N^o d'ordre :.../.....

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY of KASDI MERBAH OUARGLA

FACULTY OF NEW INFORMATION AND COMMUNICATION TECHNOLOGIES

THESIS

Thesis submitted in partial fulfillment of the requirements for the degree of

2nd Cycle LMD Master.

In : Automatic and Systems.

By : **Aboub Zakaria and Bahi Amine.**

Thesis

The Random Forest Classifier Applied In Biometric Recognition

Publicly sustained on : ../06/2023 before the jury composed of:

Name and Surname	***Title***	***Affiliation***	***Quality***
Z. TIDJANI	*MCB*	*Univ. K. M. Ouargla*	*President*
R. CHELAOUA	*MCB*	*Univ. K. M. Ouargla*	*Thesis Director*
H. EL AGGOUNE	*MCB*	*Univ. K. M. Ouargla*	*Examiner*


بسم الله الرحمن الرحيم


وقل رب زدني علما


صدق الله العظيم

Dedication

dedicate this work to my beloved family (my mother, father, and dear siblings) who have always been a strong pillar in my life. Thanks to their immeasurable love and unlimited support, I was able to achieve this accomplishment. I am grateful to them for their understanding and continuous encouragement..

I would also like to express my deep gratitude to my supervisors and teachers, especially Rachid CHELAOUA, who guided and directed me throughout this scientific journey. You have been a source of inspiration for me and have helped me develop my abilities and achieve my academic goals.

Lastly, I want to thank all the friends and loved ones who stood by my side and encouraged me to move forward, even in the toughest times. They have enriched my life with happiness, support, and love, and I am truly grateful to them.

ABOUB ZAKARIA.

Dedication

dedicate this work to my beloved family (my mother, my late father, and my dear siblings) who have been a strong pillar in my life. I thank them for their love and support, which have helped me achieve this accomplishment. I am grateful to them for their understanding and continuous encouragement...

I would also like to express my deep gratitude to my supervisor and teacher, Rachid CHELAOUA, who has guided and directed me throughout this scientific journey. You have been a source of inspiration for me and have helped me develop my abilities and achieve my goals. Lastly, I want to thank all the friends and loved ones who have stood by my side and encouraged me to move forward, even in the toughest times. They have enriched my life with happiness, support, and love, and I am truly grateful to them.

.

BAHI AMINE.

Acknowledgement

First and foremost, we are extremely grateful to our supervisors, Dr. ***Rachid CHELAOUA*** *for his invaluable advice, continuous support, and patience during us study. His immense knowledge and plentiful experience has encouraged us in all the time of our academic research and daily life.*

We also extend our sincere thanks to the members of the jury: Dr. ***Z. TIDJANI*** *and Dr.* ***H. EL AGGOUNE*** *for their acceptance to evaluate this work.*

Finally, we would like to express our gratitude to all teachers in the electronics department of University Kasdi Merbah Ouargla for their help and advice, without forgetting all colleagues and friends.

Résumé

La technologie de reconnaissance des mesures biométriques offre un niveau élevé de sécurité et de protection, rendant l'authentification simple et rapide tout en réduisant les erreurs humaines et améliorant la précision de la vérification. Dans cette thèse, nous proposons un système de reconnaissance basé sur l'empreinte biométrique de l'articulation du doigt (MFK), parce qu'il a une grande précision, fiabilité et résistance à la falsification. Cette technologie est bénéfique dans divers domaines tels que la sécurité, les applications de paiement, le contrôle d'accès aux téléphones mobiles et la reconnaissance d'identité. La technique de Discrete Cosine Transform (DCT) a été utilisée pour extraire les caractéristiques et la technique de forêt aléatoire (RFT) a été utilisée pour la classification des caractéristiques. Un système multimédia proposé a été développé et son efficacité a été évaluée à l'aide de techniques de fusion. L'évaluation a été réalisée sur une base de données contenant des images d'empreintes digitales de 500 individus. travers des expériences multiples, les configurations DCT et RFT ont été testées pour déterminer les meilleures performances du processus d'authentification. A partir de différentes expériences, les résultats obtenus ont été présentés en utilisant des systèmes de reconnaissance unimodaux et multimodaux. Sur la base des résultats, d'excellentes performances ont été obtenues dans la reconnaissance biométrique multimodale par rapport à la biométrie unimodale.

Les mots clés:

biométrique system,Transformée discrète en cosinus ,Transformation aléatoire de la forêt,jointure mineure

Abstract

Biometric recognition technology offers a high level of security and protection, making identity verification easy and fast, while reducing human errors and enhancing verification accuracy. In this study, we proposed a biometric recognition system based on minor finger knuckle (MFK), because it has high accuracy, reliability, and resistance to tampering. This technology is beneficial in various fields such as security, access control to buildings and devices, secure payment applications, and identity recognition in mobile devices. The Discrete Cosine Transform (DCT) technique was used for feature extraction, and the Random Forest (RFT) technique was used for features classification. A proposed multi-modal system was developed, and its performance evaluated by using matching score level fusion. The evaluation was conducted on a database containing fingerprint images of 500 individuals. From different experiments, obtained results were presented by using unimodal and multimodal recognition systems. Based on the results, excellent performance was achieved in multimodal biometrics recognition compared to unimodal biometrics.

key words:

Biometric Systems,Discrete Cosine Transform,Random Forest Transform , minor finger knuckle

Contents

List of Figures

List of Tables

Abbreviations

MFK	:	minor finger knuckle	FA	:	False Acceptation
ROI	:	Region of Interes	FRR	:	False Rejection Rate
DIP	:	Distal Interphalangeal	NI	:	number of the impostor
DCT	:	Discrete Cosine Transform	NG	:	number of total genuine user
RFT	:	Random Forest Transform	GAR	:	Genuine Accept Rate
EER	:	Equal Error Rate	FTC	:	Failure To Capture
FAR	:	False Acceptance Rate	FTE	:	Failure To Enrol
RPR	:	Rank of Perfect Recognition	TR	:	True Rejection
CMC	:	Cumulative Match Curve	ROC	:	Receiver Operating Curve
TA	:	True Acceptance	ROR	:	Rank One Recognition
FR	:	False Rejection			

Chapter 1

INTRODUCTION

PREVIOUSLY , the most common ways to protect information and valuable items from prying eyes and the hands of thieves were classical methods. That relied on something you have or know, such as keys, passwords, and cards. Each time these methods failed to protect the information, whether by losing keys, having them stolen by thieves, or forgetting passwords. To this day, researchers are trying to improve the protection methods they use against these problems that persist [1].

In the beginning, passwords consisted of names and letters, and then evolved to include symbols and characters. After that, they were improved to include ink-printed fingerprints. In the sixties of the last century, with the emergence of electronic locks, the system relied on numbers as a security solution, with a mix of letters and numbers added later on. Since then, electronic hackers have started to create programs that allow them to penetrate these protected systems. These problems have led to the development of the traditional password to now rely on biometric measurements, which programmers call "biometric security" [2].

Biometric security is considered one of the latest technologies used in the field of protection and security, as it relies on using unique characteristics of individuals, such as fingerprints, face, voice, and iris, to identify and verify their identity. This technology is one of the safest and most protective for sensitive information and personal data. One of the advantages of this modern technology is that it relies on unique features for each individual that cannot be replicated, which makes it superior to classic security technologies that can be easily breached and stolen [3].

Biometric provides a high level of security and protection, making identity verification easy and fast. It also reduces human errors and improves verification accuracy. However, there are some drawbacks that must be considered. For instance, objective biometric systems can sometimes be costly and require specialized equipment and complex software for

analysing and recognizing biological features of individuals. Biometric recognition technology may also face issues in accurately reading and recognizing biometric features due to interference, such as a lighting and a distorted print etc, which hinders its recognition [4].

Artificial intelligence is considered one of the popular modern technologies with various important uses in many fields, including biometric systems. Artificial intelligence technologies can be used to develop these systems in terms of accurately and effectively. And, it can enhance their security and protection against hacking and forgery. Artificial intelligence can be also used to analyse images, sound data, genetics, and other data to extract unique characteristics. In addition, modern artificial intelligence technologies can be used to develop innovative and advanced biometric systems that are fast, accurate, and reliable in many applications.

The rest of the thesis is organized as follows. In Chapter 2, we focused on biometric security by discussing the components of biometric systems. We also covered the architecture of multimodal systems compared to unimodal biometric systems, as well as the different scenarios involved in developing multimodal biometric systems. Additionally, this chapter provides an overview of advanced machine learning applications such as Discrete Cosine Transform (DCT) and Random Forest Transform (RFT).

In Chapter 3. we focused on fingerprint biometrics, which is renowned for its high accuracy, reliability, and resistance to tampering. In this chapter, we illustrate the proposed methodology for a biometric system based on fingerprint technology. We also explain the justification for using deep learning methods and their hierarchical structures, which can be applied to intelligent biometric applications. Furthermore, all the different processes of our proposed system are described in more detail in this chapter.

The efficiency of the proposed biometric identification system was tested in Chapter 4. Accordingly, Chapter 4 presents the outcomes of experiments conducted on fingerprint databases. This chapter also includes an experimental setup to adapt our algorithms. Subsequently, the results of the proposed system are presented. Through our experimental results and literature research, we provide explanations and evaluations of the deep learning methods in our proposed biometric systems.

Lastly, Chapter 5 summarizes the thesis and its contribution and provides concluding remarks. Possible future directions for this research are also discussed in this chapter.

Chapter 2

THEORETICAL BACKGROUND

2.1 Introduction

BIOMETRICS is a modern technology that utilizes statistical analysis to measure and identify individuals based on their biological and behavioral characteristics, such as facial, fingerprint and voice patterns, etc. Derived from the ancient Greek words "Bio" meaning life and "Metrikos" meaning to measure [5]. It relies on the "who you are" identification method, rather than the traditional "what you have" (such as an ID card) or "what you know" (such as a password) methods. The biometric system consists of a combination of electronic devices and pattern recognition algorithms based on unique physiological and behavioral characteristics of each individual to accurately and uniquely identify their identity [6].

2.2 Biometric Systems

2.2.1 Biometric Characteristics

Biometric measurements can be divided into two categories: physiological and behavioral characteristics. The former is called static measurements, which rely on extracting data from anatomical measurements of the person. The latter is called dynamic measurements, which rely on extracting data from the actions of the person [6]. The second category is less stable than the first and can be affected by stress or pressure. However, it has an advantage over the first category in that it may not be apparent to the person being measured, meaning their identity can be determined without their knowledge. Also, it is more widely accepted by less-curious individuals [6]. Physical and behavioral characteristics are shown in Figure.2.1.

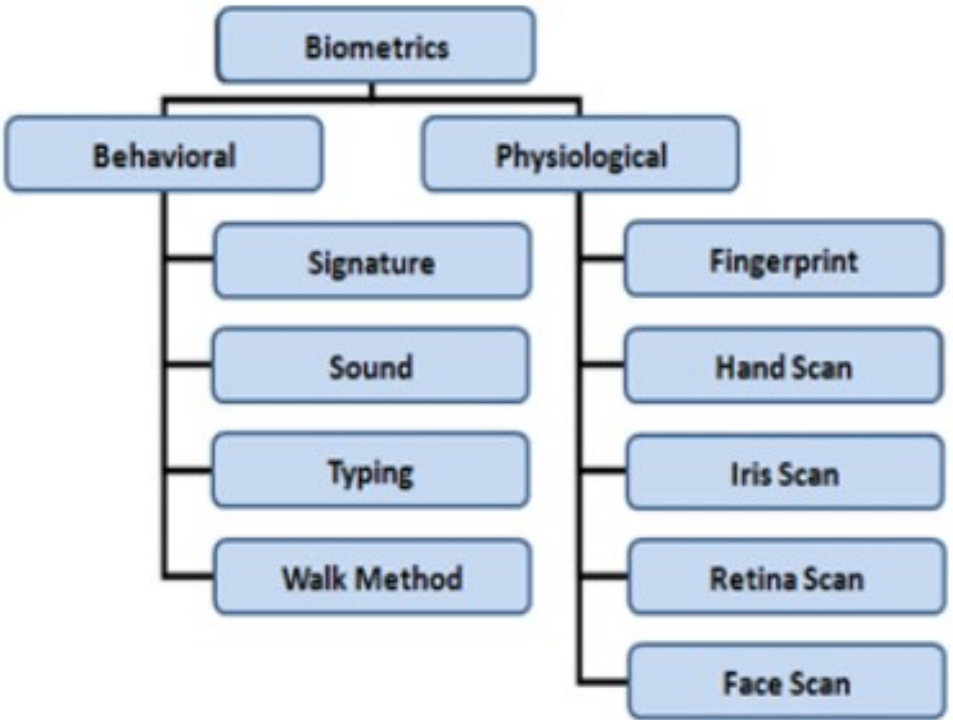

FIGURE 2.1: The physical and behavioral biometric characteristics.

