People's Democratic Republic of Algeria
Ministry Of Higher Education and Scientific Research

University of Mohamed Bachir El Ibrahimi Bordj Bou Arreridj

Faculty of Mathematics and Computer science

Department of Computer Science

Submitted for the Degree of

Masters of Computer Science

Title

Multimodal Biometric System using FKP recognition pattern

Presented by:

FARES Mohamed Aymen **Information and communications technology**

HAROUN Moundhir AbdelHamid **Business intelligence**

Defended publicly on 11/07/2021, before the jury composed of

President:	Mr.BELHADJ Foudil	MCA à L’UBBA.
Examiners:	Ms.BENABAID Sonia	MCA à L’UBBA.
	Ms.LAIFA Meriem	MCA à L’UBBA.
Supervisor:	Mr.MAZA Sofiane	MCA à L’BBA.

Promotion : 2020/2021

Table of Contents

Chapter 02: FKP Minor-Major System

Chapter 03: Experimented Results

Acknowledgements

In the name of Allah, the Most Gracious and the Most Merciful.

All praises to Allah and His blessing for the completion of this thesis. We thank God for all the opportunities, trials and strength that have been showered on us to finish writing the thesis. We experienced so much during this process, not only from the academic aspect but also from the aspect of personality. Our humblest gratitude to the holy Prophet Muhammad (Peace be upon him) whose way of life has been a continuous guidance for us.

First and foremost, we would like to sincerely thank our supervisor **Dr. Maza Sofiane** for his guidance, understanding, patience and most importantly, he has provided positive encouragement and a warm spirit to finish this thesis. It has been a great pleasure and honor to have him as our supervisor.

We thank the members of the jury **Dr.Belhadj Foudil ,Dr.Laifa Meriem** and **Dr.Benabaid Sonia** for their distinguished contributions to the evaluation of this thesis.

Finally, we address our most sincere thanks to all our relatives and friends, who have always supported and encouraged during carrying out this work.

Dedicace

To my parent,

To my beloved sister,

To My both aunts Dr.FARES Nour Elhouda & Dr.FARES Fahima who taught me that it is never too late to change careers to pursue your true passion and that context is everything,

To all my family and my friends.

FARES Mohamed Aymen
June 2021

To my parents who gave me so much to make me what I am,

To my dear sisters, with all my best wishes for success in their lives,

To all my family,

All my friends,

To everyone I love, I dedicate this works.

HAROUN Moundhir Abdelhamid
June 2021

Abbreviations

FKP: Finger knuckle print

CMC: Cumulative Match Curve

EER: Equal Error Rate

FAR: False Accept Rate

FRR: False Rejection Rate

UBS: Unimodal biometric system

MBS: Multimodal biometric system

TP: True positive

FP: False positive

FTE: Failure-to-enroll rate

FTA: Failure-to-acquire rate

FMR: False match rate

FNMR: False non-match rate

ROC: Receiver operating characteristic

CMC: Cumulative Matching Characteristics

LDA: Linear Discriminant Analysis

PCA: Principal Component Analysis

BSIF: Binarized Statistical Image Features

TPLBP: Three-Patch Local Binary Patterns

List of figures

List of tables

General Introduction

Scientific research has taken a wide range in IT security technologies, so identifying persons now is quite easy and effective compared to the traditional ways such as identifying a person by username and password, which in case of forgetting those information the person cannot be verified or authentified. Indeed biometrics systems has invaded worldwide security by their efficiency and performance, moreover their traits are divided into two categories the physical (iris, retina, fingerprints, face recognition, vascular structure etc.) and behavioral ones (voice features, signature, typing dynamics, gait etc.).

In general, authenticating persons can be performed based on what a person is, what he has, what he knows and what he does. Each human being is born with his unique observed characteristics such as face. Therefore, we recognize people based on who they are. Another way to identify an individual is based on what an individual has like (ID cards and Passwords). When a person tries to login into his bank account or other online activity by using his username and password, this way is based on what that person knows. The last way to recognize an authorized person is based on how that person behaves. Behavioral biometrics like voice, gait and signature are the most famous methods for security sector. These recognition technologies have attracted a lot of researchers due to its lowcost of implementation in comparison to the physiological traits , friendly use and complexity to mimic others typing habits. [1] Deploying such authenticating methods instead of passwords, which can be easily lost or forgotten.

Therefore, biometrics recognition techniques can significantly provide higher and better security features for real time identification in order to decrease any unauthorized access to many applications and services.

In our thesis, we pick a particular authentication system using finger joints (FKP pictures) for both index and middle fingers as a characteristic for biometric identification of an individual, the motivation behind this particular authentication system is that in today's world fingerprints quality can be very poor. The cultivators and hard workers use their hands very roughly, causing sever damage to their fingerprints permanently. Unlike knuckle print quality which remains in good state because they are not used as much or at all, also we have chosen to apply both fingers (index and middle) for a higher accuracy and low error rate.

Our work consist of proposing an authentication FKP architecture. The goal is to extract a model by applying a descriptor which is in our case the BSIF descriptor for both fingers (index and middle) as well as using LDA and PCA for dimension reduction of the extracted vectors.

In the first experiment, the goal is to conceive unimodal system which uses one modality, applying BSIF descriptor at feature extraction process to all of minor & major of both fingers (index and middle) at a time.

In the second experiment, the goal is applying multimodal fusion to achieve better results and low error identification rate which could make the system more effective to be used in high security application.

Finally, to achieve the best possible results, a comparison has been made for fusion and concatenation of FKP imaging in different levels and methods.

The rest of this thesis is organized as follows:

Chapter 1 presents some basic concepts of biometrics also a couples issues related to unimodal system and why is multimodal is more effective.

In chapter 2, we explain more the proposed system, which we use multimodal system and fusions using BSIF descriptor. Describing all steps of both methods (fusion at feature extraction level and fusion at feature extraction & score level at a time).

In chapter 3, we review the experimented results of our proposed system and we discuss about the results of both fusions that we have mentioned.

At the end, we reach to a general conclusion on how multimodal FKP system can be more accurate and performant among some of biometrics systems.

1. Introduction

Unimodal biometric systems is a technique, which guarantees authentication information by processing distinctive characteristic sequences, and these are fetched out from individuals [2]. However the performance of unimodal biometric systems restricted in terms of susceptibility to spoof attacks, non-universality accuracy and noise in sensed data.

The Multimodal biometric systems defeat those various limitations of unimodal biometric systems as the sources of different biometrics typically compensate for the inherent limitations of one another.

2. Definition

Biometrics means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities [3].

Biometric technologies also defined as "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic." [3]. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc.

3. Biometric characteristics

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics [3]:

- **Universal:** Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

- **Invariance of properties:** They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

- **Measurability:** The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

- **Singularity:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

- **Acceptance:** The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

- **Reducibility:** The captured data should be capable of being reduced to a file which is easy to handle.

- **Reliability and tamper-resistance:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

- **Privacy:** The process should not violate the privacy of the person.

- **Comparable:** Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

- **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

4. How biometrics work

Biometric systems are highly complex and involve a variety of components and processes. Biometric system concepts, underlying technology, and how the technology functions are described below.

4.1 Verification and Identification

Biometric systems can be used for verification or identification. Verification, sometimes referred to as one-to-one matching, determines if a person is whom he or she claims to be. This process involves capturing a person's biometric data and matching it against an existing record for that person. Typical applications of these types of systems include controlling access to a secure facility or granting permission to use a secure computer system.

Alternatively, identification determines who an individual is through a process referred to as one-to-many matching. With these systems, a record of a person may be known to exist in the database (i.e., closed-set identification) or may not be known to exist in the database (i.e., open-set identification). His or her biometric data is compared against all existing records in a database in order to find a match. For example, law enforcement could use this type of system to identify an individual who does not have a driver's license at a traffic stop.

Biometric systems automate the verification and identification processes by capturing characteristics of individuals, extracting measurable features, and comparing the data against enrolled biometric records. [4]

4.2 Enrollment

Enrollment is the process by which the biometric data of individuals is captured and stored so that it can later be used for matching. A verification system, for example, could require the creation of a relatively small enrollment database for all personnel authorized access to a particular facility. In contrast, an effective identification system may require a much larger biometric database. The entire collection of fingerprints maintained by the Federal Bureau of Investigation (FBI) would be one example [4].

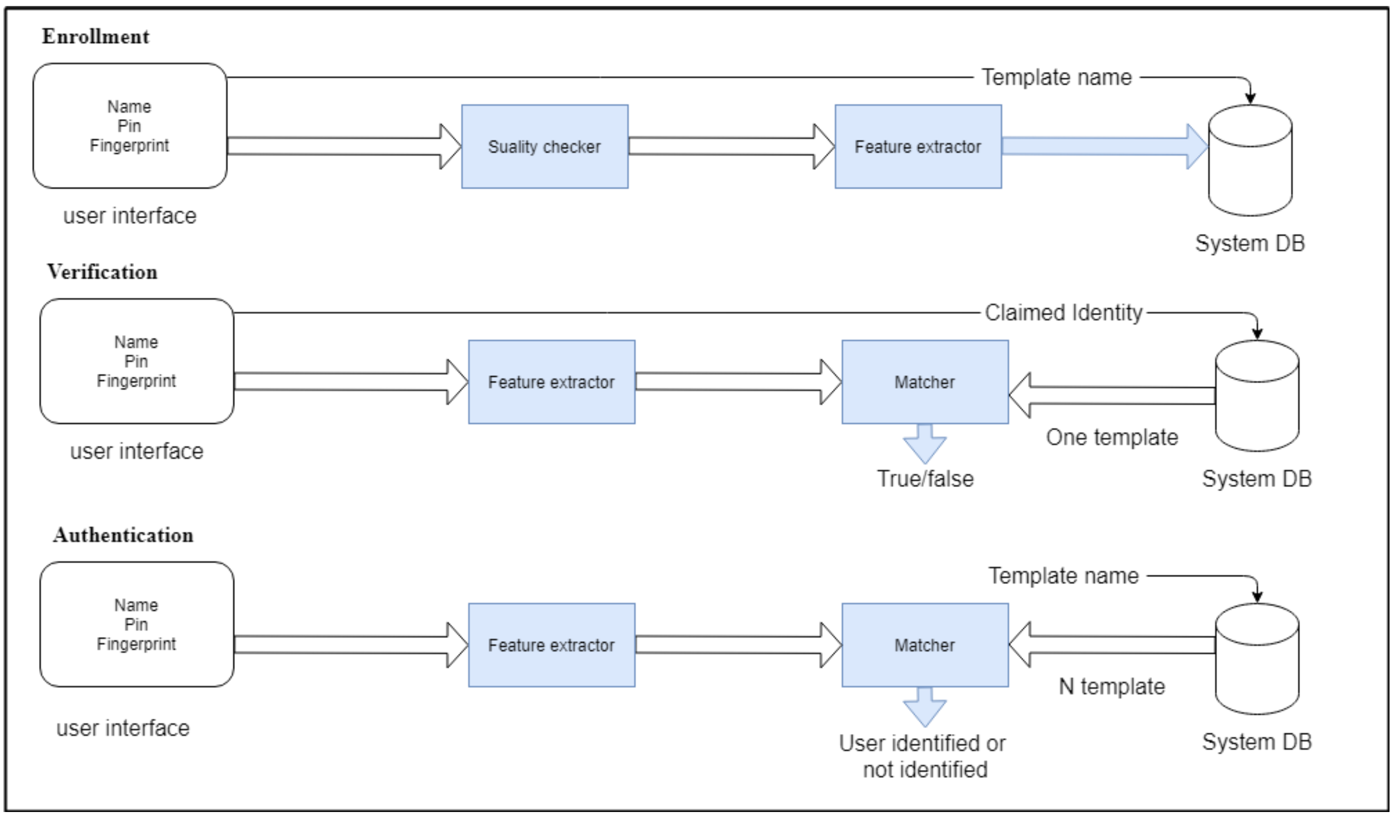


Figure 4-1 Block diagrams of enrollment, verification, and identification in a Biometric System

5. Biometric Modalities

Biometric systems can perform capture and recognition of a single characteristic, or they can be multi-modal, addressing two or more characteristics. They may be intrusive, requiring the individual to have direct contact with the capture device, or non-intrusive in which the biometric data is captured from a distance. Below is an overview of some biometric modalities

5.1 Fingerprints

Fingerprints are the biometric modality most commonly used in law enforcement. Fingerprints can contain as many as 70 to 75 unique characteristics, or print pattern features, such as details in the ridge endings and bifurcations (where a ridge splits into two ridges). Fingerprints can be flat or rolled. A flat fingerprint image, as shown in Figure 5-1, is taken by touching a single finger to a platen, or paper card, without any rolling motion. A fingerprint enrollment record may include one or more flat fingerprints. A slap image is taken by simultaneously pressing the four fingers of one hand onto the platen or card. Slaps are typically captured using the “4-4-2 method” where by the individual’s right and left four fingers are captured first, then flat impressions are taken of both thumbs [4].

