UNIVERSITI PUTRA MALAYSIA

MULTIMODAL FINGERPRINT AND FACE BIOMETRICS WITH FRAGILE WATERMARKING AND CONVOLUTIONAL NEURAL NETWORK

ABDULMAWLA NAJIH

MULTIMODAL FINGERPRINT AND FACE BIOMETRICS WITH FRAGILE WATERMARKING AND CONVOLUTIONAL NEURAL NETWORK

By

ABDULMAWLA NAJIH

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

August 2020

DEDICATION

This thesis is dedicated to my beloved mother, father, wife and my children

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

MULTIMODAL FINGERPRINT AND FACE BIOMETRICS WITH FRAGILE WATERMARKING AND CONVOLUTIONAL NEURAL NETWORK

By

ABDULMAWLA NAJIH

August 2020

Chairman : Syed Abdul Rahman Al-Haddad Bin Syed Mohammed, PhD
Faculty : Engineering

The rapidly growing use and storage of private, sensitive, and personal information across different applications have given rise to the need to restrict access to such information; thus, leading to the development of biometric authentication. Multimodal biometric authentication has improved system accuracy, but it has not been able to overcome all the vulnerabilities of biometric authentication. To reduce the amount of data that is stored or communicated during the authentication process and to ensure the authenticity of the biometric templates, image watermarking techniques have been used to embed the information in one template over the other. These techniques are either robust or fragile. The robust method can compress the watermarked images but has a limited ability to detect tampering, whereas fragile methods can detect tampering but does not allow watermarked images to be compressed.

In this thesis, a new watermarking method is proposed, based on the Discrete Cosine Transform (DCT) method and the Least Significant Bit (LSB) method. The LSBs of the quantized DCT coefficients of a face image are manipulated according to the values of a binarized fingerprint image. This combination was used to allow the storing and communication of the watermarked images using the popular JPEG format. Since the binarized fingerprint image passes only through lossless compression, i.e. Huffman encoding, the results showed that the fingerprint information before watermarking and that extracted from the watermarked image are identical. Moreover, because all frequency ranges were used in the DCT format of the face image, the results showed that the proposed method had not significantly affected the image, i.e. the cover image, unlike other existing methods.

As the watermark information is not hand-crafted, tamper detection could not be achieved by comparing a static image to the extracted watermark. Thus, a Machine-Learning (ML)-based method was implemented to detect the existence of fingerprint patterns in the watermark. However, as the proposed system used a Convolutional Neural Network (CNN) to measure the similarity between the templates collected from the user and those stored in the model database, tamper detection was already embedded in the same neural network. Accordingly, this neural network output an authentication measure that represents the probability that the collected templates are authentic. A high authenticity measure indicates that the collected templates match the model's templates and that there was no tampering of the received templates.

Experiments were conducted to evaluate the performance of the proposed system. The results show a 98.96% average accuracy, where each prediction took an average processing time of 139.06 ms. The results also showed that the accuracy of tampering detection was 100%. Besides, the size of the files on the disk (or the bandwidth required to communicate the files) was reduced to less than 50% of their original size using the proposed fragile multibiometric watermarking technique. Hence, the proposed methodology was able to yield outstanding performance, compared to existing state-of-the-art methods, while achieving the objectives of the study, namely, to reduce the file size and the time required to authenticate legitimate users while retaining the ability to detect tampering.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

BIOMETRIK MULTIMOD CAP JARI DAN MUKA MENGGUNAKAN PENANDAAN AIR RAPUH DAN RANGKAIAN NEURAL PERLINGKARAN

Oleh

ABDULMAWLA NAJIH

Ogos 2020

Pegerusi : Syed Abdul Rahman Al-Haddad Bin Syed Mohammed, PhD
Fakulti : Kejuruteraan

Kepesatan penggunaan dan penyimpanan maklumat peribadi yang sensitif dan personal secara meluas dalam pebagai aplikasi telah menyebabkan perlunya kepada keterbatasan capaian maklumat personal ini, justeru membawa kepada pembangunan pengesahihan biometrik. Pengesahihan biometrik multimod mempunyai kejituan sistem yang lebih baik tetapi kaedah ini tidak mampu mengatasi kesemua kelemahan pengesahihan biometrik. Untuk mengurangkan jumlah data yang disimpan dan dikomunikasi semasa proses pengesahihan dan untuk memastikan kesahihan templat biometrik, teknik-teknik menanda air imej telah digunakan untuk membenam maklumat dalam satu templat ke atas templat yang lain. Teknik ini terbahagi kepada teknik teguh atau teknik rapuh. Teknik teguh boleh memampatkan imej yang telah ditanda air tetapi tidak boleh mengesan pengacauan manakala teknik rapuh mampu mengesan pengacauan tetapi tidak membolehkan pemampatan imej yang telah ditanda air.

Tesis ini mencadangkan sebuah teknik tanda air baru berdasarkan kaedah Jelmaan Kosinus Diskret (JKD) dan kaedah Bit Terkurang Bererti (BTB). BTB kepada pekali JKD terkuantum imej muka dimanipulasi mengikut nilai imej cap jari dibinari. Kombinasi ini digunakan untuk membolehkan penyimpanan dan komunikasi imej yang ditanda air menggunakan format popular JPEG. Oleh sebab imej cap jari dibinari telah melalui pemampatan tak hilang iaitu pengekodan Huffman, keputusan menunjukkan bahawa maklumat cap jari sebelum ditanda air dan maklumat yang dicabut daripada imej yang telah ditanda air adalah serupa. Selain itu, semua julat frekeunsi untuk imej muka dalam kajian ini merupakan format JKD, jadi keputusan menunjukkan bahawa kaedah yang dicadangkan tidak memberi kesan yang signifikan kepada imej, iaitu imej penutup, berbanding dengan kaedah-kaedah sedia ada. Oleh sebab maklumat tanda air tidak dikawal dengan tangan, pengacauan tidak dapat dikesan dengan membandingkan imej statik dengan tanda air yang dicabut. Justeru,

kaedah Pembelajaran Mesin (PM) digunakan untuk mengesan kewujudan corak cap jari dalam tanda air tersebut. Walaubagaimanapun, sistem yang dicadangkan menggunakan Rangkaian Neural Perlingkaran untuk mengukur persamaan antara templat yang dikumpul dari pengguna dan templat yang disimpan dalam pangkalan data model. Oleh itu, pengesanan pengacauan telahpun terbenam dalam rangkaian neural yang sama. Akibatnya, rangkaian neural ini memberikan ukuran pengesahihan yang menunjukkan kebarangkalian kesahihan templat yang dikumpulkan. Ukuran kesahihan yang tinggi menandakan bahawa templat yang dikumpulkan berpadanan dengan templat model dan tiada pengacauan berlaku ke atas templat yang diterima.