It is important that the physical and behavioral characteristics used for identification are unique, meaning they exist in only one person in the world, are permanent, and do not change over time. They must also be measurable and stored effectively and comparably in a biometric database to identify individuals. Obtaining these features should not be harmful to the person being measured.

2.2.2 Biometric Systems Steps

Biometric measurement technologies vary in complexity, ability, and performance, but they all share many common elements. They are systems designed primarily to identify individuals, using tools such as imaging and scanning devices to obtain images or recordings or measurements of individual characteristics. Computers and software are also used to extract, differentiate, store, and compare these characteristics. Although biometric measurement technologies measure different characteristics in different ways, biometric measurement systems rely on the same processes, which can be divided into two distinct stages: registration and identity proofing or determination. The steps in each stage can be summarized as follows [6]:

- Obtain samples from the individual, whether physical or behavioral, using appropriate devices.
- Process the samples to extract unique features.
- Store the sample templates.
- Match the stored sample templates with the features extracted from the individual to be identified.
- Make a decision as to whether the individual is the intended person or not.

2.2.3 Biometric System Modes

a. Verification Mode:

Biometric measurement systems can be used to verify individuals' identity, and their identity is verified through authentication by comparing previously recorded data with current sample. This comparison is called "one-to-one" comparison. For example, in computer access, this mode involves entering the username of account, and instead of a password, placing the biometric print on the sensor device to verify the identity [14]. This principle illustrate in Figure.2.2.

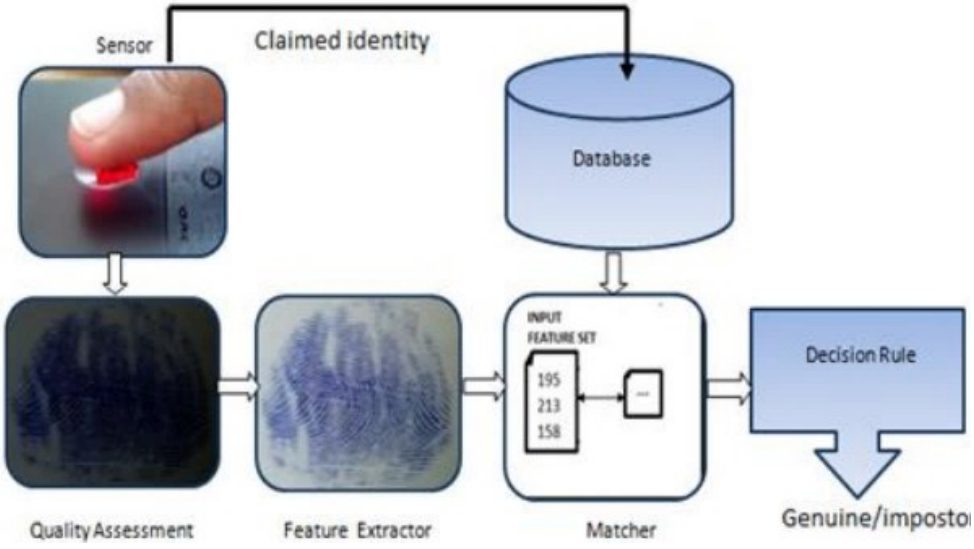

FIGURE 2.2: Example of verification mode in biometric system.

b. Identification Mode:

In the case of identification, biometric measurement systems identify the person among all individuals registered in the database (meaning the system works to determine who this person is?), and this method is sometimes called one-to-many matching [14]. This principle illustrate in Figure.2.3.

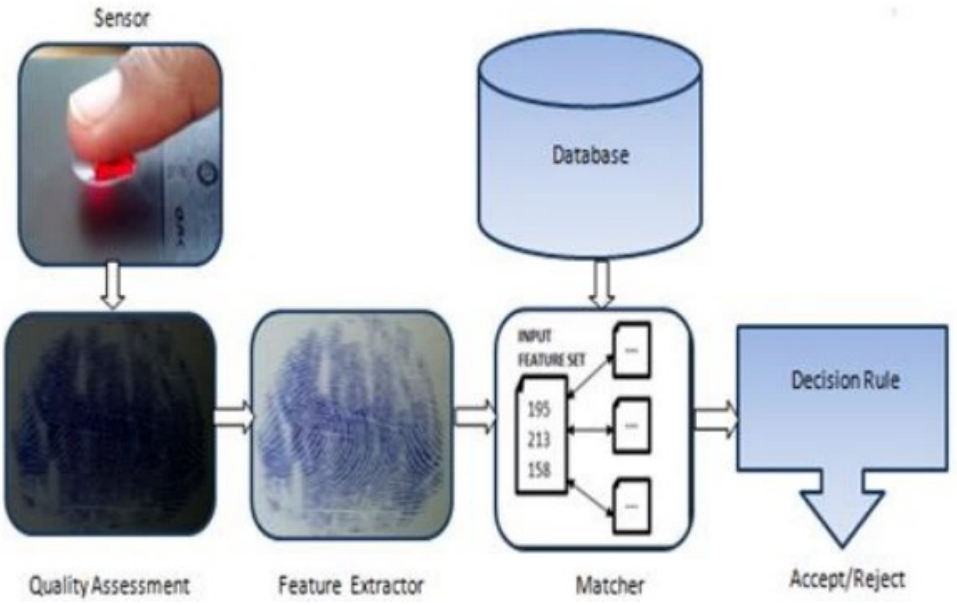

FIGURE 2.3: Example of identification mode in biometric system.

2.3 Multimodal Biometric Systems

Unimodal biometric system uses a single biometric for identification purposes [7]. These systems able to identify various individuals using a single identifier. However, this technology has some drawbacks, including inaccurate results, weak security, poor recognition, vulnerability to spoofing attacks, and lack of effectiveness for people with disabilities. It is also heavily influenced by environmental and physical factors such as noisy data and small sample size [8, 9, 10]. These issues can be addressed by using multiple biometric modalities. Integrating more evidence is a way to improve the performance and tasks of biometrics [11, 12, 13].

Multimodal biometric systems use multiple complementary feature extraction methods, unlike single modality systems. These systems are known for their high security against

spoofing attacks and high reliability and robustness in dynamic environments. The advantages and features of multimodal biometric systems stem from the existence of multiple sources of information [14], which increase the accuracy of recognition while reducing registration problems and enhancing security. According to Figure.2.4, we have the following five possibilities:

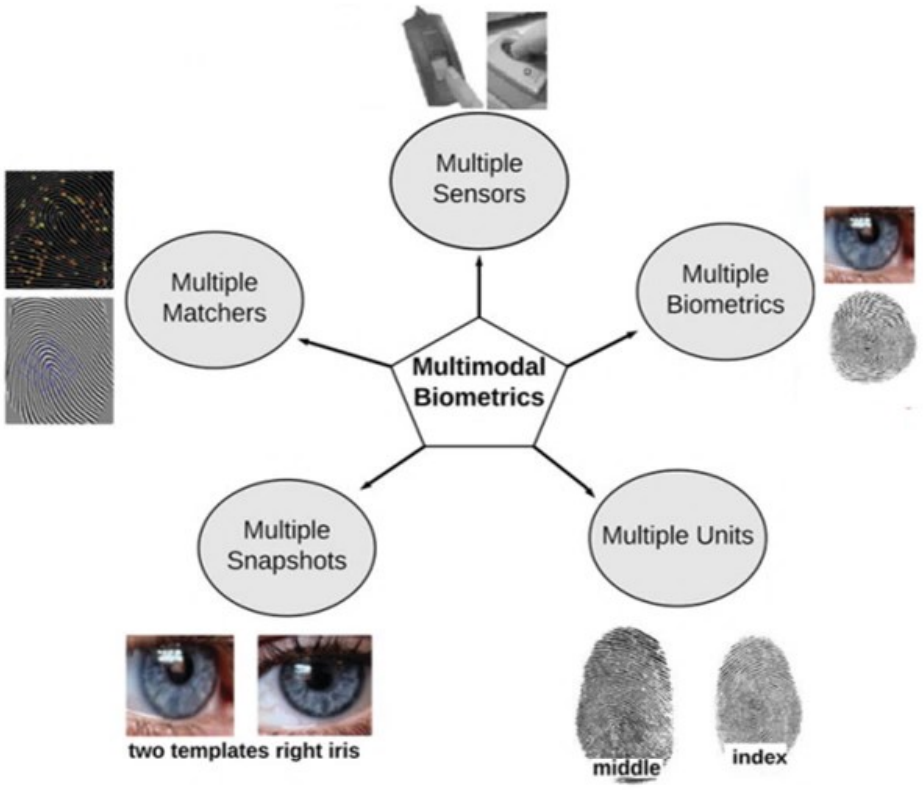

FIGURE 2.4: The scenarios of multimodal biometric system.

In conclusion, it can be said that multimodal biometrics is the most effective and efficient method for dealing with individual biometric limitations when compared to other scenarios [15]:

1. Increasing the accuracy of reliable recognition in multimodal biometric systems is attributed to their ability to effectively deal with similarities between classes, noisy or weak data, and other factors [14].

2. Multimodal biometric systems address the problem of insufficient coverage or lack of inclusiveness and provide alternative options for claimants who cannot provide a specific biometric. This can significantly reduce the registration failure rate [16].

3. Multimodal biometric systems provide security and protection as they are difficult to forge or cheat. It would require a frauds to be able to falsify more than one biometric at the same time [14].

2.4 Discrete Cosine Transform (DCT)

Nasir Ahmed is the inventor of the discrete cosine transform (DCT), which he first proposed in 1972. DCT uses an orthogonal transformation and contains a fixed set of basic functions, where the image space is assigned to frequency. DCT is characterized by its ability to pack energy in the lower frequencies of image data and reduce the blocking artifact effect, which results from the presence of barriers between sub-images and the appearance of boundaries between images [18].

Image compression is a specific technique used in image processing to reduce redundancy in image data, enabling the storage or transmission of fewer samples. The goal of image compression is to reconstruct the original image in a way that is consistent with human visual perception, playing an important role in the efficient transmission and storage of images [17]. In recent years, DCT is the most common technique for image compression and its selection as the standard for JPEG compression. Also, DCT is used in many non-analytical applications such as image processing and signal processing applications. DCT is variants made to the discrete signal. Generally, we use the DCT -II which corresponds to the DCT of a discrete signal to two dimensions. It is assumed that it was an input signal $f(n, m)$ the image of size $N \times M$, its transformed into discrete cosine $C(U, V)$ would be:

$$C_(ij)(U,V) = \alpha(u)\alpha(v) \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} f_(ij)(n,m) \cos(\frac{\Pi(2n+1)u}{2N}) \cos(\frac{\Pi(2m+1)v}{2M}) \quad (2.1)$$

$C_(ij)(U, V)$ is DCT of image , and $f_(ij)(n, m)$ luminance the pixle of image, $N \times M$ is size of image.

2.4.1 The Zigzag Arrangement of DCT:

The quantized coefficients are ordered in a "zig-zag" sequence, as shown in Figure.2.5. The "zig-zag" sequence first encodes the coefficients with lower frequencies, which typically have higher values, followed by the higher frequencies, which are typically zero or almost zero.

This results in an extended sequence of similar data bytes, allowing for efficient entropy encoding [19]. Remaining coefficients, arranged in a zigzag manner as shown in Figure.2.5, carry information in the decreasing order. Therefore, to achieve compression, the coefficients starting from the end can be dropped depending on the quality required for the decompressed image.