Figure 5-1 Flat Fingerprint [4]

5.2 Facial recognition

Facial recognition is the most natural means of biometric identification. The method of distinguishing one individual from another is an ability of virtually every human. Any camera with sufficient resolution can be used to obtain the image of the face (scanned pictures can be used as well). Generally speaking the better the image source the more accurate results we get. The image recognition algorithm can be based on a 2 dimensional or 3 dimensional face properties. Facial recognition systems usually use only the grey-scale information. Colors (if available) are used only to locate the face in the image only. The lighting conditions required are mainly dependent on the quality of the camera used. In poor light condition, individual features may not be easily discernible. There exist even infrared cameras that can be used with facial recognition systems [5].

Figure 5-2 Facial Features [4]

5.3 Iris

The iris is the coloured ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different too. A near infrared grey-scale camera in the distance of 10 – 40 cm takes the iris pattern from the camera. There are several types or iris cameras with different requirements on user behaviour and different levels of user friendliness. The iris scanning technology is not intrusive and thus is deemed acceptable by most users. The iris pattern remains stable over a person's life, being affected only by some diseases. There is a standardized format of the iris image, but no standard exists for the iris template [4].

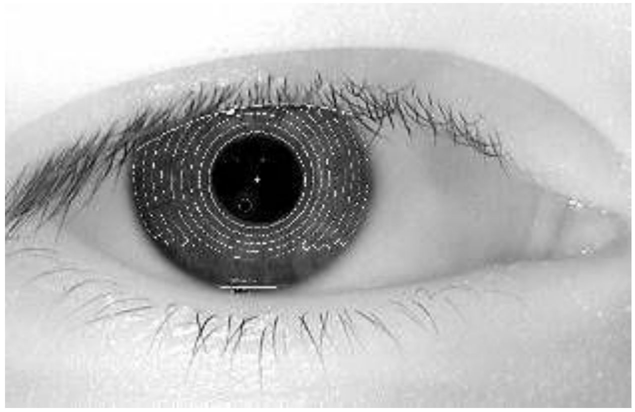


Figure 5-3 Biometrics based on the unique pattern of the iris.

5.4 Hand Geometry

Hand geometry is a recognition technology that uses the structure, shape, and proportions of the hand to aid in verifying an individual's identity. The human hand is not unique; therefore, hand geometry cannot be used effectively for identification in a large dataset. However, it can be paired with other forms of identification, such as a personal identification number or badge, as part of an access control system. During the capture process, the individual places their palm on the surface of a specialized reader. Characteristics such as length and width of the fingers, width of the palm, and finger curve are measured and used to create a template for one-to-one matching [4].

Figure 5-4 Hand geometry [24]

5.5 Retina

This recognition technology images the retina at the back of the eye and compares the pattern of blood vessels with existing data in an enrollment database. A specialized retinal scanner casts a beam of low-energy infrared light into the individual’s eye and captures an image. The retinal blood vessels absorb the light more readily than the surrounding tissue, and the resulting pattern of variations is converted into a biometric template. It should be noted that retina images are declining in use for recognition systems. The medical community has found that they can be used to diagnose certain medical conditions. This has led to privacy concerns [4].

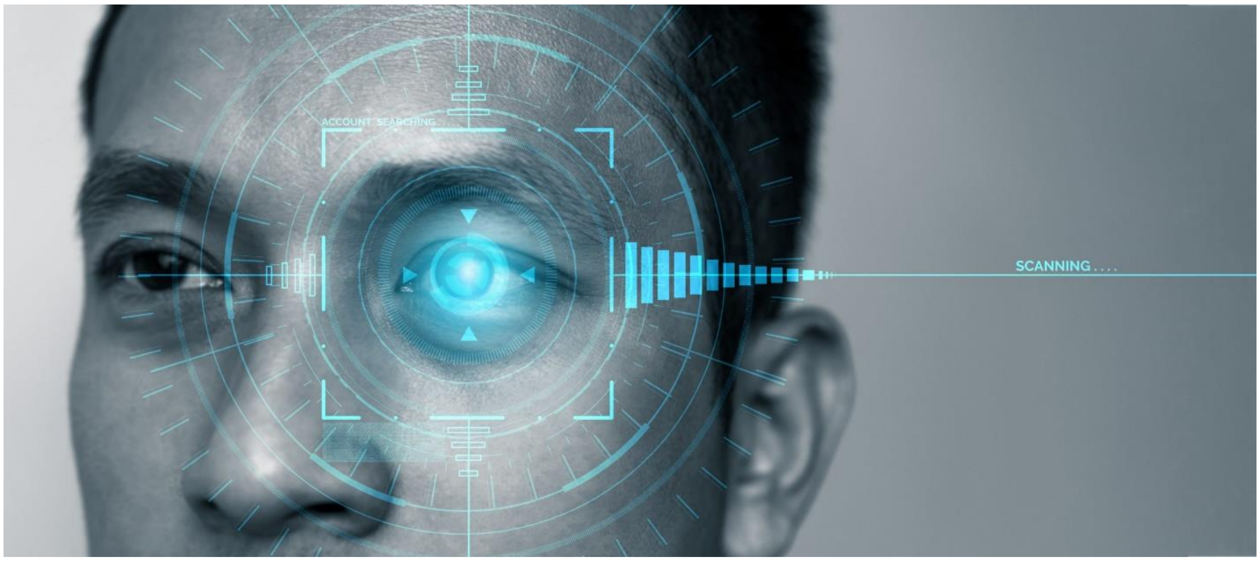


Figure 5-5 retina scanning [24]

5.6 Keystroke Dynamics

Keystroke dynamics is a biometric modality that measures a person's typing patterns and rhythm and uses them for recognition. [4]

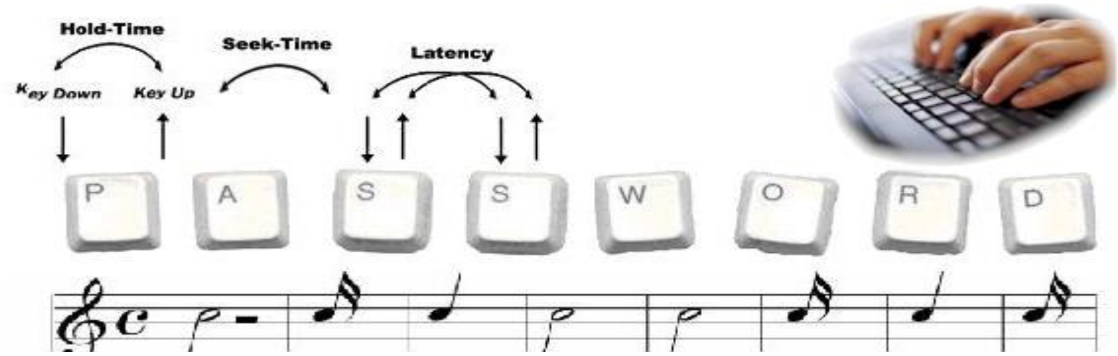


Figure 5-6 Keystroke dynamics biometrics [24]

5.7 Gait/Body

Gait/body technology recognizes individuals by their distinctive walk. Motion characteristics are derived from a sequence of images captured with a camera or data produced by the accelerometer in a smart phone. These characteristics are processed to produce a template that can be used for identification. The characteristics can be obscured by obstructions such as loose-fitting clothing. [4]

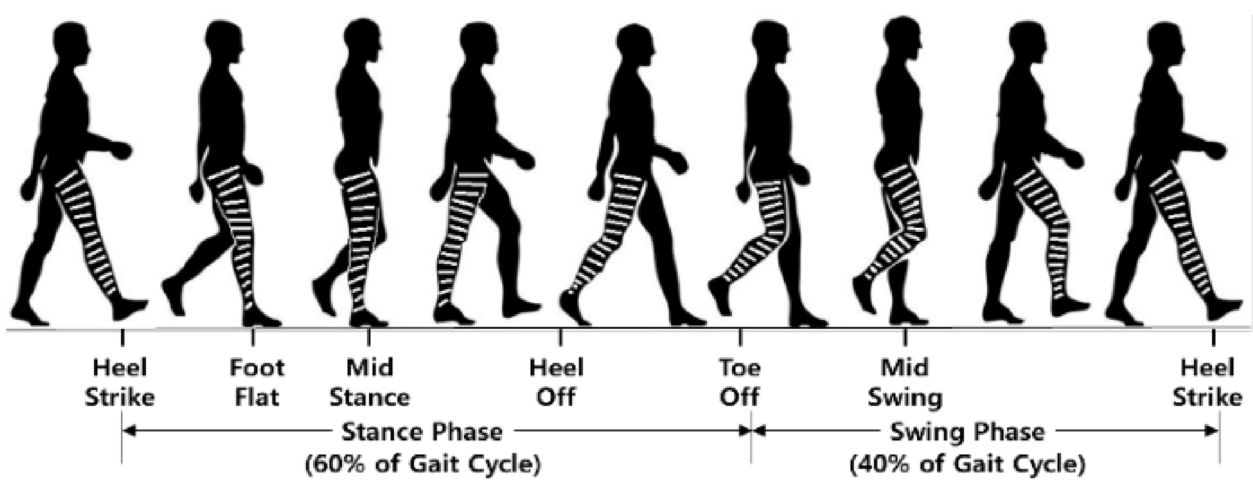


Figure 5-7 Gait Cycle Phases [24]

6. Performance evaluation

The performance evaluation has for objective to provide some quantitative measures on the efficiency of biometric systems. The classical statistical metrics used to quantify the performance of a biometric system are [6]:

- **Computation time:** the necessary time for the acquirement, enrollment, verification / identification.

- **True positive (TP):** number of users that have been correctly authenticated.

- **False positive (FP):** number of impostors that have been authenticated.

- **False reject rate (FRR):** Proportion of authentic users that are incorrectly denied. It is calculated as:

  FRR = 1-TP/ (number of genuine users)

- **False accept rate (FAR):** proportion of impostors that are accepted by the biometric system. It is calculated as:

  FAR = FP/ (number of impostor users)

- **Failure-to-enroll rate (FTE):** proportion of the user population for whom the biometric system fails to capture or extract usable information from biometric sample. This failure may be caused due to behavioral or physical conditions pertaining to the subject which hinder its ability to present correctly the required biometric information.

- **Failure-to-acquire rate (FTA):** proportion of verification or identification attempts for which a biometric system is unable to capture a sample or locate an image or signal of sufficient quality.

- **False match rate (FMR):** The rate for incorrect positive matches by the matching algorithm for single template comparison attempts. FMR equals

FAR when the biometric system uses one attempt by a user to match its own stored template.

- **False non-match rate (FNMR):** The rate for incorrect negative matches by the matching algorithm for single template comparison attempts. FNMR equals FRR when the biometric system uses one attempt by a user to match its own stored template.

- **Identification rank:** It is the smallest value k for which a user's correct identifier is in the top k identifiers returned by an identification system.

- **Receiver operating characteristic curve (ROC curve):** The method most commonly used to assess the performance of a biometric system is the ROC

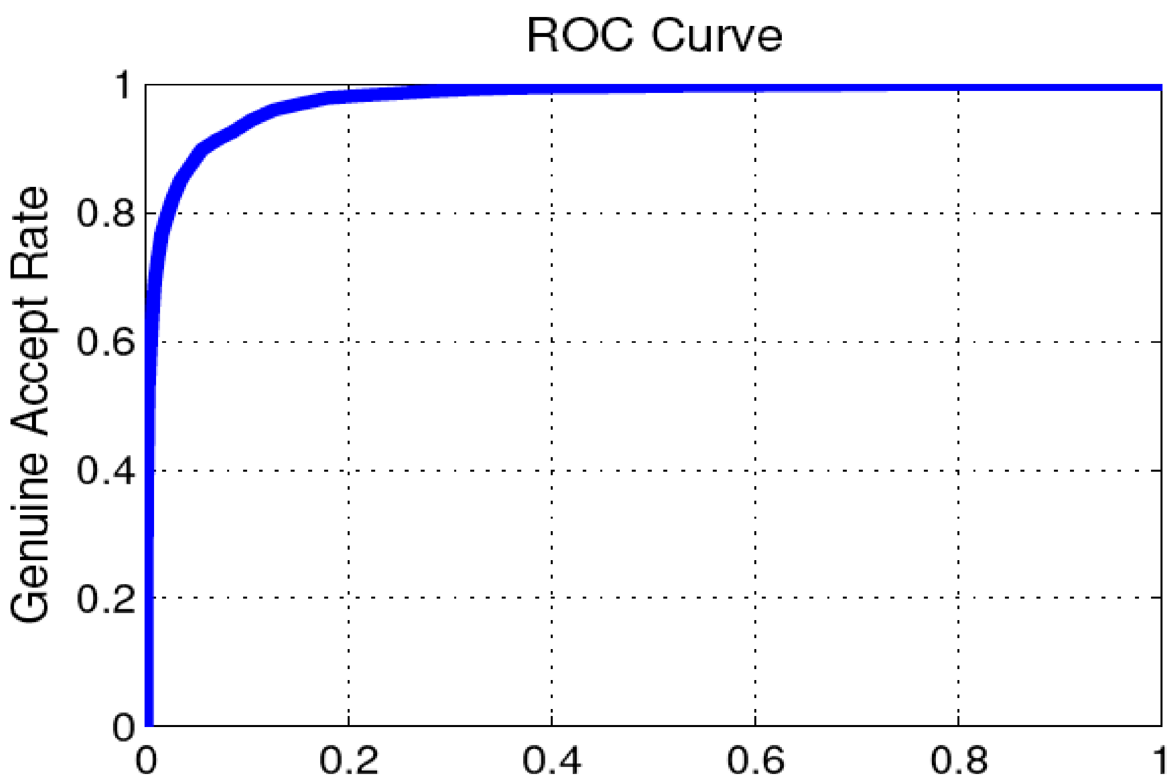


Figure 6-1 ROC Curve

curve. The aim is to plot a curve representing FAR according to the FRR. In order to plot this type of curve, we have to changes the value of the decision threshold. For each value of the threshold, we calculate the associated FRR and FAR that we plot on the curve. The advantage of this method is that it gives a compact representation of the performance of a biometric system through a single curve allowing the comparison of different biometric systems. In order to compare easily several biometric systems, we can then compute the area under the curve AUC and the equal error rate ERR where FAR = FRR. The optimal result is obtained if the AUC equals 1 and the ERR equals 0.