Eksperimen dijalankan untuk menilai prestasi sistem yang dicadangkan. Keputusan menunjukkan kejituan sistem purata sebanyak 98.96%, di mana setiap ramalan mengambil purata masa pemprosesan sebanyak 139.06 ms. Keputusan turut menunjukkan pengesanan pengacauan adalah tepat 100%. Di samping itu, saiz fail dalam cakera (atau lebar jalur yang diperlukan untuk komunikasi fail) telah dikurangkan kepada kurang daripada 50% saiz asli fail menggunakan teknik multibiometrik penandaan air rapuh yang dicadangkan. Kesimpulannya, metodologi yang dicadangkan mampu menghasilkan prestasi yang menonjol berbanding kaedah-kaedah canggih yang lain selain mampu mencapai objektif kajian, iaitu mengurangkan saiz fail dan masa yang diperlukan untuk mengesahihkan pengguna sah sambil mengekalkan kebolehan untuk mengesan pengacauan.

ACKNOWLEDGMENTS

First and foremost, I would like to thank and pray to God for blessing my postgraduate study and giving me strength and courage. I also would like to thank my father and mother for their encouragement and support by praying for me to do my thesis successfully.

Furthermore, I would like to express my gratitude and convey my thanks to my supervisor, **A.P. Dr. S.A.R Al-Haddad Bin Syed Mohammad,** for his supervision, advice, and guidance from the early stage of this research until the completion of the research.

Similarly, I would like to record my gratitude to my co-supervisors **A.P. Dr. Abdul Rahman Ramli** and **A.P. Dr. Shaiful Jahari Hashim,** for their guidance, advice, and continuous support during the entire course of this research. I am deeply thankful to all of my dear classmates and friends, and others who have supported me continuously during the entire course of this research. I would like to express my deepest regards and blessings to my family who have supported me continuously during my study until the completion of my thesis work.

Lastly, I would like to express my special thanks to University Putra Malaysia for providing a beautiful, peaceful, and calm academic environment for research and study.

Abdulmawla Mohammad Ali Najih

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Syed Abdul Rahman Al-Haddad, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Shaiful Jahari b. Hashim, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Abdul Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

____
ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 December 2020

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: ______________________ Date: ________________

Name and Matric No: Abdulmawla Najih, GS35603

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature:	______________________
Name of Chairman of Supervisory Committee:	Professor Syed Abdul Rahman Al-Haddad

Signature:	______________________
Name of Member of Supervisory Committee:	Associate Professor Dr. Shaiful Jahari b. Hashim

Signature:	______________________
Name of Member of Supervisory Committee:	Associate Professor Dr. Abdul Rahman Ramli

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	Artificial Neural Network
ATM	Automated Teller Machines
BICU	Biometric Information Collection Unit
CNN	Convolutional Neural Network
CS	Compressive Sensing
DCT	Discrete Cosine Transform
DTCWT	Dual-Tree Complex Wavelet Transform
DWT	Discrete Wavelet Transform
EER	Equal Error Rate
FAR	False Acceptance Rate
FP	False Positive
FN	False Negative
FRR	False Rejection Rate
IT	Information Technology
LBPH	Local Binary Pattern Histogram
LSB	Least Significant Bit
MSE	Mean Squared Error
MTCNN	Multi-Task Convolutional Neural Network
NFC	Near-Field Communication
PIN	Personal Identification Number
PSNR	Peak Signal to Noise Ratio
ReLU	Rectified Linear Unit

RFID	Radio Frequency Identification
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristic
SIFT	Scale-Invariant Feature Transform
SSIM	Structural Similarity Index Measure
SURF	Speeded-Up Robust Feature
SVD	Singular Value Decomposition
TanH	Hyperbolic Tangent
TP	True Positive
TN	True Negative

CHAPTER 1

INTRODUCTION

1.1 Overview

The rapid growth in Information Technology (IT) has revised the need to protect sensitive and personal data from any unauthorized access. Many techniques have been proposed to protect these data, such as the knowledge-based method, where login credentials, such as passwords, Personal Identification Number (PIN) or patterns, are required from the users to access these data. However, the importance of protecting these data and the sensitivity of such methods to simple attacks, such as shoulder surfing, have imposed the need for more secure techniques (Nagatomo et al., 2018; Sunet al., 2018). Therefore, many methods have been proposed to protect these techniques from known attacks but the tendency of humans to use easy-to-remember credentials has limited the capabilities of such techniques, as easy-to-remember credentials are also easy-to-predict (Gokhale et al., 2016; Jiang et al., 2015).

To protect such data, and according to the limited security that Knowledge-based techniques provide, many techniques have been proposed based on biometric information. This information is collected from the user upon authentication and compared to the information of the legitimate users who are allowed to access the system. The user of such information has shown better resistance against attacks that rely on identifying the information used for authentication, as it is more complex to replicate biometric features, than the traditional methods, such as passwords or patterns, in Knowledge-based authentication (Chaudhry et al., 2015).

Despite the better performance of the biometric authentication systems, these systems still have some vulnerabilities that can be exploited by attackers to manipulate the authentication decision made by these systems. Such manipulation can be of two categories, the first is to deny legitimate users from accessing the information that they are supposed to access, while the other is gain access to such information by intruders, which are users that do not have the right to access such information. Both categories of manipulation can downgrade the performance of the authentication system, as blocking legitimate users from accessing their data affects the usability of the system, while gaining access to these data by intruders affects the security measure of the authentication system (Dasgupta, 2017).

The generic biometric system shown in Figure 1.1 illustrates the main component of such systems. According to Ratha et al. (Ratha et al., 2001), an attacker may attack any of these components, as well as, manipulating the information being transferred from one component to another, in order to execute the required attack. Thus, different techniques have been proposed to overcome the vulnerabilities in biometric systems. Some of these techniques can protect the systems against certain attacks, while some other vulnerabilities still persist in such systems.

These attacks, according to their positions, are:

A. **Sensor attacks:** Intruders in such attacks attempt to provide false biometric information to the sensor, where this biometric information is acquired from a legitimate user. A fake finger, mask or audio recording are examples of such attacks.
B. **Reproducing captured biometrics signals:** In this type of attacks, intruders capture data transmitted by the sensor and replay it, bypassing the data collection of the sensor, in order to authenticate to the system. For example, transmitting data captured from the output of the sensor during a legitimate fingerprint scan.

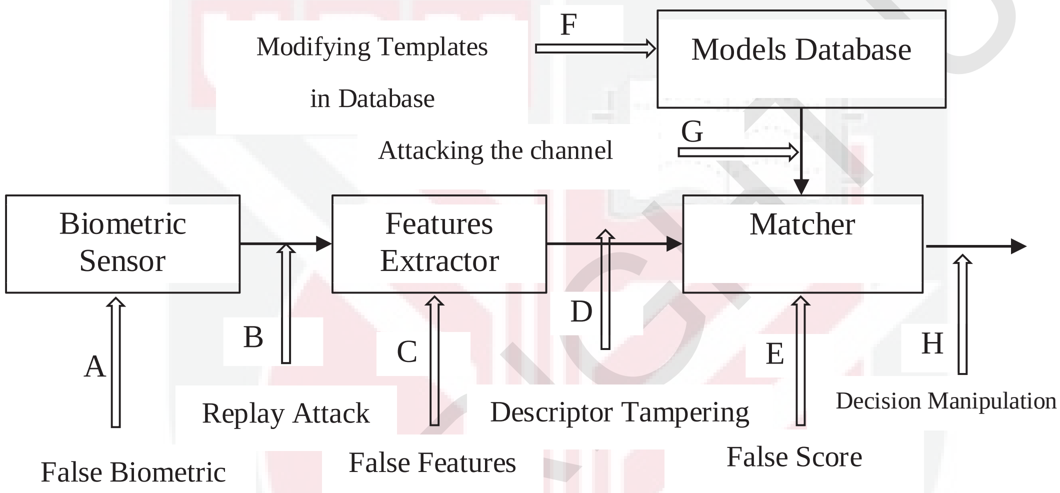


Figure 1.1 : The main components of a generic biometric authentication system with the main vulnerable points (Ratha et al., 2001)

