. This switching was based on a chaos- feedback mechanism. The main feature of the

proposed scheme depended on the utilization of a biometric secret image to drive an external secret key, which in turn deduces the control parameters of the maps. The cipher of each pixel relied on the secret key, the previous encrypted information and the yield of the Tent map or the Logistic map. The conducted experimental results illustrate that the encrypted image had a small correlations among neighbor pixels, nearly uniform image histogram (approximately random image). Moreover, the security analyses also confirm that the suggested cipher is especially sensitive to variations in the encryption key and the plain image. Thus, the proposed scheme had a sufficient robustness against common attacks.

8. In(2016). Yankanchi. P, and Shanmukhappa A. Angadi [17] suggested image steganography method through which secret text data was embedded in the cover image using a key which had generated from hand geometric extracted features. New data embedding technique was implemented in which data is going to embed by utilizing a unique key which had been generated by extracted hand geometric feature. The proposed system worked for different message lengths and the distortion of original cover image and stego image were calculated using PSNR and MSE. When the message length was 10 characters, the PSNR and MSE was 89.31 and 0.000076 respectively; and when the message length was 100 characters, the PSNR and MSE was 76.13 and 0.001587 respectively.
9. In (2017). Redha.D.A, and Mohsen.M.M [18]proposed a method consist of three levels of security: generating pseudo-random number based on multi-chaotic maps and magic cube to generate the secret key, using the output of key generator to encrypt of the original image, and using the audio cover to stego the cipher image. The proposed algorithm gave a high security where the resulting key pass all the statistical tests with success and had high random and high security . while the goodness of the stego-audio was analyzed using MSE and SNR and the results showed good embedding technique.
10. In (2018). Dwivedia.R et.al [19] proposed a framework for secure communication between two users using fingerprint

based crypto-biometric system has been proposed. Diffie Hellman (DH) algorithm was employed to generate public keys from private keys of both sender and receiver which are shared and further used to produce a symmetric cryptographic key at both ends. In this approach, revocable key for symmetric cryptography was generated from irrevocable fingerprint. The method was evaluated onto all four datasets i.e.DB1-DB4 of FVC2002 and NIST special database 4. The experimental results demonstrate that the GAR of 96.49% and 95.89% for FVC2002 database and NIST special databases, respectively which indicates that our approach performs better than the existing approaches. The proposed method outperforms against different attacks such as network attack, attack on a host, replay attack and MiM attacks.

1.4 Aim of the thesis

The primary aim of this thesis to design and build secure system with true random number generator(TRNG) based on retina images to generate robust keys that the pass most standard statistical tests of randomness and have acceptable bit rate for cryptographic and steganography applications. The system must have significant cryptographic and steganographic qualities for a good security level.

1.5 Thesis organization

The rest of this thesis consists of the following chapters:

- **Chapter Two: Theoretical Background**

Defines and explicates the basic concepts and related subjects of retina vessel extraction , RNG, chaotic system, encryption, and hiding.

- **Chapter Three**: **The Proposed System**

Presents the design of the proposed system exploiting the majority important and related concepts which have been mentioned in chapter two, in addition to present the proposed algorithms and procedures used in system stages.

- **Chapter Four**: **Experimental Results and Evaluation**

Demonstrates the implementation of the proposed system and discusses the results of the system.

- **Chapter Five: Conclusions and Suggestions for Future work** presents the conclusions of this work and recommendations for future works.