- **Cumulative Matching Characteristics (CMC curves):** are the most popular evaluation metrics for person re-identification methods. Consider a simple single-gallery-shot setting, where each gallery identity has only one instance. For each query, an algorithm will rank all the gallery samples according to their distances to the query from small to large, and the CMC top-k accuracy is

  Acck= {1 if top-k ranked gallery samples contain the query identity
  0 otherwise}

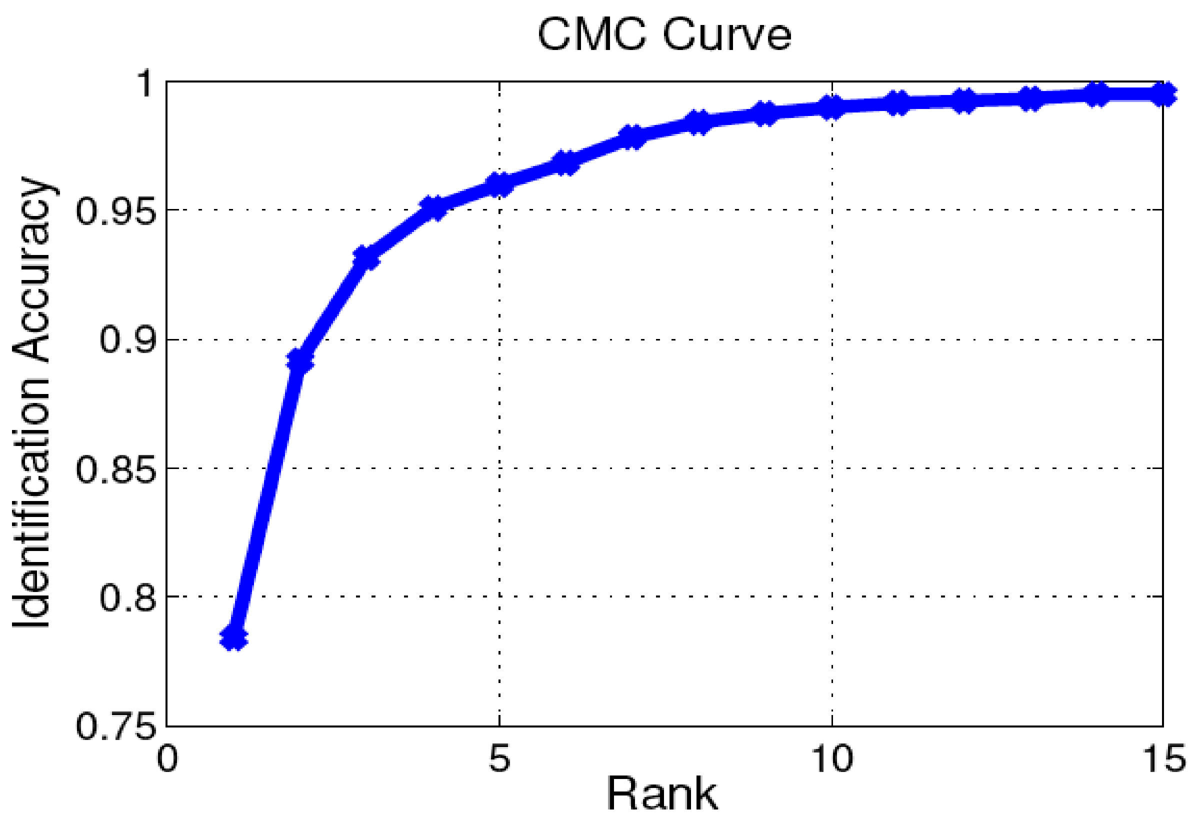


Figure 6-2 CMC Curve

- **Precision/recall curve (PR curve):** has a similar behavior to ROC curves. In order to draw the PR curve, we plot the positive predictive value (PPR = TP /(TP+FP)), also known as the precision versus the recall. We can then compute AUC and ERR in a similar way as in ROC curves. One advantage is that we do not need the number of true negative in this method.

7. Multimodal biometrics

The multimodal biometrics is a promising area of information processing research which is directed towards understanding of traits and methods for more accurate and reliable personal information representation for subsequent decision making and matching. In the recent years, there is a significant increase in research activity directed at understanding all aspects of biometric information system representation and utilization for decision making support, for use by public and security services, medical diagnostics, and for understanding the complex processes behind biometric matching and recognition.

7.1 Multi algorithmic biometric systems

Multi algorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms [7].

7.2 Multi-instance biometric systems

Multi-instance biometric systems use one sensor or possibly more sensors to capture samples of two or more different instances of the same biometric characteristics. Example is capturing images from multiple fingers [7].

7.3 Multi-sensorial biometric systems

Multi-sensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or combination of algorithms. Example :face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency [7].

8. Review of Information Fusion Techniques

Broadly speaking, the term information fusion encompasses any area which deals with utilising a combination of different sources of information, either to generate one representational format, or to reach a decision. This includes: consensus building, team decision theory, committee machines, integration of multiple sensors, multi-modal data fusion, combination of multiple experts/classifiers, distributed detection and distributed decision making [8] .

In pre-mapping fusion, there are two main sub-categories: sensor data level fusion and feature level fusion. In post-mapping fusion, there are also two main sub-categories: score level fusion and decision fusion.

8.1 Pre-mapping Fusion

8.1.1 Sensor Data Level

It combines the biometric characteristics from different sensors to get a compound result for processing.

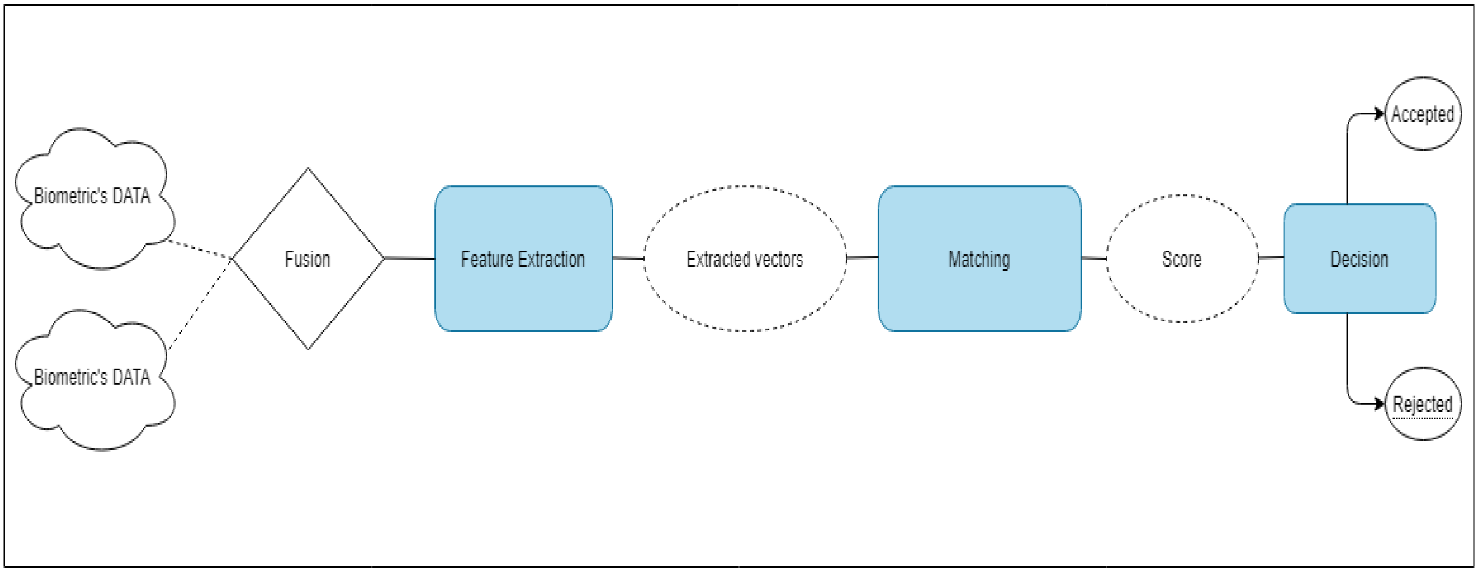


Figure 8-11 Sensor level fusion

8.1.2 Feature level Fusion

Data coming from different sensors first pre-processed and features are extracted independently of this data [9], and then these results are combined to get a compound feature vector.

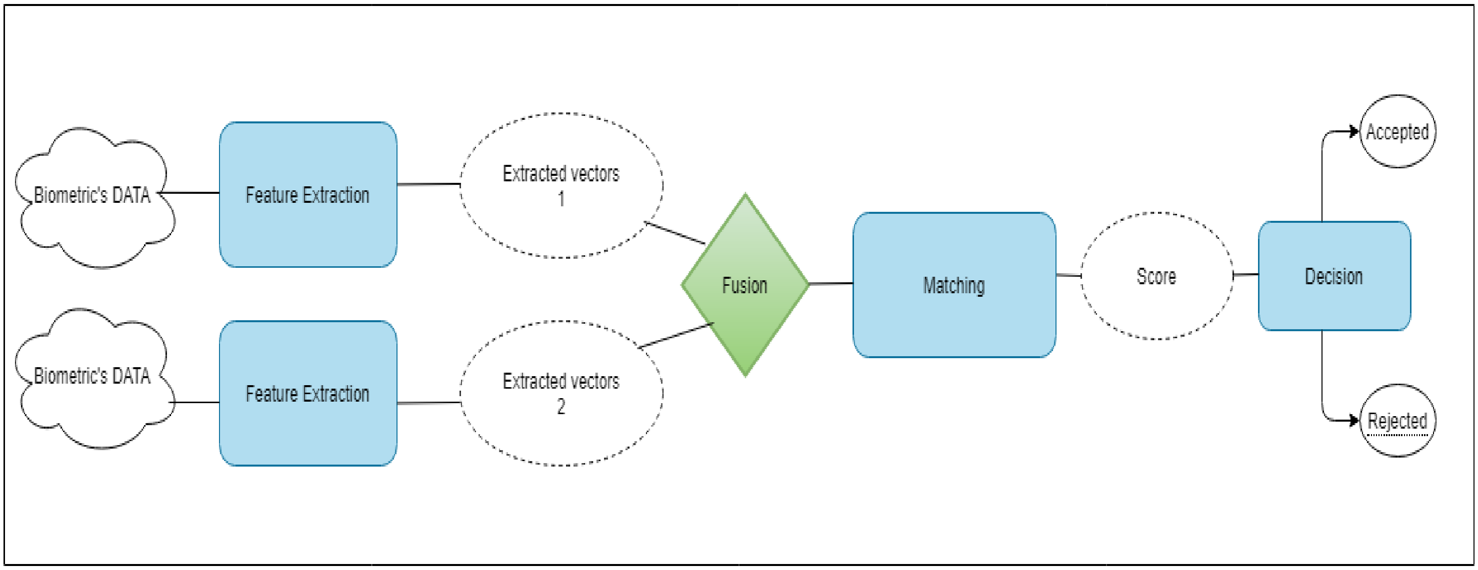


Figure 8-1 Feature extraction fusion level

8.2 Post-Mapping Fusion

8.2.1 Matching score level fusion

In this fusion level instead of combining feature vectors, they processed separately. After those scores are individually found and based on that, accuracy is measured.