C. **Producing false features:** Intruders, in this type of attack, produce false features, selected by the intruder, in the feature extractor, so that, the descriptors generated for these features are matched by the matcher. For example, a Trojan horse is used to inject the preselected features into the feature extractor, to override its original output.
D. **Tampering biometric features descriptor:** In such attacks, the intruders modify the contents of the template sent from the features extractor to the matcher, by tampering the network packets communicated between them. Although most of the features extractors and matches run on the same machine, using separate machines or network communications can dramatically affect the security of the transmitted data.
E. **Modifying matcher's scores:** By compromising the security of the matcher, the intruders send false similarity scores instead of those produced based on the matching result, so that, intruders are authenticated into the system despite no matching biometrics could be detected.

F. **Tampering stored models:** By attacking the data management servers, the model biometrics stored on those servers have tampered, so that, intruders gain access to the system, or legitimate users are denied.
G. **Modifying retrieved model biometrics:** Instead of attacking the data management server, intruders in this type of attacks intercept the template, sent from that server to the matcher, and change their contents.
H. **Final decision override:** Regardless of the results of all the stages of the biometric authentication system, intruders compromise the security of the matcher and send false decisions. Thus, no matter how good the performance of the biometric authentication system is, executing and succeeding in such attacks can cause dramatic harm to the system protected by the compromised biometric authentication.

One of the widely used techniques to protect the authenticity of information communicated between different parts of the authentication system is digital watermarking, where biometric information is added to the captured biometric image that the biometric features are extracted from. Watermarking techniques are normally used for one of two reasons, which are to prove ownership of the biometric image or to detect any tampering with it. Moreover, some of the watermarking techniques add visible watermarks to the biometric image, while others hide the watermark inside the biometric image, so that, it is not visible unless it is extracted. For tamper detection, hidden watermarks are added to the biometric images, so that, the absence of the watermark or any distortion in the extracted watermark indicates tampering with the original biometric image. Moreover, the watermarking techniques used for tamper detection is fragile, so that, the extracted watermark is highly affected when any attack is executed against the watermarked biometric image (Hämmerle-Uhl et al., 2011; Kumar et al., 2016; B. Ma et al., 2014; Rohit Thanki et al., 2016).

Moreover, to improve the security of the data protected by biometric authentication systems, biometric information is collected from different parts of the body, which are known as multibiometric authentication systems (Gupta et al., 2018). However, this increases the amount of data communicated among the different components of the biometric authentication system and storage space required for the model images of legitimate users. Therefore, many multibiometric authentication techniques have been proposed that watermark the feature of one biometric image using another, so that, the addition to the amount of transferred and stored data remains minimum (Ghouzali, 2015). These methods also encrypt the hidden watermark to reduce the vulnerability of the system, as the extracted watermark is still unknown, unless the encryption key is discovered (Murilloet al., 2015). However, the existing watermarking techniques either lose significant information from the biometric image used as the watermark, impose significant distortion to the cover image or loses the watermark information when the resulting image is compressed, which again affects the size of the stored and transferred data.

Convolutional neural networks are being widely used to detect and extract distinctive and robust features from images. According to the employment of multi-dimensional filters, these networks have the ability to detect local multi-dimensional features, i.e. regardless of the relation between the positions of these features and boundaries of the image. As a filter at a certain convolutional layer detects features that consist of features detected in the previous layer, deep convolutional neural networks have gained the ability to detect complex features. Additionally, during the training of these networks, the features that define the required inter-class variations are emphasized, while those that define intra-class variations are neglected. Hence, unlike computer vision methods that rely on hand-crafted features, these networks have the ability to learn only distinctive features, regardless of the complexity of these features (O'Mahony et al., 2019).

1.2 Problem Statements

The use of multiple biometric templates for authentication has been able to significantly improve the accuracy of biometric authentication systems, compared to the use of a single biometric template. However, multimodal biometric authentication has not been able to handle the vulnerability of the these systems toward different types of attacks (Ratha et al., 2001;Yang et al., 2019). These attacks mainly target the data being stored in, or communicated among, the different parts of the system. Therefore, digital watermarking techniques are being employed to ensure the authenticity of the biometric images received by any part of the system and detect any tampering with them. Moreover, according to the use of multiple biometric templates in these systems, recent methods use one of the templates as a watermark on the other, so that, the authenticity of the received biometric image can be verified, whereas both template, cover and watermark, can still be used in the authentication process. Thus, the use of multi-modal biometric authentication faces the following problems:

The first problem is imposed by the use of robust techniques to protect the biometric templates allows the watermarked biometric templates to be compressed, according to the robustness of the embedded information (Bousnina et al., 2019; O. Nafea et al., 2016). However, such robustness limits the ability to detect tampering with these watermarked biometric templates. Thus, fragile watermarking techniques (R. Thanki et al., 2015; Rohit Thanki et al., 2016; R. M. Thanki et al., 2018) are used for tamper detection, in which the watermark biometric template is lost when the watermarked biometric image is compressed. As the JPEG format is widely used to store and communicate compressed biometric images, a fragile multibiometric watermarking technique that embeds the watermark biometric template to the compressed biometric image is required. Such a technique can provide a tradeoff between the size of the produced biometric image and tamper detection. Hence, it combines the lower file sizes that can be produced with robust watermarking while maintaining the ability to detect tampering with the watermarked biometric image.

The second problem is imposed by the use of one biometric template as the watermark, as the exact information of the watermark becomes unknown (C.-C. Han et al., 2003). Validating such watermarked template requires detecting the patterns that form the biometric templates in the watermarked images, the existing biometric templates detection methods (Isa et al., 2017; B. Ma et al., 2014; Wojtowicz et al., 2016) detect template in the watermarked image in a separate stage, which increase the time required to authenticate legitimate user. Consequently, to reduce the time required to authenticate the legitimate users, the tamper detection and biometrics matching are required to be combined in a single stage, so that, no additional processing is required for legitimate users.

The third problem is imposed by the separation of the features extraction and the matching score computation stages, which is exploited by intruders to breach into the biometric system or deny legitimate users from accessing it, (Isa et al., 2017; B. Mang et al., 2014;R. Thanki & Borisagar et al., 2015; Rohit Thanki et al., 2016; R. M. Thanki et al., 2018). By manipulating the biometric template on the communication channel, before delivered to the similarity score stage, attackers can deceive the similarity score technique to produce false matching. Therefore, fusing these stages in a single technique that measures the similarity between biometric template directly from the raw pixel of a biometric image can eliminate the risk of manipulating the biometric template extracted from the biometric images.

