شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

بسم الله الرحمن الرحيم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

HANAA ALY

شبكة المعلومات الجامعية

التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HANAA ALY

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics and Electrical Communication Engineering Dept.

Development of Efficient Algorithms for Cancelable Biometrics

A Thesis submitted in partial fulfilment of the requirements of the degree of

Ph.D in Electronics and Electrical Communication Engineering.

(Communication Engineering)

by

Eng. Lamiaa Atef El-sayed Abou Elazm

M.Sc. in Electronics and Electrical communication Engineering.

(Communication Engineering)

Faculty of Engineering, Ain Shams University, 2021

Supervised By

Prof. Mohamed Kamel Elsaid

Dr. Sameh Assem Ibrahim

Dr. Heba Shawkey

Dr. Mohamed Gamal Egila

Cairo - (2021)

AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics and Electrical Communication Engineering Dept.

Development of Efficient Algorithms for Cancelable Biometrics

by

Eng. Lamiaa Atef El-sayed Abou Elazm

M.Sc. in Electronics and Electrical communication Engineering.

(Communication Engineering)

Faculty of Engineering, Ain Shams University, 2021

Examiners' Committee

Name and Affiliation	**Signature**
Prof. **Elsayed Mostafa Saad** Faculty of Engineering, Helwan University	…….
Prof. **Salwa Hussein Elramly** Faculty of Engineering, Ain Shams University	…….
Prof. **Mohamed Kamel Elsaid** Faculty of Engineering, Ain Shams University	…….

Date:28 June 2021

Statement

This thesis is submitted as a partial fulfilment of Ph.D. Degree in Electronics and Electrical Engineering, Faculty of Engineering, Ain shams University.

The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Student name

Lamiaa Atef El-Sayed Abou Elazm

Signature

……..…….

Date:28 June 2021

Researcher Data

Name	: Lamiaa Atef El-Sayed Abou Elazm
Date of birth	: 12 March 1985
Place of birth	: Cairo
Last academic degree	: M.Sc.
Field of specialization	: Electronics and Electrical Engineering
University issued the degree	: Menoufia University
Date of issued degree	: 2012
Current job	: Researcher Ass. at Electronics Research Institute

Summary

Biometrics are defined as either signals or images extracted from humans for the purpose of identification. The most common biometrics is fingerprints, faces, iris, and speech signals. The basic idea of operation of biometric systems is to collect the biometrics from some authorized persons, extract discriminating features from the biometrics as a tool for data reduction and store these features in a database along with the associated person's identities. This is known as the training phase. In the other phase of biometric systems, which is the testing phase, features are extracted from the incoming biometrics for new persons and the detected persons identities are matched to the identities stored in the database.

Most modern security systems depend on encryption and password techniques in data transfer and on biometrics to secure the access to different systems. These traditional systems have suffered for a long time from hacking trials; hence, the researchers have concentrated on biometric systems to avoid these security breaches. Biometric systems require the generation of databases storing the discriminating features extracted from the biometrics. Unfortunately, if the biometric databases are hacked for any reason, the biometrics saved in these systems would be revealed forever.

The basic concept of Cancelable biometrics is to use another version of the original biometric template created through a 1-way transformation of a high-security encryption algorithms, which keeps the original biometrics safe and away from utilization in the system. The new biometrics template can be changed easily in emergency cases without the need to change the system at all. For geometric biometrics as in face recognition, it is possible to use some one-way geometric

distortion transforms that can change the indices in the biometric at hand. These transforms can be designed and changed easily. In the case of biometrics that depend on transform-domain features as in the iris recognition case, it is possible to use techniques such as random projection, and bio-hashing.

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important need of computer security. Many cryptographic algorithms are available for securing information. In general, data will be secured using a symmetric cipher system, while public-key systems will be used for digital signatures and for secure key exchange between users.

However, regardless of whether a user deploys a symmetric or a public-key system, the security is dependent on the secrecy of the secret or private key, respectively. Because of the large size of a cryptographically-strong key, it would clearly not be feasible to require the user to remember and enter the key each time it is required. Instead, the user is typically required to choose an easily remembered passcode that is used to encrypt the cryptographic key. This encrypted key can then be stored on a computer's hard drive. To retrieve the cryptographic key, the user is prompted to enter the passcode, which will then be used to decrypt the key.