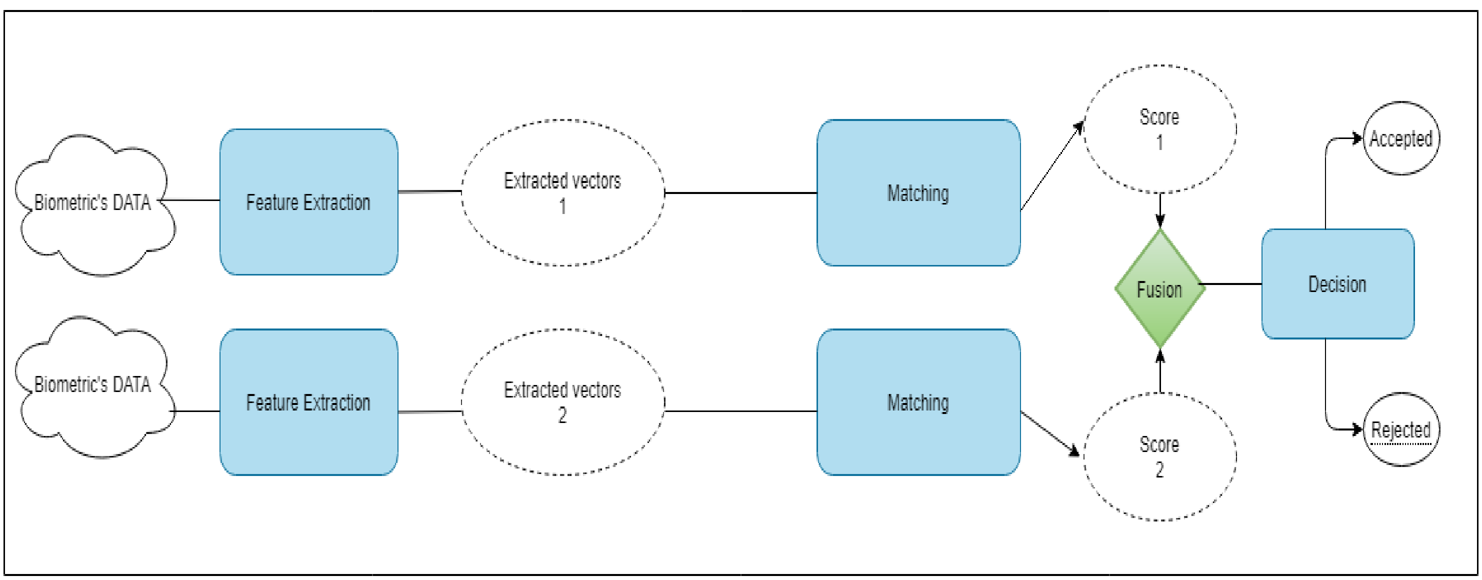


Figure 8-2 Matching score level fusion

The common methods used in matching score level fusion are:

Summation with the equation below:

$$S = \sum_{i=1}^{n} S(i)$$

Product with the equation below:

$$S = \prod_{i=1}^{n} S(i)$$

Minimum with the equation below:

$$S = Min\ S(i)$$

Maximum with the equation below:

$$S = Max\ S(i)$$

8.2.2 Decision level fusion

In this fusion level, each characteristic are firstly processed individually and then fusion takes place at decision level module.

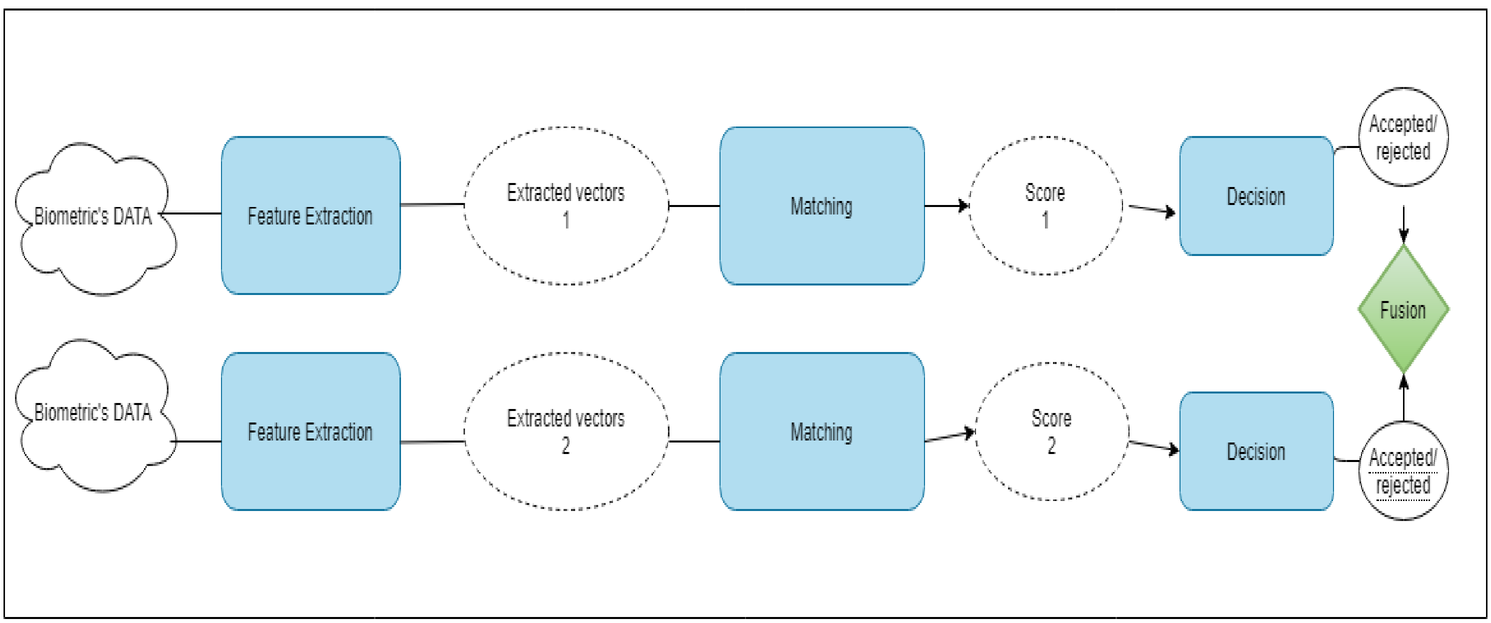


Figure 8-3 Decision level fusion

9. Feature extraction descriptors

9.1 Binarized Statistical Image Features (BSIF descriptor)

The binarized statistical image features (BSIF) is a descriptor proposed by Kannala and Rahtu [10], which does not use a manually predefined set of filters. Instead, it learns the filters using the statistics of natural images. BSIF is among the best texture descriptors for face recognition and texture classification applications [11].

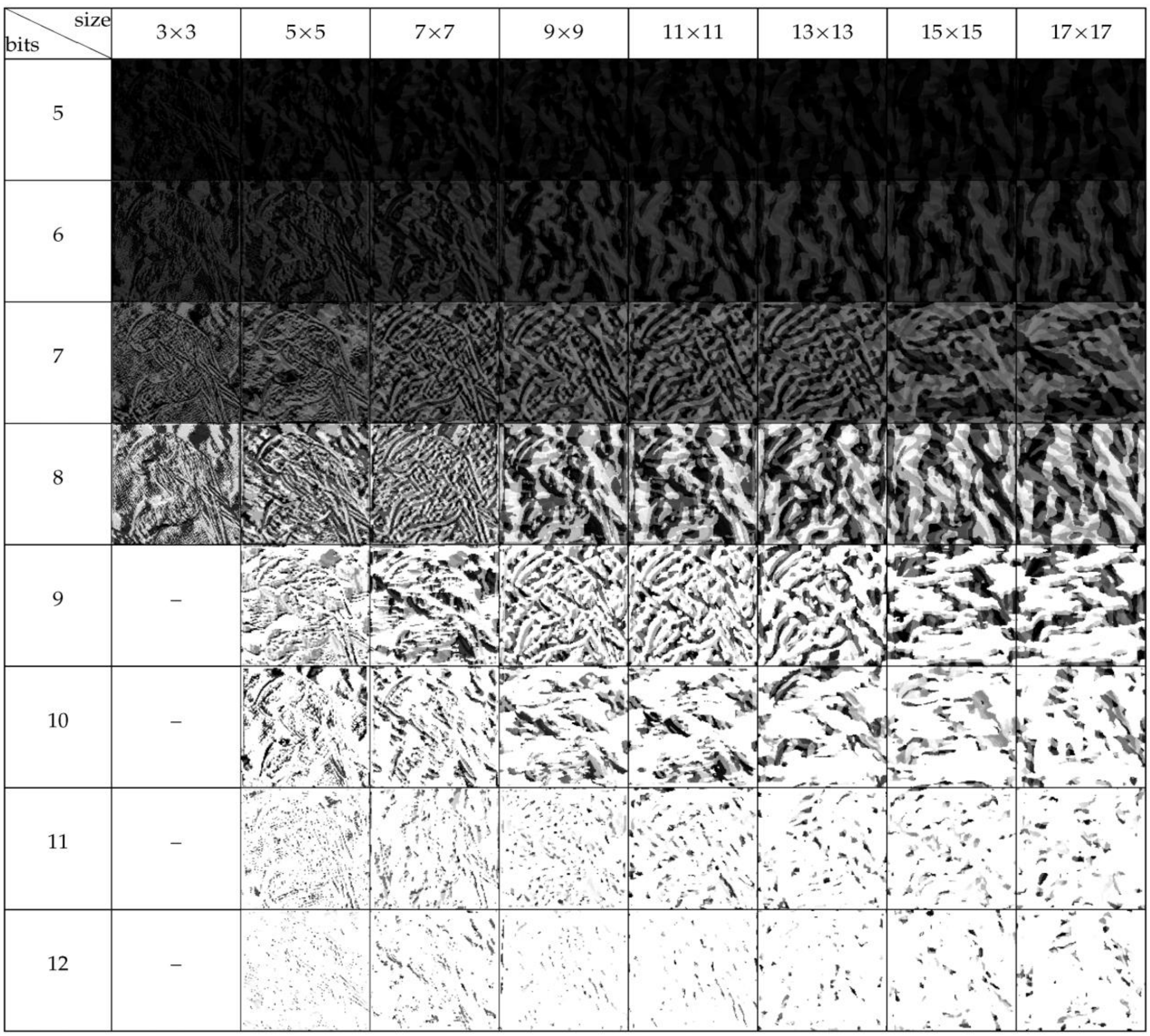


Figure 9-1 BSIF code images at different scales

9.2 Three-Patch Local Binary Patterns (TPLBP Descriptor)

Wolf et al. [12] proposed a family of LBP-related descriptors designed to encode additional types of local texture information. While variants of LBP descriptor use short binary strings to encode information about local micro-texture pixel-by-pixel, the authors considered capturing information which is complementary to that computed pixel-by-pixel. These patch-based descriptors are named Three-Patch LBP (TPLBP) and Four-Patch-LBP (FPLBP). TPLBP considers a w X w patch centered on a pixel and and S additional patches distributed uniformly on a ring of radius r around it, as illustrated in Figure 9-2. For an angle a, we get a set of neighboring patches along a circle and compare their values with those of the central patch. More specifically, the TPLBP is given by:

$$TPLBP_{r,S,w,\alpha}(p) = \sum_{i=0}^{S} f\left(\sigma\left(C_i, C_p\right) - \sigma\left(C_{i+\alpha \bmod S}, C_p\right)\right). 2^i$$

Where

$$f(xt) = \begin{cases} 1, & if\ t \geq \tau \\ 0, & otherwise \end{cases}$$

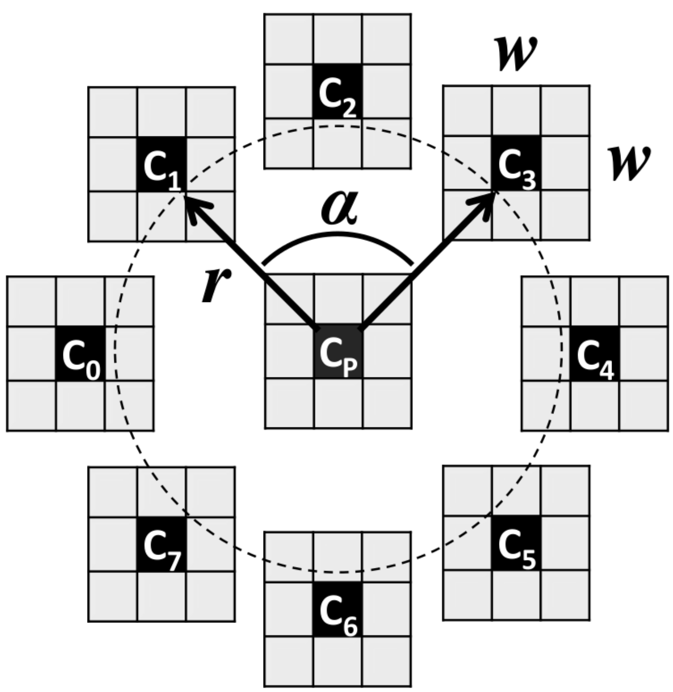


Figure 9-2 The Three-Patch LBP code with a = 2, w = 3 and S = 8

10. Conclusion

This chapter presents the biometric technologies which the performance evaluation is done by performing many genuine and impostor comparisons and analyzing produced similarity scores or match decisions. Very few people have difficulties using biometric systems, so these few people have huge impact on estimated biometric performance. It is easy to tamper results by omitting them.

Besides that, fusion in multimodal system can be an extremely great idea in term of accuracy and better performance by using a specific descriptors and precise techniques such as PCA and LDA.

1. Introduction

In this chapter, we will explain on how our proposed system works to identify people through their fingers knuckle. The current work describe many experiments which some algorithms and processes have been used such as BSIF descriptor and PCA for dimension reduction process.

We collected the couple two areas Minor and major from both right index and right middle finger's back-surface to work on. However our works is based on fusions between the mentioned areas at several levels in our case feature extraction level and feature extraction and score level at a time

In addition, we experienced a feature extraction in unimodal system as well as the multimodal system for the promising areas that we mentioned before.

The intent behind this study is to suggest and provide another dependable FKP method to be applied for better authentication.

2. Background

2.1 Region of Interest

Specific algorithms are applied in ROI extraction process , the available one is based on Convex Direction Coding (CDC), in our case we only extracted both area of finger's knuckle minor and major for both fingers (index and middle).