1.3 Objectives

The aim of this study is to provide security biometric data over a communication channel between two models and at system database of the multibiometric system. Hence, the three problems described in Section 1.2 must be solved as in the following objectives:

1. To design a multibiometric watermarking technique by adding watermark information to the compressed face image, so that, the bandwidth required to communicate these biometric templates is reduced.
2. To implement tamper detection, based on the patterns of the biometric template in the watermark, in the same scheme used to match the biometric templates collected from the user being authenticated with those in the database, so that, no additional computations are required to authenticate the legitimate users.
3. To develop a similarity measurement technique that has the ability to extract the features, measure the similarity and produce a proper authentication decision in one stage, so that, no information is communicated among the different stages, which imposes vulnerabilities to the authentication system.

1.4 Thesis Scope

In This thesis multibiometric watermarking technique using face and fingerprint biometrics is designed, in order to improve the protection of biometric templates against spoofing and modification attacks at system database, also to protect the communication channel of the biometric system, at the same time , reducing the size and bandwidth required by the multibiometric system. For this purpose, a fragile watermarking method is developed by adding fingerprint information to the compressed version of the face image. As the JPEG compression format is widely used to store and communicate biometric images, the developed fragile multibiometric watermarking technique embeds the fingerprint template in the quantized DCT coefficient of the cover face image before being compressed using entropy encoding, following the JPEG standard. Hence, the presence of the watermark pattern can be investigated to examine the authenticity of the received biometric image, without the need to store the watermarked biometric image in full-size to maintain the watermark information. Hence, the authenticity of the compressed watermarked biometric images can be investigated, to secure the system against tampering with these images, without imposing the need of additional bandwidth for communication.

According to the good performance of artificial neural networks in the authentication system, a method is developed in this thesis based on these networks to authenticate users. The developed method produces an authenticity score, which combines both the similarity measure and tampering detection, in a single neural network, so that, the authenticity measure is computed directly from the raw pixel values of the input face images. However, according to the limited number of datasets that can be used to train the neural network for such a task, transfer learning is used to accelerate the training of the neural network and maintain good performance measures. A pre-trained neural network, using an enormous number of training data, is wrapped in a larger neural network, so that, the feature vectors produced by these networks are used to compute the authenticity score in a single neural network. The developed neural network provides the following features:

- Less vulnerabilities to attacks, according to the fusion of multiple stages, i.e. feature extraction, matching and tamper detection, in a single stage.
- Processing the feature vectors in the same neural network allows embedding tamper detection in the same stage, i.e. neural network, as the further layers in the neural network can detect the existence of fingerprint patterns in the fingerprint images. Measuring the similarity between the feature vectors without the use of a neural network cannot accomplish tamper detection, as it only relies on the similarity between the feature values in these vectors.
- Less time to authenticate legitimate users as the same neural network that is used for similarity measurement is used for tamper detection, i.e. no additional time is required for tamper detection in case a legitimate user is authenticating into the system.
- Maintaining separate similarity measurements for face and fingerprint features by using a convolutional layer that processes the values of the vectors from each type separately before being fused into further layers.

As the proposed watermarking technique imposes deformation in the cover image and according to the ability to compress the watermarked face images, the effect of the proposed watermarking method over the authentication accuracy is evaluated in different compression rates. The evaluation also includes the size of the data produced by the proposed watermarking method at different compression rates, so that, a balanced performance can be selected depending on the type of the application the proposed method is being employed in. Figure 1.2 summarizes the scope of the thesis.

1.5 Thesis Structure

The remainder of this thesis is illustrated as follows:

- Chapter Two reviews the literature related to the biometric authentication and watermarking techniques. This review provides a rigid background to what and where the earlier studies have reached, in addition to the weakness and strength points of the techniques proposed in each study. This background can be used for the proposal of the new authentication system and the techniques employed in it.
- Chapter Three describes the techniques proposed to improve the accuracy and security of the proposed biometric authentication system, compared to the systems existing in the literature. These techniques are the watermarking, tamper detection and similarity measurements, as well as, the entire topology of the proposed system.
- Chapterer Four describes the experimental setup used to conduct the experiments that evaluated each technique proposed in this study, as well as, the overall performance of the proposed multibiometric authentication system. These results are also compared to the state-of-the-art techniques proposed in recent studies, to illustrate the superiority of the proposed method. Finally, the overall performance of the proposed system is evaluated by combining all these techniques in a single system.
- Chapter Five illustrates the conclusions distinguished during this study, the future work that is recommended regarding the proposed system, other applications that can employ the techniques proposed in this study and the main contributions of this study.