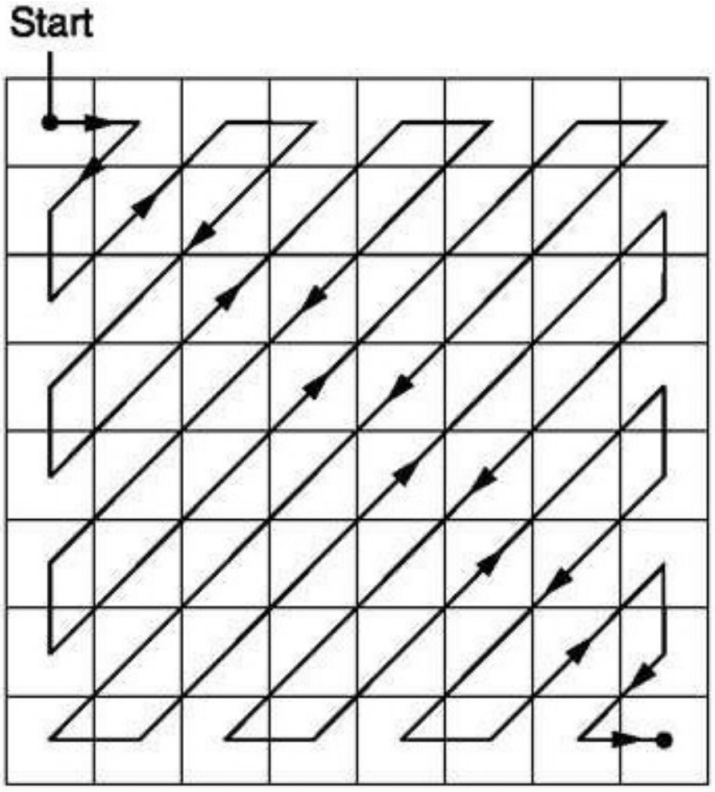

FIGURE 2.5: The Zigzag arrangement of DCT coefficients.

2.4.2 Advantages /Disadvantages of DCT [20]

- Compression efficiency: DCT is highly efficient in compressing images and videos, and can be used to achieve high compression rates without losing image quality.
- Easy implementation: DCT can be easily implemented using common computer programs, making it a preferred technique for many users.
- Noise resistance: DCT is resistant to noise, as it helps reduce errors that occur due to interference or distortion.
- One of the main drawbacks of the DCT is the potential loss of information, especially when using high compression ratios. This occurs because the technique is based on approximating the original image data using a limited set of cosine functions, and finer details of the image may be lost during this process.

Type your text

- The DCT technique is not very effective at handling images with sharp edges or sudden changes in brightness. This can lead to distortion or artifacts in the compressed image, reducing its overall quality.

- Another drawback of the DCT technique is its limited effectiveness in handling images with a large amount of noise.

2.5 Random Forest Transform (RFT)

Random forest builds multiple decision trees and merges them together to get a more accurate and stable prediction (see Figure.2.6). One big advantage of random forest is that it can be used for both classification and regression problems, which form the majority of current machine learning systems. Decision tree classifiers have been known for a long time [22] but they have shown problems related to over-fitting and lack of generalization. The main idea behind Random Forest is to try and mitigate such problems by: (i) injecting randomness into the training of the trees, and (ii) combining the output of multiple randomized trees into a single classifier. Random Forests have been demonstrated to produce lower test errors than conventional decision trees [23].

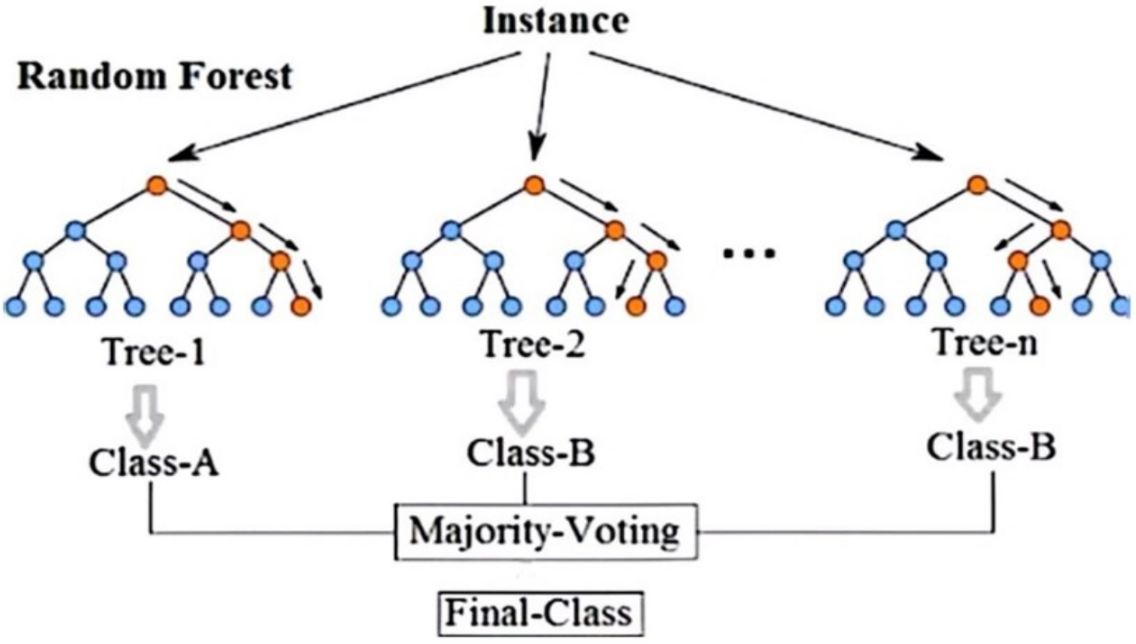

FIGURE 2.6: Random forest from multiple decision trees.

2.5.1 The RFT algorithm [21]

- **Step 1:** Determine the number of training cases and the number of variables used in the model.
- **Step 2:** Determine the number of variables used in the decision making at each node of the tree.
- **Step 3:** Choose a training set for the decision tree by randomly selecting samples with replacement from all available training cases, using bootstrap sampling.
- **Step 4:** At each node of the tree, randomly select variables to search for the best split.
- **Step 5:** Calculate the best split based on the chosen variables in the training set and build the tree.
- **Step 6:** Build the tree fully without pruning, unlike many other techniques that try to reduce the size of the tree by removing small nodes
- **Step 7:** Select the best split based on the lowest error in the training set. Use the resulting tree to predict new values that were not in the training set by calculating the majority votes in the tree.

2.5.2 Advantages and Disadvantages

Random Forests are appealing because they [21] :

- RFT is able to make accurate predictions for a wide applications of regression or classification.
- RFT is fast to train, because it depend only on one or two tuning parameters.
- . It has the ability to determine the importance of each feature based on the training data set.
- RFT can calculate pairwise proximity between samples using the training data set.

The RFT has a few limitations such as [21]:

- When dealing with data that includes categorical variables with different levels, RFT tends to favor those attributes with more levels over those with fewer levels.
- RFT tends to favor smaller groups over larger groups if the data contains groups of correlated features of similar relevance for the output.

2.6 conclusion

Biometric is the automated recognition of person which based on a physiological or behavioral characteristic. In this chapter, we focused on biometric security by discussing about the components of biometric system. Also, we covered architecture of multimodal systems compared to unimodal biometric systems, as well as the different scenarios involved in multimodal biometric system development. Furthermore, this chapter includes overview on advanced of machine learning application such as: Discrete Cosine Transform (DCT) and Random Forest Transform (RFT). Actually, artificial intelligence algorithms are represented the true development in all daily applications.

Chapter 3

OUR PROPOSAL RECOGNITION

3.1 Introduction

BIOMETRICS , based methods, which use unique physical or behavioral characteristics of individuals have garnered widespread interest and possess great potential in the modern digital world. These methods offer high accuracy and convenience in user identification. With the rapid development of computing techniques, researchers have extensively studied the use of various biometric traits over the past few decades. One of the most important biometric traits is the hand, which provides a high level of discrimination, accuracy, and security.

3.2 Hand Dorsal Recognition

In recent years, hand-based biometric recognition has become a major focus among various types of biometric person identification. Many have been proposed and studied, such as fingerprints, handprints, hand geometry and hand veins. Recently, it has been discovered that the pattern of folds and creases on the surface of the outer finger joint is highly unique and can therefore be used as a distinctive biometric identifier.

Compared to fingerprints, the outer finger joint surface has some advantages as a biometric identifier, as it does not easily wear down due to people holding objects on the inside of their hand. In addition, unlike fingerprints, the outer finger joint surface is not subject to criminal investigation, making it highly accepted by users. Therefore, the advantage of the outer finger joint surface has great potential for wide acceptance as a biometric identifier [24].

Minor Finger Knuckle **MFK** reflects the unique skin pattern around the external finger joint. The system consists of four basic components: finger and knuckle imaging, ROI extraction, feature extraction, and feature matching. From [25], The **MFK** imaging system is characterized by its small size and ease of initial steps such as finger division and ROI extraction. Additionally, unique skin patterns can be captured clearly, even when the finger joint is bent during imaging, which helps to better use **MFK** features. Figure.3.1.*(a)* shows the **MFK** imaging device of the system. While, Figure.3.1.*(b)* illustrates a typical **MFK** image. Figure.3.1.*(c)* demonstrates the ROI extraction process and Figure.3.1.*(d)* presented a cropped ROI image.

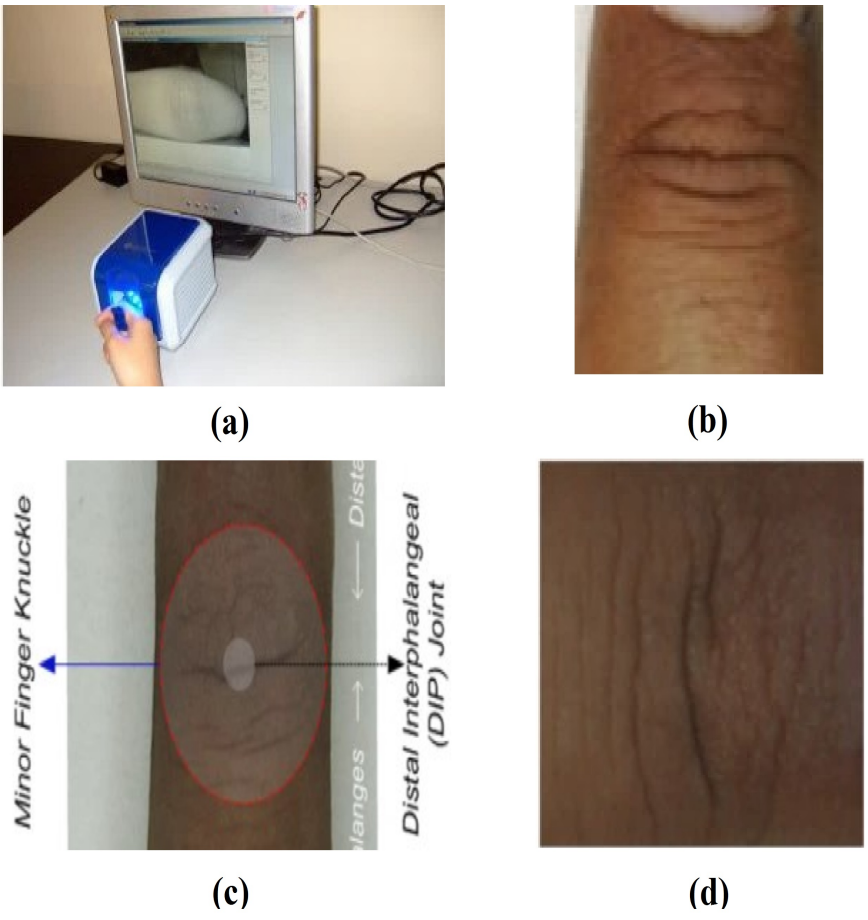

FIGURE 3.1: (a) MFK image acquisition device; (b) a typical MFK image; (c) the determination of ROI and (d) a cropped ROI image from the original MFK image.

3.3 Our Contribution:

In our proposal, we have made contributions in the field of biometric recognition based on the minor knuckle print of hand dorsal. Our contribution lies in using the minor knuckle print as a distinctive biometric for recognition, which refers to the distinct pattern present on the dorsal side of the hand.

Other main contribution is the utilization of the Discrete Cosine Transform (DCT) as features extraction technique for proposed recognition. DCT plays a crucial role in our system as it allows us to compress the fingerprint image while preserving its essential features. This enables efficient storage and processing of biometric data, leading to improved recognition performance.

Additionally, we have integrated the Random Forest Transform (RFT) into our biometric recognition system for classification stage. RFT is a powerful machine learning algorithm that relies on an ensemble of decision trees to perform classification tasks. By employing this technique, we enhance the accuracy and reliability of our system performance.

Through these advancements, we aim to provide a strong and effective solution for biometric recognition applications. Lastly, Figure.3.2 summarizes our contributions, where using the minor knuckle print of hand dorsal as a biometric recognition.