Biometric authentication offers a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a passcode to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data. Thus, biometric authentication can replace the use of passcodes to

secure a key. This offers both conveniences, as the user no longer has to remember a passcode, and secure identity confirmation, since only the valid user can release the key.

Biometric Encryption refers to a process of secure key management. Biometric Encryption does not directly provide a mechanism for the encryption/decryption of data, but rather provides a replacement to typical passcode key-protection protocols. Specifically, Biometric Encryption provides a secure method for key management to complement existing cipher systems. This thesis aims to develop the cancelable biometric systems, through a 1-way transform of high-security encryption algorithms, which keeps the original biometrics safe and away from utilization in the system.

The new biometrics template can be changed easily in emergency cases without the need to change the system at all. The system will be then tested over Field Programmable Gate Array (FPGA) to assess its efficiency.

Key words: Cancelable Biometrics, Cryptography, Authentications, FPGA.

Acknowledgements

I express my deep sense of respect and profound gratitude to my supervisor Prof. Mohamed Kamel Elsaied for his invaluable guidance, encouragement, and constant support in every stage for completing this thesis successfully.

I highly appreciate Dr. Sameh Ibrahim, Dr. Heba shawkey, and Dr. Mohamed Gamal Egila for their consistent support and guidance during the running of this Thesis.

My sincere thanks to Prof. Fathi Abd El-Samie, and Dr. Walid El-Shafai for their valuable support throughout this research.

Finally, My deepest appreciation and gratitude to my Parents and my beloved daughters for all their unconditional and continuous support during the preparation of this work.

List of publications

1- Lamiaa A. Abou elazm, Sameh Ibrahim, Mohamed G. Egila, H. shawkey, Mohamed K. H. Elsaid,Fathi E. Abd El-Samie, Walid El-Shafai. Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption. *MultimedToolsAppl* **79,** 14053–14078(2020). https://doi.org/10.1007/s11042-019-08462-8

2- Lamiaa A. Abou elazm , Sameh Ibrahim, Mohamed G. Egila, H. shawkey, Mohamed K. H. Elsaid, Fathi E. Abd El-Samie, Walid El-Shafai, "Hardware Implementation of Cancelable Biometric Systems," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2020, pp. 1145-1152, doi: 10.1109/I-SMAC49090.2020.9243390.

3- Lamiaa A. Abou elazm, Sameh Ibrahim[2], Mohamed G. Egila, H. shawkey, Mohamed K. H. Elsaid, Fathi E. Abd El-Samie, Walid El-Shafai. Software Design and FPGA Implementation of 3D Chaotic Encryption Algorithm based Cancelable Biometric Recognition System. *MultimedToolsAppl (*Revised*)*

Abstract

The security systems depend on encryption and password techniques in data transfer and on biometrics to secure the access to different systems suffer for a long time from hacking trials. This thesis has concentrated on biometric systems to avoid these security breaches. Biometric systems require the generation of databases storing the discriminating features extracted from the biometrics.

This thesis aims to develop the cancelable biometric systems, through a 1-way transform of high-security encryption algorithms, which keeps the original biometrics safe and away from utilization in the system. The new biometrics template can be changed easily in emergency cases without the need to change the system at all. The system will be then tested over Field Programmable Gate Array (FPGA) to assess its efficiency.

The thesis is divided into two main parts; the first part simulate Cancelable biometrics framework that adopt Fractional Fourier Transform (FRFT) encryption algorithm with jigsaw transform. The simulated results showed that encryption algorithm is efficiently encrypting the stored biometric images and are more appreciated and recommended compared to those of the other traditional systems with EER, FAR, and FRR of $9.3997 \times 10{-}15$, $2.6288 \times 10{-}17$, and $1.8969 \times 10{-}13$, respectively, and an average AROC 0.9997.

The second part proposed an Encryption Algorithm based on 3D chaotic map. The cryptanalysis results achieved the high performance of the algorithm, it estimated perception changing in structural information with SSIM = 0.7698, FSIM= 0.9474, and PSNR = 29.427. Also tested key sensitivity analysis with NPCR= 0.9960 and UACI = 0.333; and when examined the Histogram analysis we get histogram deviation (HD) =0.4, and Irregular deviation (ID) = 0.0034. The hardware implementation of the proposed algorithm achieves a good efficiency through correlation analysis.