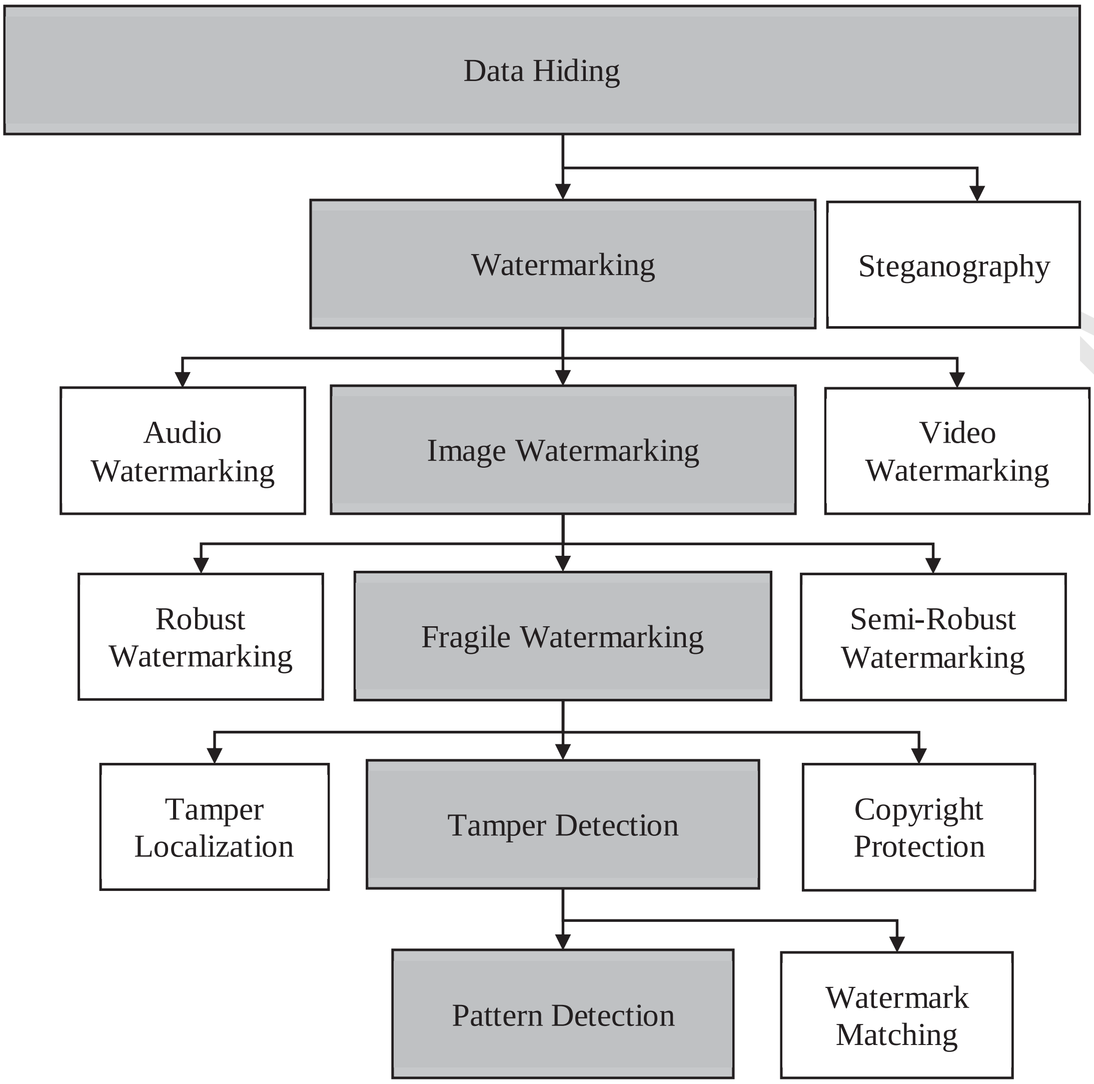


Figure 1.2 : Scope of the thesis

REFERENCES

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., . . . Isard, M. (2016). *TensorFlow: A System for Large-Scale Machine Learning.* Paper presented at the OSDI.

Agoyi, M., Çelebi, E., & Anbarjafari, G. (2015). A watermarking algorithm based on chirp z-transform, discrete wavelet transform, and singular value decomposition. *Signal, Image and Video Processing, 9*(3), 735-745.

Al-Ta'l, Z. T. M., & Abdulhameed, O. Y. (2013). *Features extraction of fingerprints using firefly algorithm.* Paper presented at the Proceedings of the 6th International Conference on Security of Information and Networks.

Anand, B., & Shah, M. P. K. (2016). Face Recognition using SURF Features and SVM Classifier. *International Journal of Electronics Engineering Research. ISSN*, 0975-6450.

Anwar, A. S., Ghany, K. K. A., & Elmahdy, H. (2015). Human ear recognition using geometrical features extraction. *Procedia Computer Science, 65*, 529-537.

Avcibas, I., Sankur, B., & Sayood, K. (2002). Statistical evaluation of image quality measures. *Journal of Electronic imaging, 11*(2), 206-224.

Barbosa, F. G., & Silva, W. L. S. (2015). *Support vector machines, Mel-Frequency Cepstral Coefficients and the Discrete Cosine Transform applied on voice based biometric authentication.* Paper presented at the SAI Intelligent Systems Conference (IntelliSys), 2015.

Bay, H., Ess, A., Tuytelaars, T., & Van Gool, L. (2008). Speeded-up robust features (SURF). *Computer vision and image understanding, 110*(3), 346-359.

Bayram, S., Sencar, H. T., & Memon, N. (2015). Sensor fingerprint identification through composite fingerprints and group testing. *IEEE Transactions on Information Forensics and Security, 10*(3), 597-612.

Behera, B., Govindan, V. J. I. J. o. C. S., & Network. (2013). Improved multimodal biometric watermarking in authentication systems based on DCT and phase congruency model. *2*(3), 123-129.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics*: Springer Science & Business Media.

Bousnina, N., Ghouzali, S., Mikram, M., & Abdul, W. (2019). *DTCWT-DCT watermarking method for multimodal biometric authentication.* Paper presented at the Proceedings of the 2nd International Conference on Networking, Information Systems & Security.

Boyat, A. K., & Joshi, B. K. (2015). A review paper: noise models in digital image processing. *arXiv preprint arXiv:1505.03489.*

Bradski, G., & Kaehler, A. (2000). OpenCV. *Dr. Dobb's journal of software tools, 3*.

Chaki, N., Shaikh, S. H., & Saeed, K. (2014). Exploring image binarization techniques.

Chaudhry, S. A., Mahmood, K., Naqvi, H., & Khan, M. K. (2015). An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *Journal of Medical Systems, 39*(11), 175.

Chollet, F. (2018). Keras: The python deep learning library. *Astrophysics Source Code Library*.

Chung, H., Lee, S. J., & Park, J. G. (2016). *Deep neural network using trainable activation functions.* Paper presented at the Neural Networks (IJCNN), 2016 International Joint Conference on.

Clayton, G., Goodhue, R., Abdelbagi, S. T., & Vecoli, M. (2017). Correlation of Palynomorph Darkness Index and vitrinite reflectance in a submature Carboniferous well section in northern Saudi Arabia. *Revue de Micropaléontologie, 60*(3), 411-416.

Dasgupta, D., Roy, A., & Nag, A. (2017). *Advances in User Authentication*: Springer.

Du, G., Su, F., & Cai, A. (2009). *Face recognition using SURF features.* Paper presented at the MIPPR 2009: Pattern Recognition and Computer Vision.

Esser, S. K., Appuswamy, R., Merolla, P., Arthur, J. V., & Modha, D. S. (2015). *Backpropagation for energy-efficient neuromorphic computing.* Paper presented at the Advances in Neural Information Processing Systems.

Ghouzali, S. (2015). *Watermarking based multi-biometric fusion approach.* Paper presented at the International Conference on Codes, Cryptology, and Information Security.

Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. *Procedia Computer Science, 79*, 490-498.

Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). *Deep learning* (Vol. 1): MIT press Cambridge.

Gore, A., & Gupta, S. (2015). Full reference image quality metrics for JPEG compressed images. *AEU-International Journal of Electronics and Communications, 69*(2), 604-608.

Gu, Y., Saad, W., Bennis, M., Debbah, M., & Han, Z. (2015). Matching theory for future wireless networks: fundamentals and applications. *IEEE Communications Magazine, 53*(5), 52-59.

Gupta, P., & Gupta, P. (2018). Multi-biometric Authentication System using Slap Fingerprints, Palm Dorsal Vein and Hand Geometry. *IEEE Transactions on Industrial Electronics*.

Gurney, K. (2014). *An introduction to neural networks*: CRC press.

Habuka, K., & Shinagawa, Y. (2004). Image interpolation using enhanced multiresolution critical-point filters. *International journal of computer vision, 58*(1), 19-35.

Hämmerle-Uhl, J., Raab, K., & Uhl, A. (2011). *Watermarking as a means to enhance biometric systems: A critical survey*. Paper presented at the International Workshop on Information Hiding.

Han, C.-C., Cheng, H.-L., Lin, C.-L., & Fan, K.-C. (2003). Personal authentication using palm-print features. *Pattern Recognition, 36*(2), 371-381.

Han, S., Pool, J., Tran, J., & Dally, W. (2015). *Learning both weights and connections for efficient neural network*. Paper presented at the Advances in neural information processing systems.

Hany, U., & Akter, L. (2015). *Speeded-Up Robust Feature extraction and matching for fingerprint recognition*. Paper presented at the Electrical Engineering and Information Communication Technology (ICEEICT), 2015 International Conference on.

Harbach, M., De Luca, A., & Egelman, S. (2016). *The anatomy of smartphone unlocking: A field study of android lock screens*. Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.

Hawkins, D. M. (2004). The problem of overfitting. *Journal of chemical information and computer sciences, 44*(1), 1-12.

Hore, A., & Ziou, D. (2010). *Image quality metrics: PSNR vs. SSIM*. Paper presented at the Pattern recognition (icpr), 2010 20th international conference on.