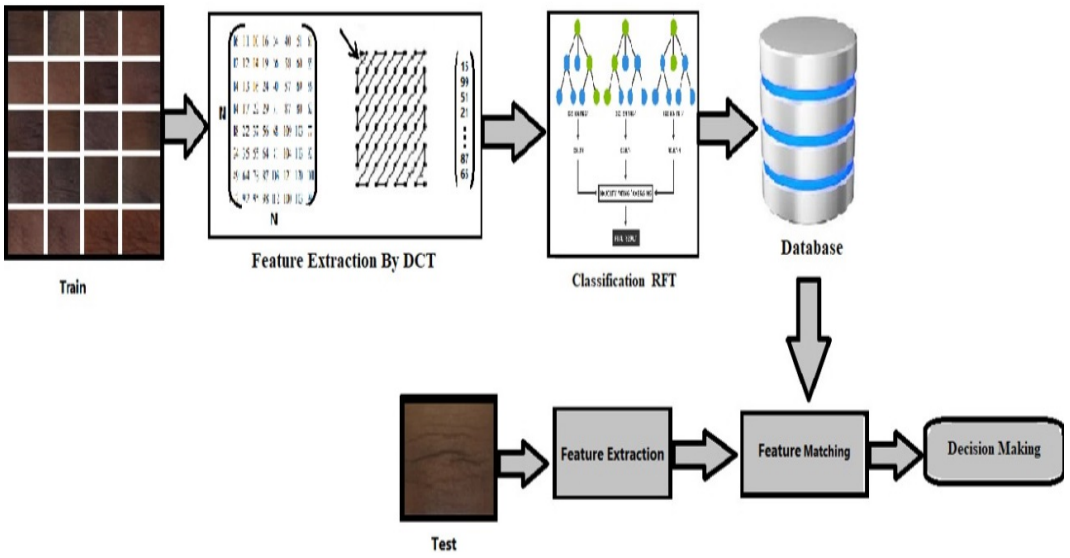

FIGURE 3.2: Block-diagram of the proposed unimodal biometric system.

3.4 Feature Extraction By DCT

The Discrete Cosine Transform (DCT) is a mathematical technique used to convert digital images into a matrix of numbers. This technique is used in image compression to reduce the size of the data used to store the image while maintaining its overall quality.

The process of transforming the image into an $N \times N$ matrix relies on the concepts of signals and frequency analysis. The image is divided into a set of numbers, and the DCT value is calculated for each number individually. DCT is a transform process that is both configurational and analytical, used to convert information from the time domain (the image) to the frequency domain (different frequencies) [26].

After transforming the images into DCT representation, a "zig-zag" process is applied to the transformed matrix to arrange the values in a way that facilitates data compression and reduces the size of the transformed image. In the zig-zag process, the values in the matrix are arranged so that they are read sequentially in a zig-zag pattern resembling the letter "Z". This pattern facilitates representing the matrix in a smaller-sized column matrix, reducing the size of the data used [27].

After applying zig-zag, the matrix is represented in a column format, where the values from the original matrix are collected into a single column, with each value having its specific place in the concatenated column. This column-wise representation is used to store data efficiently and achieve image compression. Figure.3.3 below illustrates the stages of this technique:

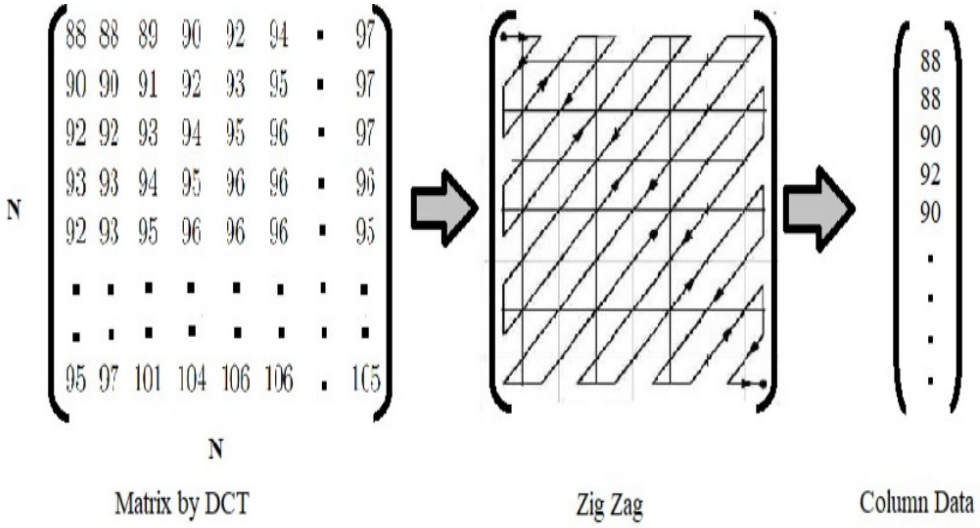

FIGURE 3.3: Block-diagram of DCT stages.

3.5 Classification And Matching

After feature extraction, a technique such as Random Forest is used to classify the fingerprints. An automated learning model is built using multiple decision trees. Each tree in the model classifies the fingerprint based on the extracted features. The final decision is made based on the majority classification of the trees as shown in Figure.3.4.

All the decisions made by the Random Forest technique are stored in the database. A unique identifier is assigned to each stored fingerprint in the database to indicate the associated person's identity [28].

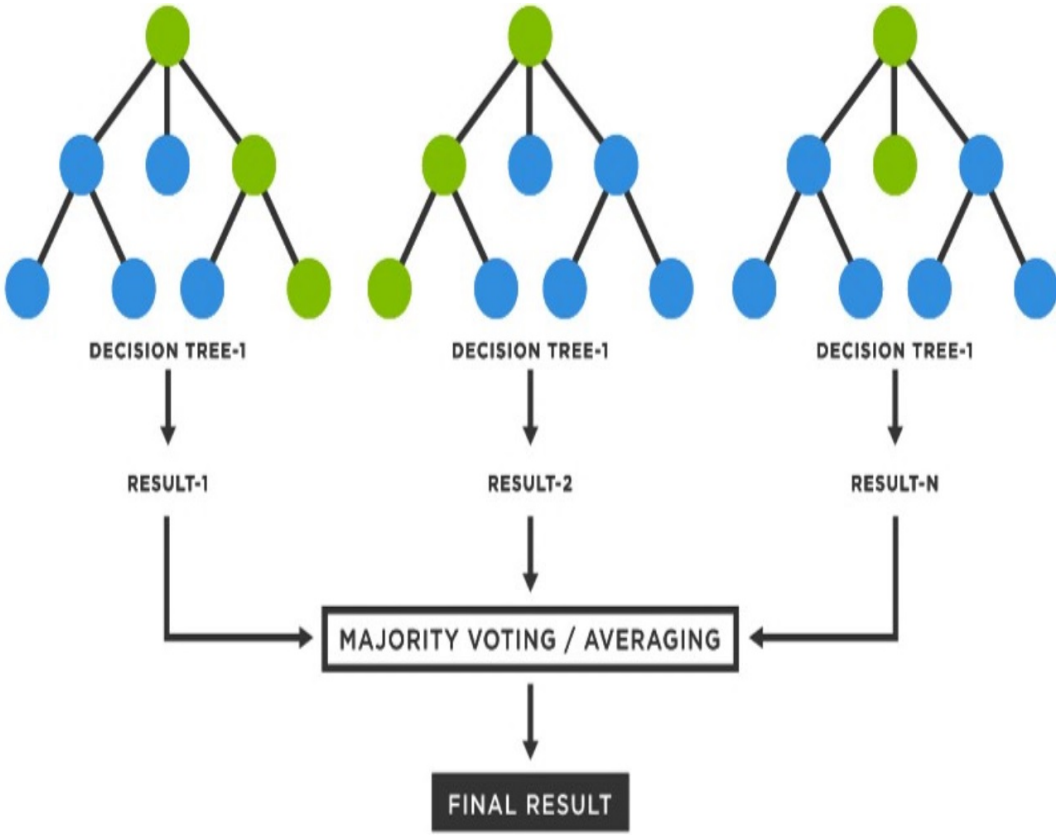

FIGURE 3.4: Schematic showing how Random Forest Transform works.

3.6 Feature fusion

In our system, we based on fusion at the matching score level, which appears to be the most beneficial fusion level due to its good performance and simplicity. Score fusion is commonly used in multi-biometric systems, which is sufficient to distinguish between genuine and imposter scores. Initially, scores are obtained from an individual, which can be either

similarity scores or distance scores, and these scores need to be converted in a similar manner to make the final decision [29].

During our series of tests, four different fusion schemes were experimented: Sum-score, Min-score, Max-score, and Weighted-score rules. Therefore, if the scalar $\widetilde{di}$ represents the score of the i^{th} sub-system and F_s repesents the fusion score.therefore, F_s is given by [30].

1. **sum-score(SUM):** combining the scores by the sum consists to calculate F_s such that.

$$F_s = \sum_{i=1}^{k} \widetilde{di} \tag{3.1}$$

2. **Min-score (MIN):** we assign to the score final (fused) the best (minimum) score calculated by the different systems. Minimum is then defined by:

$$F_s = \min(\widetilde{d1}, \widetilde{d2}....\widetilde{dk}) \tag{3.2}$$

3. **3. Max-score (Max):** we assign to the score final (fused) the best (maximum) score calculated by the different systems. Maximum is then defined by:

$$F_s = \max(\widetilde{d1}, \widetilde{d2}....\widetilde{dk}) \tag{3.3}$$

4. **Sum-weighting-score (WHT):** the weighted sum of scores consists at the extension of the sum of the scores. Indeed, the score of each system is weighted and based on the error rate associated with it, based on performance individual system or its importance in the multimodal system. The fusion of scores is calculated as follows:

$$F_s = \sum_{i=1}^{k} w_i \widetilde{di} \tag{3.4}$$

with k is the number of combained biometric sub-systems and the weight of i^{th} sub-system,w_i is defined as:

$$w_i = \frac{1}{\sum_{i=1}^{k} \frac{1}{\varepsilon_i}} \times \frac{1}{\varepsilon_i} \tag{3.5}$$

where ε_i denote the Equal Error Rate (EER) of each biometric sub-systems and $\sum_{i=1}^{k} \varepsilon_i = 1$

3.7 Conclusion

In this chapter, the use of two main techniques, Discrete Cosine Transform (DCT) and Random Forest (RFT), for extraction and classification of features, respectively. DCT is used to extract coefficients representing the features of the unclassified image. The Random Forest technique is then employed to classify the image based on these extracted features.

By combining DCT-based feature extraction with the power of Random Forest, accurate classification and matching of fingerprint-related images can be achieved. DCT extracts important features from the image, while Random Forest utilizes these features for classification. These methods are widely used in image processing applications and have a good reputation in the field.

Chapter 4

EXPERIMENTATIONS AND RESULTS

4.1 Introduction

EVALUATING the performance of biometric recognition techniques is crucial in the field of information security and identity verification. Fingerprint biometrics is known for its high accuracy rates in recognition. Since each individual's fingerprint is unique, it can be relied upon strongly to achieve precise differentiation between individuals.

However, there are challenges that need to be addressed as environmental complexities and lighting effects. Dealing with these difficulties requires appropriate utilization of data processing techniques and advanced algorithms. In this chapter, we evaluate the minor finger knuckle (MFK) print detection using MATLAB software with Hand Dorsal dataset and configurations to conduct multiple experiments and analyze the results.

4.2 Database

Our biometric system based on Hand Dorsal Images Database from the Hong Kong Polytechnic University [31]. The Hong Kong Polytechnic University Contactless Hand Dorsal Images Database is contributed from the male and female volunteers. This database has been largely acquired in IIT Delhi Campus, in The Hong Kong Polytechnic University campus and in some villages in India during 2006-2015, mostly by using a mobile and hand held camera. This database has 2505 hand dorsal images from the right hand of 501 different subjects that illustrate three knuckle patterns in each of the four fingers from the individual

subject. All the images are in bitmap (*.bmp) format. This database also has additional hand dorsal images from 211 different subjects but these images lack clarity or does not have second minor knuckle patterns.

The combined database from 712 different subjects hand dorsal images is made publicly available. This database also provides two session hand dorsal images, with many samples in different age groups that have been acquired after very long interval (4 to 8 years) to support studies relating to the stability of knuckle patterns. This database also provides segmented/normalized major, first minor and second minor knuckle images using completely automated segmentation. Such images are made available for all the subjects and different/respective fingers and can be easily identified using the names of respective images/folders in the database [31].