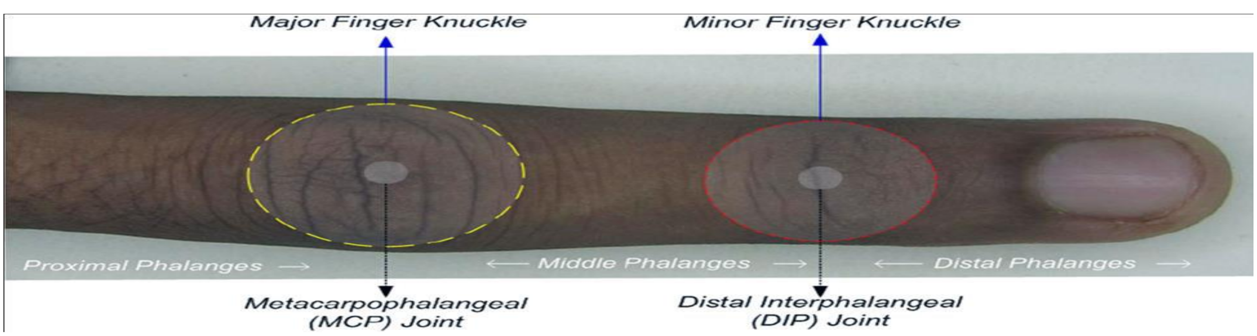


Figure 2-1 Region of interest [15]

2.2 BSIF Descriptor

Differently from previous descriptors, which operate on pixels, BSIF works on patches of pixels. Given an image patch X of size l x l pixels and a linear symmetric filter Wi of the same size, the filter response Si is obtained computing the following expression [10]:

$$S_i = \sum_{u,w} W_i(u,v)X(u,v) = W_i^T x,$$

Where vectors w and x contain the pixels of Wi and X, respectively. The binarized feature is acquired using the following function:

$$b_i = \begin{cases} 1, & S_j > 0 \\ 0, & otherwise \end{cases}$$

2.3 Principal Component Analysis (PCA)

Principal component analysis (PCA) is a technique used for identification of a smaller number of uncorrelated variables known as principal components from a larger set of data. The technique is widely used to emphasize variation and capture strong patterns in a data set. Invented by Karl Pearson in 1901, principal component analysis is a tool used in predictive models and exploratory data analysis. Principal component analysis is considered a useful statistical method and used in fields such as image compression, face recognition, neuroscience and computer graphics [13].

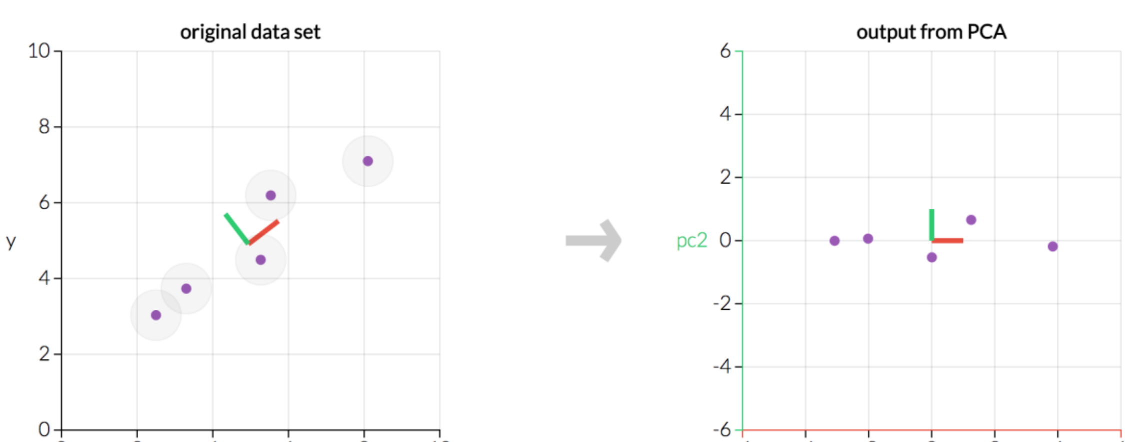


Figure 2-2 Example of principal component analysis

2.4 Linear Discriminant Analysis (LDA)

Linear discriminant analysis (LDA) is a type of linear combination, a mathematical process using various data items and applying functions to that set to separately analyze multiple classes of objects or items. Flowing from Fisher's linear discriminant, linear discriminant analysis can be useful in areas like image recognition and predictive analytics in marketing [14].

Under Linear Discriminant Analysis, we are basically looking for:

- Which set of parameters can best describe the association of the group for an object?
- What is the best classification preceptor model that separates those groups?

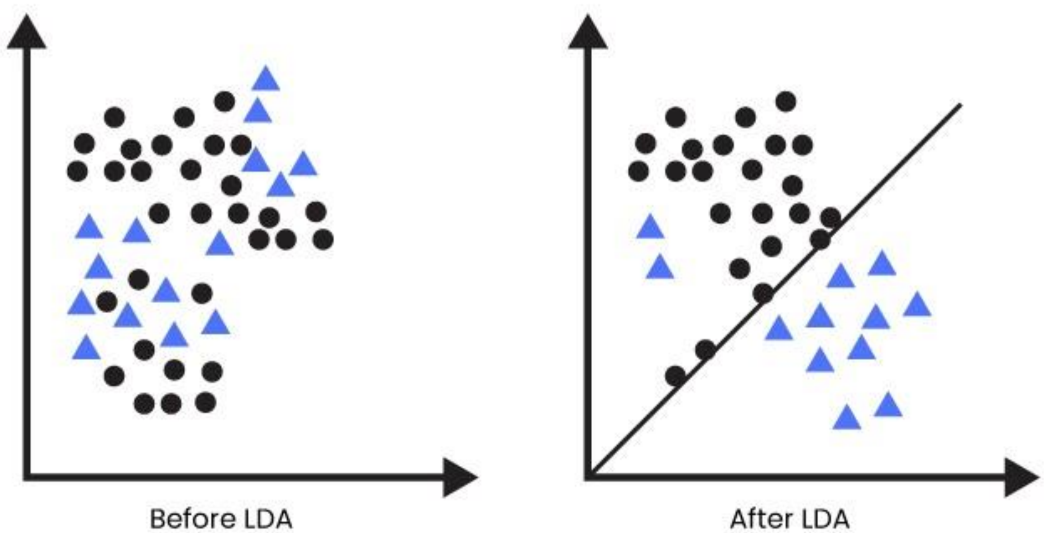


Figure 2-3 Example of LDA

3. Proposed Methods

3.1 Fusion at feature extraction level

3.1.1.1 Architecture of the feature extraction fusion level

The figure 3-1 below the proposed model architecture.

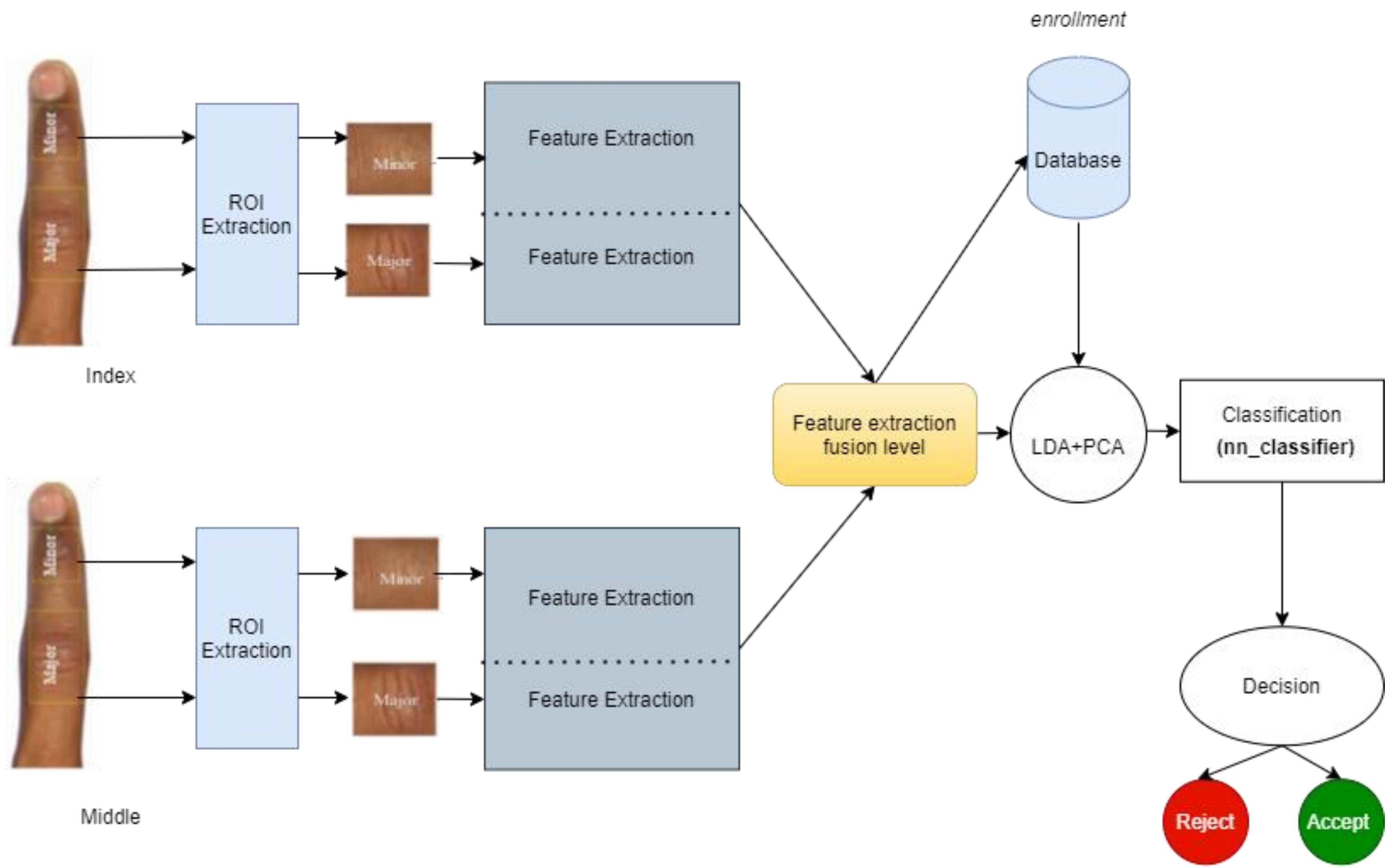


Figure 3-1 Architecture of fusion descriptor level

3.1.2 FKP database

For all experiments, we use the ROI images from Poly-U FKP database contributed from male and female volunteers, we pick right index finger and right middle finger along with each of their minor and major areas already extracted. 3560 images in each of the four files. 712 people has five taken pictures in a different angles, all these images are available in bitmap format.

3.1.3 Feature extraction

In this step, we apply the BSIF descriptor ,we pick a particular filter ICAtextureFilters_17x17_12bit duo to his high identification RANK-1 (%) and low equal error rate (%) according to [15] .however the mentioned descriptor has been applied on both minor and major of both right index and right middle fingers.

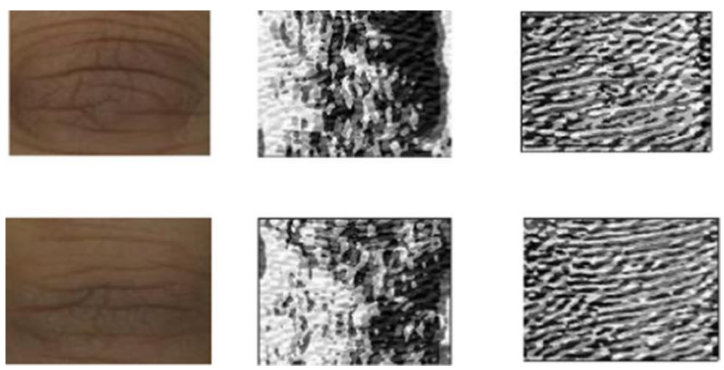


Figure 3-2 Samples of the major and minor ROI image with tier outputs BSIF filter of a size 17×17 and of length 11 and 12bits [15]

3.1.4 Feature extraction fusion

The next step is a fusion between all extracted vectors from the previous step, which includes major and minor of both right index and right middle fingers.

3.1.5 Dimension reduction

In this step, we use principal PCA and LDA as dimensionality reduction techniques, their work is to perform on large vectors with high dimensions before matching stage.

3.1.6 Evaluation protocol

FKP identification consist on matching process, in our study we took the first three pictures (n=1..3) for training model and the rest for test model (n=4..5).

3.1.7 Enrollment

In the upcoming procedure, the data is stored for a later matching step.

3.1.8 Classification

The NN classifier (nearest neighbor) is applied from PhD tool for classification phase, the function takes five parameters (trained model, trained identifiers, data for the test, ids results, 'match type'). Classified by calculating the distance to the nearest training case, the sign of that point then determines the classification of the sample.