Isa, M. R. M., Aljareh, S., & Yusoff, Z. (2017). A watermarking technique to improve the security level in face recognition systems. *Multimedia Tools and Applications, 76*(22), 23805-23833.

Jahan, S., Chowdhury, M., & Islam, R. (2017). *Robust fingerprint verification for enhancing security in healthcare system*. Paper presented at the 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ).

Jiang, M., He, A., Wang, K., & Le, Z. (2015). *Two-Way Graphic Password for Mobile User Authentication*. Paper presented at the Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on.

Jinimole, C., & Harsha, A. (2017). Comparative Study of Different Enhancement Techniques for Computed Tomography Images. *World Academy of Science, Engineering and Technology, International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering, 11*(9), 524-527.

Jordanski, M., Arsic, A., & Tuba, M. (2015). *Dynamic recursive subimage histogram equalization algorithm for image contrast enhancement*. Paper presented at the Telecommunications Forum Telfor (TELFOR), 2015 23rd.

Juan, L., & Gwun, O. (2009). A comparison of sift, pca-sift and surf. *International Journal of Image Processing (IJIP), 3*(4), 143-152.

Kamencay, P., Benčo, M., Miždoš, T., & Radil, R. (2017). A new method for face recognition using convolutional neural network.

Kanade, T. (1974). Picture processing system by computer complex and recognition of human faces.

Karpathy, A., Toderici, G., Shetty, S., Leung, T., Sukthankar, R., & Fei-Fei, L. (2014). *Large-scale video classification with convolutional neural networks.* Paper presented at the Proceedings of the IEEE conference on Computer Vision and Pattern Recognition.

Kątek, G., Holik, A., Zabłocki, T., & Dobrzyńska, P. (2016). Face recognition using the Haar classifier cascade and face detection based on detection of skin color areas. *I ELEKTRONIKA*, 29.

Khalil-Hani, M., & Sung, L. S. (2014). *A convolutional neural network approach for face verification.* Paper presented at the 2014 International Conference on High Performance Computing & Simulation (HPCS).

Krishnamoorthy, S., Rueda, L., Saad, S., & Elmiligi, H. (2018). *Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning.* Paper presented at the Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications.

Kubat, M. (2015). Artificial neural networks. In *An Introduction to Machine Learning* (pp. 91-111): Springer.

Kumar, R., Chandra, P., & Hanmandlu, M. (2016). A Robust Fingerprint Matching System Using Orientation Features. *JIPS, 12*(1), 83-99.

Labati, R. D., Genovese, A., Piuri, V., & Scotti, F. (2014). Touchless fingerprint biometrics: a survey on 2D and 3D technologies. *網際網路技術學刊, 15*(3), 325-332.

Labati, R. D., Piuri, V., & Scotti, F. (2015). *Touchless fingerprint biometrics*: CRC Press.

Lastra, M., Carabaño, J., Gutiérrez, P. D., Benítez, J. M., & Herrera, F. (2015). Fast fingerprint identification using GPUs. *Information Sciences, 301*, 195-214.

Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International journal of computer vision, 60*(2), 91-110.

Luo, W., Schwing, A. G., & Urtasun, R. (2016). *Efficient deep learning for stereo matching.* Paper presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.

Ma, B., Li, C., Wang, Y., Zhang, Z., & Wang, Y. (2010). *Block pyramid based adaptive quantization watermarking for multimodal biometric authentication.* Paper presented at the 2010 20th International Conference on Pattern Recognition.

Ma, B., Wang, Y., Li, C., Zhang, Z., Huang, D. J. M. t., & applications. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. *72*(1), 637-666.

Ma, M., & Wang, J. (2018). *Multi-View Face Detection and Landmark Localization Based on MTCNN.* Paper presented at the 2018 Chinese Automation Congress (CAC).

Mahajan, D. L., & Gogate, S. A. (2016). Overview of Digital Watermarking and its Techniques. *KHOJ: Journal of Indian Management Research and Practices*, 197-204.

Mahmud, M., Sultan, K., Aldhafferi, N., Alqahtani, A., & Musleh, D. (2018). Medical Image Watermarking for Fragility and Robustness: A Chaos, Error-Correcting Codes and Redundant Residue Number System Based Approach. *Journal of Medical Imaging and Health Informatics, 8*(6), 1192-1200.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2002. Retrieved from http://bias.csr.unibo.it/fvc2002/

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004). *FVC2004: Third fingerprint verification competition.* Paper presented at the International Conference on Biometric Authentication.

Malik, J., Girdhar, D., Dahiya, R., & Sainarayanan, G. (2014). Reference threshold calculation for biometric authentication. *IJ Image, Graphics, and Signal Processing, 2*, 46-53.

Mehta, R., Rajpal, N., & Vishwakarma, V. P. (2017). A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform. *International Journal of Machine Learning and Cybernetics, 8*(2), 379-395.

Mei, X., Ma, Y., Li, C., Fan, F., Huang, J., & Ma, J. (2015). A real-time infrared ultra-spectral signature classification method via spatial pyramid matching. *Sensors, 15*(7), 15868-15887.

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293.

Michelsanti, D., Guichi, Y., Ene, A.-D., Stef, R., Nasrollahi, K., & Moeslund, T. B. (2018). *Fast fingerprint classification with deep neural network.* Paper presented at the International Conference on Computer Vision Theory and ApplicationsInternational Conference on Computer Vision Theory and Applications.

Moenssens, A. A., Inbau, F. E., & Starrs, J. E. (1973). *Scientific evidence in criminal cases*: Foundation Press Mineola, NY.

Moon, D., Kim, T., Jung, S., Chung, Y., Moon, K., Ahn, D., & Kim, S.-K. (2005). *Performance evaluation of watermarking techniques for secure multimodal biometric systems.* Paper presented at the International Conference on Computational and Information Science.

Mukherjee, V. J. a. A. (2002). The Indian Face Databa. Retrieved from http://www.cs.umass.edu/~vidit/IndianFaceDatabase

Murillo-Escobar, M., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications, 42*(21), 8198-8211.

Nafea, O., Ghouzali, S., Abdul, W., & Qazi, E.-u.-H. (2016). Hybrid multi-biometric template protection using watermarking. *The Computer Journal, 59*(9), 1392-1407.

Nafea, O., Ghouzali, S., Abdul, W., & Qazi, E.-u.-H. J. T. C. J. (2016). Hybrid multi-biometric template protection using watermarking. *59*(9), 1392-1407.

Nagatomo, M., Kita, Y., Aburada, K., Okazaki, N., & Park, M. (2018). Implementation and user testing of personal authentication having shoulder surfing resistance with mouse operations. *IEICE Communications Express, 7*(3), 77-82.

Nair, S. A. H., & Aruna, P. (2015). Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems. *Alexandria Engineering Journal, 54*(4), 1161-1174.

Narasimhulu, C. V., & Prasad, K. S. (2011). A novel robust watermarking technique based on Nonsubsampled contourlet Transform and SVD. *The International Journal of Multimedia & its applications, 3*(1).

Naresh, S., Kumar, B. V., & Karpagam, G. (2015). A literature review on quantization table design for the JPEG baseline algorithm. *International Journal of Engineering And Computer Science, 4*(10), 14686-14691.