4.3 Parameters Selection

DCT parameter selection refers to the process of determining the appropriate values for the parameters used in the DCT transformation. The DCT transformation is a technique where a signal is transformed from the time domain to the frequency domain. The process of DCT parameter selection depends on the specific application and performance requirements. The process of parameter selection may involve conducting experiments and tests to evaluate the performance of different parameters and selecting the values that yield the best results. For that, all of these tests are activated by Minor knuckle index of finger modality.

4.3.1 Selection Numberes of DCT

To determine the number of DCT configurations in our approach, we describe the sub-results related to the proposed DCT configuration parameter. When using different numbers of configurations such as 20, 40, 80, 120, and 180 for each person, we present the test results in Table.4.1 in our fingerprint recognition systems.

Numbers	Oben_Set Identification		Closed_Set Identification	
	T_0	EER	ROR	RPR
20	0.215	10.5	39.5	499
40	0.333	9.7	47.4	499
80	0.245	9.9	51.7	499
120	0.245	9.9.	52.2	481
180	0.288	12	50.2	492

TABLE 4.1: Results of the DCT parameters for identification test.

OPEN-SET

From this Table.4.1, it is evident that the set of five configurations for DCT provides better results in terms of EER. In this case, the identification system can achieve an EER of 9.7% at a threshold of $T_0 = 0.333$. Additionally, from this table, we can observe that the configurations of 80 and 120 for DCT yield an EER of 9.9% at a threshold of $T_0 = 0.245$ for the back-of-hand position. Furthermore, using the configuration of 20 for DCT results in an EER of 10.5% at a threshold of $T_0 = 0.215$. Finally, using the configuration of 180 for DCT yields an EER of 12% at a threshold of $T_0 = 0.282$. Therefore, our system's performance is not acceptable compared to many advanced fingerprint recognition techniques. ROC curves for the five DCT configurations are shown in Figure.4.1, where the False Rejection Rate (FRR) is plotted against the False Acceptance Rate (FAR). Test results indicate that the configuration of 120 is highly effective in terms of EER performance and is better than the other configurations.

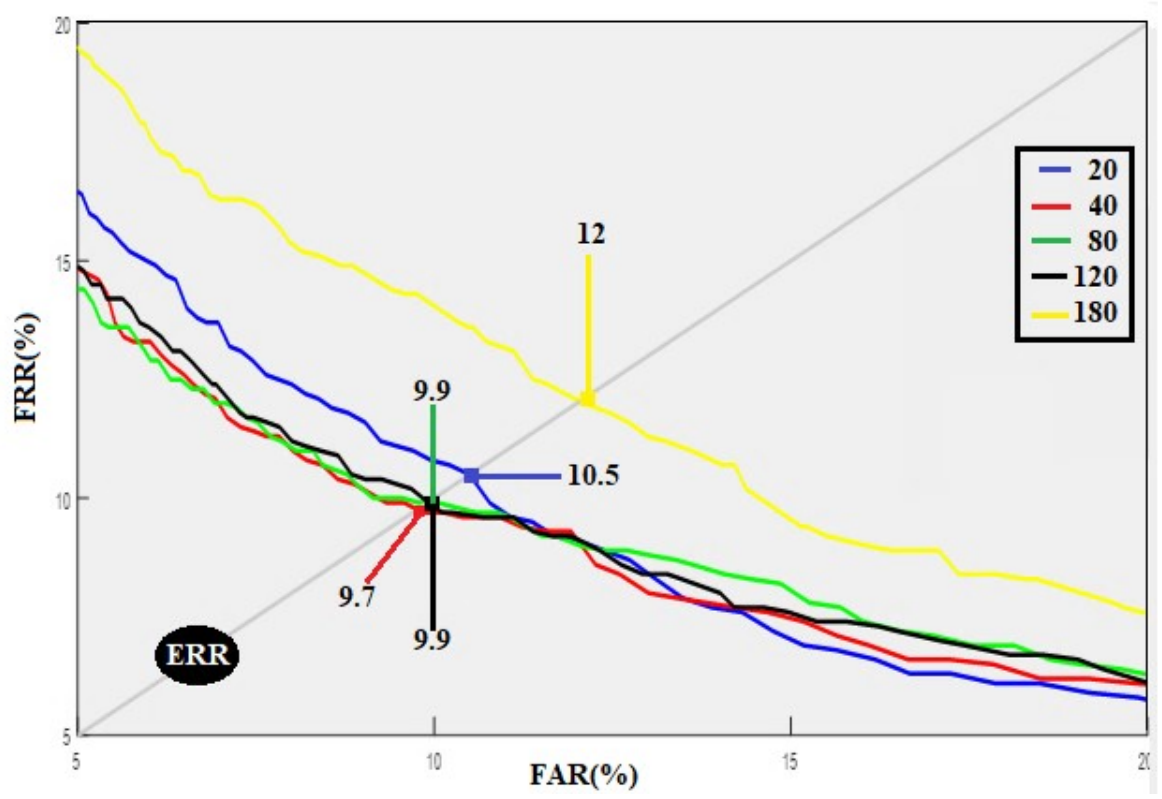

FIGURE 4.1: Results of the DCT parameters for open set identification test, ROC curves FRR vs FAR.

CLOSED-SET

In closed-set identification mode, we compare the performance of different DCT configurations to determine the best case. The results for all cases are also presented in Table.4.1. From analyzing this table, we can see that the Rank One Recognition (ROR) is between 39.5% and 52.2%. Therefore, the system can achieve accuracy with the configuration of 120 for DCT compared to the other configurations, which produces an ROR of 52.2% with a Rank of Perfect Recognition (RPR) of 5 configurations that can produce an RPR = 481. To summarize the closed-set identification experiments, graphs showing the Cumulative Match Characteristics (CMC) curves using all systems were generated in Figure.4.2.

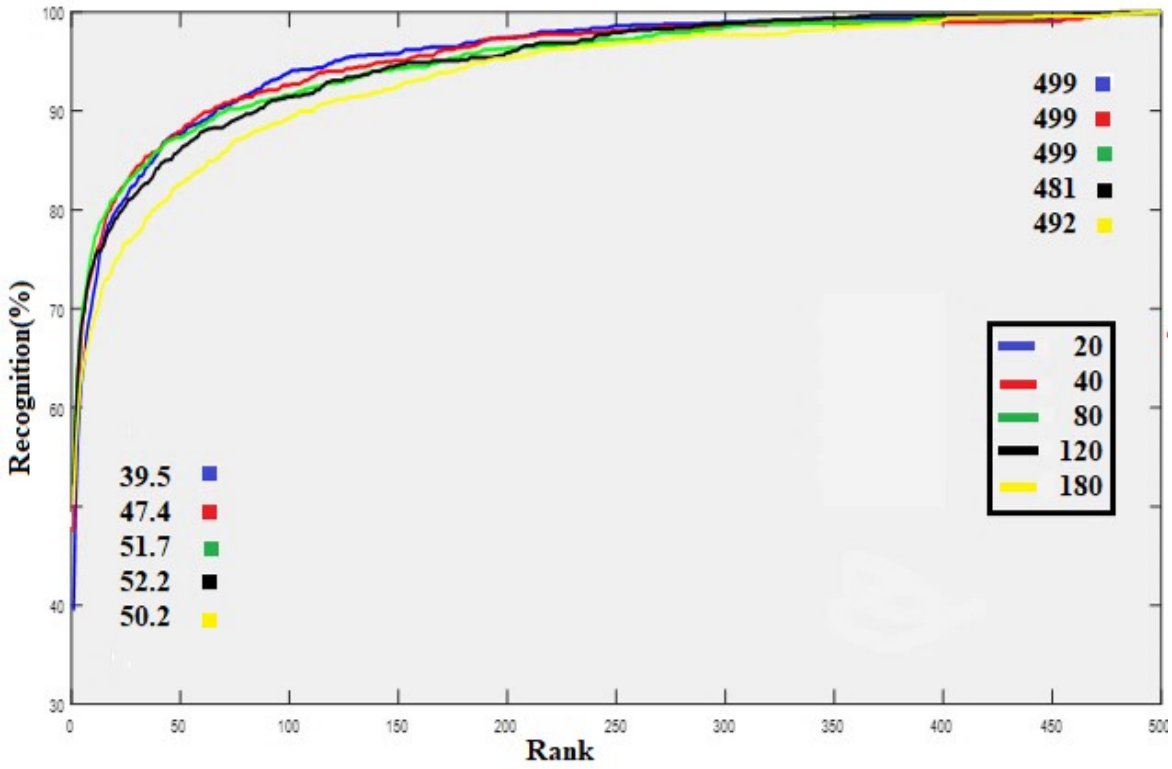

FIGURE 4.2: Results of the DCT parameters for closed set identification test, CMC curves.

4.3.2 RFT Parameters Selection:

Random Forest is a widely used machine learning algorithm that combines multiple decision trees to make predictions and forecasts. When selecting RFT parameters such as: number of trees, depth and size of feature subsets, etc. In our work, we based on the number of trees. Also, these tests are activated by Minor knuckle index of finger modality.

This subsection describes the results related to the proposed tree number parameter. When using different numbers of trees, such as 200, 300, and 400 for each person, we present the test results for the tree number parameter in our finger knuckle biometric recognition systems in Table.4.2:

Trees NUM	Oben_Set Identification		Closed_Set Identification	
	T_0	EER	ROR	RPR
200	0.254	9.9	52.2	481
300	0.391	9.7	55.1	496
400	0.395	9.5	54.9	493

TABLE 4.2: Results of the RFT parameters (numbers of trees) for identification test.

OPEN-SET

From this Table.4.2, it is evident that the number 400 trees of RFT yields better results in terms of EER. In this case, the system can achieve an EER of 9.5% at a threshold T_0= 0.395. Additionally, from this table, we can observe that using 300 trees results in an EER of 9.7% at a threshold $T_0 = 0.391$ for the dorsal finger setting, and finally, in the case of using 200 trees, the EER is 9.9% with a threshold $T_0 = 0.245$. Therefore, our system's performance is deemed unsatisfactory compared to many advanced fingerprint recognition techniques. ROC curves for three cases of RFT tree numbers are displayed in Figure.4.3, where the False Rejection Rate (FRR) is plotted against the False Acceptance Rate (FAR). Test results indicate that the case with 400 trees is highly effective in terms of EER performance and outperforms the other configurations.

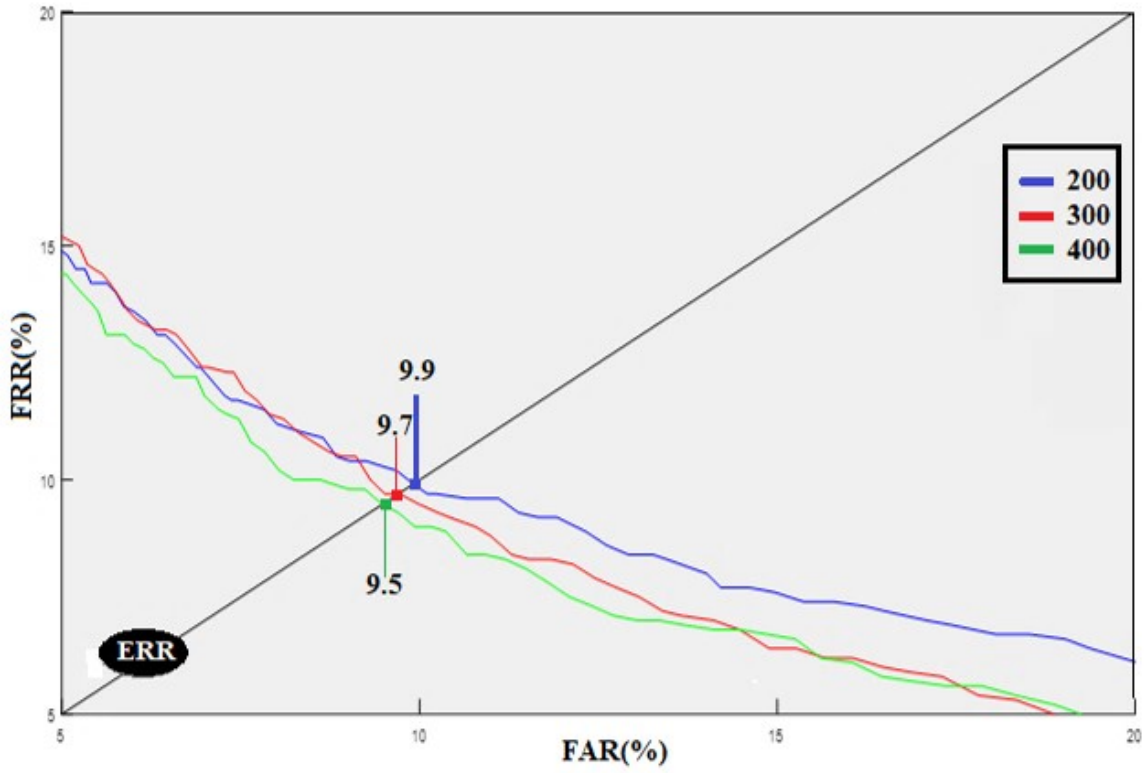

FIGURE 4.3: Results of the RFT parameters for open set identification test, ROC curves FRR vs FAR.