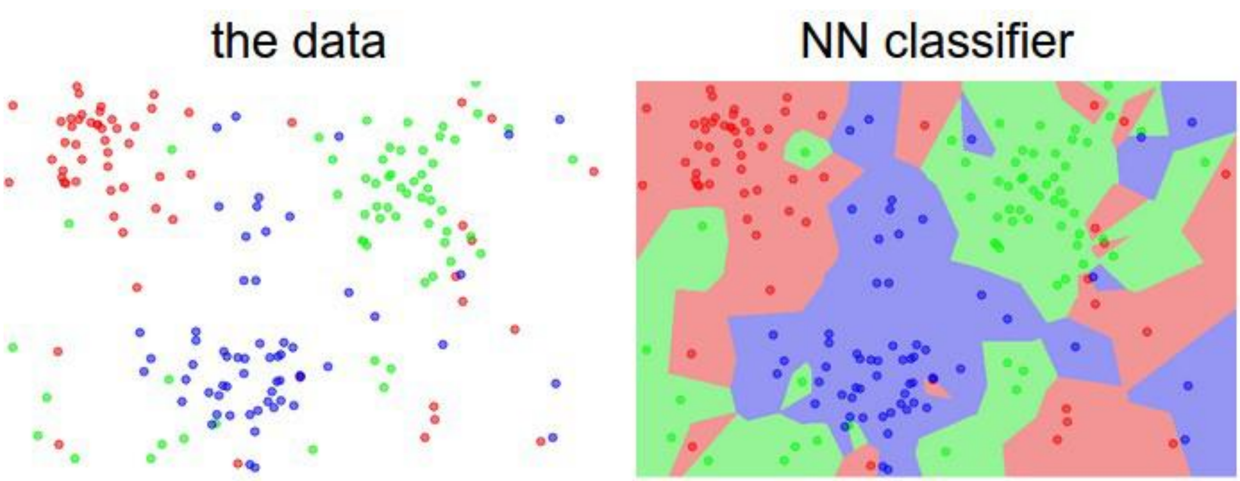


Figure 3-3 Demonstration on NN classifier

3.1.9 Decision

At last, a decision must be made in order to accept or reject person however it depend on matching phase results.

3.2 Fusion at feature extraction and matching score level at a time

All of the steps at the feature extraction level fusion are almost the same the changes happens in feature extraction phase in addition of fusion at score matching level using different rules.

3.2.1 Architecture of the feature extraction fusion level

The figure 3-4 below show the proposed model architecture.

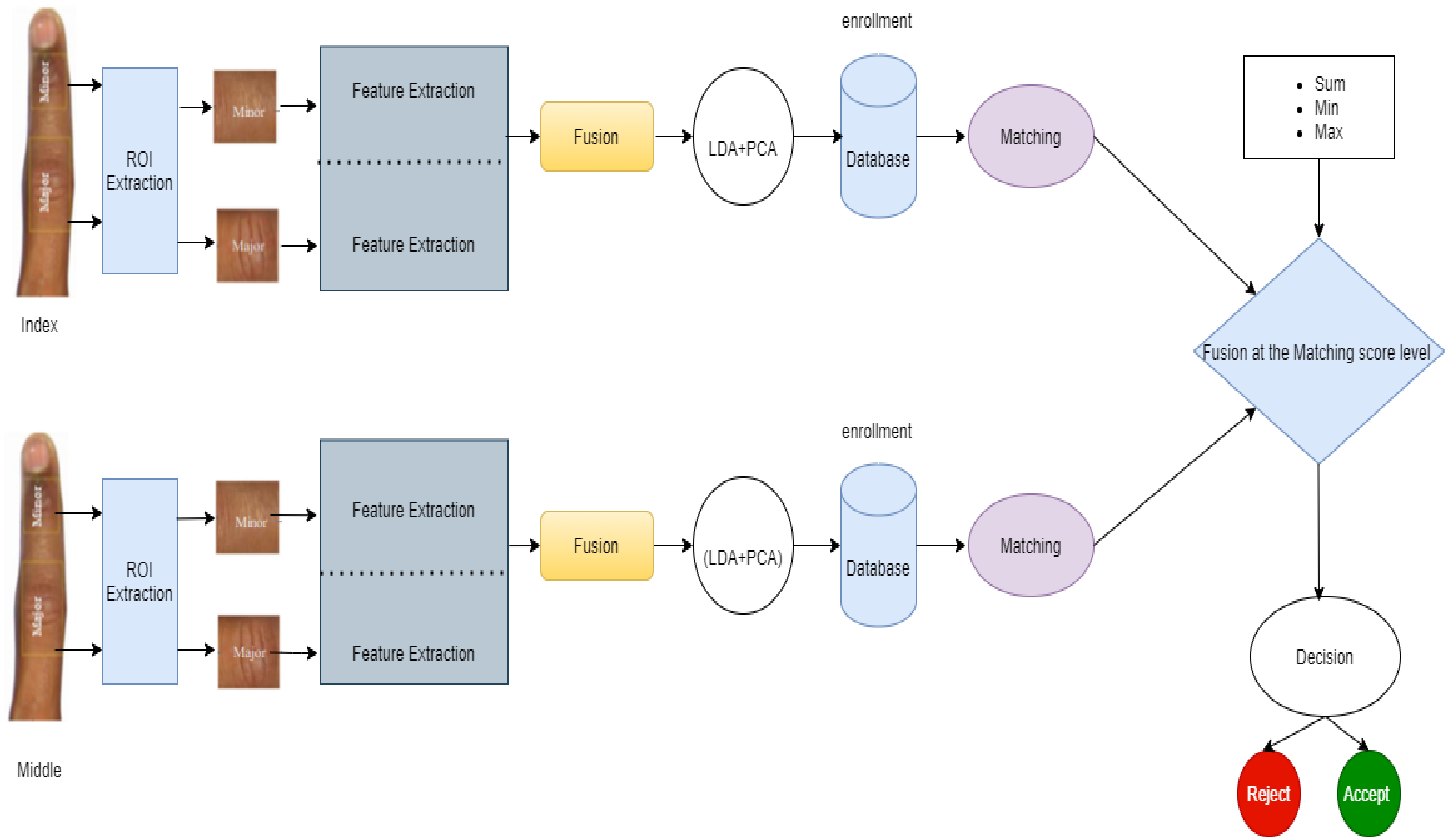


Figure 3-4 Descriptor & score fusion at a time fusion

3.2.2 Feature extraction fusion

In this step, we merge each of the extracted vectors from minor and major of the right index finger and same for the extracted vectors of minor and major of the right middle finger separately.

3.2.3 Data Matching

Matching the previous extracted features to the stored model in the system's database allows us to define divergence level.

3.2.4 Classification

In this step, each one of the merged vectors that has already passed by dimension reduction phase will be classified using "NN_classfier" which calculate the distance to the nearest training case, the sign of that point then determines the classification of the sample.

3.2.5 Score matching level fusion

SUM, MIN and MAX Rules have been applied at score level fusion in order to achieve better accuracy to the proposed FKP authentication system.

There are several matching score fusion rules integrate normalized matching scores of a user to produce the final matching score [16], [17], [18].

- Simple Sum rule: The Simple Sum rule takes the sum of the R matching scores of the (k)th user as the final matching score Sk of this user. Sk is calculated as follows:

$$S = \frac{1}{N}\sum_{i=1}^{N} S_i$$

- The minimum rule: This rule simply sets a new scores as the minimum score of each matcher's scores, is calculated as follows:

$$S = Min\ S(i)$$

- The maximum rule: This rule simply sets a new scores as the maximum score of each matcher's scores, is calculated as follows:

$$S = Max\ S(i)$$

3.2.6 Decision

At last, a decision must be made in order to accept or reject person however it depend on matching phase results.

4. Conclusion

This chapter has shown a background on how BSIF works also PCA & LDA. However this chapter explains the main steps in details using BSIF descriptor and score level rules SUM, MIN & MAX and merging in different levels, many factors are indeed shown great results such as rank identification, FAR and FFR values, therefore the experimented results which we shall discuss in the next chapter are satisfying in terms of accuracy and performance

1. Introduction

The current chapter represent a collection of the experimented results from the proposed methods for FKP authentication system in the previous chapter.

Our work consist on having a high rank identification and a low error rate values ,even so the unimodal and multimodal systems are experimented at first then we operate on multimodal system only , fusion between two particular areas of the fingers in which we propose for the work. The results for both proposed methods are demonstrated separately.

2. Development tools

2.1 Matlab R2020a

MATLAB (matrix laboratory) is a proprietary multi-paradigm programming language and numeric computing environment developed by MathWorks. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages. Although MATLAB is intended primarily for numeric computing [19].

2.2 PhD tools

The PhD (Pretty helpful Development functions for) face recognition toolbox is a collection of Matlab functions and scripts intended to help researchers working in the field of face recognition. The toolbox was produced as a byproduct of owner's research work and is freely available for download. The PhD toolbox includes implementations of some of the most popular recognition techniques, such as Principal Component Analysis (**PCA**), Linear Discriminant Analysis (**LDA**), Kernel Principal Component Analysis (**KPCA**), Kernel Fisher Analysis (**KFA**). It features functions for **Gabor** filter **BSIF** filter...etc, and all other necessary tools [20].

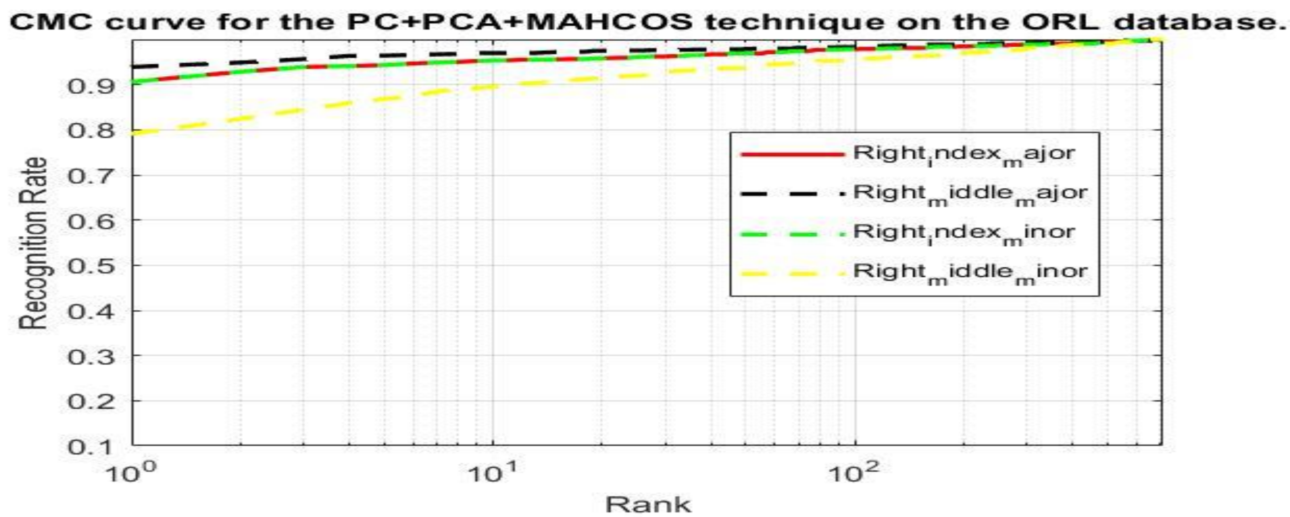
3. Obtained Results of Unimodal Minor-Major

The table below demonstrates the identification and verification rate of Minor-Major modalities of both index and middle fingers at feature extraction level using BSIF descriptor.

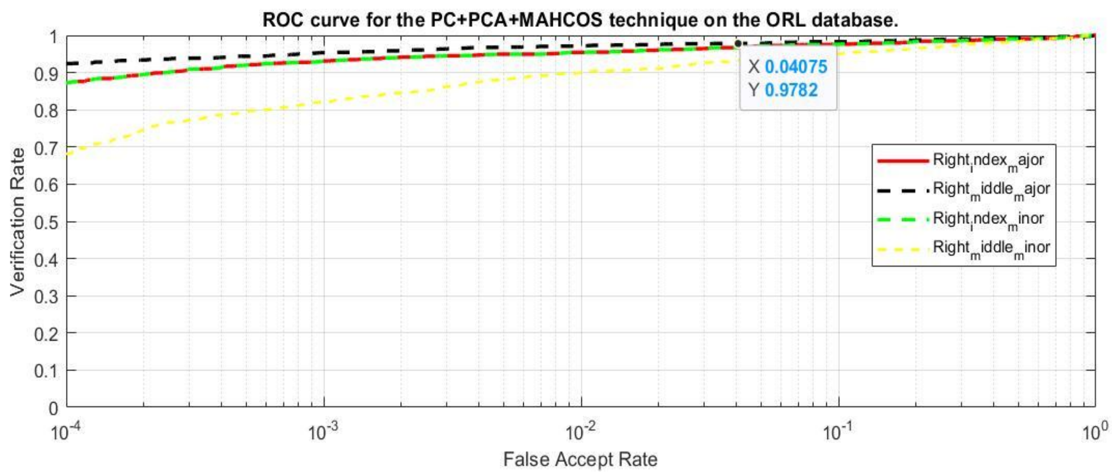
Modality	Identification	Verification				
	Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Right_index_minor	72.26	8.08	6.85	85.81	75.07	59.34
Right_index_major	**90.59**	3.30	2.73	95.44	93.12	86.94
Right_middle_minor	79.07	5.89	5.17	89.96	82.09	67.89
Right_middle_major	**93.89**	2.26	**1.81**	97.19	95.37	92.35

Table 3-1 Finger modalities results

From table 3-1, we found the highest identification rate on the major modality for both index and middle fingers with Rank1%= 90.59 and Rank1%=93.89 respectively, and we also notice the lowest **HTER** value on major modality of the right middle finger.