Nunez, P. L., & Cutillo, B. A. (1995). *Neocortical dynamics and human EEG rhythms*: Oxford University Press, USA.

O'Mahony, N., Campbell, S., Carvalho, A., Harapanahalli, S., Hernandez, G. V., Krpalkova, L., . . . Walsh, J. (2019). *Deep Learning vs. Traditional Computer Vision*. Paper presented at the Science and Information Conference.

Pandya, K. D. (2017). Face Detection–A Literature Survey. *International Journal of Computer Techniques, 3*(1).

Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). *Deep face recognition*. Paper presented at the BMVC.

Patel, H. A., & Divecha, N. H. (2018). A Feature-Based Semi-fragile Watermarking Algorithm for Digital Color Image Authentication Using Hybrid Transform. In *Advances in Computer and Computational Sciences* (pp. 455-465): Springer.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., . . . Dubourg, V. (2011). Scikit-learn: Machine learning in Python. *Journal of machine learning research, 12*(Oct), 2825-2830.

Peralta, D., Triguero, I., Sanchez-Reillo, R., Herrera, F., & Benítez, J. M. (2014). Fast fingerprint identification for large databases. *Pattern Recognition, 47*(2), 588-602.

Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

Phillips, P. J., Der, S. Z., Rauss, P. J., & Der, O. Z. (1996). *FERET (face recognition technology) recognition algorithm development and test results*: Army Research Laboratory Adelphi, MD.

Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., . . . Worek, W. (2005). *Overview of the face recognition grand challenge.* Paper presented at the 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05).

Phillips, P. J., Moon, H., Rizvi, S. A., & Rauss, P. J. (2000). The FERET evaluation methodology for face-recognition algorithms. *IEEE transactions on pattern analysis and machine intelligence, 22*(10), 1090-1104.

Raghavendra, R., Raja, K. B., Surbiryala, J., & Busch, C. (2014). A low-cost multimodal biometric sensor to capture finger vein and fingerprint. *IJCB, 2014*, 1-7.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal, 40*(3), 614-634.

Raval, M., Joshi, M., Rege, P., & Parulkar, S. (2011). Image tampering detection using compressive sensing based watermarking scheme. *Proceedings of MVIP 2011*.

Sanner, M. F. (1999). Python: a programming language for software integration and development. *J Mol Graph Model, 17*(1), 57-61.

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural networks, 61*, 85-117.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). *Facenet: A unified embedding for face recognition and clustering.* Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Shang, S., Zhao, Y., & Ni, R. (2016). *Double JPEG detection using high order statistic features.* Paper presented at the 2016 IEEE International Conference on Digital Signal Processing (DSP).

Shekaramiz, K., & Naghsh, A. (2017). *Embedding and extracting two separate images signal in salt & pepper noises in digital images based on watermarking.* Paper presented at the 2017 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA).

Shoemaker, C. (2002). Hidden bits: A survey of techniques for digital watermarking. *Independent study, EER, 290*, 1673-1687.

Shrivastava, K., Manda, S., Chavan, P., Patil, T., & Sawant-Patil, S. (2018). Conceptual Model for Proficient Automated Attendance System based on Face Recognition and Gender Classification using Haar-Cascade, LBPH Algorithm along with LDA Model. *International Journal of Applied Engineering Research, 13*(10), 8075-8080.

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

Spolaor, R., Li, Q., Monaro, M., Conti, M., Gamberini, L., & Sartori, G. (2016). Biometric Authentication Methods on Smartphones: A Survey. *PsychNology Journal, 14*(2).

Sreeja, N., & Sankar, A. (2015). Pattern matching based classification using ant colony optimization based feature selection. *Applied Soft Computing, 31*, 91-102.

Sukthankar, G. (2000). *Face recognition: a critical look at biologically-inspired approaches*: Carnegie Mellon University, the Robotics Institute.

Sun, H.-M., Chen, S.-T., Yeh, J.-H., & Cheng, C.-Y. (2018). A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing, 15*(2), 180-193.

Sung, F., Yang, Y., Zhang, L., Xiang, T., Torr, P. H., & Hospedales, T. M. (2018). *Learning to compare: Relation network for few-shot learning*. Paper presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.

Surya, D., & Krishnaveni, R. (2015). *A novel method for face recognition using neural networks with optical and infrared images*. Paper presented at the Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., . . . Rabinovich, A. (2015). *Going deeper with convolutions*. Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). *Deepface: Closing the gap to human-level performance in face verification*. Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition.

Thanki, R., & Borisagar, K. (2015). Multibiometric Template Security Using CS Theory–SVD Based Fragile Watermarking Technique. *WSEAS Transactions on Information Science and Applications, 12*, 1-10.

Thanki, R., & Borisagar, K. (2016). *Biometric Image Protection Using Compressive Sensing and DCT based Watermarking Technique*. Paper presented at the proceedings of RK University's First International Conference on Research & Entrepreneurship (ICRE–2016).

Thanki, R., & Borisagar, K. (2016). Biometric watermarking technique based on cs theory and fast discrete curvelet transform for face and fingerprint protection. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 133-144): Springer.

Thanki, R. M., Dwivedi, V. J., & Borisagar, K. R. (2018). Multibiometric Watermarking Technique Using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In *Multibiometric Watermarking with Compressive Sensing Theory* (pp. 91-113): Springer.

Thomaz, C. E. (2006). FEI Face Database. Retrieved from https://fei.edu.br/~cet/facedatabase.html

Tome, P., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2015). Facial soft biometric features for forensic face recognition. *Forensic science international, 257*, 271-284.

Ulker, M., & Arslan, B. (2018). *A novel secure model: Image steganography with a logistic map and secret key.* Paper presented at the Digital Forensic and Security (ISDFS), 2018 6th International Symposium on.

Van der Putte, T., & Keuning, J. (2000). Biometrical fingerprint recognition: don't get your fingers burned. In *Smart Card Research and Advanced Applications* (pp. 289-303): Springer.

Vatsa, M., Singh, R., Noore, A., Houck, M. M., & Morris, K. (2006). Robust biometric image watermarking for fingerprint and face template protection. *IEICE Electronics Express, 3*(2), 23-28.

Vinyals, O., Blundell, C., Lillicrap, T., & Wierstra, D. (2016). *Matching networks for one shot learning.* Paper presented at the Advances in neural information processing systems.

Viola, P., & Jones, M. J. (2004). Robust real-time face detection. *International journal of computer vision, 57*(2), 137-154.

Wallace, G. K. (1992). The JPEG still picture compression standard. *IEEE transactions on consumer electronics, 38*(1), xviii-xxxiv.

Wang, K., Cui, H., Cao, Y., Xing, X., & Zhang, R. (2016). *A Preprocessing Algorithm for Touchless Fingerprint Images.* Paper presented at the Chinese Conference on Biometric Recognition.

Wang, Y.-S., Tai, C.-L., Sorkine, O., & Lee, T.-Y. (2008). *Optimized scale-and-stretch for image resizing.* Paper presented at the ACM Transactions on Graphics (TOG).

Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *IEEE signal processing letters, 9*(3), 81-84.

Wang, Z., & Bovik, A. C. (2009). Mean squared error: Love it or leave it? A new look at signal fidelity measures. *IEEE signal processing magazine, 26*(1), 98-117.