CLOSED-SET

In closed-set identification mode, we compare the performance of different tree numbers to determine the best case. The results for all cases are also presented in Table.4.2 . From analyzing this table, we can see that the Rank One Recognition (ROR) is between 52.2% and 55.1%. Therefore, the system can achieve accuracy when using 300 trees of RFT compared to other tree numbers, which produces an ROR equal to 55.1% with a Rank of Perfect Recognition (RPR). At 200 trees, RPR can reach 481. To summarize the closed-set identification experiments, graphs illustrating the Cumulative Match Characteristics (CMC) curves using all systems were generated in Figure.4.4.

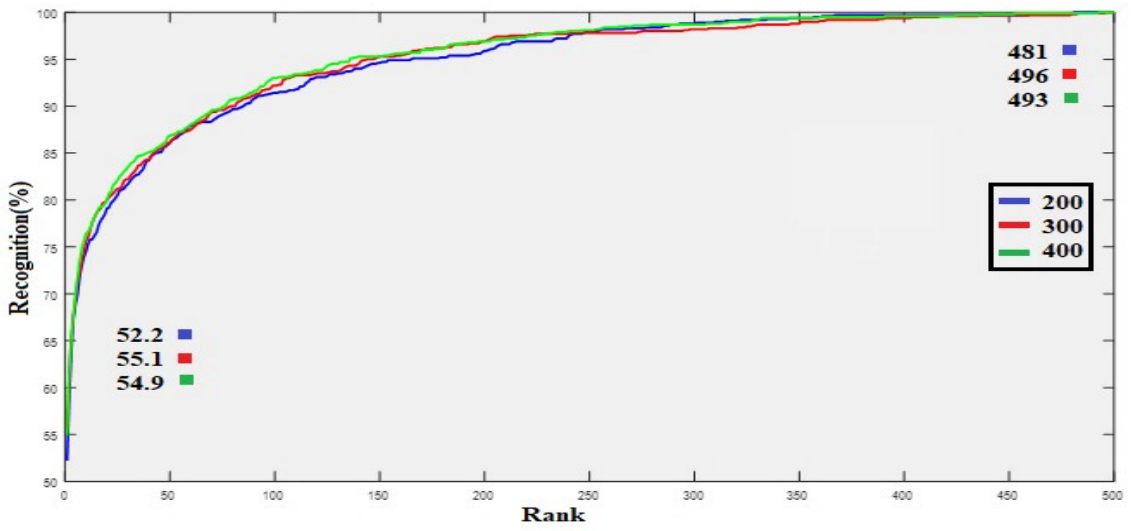

FIGURE 4.4: Results of the RFT parameters for closed set identification test, CMC curves.

4.4 Biometric System Evaluation

Based on the previous sections, the parameters of DCT can be summarized as follows: the number of DCT is 120, and the number of RFT trees is 400. Therefore, we have decided to choose these parameters in the remaining test study.

4.4.1 Unimodal Systems Test Results

Fingers	Open_Set Identification		Closed_Set Identification	
	T_0	EER	ROR	RPR
Middle	0.425	7.7	59.9	491
Ring	0.327	8.7	57	462
Little	0.378	9.1	57.9	500
Index	0.39	9.5	54.9	494

TABLE 4.3: Test results of unimodal systems.

Open-set

In single-modality tests, four samples were tested. The results of single-modality systems based on DCT are shown in Table.4.3. In the open-set identification case, the system achieves better results than the middle finger. The Equal Error Rate (EER) reaches a minimum of 7.7% at threshold $T_0 = 0.425$. The EER for the Ring finger is 8.7% at a threshold of $T_0 = 0.327$. The EER for the Little finger is 9.1% at a threshold of $T_0 = 0.378$. Finally, the EER for the Index finger is 9.5% at a threshold of $T_0 = 0.391$. The performance of our DCT system for the four fingers is presented in Figure.4.5, which plots the False Acceptance Rate (FAR) against the False Rejection Rate (FRR) for the ROC curves.

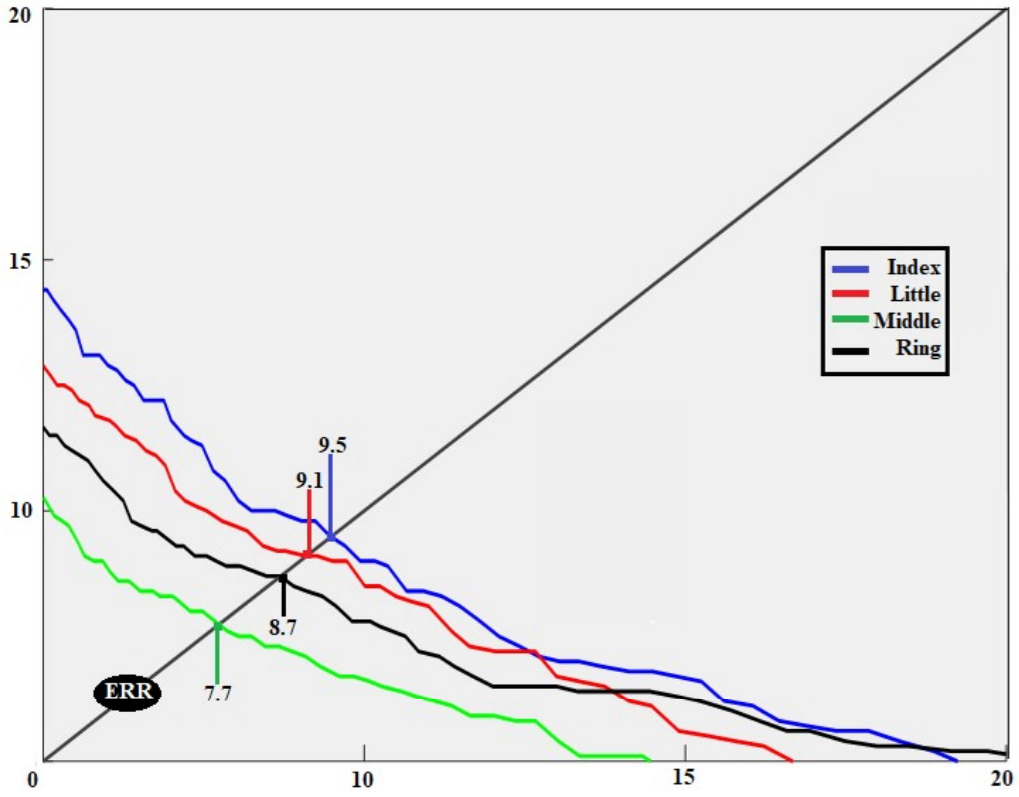

FIGURE 4.5: Unimodal open-set identification test results, ROC curves.

closed-set:

the performance of all different samples is presented in Table.4.3. The results in closed-set identification tests showed that the Rank-One Recognition Rate (ROR) ranged from 54.9% to 59.9%. For the Middle finger, the system can achieve an ROR accuracy of 59.9% with a Rank Placement Rate (RPR) equal to 491. As for the Ring finger, it exhibits an ROR of 57%

and the best RPR of 462. For the Little finger, it shows an ROR of 57.9% and the best RPR of 500. Finally, for the Index finger, it shows an ROR of 54.9% and the best RPR of 494. To summarize the closed-set identification experiments, the Cumulative Match Characteristic (CMC) curves in Figure.4.6 illustrate the obtained recognition rates.

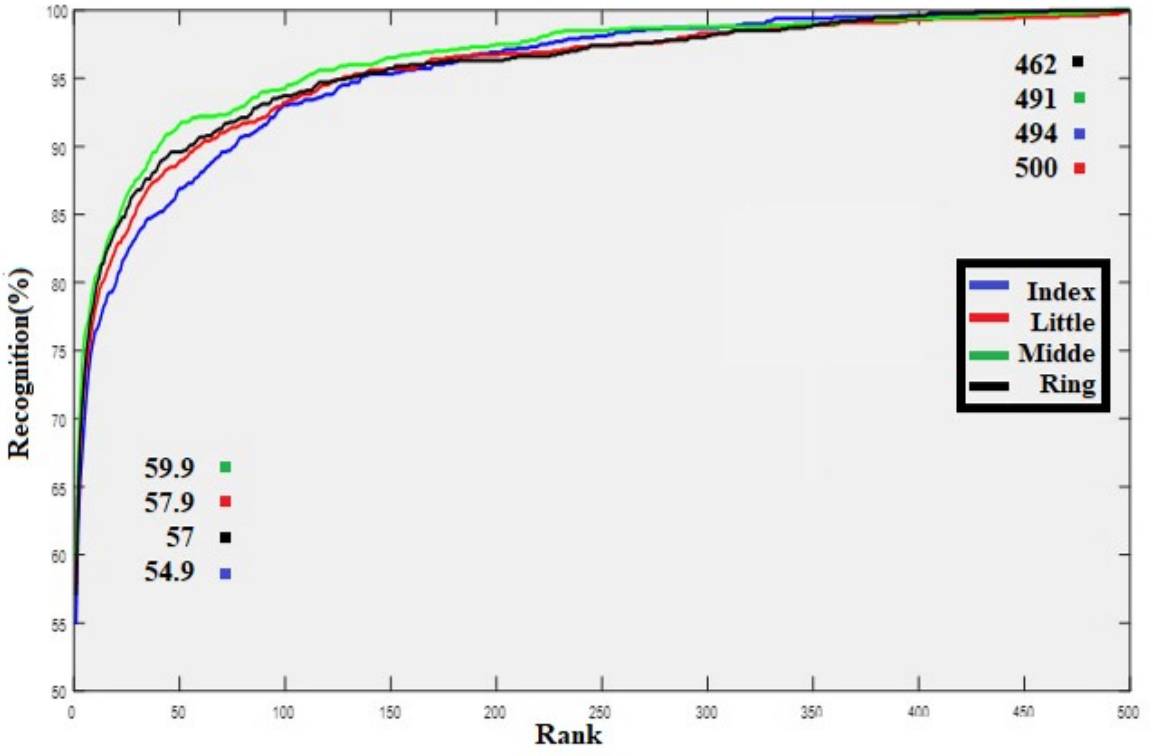

FIGURE 4.6: Unimodal closed-set identification test results, CMC curves.

4.4.2 Multimodal Systems Test Results

To improve the performance of the unimodal biometric identification system, we use multiple information from the different samples. The important keys to improve the accuracy of multimodal biometric system are the choice of fusion level as well as the technique deployed for data fusion. In our work, we choose only the matching score level because it's usually preferred and it can easily combine the scores presented by the different samples. The idea behind using fusion at matching score level is the possibility to combine the scores obtained with a simple rules Sum, Min, Max and Wht.

Combination	Oben_Set Identification		Closed_Set Identification	
	T0	EER	ROR	RPR
SUM	0.665	1.1	91	283
MIN	0.309	8.2	73	483
MAX	0.530	7	58.5	486
WITH	0.665	1.1	91	283

TABLE 4.4: Test results of multimodal systems.