(a)



(b)

Figure 3-1 Performance measures of finger modalities with BSIF Descriptor

(a): CMC Curve of minor & major of both index and middle fingers
(b): ROC Curve of minor & major of both index and middle fingers

The figure 3-1 above illustrates both CMC & ROC curves of minor and major modalities (index and middle fingers).

We can notice from both CMC & ROC (a, b) curves that the black which is the major modality of the middle finger has the highest value therefore it is the best for now in term of identification and verification rate.

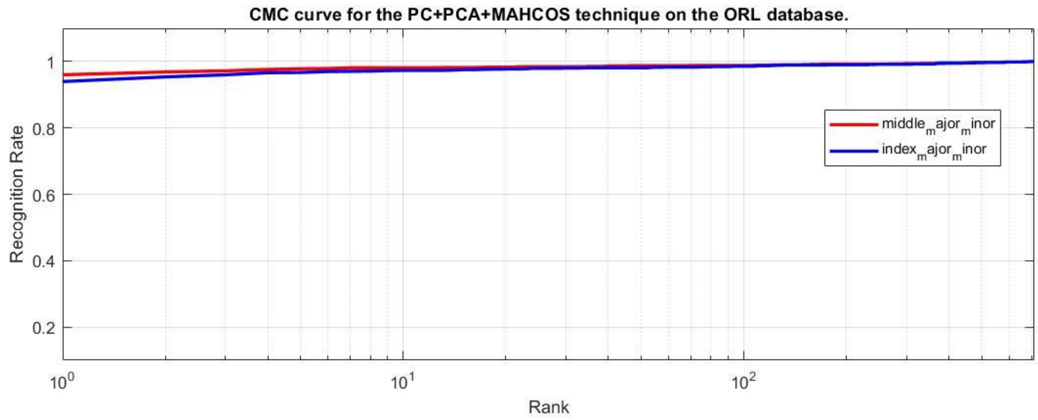
4. Obtained Results of Multimodal Fusion Minor-Major

The table below demonstrates the identification and verification rate of the multimodal fusion between each of minor and major modalities of both right index & middle fingers only at feature extraction level using BSIF descriptor.

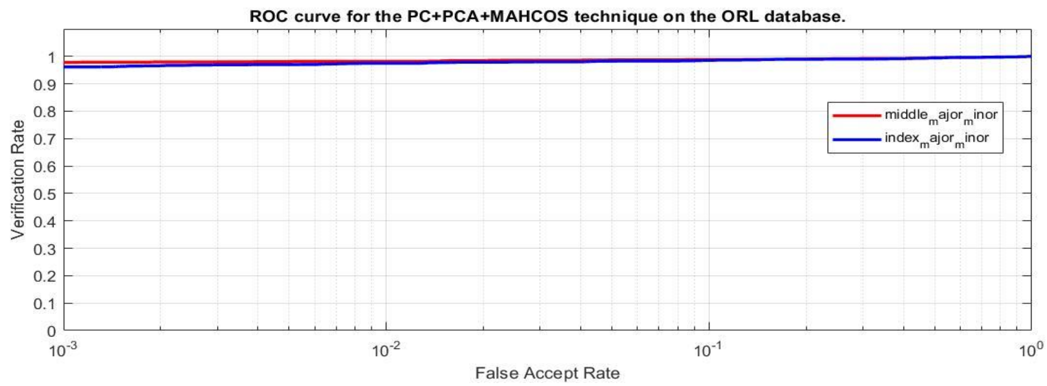
Modality	Identification	Verification				
	Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Right_index_minor Right_index_major	93.96	2.10	1.68	97.47	96.14	91.29
Right_middle_minor Right_middle_major	**96.00**	**1.55**	**1.11**	98.17	97.82	94.73

Table 4-1 Results of Multimodal Fusion

From table 4-1, we found the highest identification rate on the fusion between minor & major modality of middle finger with Rank1%= 96.00 and with low value of EER & HTER “1.55, 1.11” respectively.



(a)



(b)

Figure 4-1 Performance measures of modalities fusion with BSIF Descriptor

(a): CMC Curve of the fusion between minor & major of both fingers
(b): ROC Curve of the fusion between minor & major of both fingers

The figure 4-1 above illustrates both CMC & ROC curves of fusion between minor and major modalities (index and middle fingers).

We can notice from both CMC & ROC (a, b) curves that the Red which refer to minor and major fusion of index finger has the highest value therefore multimodal fusion is performant in term of identification and verification processes.

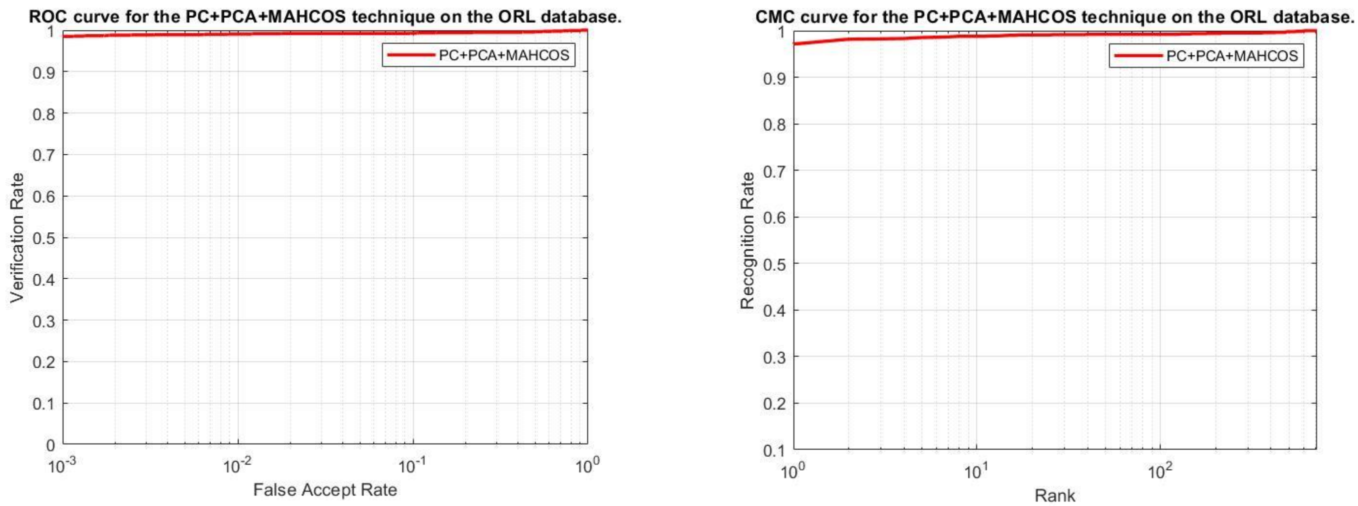
5. Obtained Results of Fusion at Feature extraction Level

The table below demonstrates the identification and verification rate of a multimodal fusion of both right index and right middle fingers, merging all of their minor and major modalities

Modality	Identification	Verification				
	Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Right_index_minor Right_index_major + Right_middle_minor Right_middle_major	**97.12**	**0.91**	**0.69**	99.09	98.53	96.84

Table 5-1 Results of Fusion at Feature extraction Level

From table 5-1, we found a high record of identification rate on the fusion between all of minor & major modalities of both fingers with Rank1%= 97.12 and with low value of EER & HTER “0.91, 0.69” respectively.



(b) (a)

Figure 5-1 Performance measures of modalities fusion at descriptor level

(a): CMC Curve of the fusion between all of minor & major of both fingers
(b): ROC Curve of the fusion between all of minor & major of both fingers

The figure 5-1 above illustrates both CMC & ROC curves of fusion at descriptor level with minor and major modalities (from index and middle fingers).

We observe a high recognition rate beside high verification rate almost 1 in the fusion at descriptor level only.

6. Obtained Results of fusion at feature extraction level and Matching Score level at a time

The experimented results below are acquired from fusion of both Minor-major of the index and middle fingers at feature extraction level and matching score level at a time, using BSIF descriptor and with different rules Sum, Max, and Min respectively.

6.1 Results of Sum Rule-based Fusion

The table 6-1 below demonstrates the identification and verification rate of a fusion at two levels. First at **feature extraction level** using **BSIF** descriptor then at **matching score level** using **SUM-rule** respectively.

	Modality	Identification	Verification				
		Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Sum-Rule	Right_index_minor Right_index_major + Right_middle_minor Right_middle_major	**97.12**	**1.17**	**0.78**	98.81	98.31	97.05

Table 6-1 Results of Sum Rule-based Fusion

Table 6-1 show a high identification rate Rank1%=97.12, beside low EER & HTER “1.17, 0.78” respectively, which means sum-rule is very performant and effective on score matching level.

6.2 Results of Max Rule-based Fusion

The table 6-2 below demonstrates the identification and verification rate of a fusion at two levels. First at **feature extraction level** using **BSIF** descriptor, then at **matching score level** using **MAX-rule** respectively.

	Modality	Identification	Verification				
		Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Max-Rule	Right_index_minor Right_index_major + Right_middle_minor Right_middle_major	**96.14**	**1.76**	**1.30**	97.96	97.26	96.07

Table 6-2 Results of Max Rule-based Fusion

Table 6-2 show a high identification rate Rank1%=96.14, beside low EER & HTER “1.76, 1.30” respectively, which means max rule is performant and effective also on score matching level.

6.3 Results of Min Rule-based Fusion

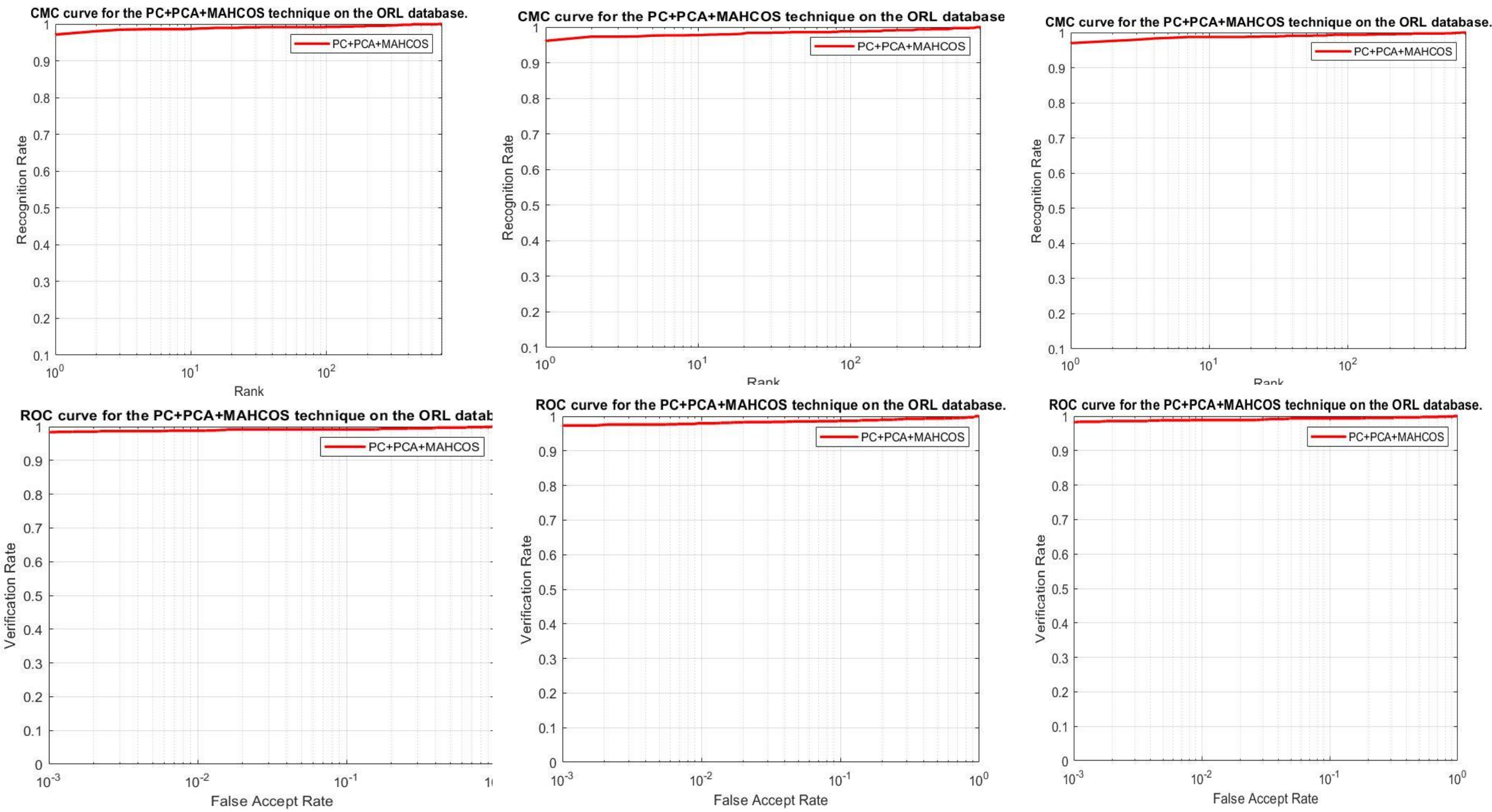
The table 6-3 below demonstrates the Minimum rule of the fusion between all of minor and major modality of both right index & middle fingers at descriptor level and score level at a time, with their identification and verification rate featured using BSIF descriptor.