Wiskott, L., Fellous, J.-M., Krüger, N., & Von Der Malsburg, C. (1997). *Face recognition by elastic bunch graph matching*. Paper presented at the International Conference on Computer Analysis of Images and Patterns.

Wojtowicz, W., & Ogiela, M. R. (2016). Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. *Journal of Visual Communication and Image Representation*, *38*, 1-10.

Wu, L., Zhang, J., Deng, W., & He, D. (2009). *Arnold transformation algorithm and anti-Arnold transformation algorithm*. Paper presented at the Information Science and Engineering (ICISE), 2009 1st International Conference on.

Yip, P. (1990). Discrete Cosine Transform Algorithms, Advatages, Applications. In: Academic Press Inc., London.

Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE Signal Processing Letters*, *23*(10), 1499-1503.

Zhang, Y., & Wallace, B. (2015). A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification. *arXiv preprint arXiv:1510.03820*.

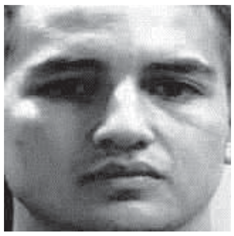
Zhang, Z. (2018). Artificial neural network. In *Multivariate Time Series Analysis in Climate and Environmental Research* (pp. 1-35): Springer.

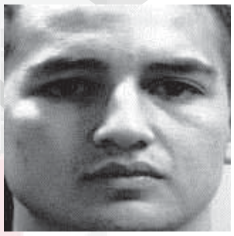
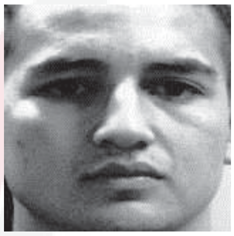
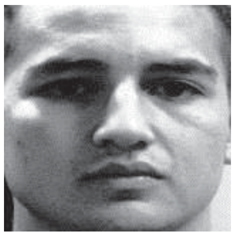
Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM computing surveys (CSUR), 35*(4), 399-458.

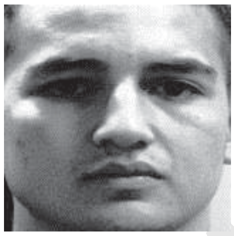
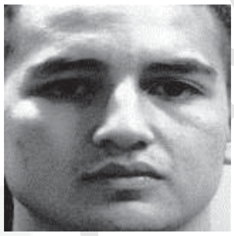
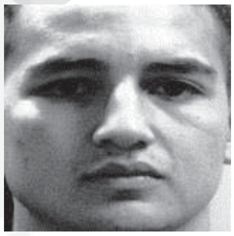
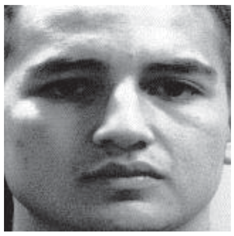
APPENDICES

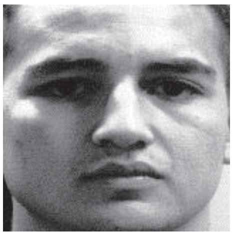
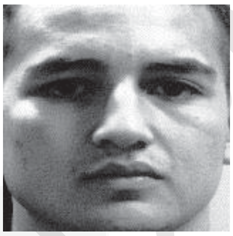
APPENDIX A

Sample Watermarked Compressed Face Images

JPEG Quality (%)	Setup A (Indian-FVC2004DB4)	Setup B (Indian&FEI-FVC2002DB3& FVC2004DB4)	Setup C (ORL-FVC2002DB1)	Setup D (FRGC-FVC2002)
5				
10				
15				
20				

30				
35				
40				
45				
50				
55				

60				
65				
70				
75				
80				
85				

90				
95				

BIODATA OF STUDENT

Abdulmawla Mohammad Ali Najh was born in 1969 in Gharian, Libya. He received his Bachelor of science degree in computer engineering (hardware) from Sebha University in 1993. He completed his master's degree in computer engineering in University Putra Malaysia (UPM), Malaysia in 2003. He joined University Putra Malaysia (UPM) as a PhD student in 2013. His research interests include digital signal processing, biometric recognition and digital watermarking.

Contact him: nabdulmawla@gmail.com

LIST OF PUBLICATIONS

Journal

Abdulmawla Mohamed Ali Najih, S.A.R Al-Haddad, A, R., Ramli, A. R., Hashim, S. J., & Nematollahi, M.A. " Digital image watermarking based on angle quantization in discrete contourlet transform." Journal of King Saud University (2017): Volume 29, Issue 3, pp 288–294, Elsevier.

Najih, A., Al-Haddad, S. A. R., Ramli, A. R., Hashim, S. J., & Khmag, A. (2017). Face Selection for Digital Image Watermarking. *International Journal of Applied Engineering Research*, *12*(5), 572-577.

Abdulmawla Mohamed Ali Najih, Al-Haddad, S. A, R., Ramli, A. R., Hashim, S. J., & Nematollahi, M.A (2016). "Research Article an Overview of Multimodal Biometric Approaches Based on Digital Image Watermarking", Research Journal of Applied Sciences, Engineering and Technology 13(6): 481-494, 2016 DOI:10.19026/rjaset.13.3008

Abdulmawla Mohamed Ali NAjih, S.A.R Al-Haddad, A. R., Ramli, Hashim, S. J., & Nabila Albannai "Matching Fingerprint Images for Biometric Authentication Using Convolutional Neural Networks", Pertanika Journal of Science & Technology 27(4): 1723-1733(2019)

Abdulmawla Mohamed Ali NAjih, S.A.R Al-Haddad, A. R., Ramli, Hashim, S. J., & Nabila Albannai "Tamper Detection in Multimodal Biometric Authentication System Using Fragile Fingerprint Watermarking", **Submitted to** IEEE ACCESS Journal.

Conference

Najih, A. M., Al-Haddad, S. A. R., Ramli, A. R., & Hashim, S. J. (2015, August). A New Colour Image Watermarking Technique Using Special Domain. In *2015 5th International Conference on IT Convergence and Security (ICITCS)* (pp. 1-5). IEEE.

Abdulmawla Mohamed Ali NAjih, S.A.R Al-Haddad, A. R., Ramli, Hashim, S. J., & Nabila Albannai "Matching Fingerprint Images for Biometric Authentication Using Convolutional Neural Networks", **presented at** the **6th SmartCity Symposium 2018**.

Abdulmawla Mohamed Ali NAjih, S.A.R Al-Haddad, A. R., Ramli, Hashim, S. J., & Nabila Albannai "Matching Face Images for Biometric Authentication "presented at IEEE CSUDE19.

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : First Semester 2020/2021

TITLE OF THESIS / PROJECT REPORT :

MULTIMODAL FINGERPRINT AND FACE BIOMETRICS WITH FRAGILE WATERMARKING AND CONVOLUTIONAL NEURAL NETWORK

NAME OF STUDENT: ABDULMAWLA NAJIH

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☐	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐	**PATENT**	Embargo from_____________ until _____________ (date) (date)

Approved by:

_______________________ (Signature of Student) New IC No/ Passport No.:	_______________________ (Signature of Chairman of Supervisory Committee) Name:
Date :	Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]