Open-set

Using the DCT method, based on the open set recognition results presented in Table.4.4 , we can see that the fusion rules Sum and Wht also reduce the ERR rate from 7.7% in the binary mode system to 1.1% in the multimodal system. However, in the case of Min and Max, the EER rate is 8.2% at the threshold $T_0 = 0.309$ and 7% at the threshold $T_0 = 0.530$, respectively. The ROC curves in Figure.4.7 directly compare the performance obtained using all fusion rules. Therefore, combining all samples provides a significant improvement, especially when using the Sum and Wht rules

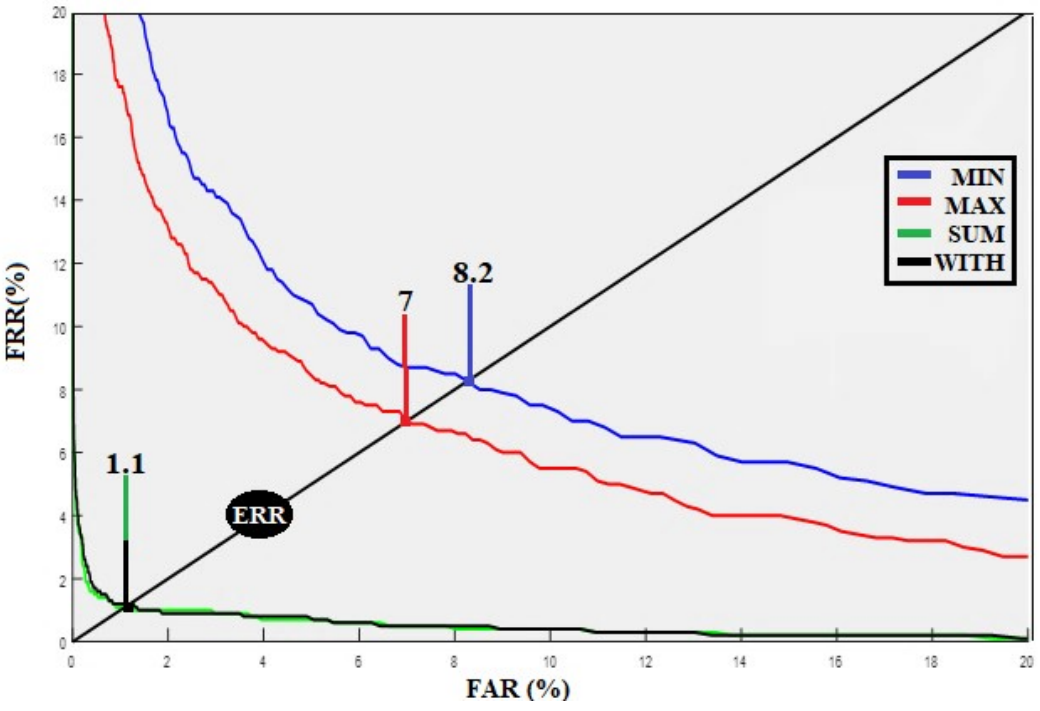

FIGURE 4.7: Multimodal open set identification test results, ROC curves.

closed-set

For closed set recognition mode, the table also includes results for different fusion rule combinations in multimodal DCT systems. From this Table.4.4, it is evident that the Rate of Correct Recognition (ROR) for combining all samples using Sum and Wht rules is higher than the other systems, with ROR reaching 91% and a Rate of Remaining Recognition (RPR) of 283 in both cases. In the case of Min and Max rules, ROR achieves 73% with the best RPR rate of 483, and ROR of 58.5% with RPR of 486, respectively. All these combinations' results are displayed in the table. Finally, the CMC curves illustrate the recognition error rates in the closed set recognition mode for all cases, demonstrating the efficiency of point matching. Figure.4.8 provides a comparison between different fusion rules based on the DCT method.

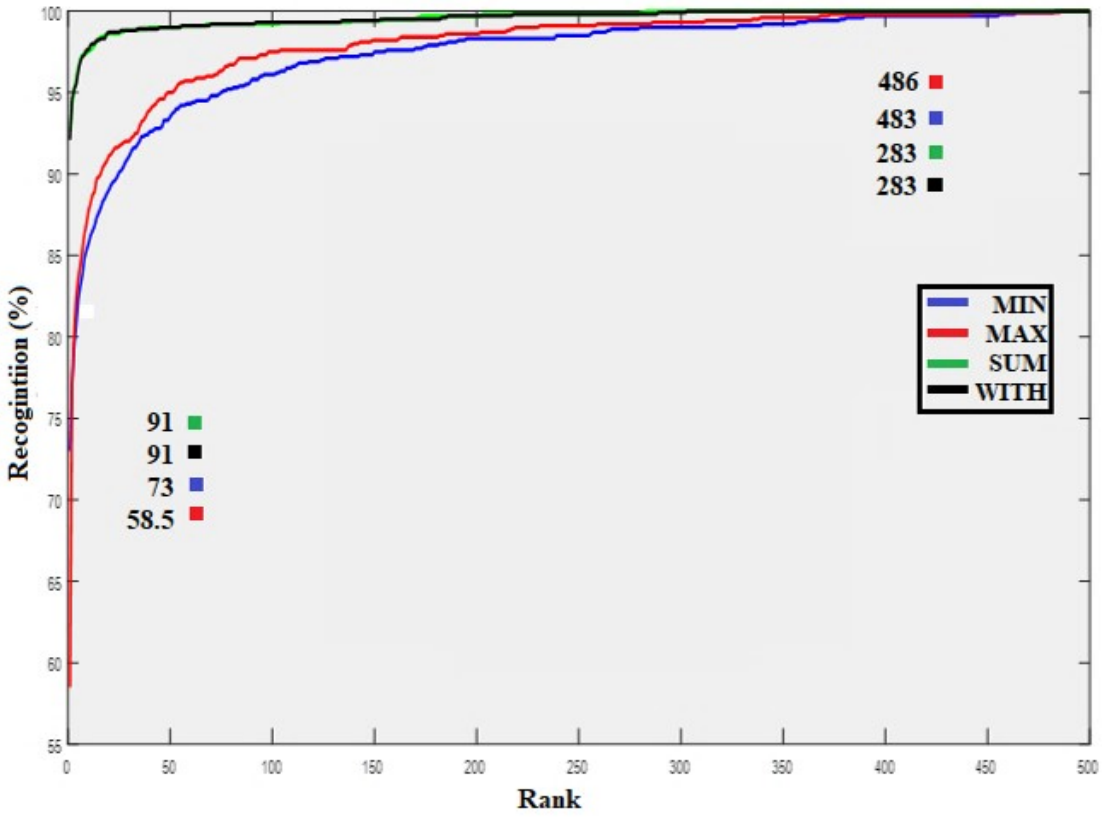

FIGURE 4.8: Multimodal closed-set identification test results, CMC curves.

4.5 Evaluation of Our Method

The aim of this study is to improve the performance and effectiveness of recognition and classification systems and provide biometric identification based on fingerprint recognition.

The obtained results showed modest recognition rates of 92.3% and 98.9% for the unimodal and multimodal systems, respectively. This is attributed to the working conditions. Some of the reasons can be summarized as follows:

- The preprocessing of the database images requires further processing to eliminate noisy data.
- On the hardware side, the CPU used was extremely weak, which limited the achievement of higher recognition rates in the study.
- The training process was not sufficient due to the limited size of the dataset

4.6 Conclusion

The proposed multimodal system was developed and its performance was evaluated using fusion approaches of match scores. The tested database contains fingerprint images of 500 individuals. Through multiple experiments, the DCT and RFT parameters were tested to select the best authentication performance. These parameters include 120 number of DCT points and 400 tree of RFT algorithm.

Different results were obtained from various experiments using unimodal and multimodal recognition systems. Based on the results, the recognition performance achieved an important leap by using multimodal biometrics, compared with the using unimodal biometrics.

Furthermore, the recognition system performance is significantly improved by integrating all types of samples, and it can achieve an EER (Equal Error Rate) of 1.1%, while unimodal recognition only achieves an EER of 7.7%. Thus, multimodal recognition systems demonstrate efficiency and strength in the recognition rates.

Chapter 5

GENERAL CONCLUSION

BIOMETRIC technology provides a high level of security and protection, making identity verification easy and fast. It reduces human errors and improves verification accuracy. In this research, we used fingerprint biometrics, which is known for its high precision, reliability, and difficulty of manipulation.This technology is useful in various fields such as security and access control to buildings and devices, secure payment applications, and identity recognition in mobile devices. In this work, two main techniques used, were Discrete Cosine Transform (DCT) for feature extraction and Random Forest Tree (RFT) for image classification.

DCT was used to extract features representing the unclassified image. Then Random Forest technology was used to classify the image based on these extracted features. A proposed multimodal system was developed and its performance was evaluated using fusion techniques for matching results. The tested database contained fingerprint images of 500 individuals. Through multiple experiments, DCT and RFT parameters were tested to select the best authentication performance. These parameters included 120 DCT points and 400 trees for the RFT algorithm.

From different experiments, obtained results were presented by using unimodal and multimodal recognition systems. Based on the results, excellent performance was achieved in multimodal biometrics recognition compared to unimodal biometrics. Furthermore, the performance of the recognition system has been significantly improved by integrating all types of samples, achieving an Equal Error Rate (EER) of 1.1%, whereas single-modal recognition only achieves an EER of 7.7%. Thus, multi-modal recognition systems demonstrate efficiency and robustness in recognition rates. As future work, we will apply deep learning methods at more credible big database.

Appendix A

PERFORMANCE EVALUATION

A.1 Introduction

THE performance of biometric systems is an important issue in high security applications. Where, the matching between the stored template and the template constructed generates a confidence score to verify whether they are an impostor or a genuine user.

A.2 Error Rates

For each type of decision, there are two possible outcomes, true or false. Therefore, there are a total of four possible outcomes: a genuine is accepted (True Acceptance (TA)) or a False Rejection (FR) occurred, and an impostor is rejected (True Rejection (TR)) or a False Acceptation (FA) occurred [14]. Moreover, there is always overlap region between the score distributions of the genuine user and impostor for a practical biometric system as shown in Fig. A.1. It causes the difficulty in classifying the claimant into the correct categories. In evaluating the performance for any biometric based recognition system, there are mainly two types of factors: False Acceptance Rate (FAR) and False Rejection Rate (FRR). A verification threshold, T_0 is needed in the overlap region as a reference to do the classification.

According to the distribution shown in Fig. A.1, T_0 is used to establish the security level of a biometric systems. It can be seen that for those who obtain a similarity matching score less than T_0 will be classified as an impostor. If one is verified with the similarity matching score higher or equals to the threshold, his (her) claimed identity will be accepted as a genuine. A higher T_0 represents a High-security level. Undoubtedly, less impostors will get through verification but a genuine user with score less than T_0 will also be rejected at the same time. Conversely, by adjusting the threshold to a lower level will reduce the number of

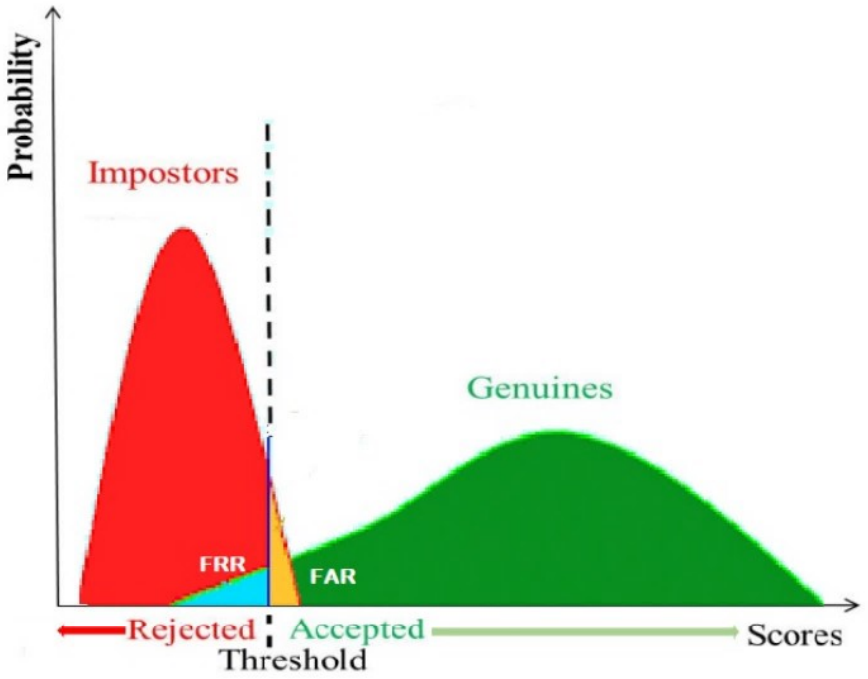

FIGURE A.1: Distribution of curves impostor and genuine users.

the genuine users being falsely rejected. However, this will also cause an increase of falsely accepted impostors. In brief, there is a trade-off between these two types of errors.

A.2.1 False Accept Rate (FAR)

FAR is defined as the probability of an impostor being accepted as a genuine individual [14]. That is, in a biometric authentication system, the FAR is computed as the rate of number of people is falsely accepted FA over the total number of the impostor (NI) for a predefined threshold T_0. This is denoted

$$FAR = \frac{FA(T_0)}{NI} \times 100\%.$$

A.2.2 False Rejection Rate (FRR)

FRR is defined as the probability of a genuine individual being rejected as an impostor [14]. That is, in a biometric authentication system, the FRR is computed as the rate of number of people is falsely rejected FR over the total number of total genuine user (NG) for a predefined threshold T_0. The formula for the FRR is denoted

$$FRR = \frac{FR(T_0)}{NG} \times 100\%.$$

A.2.3 Genuine Accept Rate (GAR)

GAR is used to measure the accuracy of a biometric system [14]. It is measured as the rate of number of people is genuinely accepted over the total number of enrolled people for a predefined threshold. In other words, GAR can be obtained by subtracting the number of falsely rejected people from the total number of genuine people. The GAR is denoted

$$GAR = 1 - FRR(\%).$$

A.2.4 Equal Error Rate (EER)

EER is a point defines the trade-off between the false rejects and the false acceptances, based on FAR and FRR. Thus, EER is a common way of evaluating the performance of a biometric system where low value of EER is considered to represent a biometric system with highly accurate performance. In general, the EER is the value on $FFR = FAR$.

A.2.5 Other Errors

Other errors that may arise in a biometric system are Failure To Capture (FTC) and Failure To Enrol (FTE). These two errors are crucial for live applications. The FTC error takes place when the data acquisition unit is not capable to capture a satisfactory quality of the biometric trait. Whilst, the error of FTE usually occurs when the user tries to enrol in the recognition system are unsuccessful. All these factors are dependent on the decision threshold T, and by varying decision threshold we can obtain a multiple operating points of the system.

A.3 Performance Curves

The values of the performance metrics are usually plotted in different graphs or curves to represent the recognition accuracy of the biometric system. The most commonly used plotting curve is the Receiver Operating Characteristics (ROC) curve [32]. It is as shown in Fig. A.2, the ROC curve plots the GAR against FAR in a semi-logarithmic scale in biometrics research field. Also can be represented the variation of the FRR as a function of FAR; this graph graphically represents the performance of a verification or identification system. The equality error rate (EER) squares at the intersection of the ROC curve with the first bisector. It is frequently used to give an overview of the performance of a system. It is observed that the curve illustrates in the Fig. A.2.

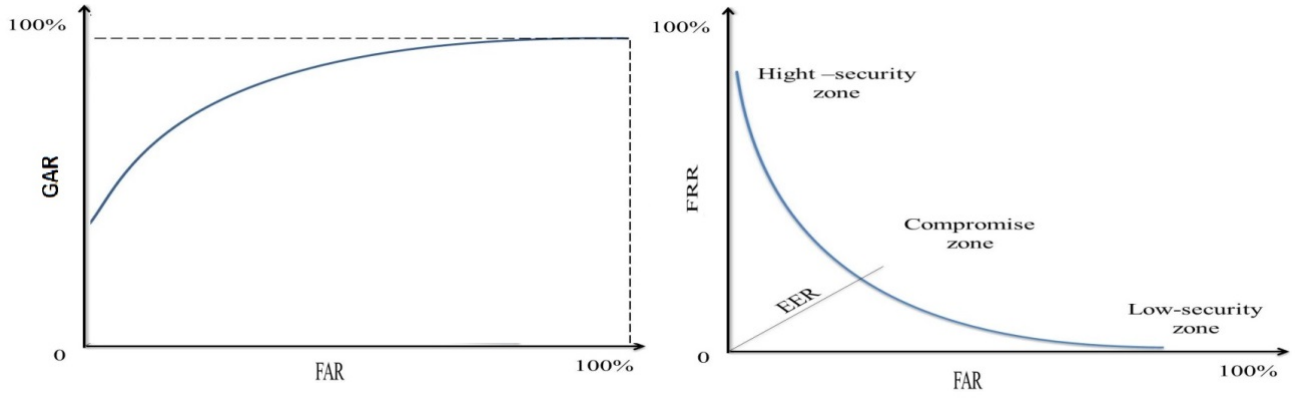

FIGURE A.2: ROC Curves.

Another commonly used curve is Cumulative Match Characteristics (CMC) curve [33] which is mainly used for closed set identification. The Fig. A.3 illustrates an example for CMC curve. This curve gives the percentage of people recognized according to a variable called rank. This curve is associated by two criteria Rank of Perfect Rate (RPR) and Rank-One Recognition (ROR); ROR represents the most commonly used measure but it is not always sufficient. RPR which corresponds to ROR = 100% [34]. CMC curves show the chance of a good system will start with a high identification rate for low ranks identities.

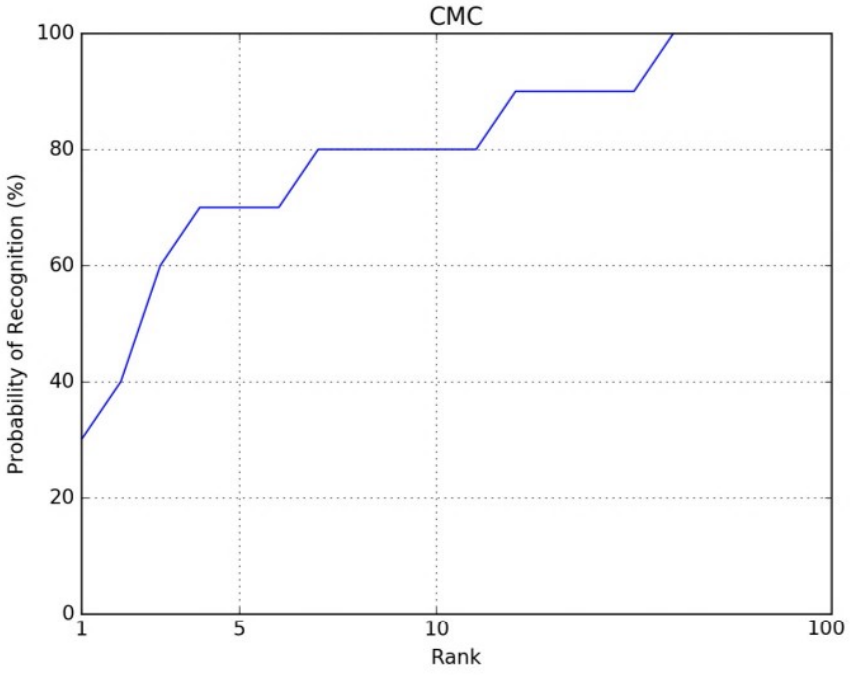

FIGURE A.3: CMC Curve.

Bibliography

[1] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security", in Proc. 2nd USENIX Workshop Security, 1990.

[2] H. T. F. Rhodes, Alphonse Bertillon. "Father of Scientific Detection", AbelardSchuman, New York. 1956.

[3] A. K. Jain, P. Flynn, A.A. Ross. "Handbook of Biometrics"; Springer: New York, NY, USA, 2007.

[4] Y. Chen, S. C. Doss, A. K. Jain. "Fingerprint Quality Indices for Predicting Authentication Performance", Proceedings of the Fifth International Conference on Audio and Video-Based Person Authentication, pp. 160-170, 2005.

[5] G. Koltzsch. "Biometrics-Market Segments and Applications", Journal of Business Economics and Management, Vol. 8(2), pp. 119-122, 2007.

[6] T. Dunstone, N. Yager. "Biometric system and data analysis: Design, evaluation, and data mining", Springer, 2006.

[7] A. K. Jain, A. Ross, and S. Prabhakar. "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14(1), pp. 4-20, 2004.

[8] D. W. Aha, D. Kibler, M. K. Albert. "Instance based learning algorithms", Machine Learning, Vol. 6, pp. 37-66, 1991.

[9] H. Kang, B. Lee, H. Kim, D. Shin, J. Kim. "A study on performance evaluation of the liveness detection for various fingerprint sensor modules", Proceedings of KES, pp. 1245-1253, 2003.

[10] Y. Chen, S. C. Dass, A. K. Jain. "Fingerprint Quality Indices for Predicting Authentication Performance", Proceedings of the Fifth International Conference on Audio and Video-Based Person Authentication, (AVBPA?05), , pp. 160-170, 2005.

[11] E. Bigun, J. Bigun, S. Fisher. "Expert conciliation for multimodal person authentication systems using baysian statistics", Proceedings of the International Conference on Audio and Video-Based Biometric Person Authentication, Vol. 12(6), pp. 291-300, 1997.

[12]] R. Brunelli, D. Falavigna. "Person identi?cation using multiple cues" , IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 17(10), pp. 955-966, 1995.

[13] J. Kittler, M. Hatef, R. Duin, J. Matas. " On combining classifiers", Pattern Analysis and Machine Intelligence, IEEE Transactions on,Vol. 20(3), pp. 226-239, 1998.

[14] A. Ross, K. Nandakumar, A. K. Jain. "Handbook of Multibiometrics", Springer, 2006.

[15] A. Ross, A. K. Jain. “Multimodal biometrics: An overview”, In proc. of 12th European Signal Processing Conference (EUSIPCO), pp.1221-1224, 2004.

[16] R. Frischholz, U. Dieckmann. “BioID: A multimodal biometric identification system”, IEEE Journal of Computer Science, vol. 33, no. 2, pp. 64-68, Feb 2000.

[17] B. L.Stephens. “Student Thesis on ?Image Compression algorithms”, California State University, Sacramento, August 1996.

[18] R. C. Reiningek, J. D. Gibso. “Distributions of the Two-Dimensional DCT Coefficients for Images”, IEEE Transactions on Communications, Vol. 31, Issue 6, June 1983.

[19]] R. C. Gonzalez, R. E. Woods. “Digital Image Processing”, ISBN-10: 013168728X. ISBN-13: 978-0131687288, Prentice Hall, 3rdedition, August 2007.

[20] K. R. Rao, P. Yip. “Discrete cosine transform: Algorithms, advantages, applications”, San Diego CA: Academic Press, 1990.

[21] H. B. Li, W. Wang, H. W. Ding, J. Dong. “Trees Weighting Random Forest Method for Classifying HighDimensional Noisy Data”, IEEE 7th International Conference, pp. 160-163; 2010.

[22] J. R. Quinlan. “programs for machine learning”, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1993.

[23] P. Yin, A. Criminisi, J. Winn, and I. Essa. “Tree-based Classifiers for Bilayer Video Segmentation”, In Proc. CVPR, 2007.

[24] A. Kumar, Y. Zhou. “Personal identification using finger knuckle orientation features”, Electronic Letters 45 (20), pp. 1023-1025, 2009.

[25] New Biometric Technology Improves Security and Facilitates, Available at: 2014.

[26] N. Vasconcelos. “Discrete Cosine Transform”, Available at: , 2015.

[27] J. J Ding, P. Y. Lin, H. H. Chen. “Generalized Zigzag Scanning Algorithm for Non-square Blocks”, Volume 6524 of the series Lecture Notes in Computer Science pp. 252-262, 2007.

[28] M. Schonlau, R. Y. Zou, “The random forest algorithm for statistical learning”, The Stata Journal, vol. 20, no. 1, 2020.

[29] M. V. Karki, S. S. Selvi. “Multimodal biometrics at feature level fusion using texture features”, International Journal of Biometrics and Bioinformatics, Vol. 7(1), pp. 58-73, 2013.

[30] M. J. Sudhamani, M.K. Venkatesha, K.R. Radhika. “Revisiting Feature level and Score level Fusion Techniques in Multimodal Biometrics System”, Proceedings of International Conference on Multimedia Computing and Systems (ICMCS), pp. 881-885, 2012.

[31] Available at: .

[32] Egan. “Signal detection theory and ROC-analysis”, Academic press, 1995.

[33] H. Moon and P. J. Phillips, “Computational and performance aspects of pca-based face-recognition algorithms”, Perception, vol. 30, no. 3, pp. 303-321, 2001.

[34] A. Meraoumia, S. Chitroub, A. Bouridane. “Multimodal biometric person recognition system based on fingerprint finger-knuckle-print using correlation fil- ter classifier”, IEEE International Conference on Communications (ICC), pp. 820-824, 2012.