	Modality	Identification	Verification				
		Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Min-Rule	Right_index_minor Right_index_major + Right_middle_minor Right_middle_major	**96.98**	**1.12**	**0.79**	98.88	98.24	95.72

Table 6-3 Results of Min Rule-based Fusion

Table 6-3 show a high identification rate Rank1%=96.98, beside low EER & HTER “1.12, 0.79” respectively, which means Min rule is performant and effective as well on score matching level.

(a) (b) (c)



(Sum-Rule) (Max-Rule) (Min-Rule)

Figure 6-1 CMC & ROC curves obtained from descriptor-score fusion with different rules

(a): CMC & ROC Curves obtained from descriptor-score fusion with Sum-Rule
(b): CMC & ROC Curves obtained from descriptor-score fusion with Max-Rule
(c): CMC & ROC Curves obtained from descriptor-score fusion with Min-Rule

The figure 6-1 above show all CMC & ROC curves of fusion at descriptor-score level at a time with different matching score rules Sum, Max and Min (a),(b),(c) respectively .We can notice that CMC curves are very close at a high recognition rate beside a high verification rate almost 1. While ROC curves has just small difference in values , sum and min rules are very close in verification rate unlike max-rule which has a little less verification rate compared to the other rules.

7. Contrasting differences and similarities between both methods

The table 7-1 below demonstrates a contrasting differences and similarities between both proposed methods using BSIF descriptor.

Methods	Identification	Verification				
	Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Fusion at feature extraction & matching-score level at a time with the SUM-rule	**97.12**	**1.17**	**0.78**	98.81	98.31	97.05
Fusion at feature extraction level	**97.12**	**0.91**	**0.69**	99.09	98.53	96.84

Table 7-1 Differences and similarity between both proposed methods

The following figure 7-1 shows a contrasting differences and similarities between both proposed methods.

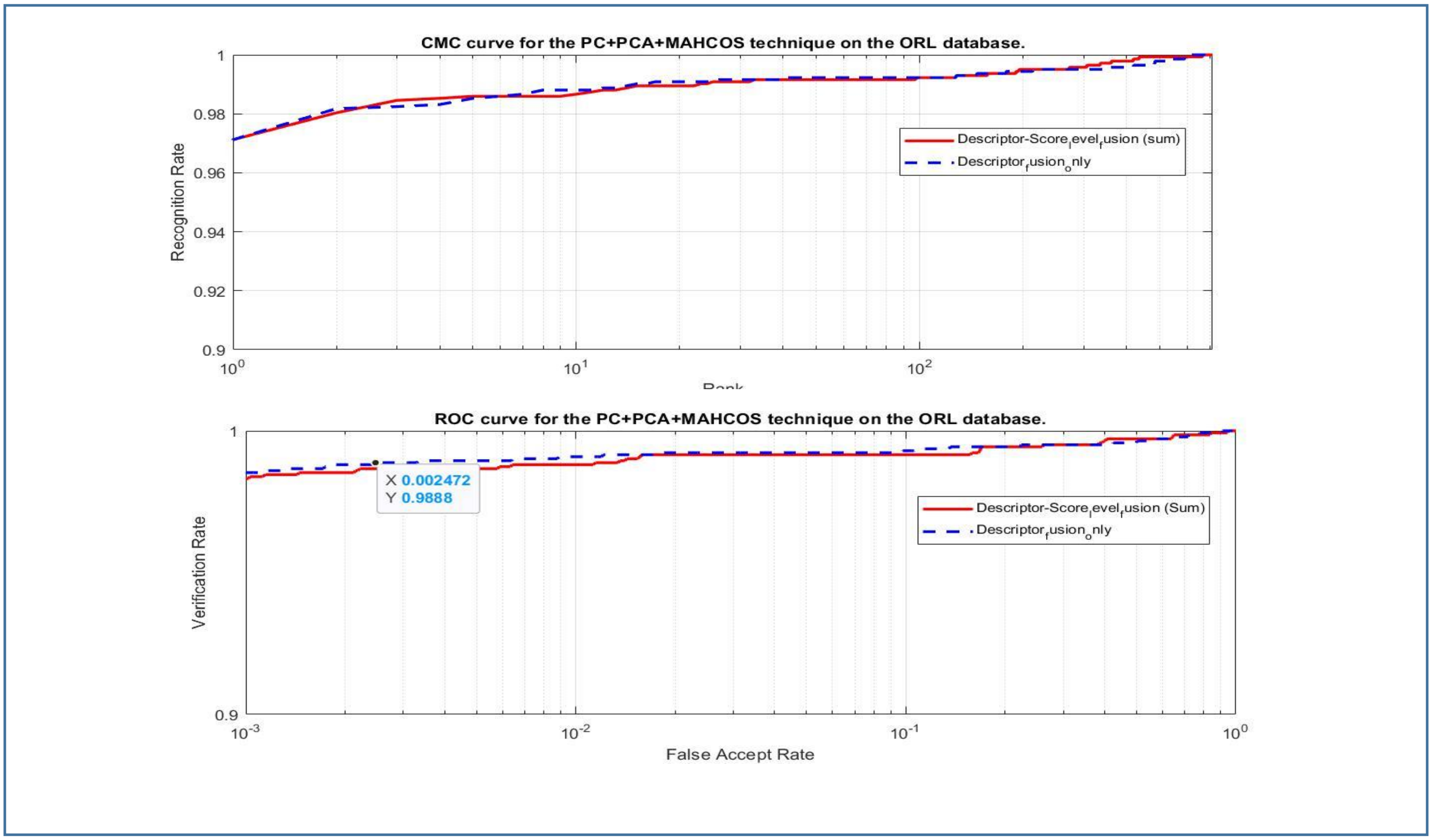


Figure 7-1 CMC & ROC curves for contrasting differences and similarities between both proposed methods

The figure 7-1 above show CMC & ROC curves for contrasting differences and similarities between both proposed methods. We can notice that CMC curves are almost the same with high recognition rate 97.12% beside high verification rate which we can see a small difference between both methods. Unlike fusion at feature extraction-score level at a time (sum-rule) the fusion at extraction level only has low EER & HTER.

8. Comparative Study

In order to evaluate the effectiveness of the achieved results of our proposed methods, we conducted a comparative study with two similar works proposed by N.Chalabi,A.Attia,A.Bouziane [21] and also D.Thapar,G.Jaswal,A.Nigam [22] the results are shown in Table 8-1.

Methods	Identification	Verification				
	Rank 1%	EER%	HTER %	VAR@1 %	VAR@0.1 %	VAR@0.01%
Fusion at feature extraction & matching-score level at a time with the SUM-rule	**97.12**	**1.17**	**0.78**	98.81	98.31	97.05
Fusion at feature extraction level	**97.12**	**0.91**	**0.69**	99.09	98.53	96.84
N.Chalabi,A.Attia,A.Bouziane [21]	93.44	2.59		96.62		
D.Thapar,G.Jaswal,A.Nigam [22]	94.83	2.22				

Table 8-1 Performance for different methods

From Table 8-1, we can observe that our proposed methods performance are better from the other works. However the identification rate is remarkably high than the others.

9. Discussion

At last, the results were satisfying in both proposed methods, therefore fusion at feature extraction-matching score level at a time using BSIF descriptor & max and min rules has just little less results compared to the same fusion using sum-rule, which this last one has the highest identification value among them. Additionally the fusion at feature extraction level only using BSIF descriptor was very accurate and provides better performance.

10. Conclusion

In this chapter, we made the comparison between results of unimodal and multimodal biometric systems, unlike unimodal biometric system the multimodal showed better results in term of identification and verification rate. Therefore in term of accuracy we recommend using multimodal biometric system.

The experimented results showed that fusion at feature extraction & matching-score level at a time with the SUM-rule improves the performance of the system as well as the fusion at feature extraction level only with the proposed descriptor BSIF.

The obtained results of the fusion at feature extraction & matching-score level at a time, and the fusion at feature extraction level were the same with 97.12% identification rate, the main difference was in EER & HTER values.

General Conclusion

Biometrics is a rich scientific field which study the biology and metrics, or measurement, especially for the purpose of identifying individuals based on unique characteristics. Among them the finger knuckle print which can be very interesting in the future in term of better accuracy or performance compared to fingerprint.

Multimodal fusion of fingers modalities can be very effective and more accurate from the use of multiple fingers. The proposed fusion methods with multiple fingers approache clearly performed better than approaches of a single finger.

In the future, we will work on the use of other finger knuckle print databases .And different biometric modalities (Face and Finger vein) as well as the use of other fusion level like sensor and decision levels.

References

[1] I. M. Alsaadi, "Study On Most Popular Behavioral Biometrics,Advatages,Disadvantages And Recent Application : A Review," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,* vol. 10, no. 01, p. 7, 2021.

[2] V. A.S.Raju, "A Survey on Unimodal, Multimodal Biometrics and Its Fusion Techniques," *International Journal of Engineering & Technology,* p. 7, 2018.

[3] "Biometric Research Lab," [Online]. Available: https://www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm. [Accessed 2021].

[4] S. a. N. W. S. C. Atlantic, "Biometric Systems Application Note," *System Assessment and Validation for Emergency Responders,* p. 23, June 2015.

[5] Z. R. Jan Loeschner, "BIOPASS Study on Automated Biometric Border Crossing Systems for Registered," 2007.

[6] B. H. R. G. M. P. C. R. F. Cherifi, "Performance Evaluation Of Behavioral Biometric," *GREYC Laboratory,* 2014.

[7] V. L. K. K. R. K. K.Sasidhar, "MULTIMODAL BIOMETRIC SYSTEMS STUDY TO IMPROVE ACCURACY AND PERFORMANCE," *International Journal of Computer Science & Engineering Survey,* vol. 1, no. 2, p. 8, 2010.

[8] C. S. a. K. K. Paliwal, "Information Fusion and Person Verification Using Speech & Face Information," IDIAP Research, Queensland 4111, 2002.

[9] M. M. Kulkarni, "Study of Multimodal Biometric System: A Score Level Fusion Approach," *International Journal of Engineering Research & Technology,* vol. 3, p. 4, 2014.

[10] J. R. Kannala, "Bsif: Binarized statistical image features," in *In Proceedings of the 2012 21st International Conference on Pattern Recognition (ICPR)*, Tsukuba, 2012.

[11] Y.-A. Hadid.A, "Gender and texture classification: A comparative analysis using 13 variants of local binary patterns," *Pattern Recognition Letters*, 2012.

[12] H. T. Wolf.L, "Descriptor Based Methods in the Wild," 2008.

[13] "techopedia," [Online]. Available: https://www.techopedia.com/definition/32509/principal-component-analysis-pca#. [Accessed 2021].

[14] "Analytic Steps," [Online]. Available: https://www.analyticssteps.com/blogs/introduction-linear-discriminant-analysis-supervised-learning. [Accessed 2021].

[15] Z. A. Y. C. Abdelouahab Attia, "Feature-level fusion of major and minor dorsal finger," p. 10, 2020.

[16] S. D. D. S. T. Joshi, "Multimodal biometrics: state of the art in fusion techniques," *International Journal of Biometrics*, vol. 1, no. 4, 2009.

[17] K. N. A. R. A.JAIN, "Score normalization in multimodal biometric systems," *Pattern Recognition*, 2005.

[18] M. M. L. A. a. B. D. S.GARCIA-SALICETTI, "Multimodal biometric score fusion : the mean rule versus support vector classifiers," *Proceeding EUSIPCO*, 2005.

[19] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/MATLAB. [Accessed 2021].

[20] V. ˇ. Struc, Writer, *PhD manual.* [Performance]. University of Ljubljana, 2012.

[21] A. N.Chalabi, "MULTIMODAL FINGER DORSAL KNUCKLE MAJOR AND MINOR PRINT RECOGNITION SYSTEM BASED ON

PCANET DEEP LEARNING," *ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING*, vol. 10, p. 6, 2020.

[22] G. J. N. Daksh Thapar, "FKIMNet: A Finger Dorsal Image Matching Network Comparing Component (Major, Minor and Nail) Matching with Holistic (Finger Dorsal) Matching," *International Joint Conference on Neural Networks,* p. 8, 2019.

[23] Y. K. w. Kim, "Human Body Model using Multiple Depth Camera for Gait Analysis," *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD),* 2018.

[24] "Deepnet security," [Online]. Available: https://deepnetsecurity.com/authenticators/biometrics/typesense/. [Accessed 2021].

[25] "Keesing technologies," [Online]. Available: https://platform.keesingtechnologies.com/retinal-recognition-pros-and-cons/. [Accessed 2021].

[26] "Eter - Biometric technologies," [Online]. Available: http://www.eter.it/en/hand-geometry. [Accessed 2021].

Abstract

Biometrics technologies are becoming the foundation of an extensive array of highly secure identification and personnel verification solution.

Presently, a variety of biometric modalities are applied to perform human identification or user verification for example the UBS and MBS. We have relied on the distinctive finger joint modality. We are introducing a biometric FKP authentication system using knuckle imaging from both index and middle fingers. Several experiments have been presented in our thesis such as an efficient FKP recognition algorithm for feature extraction. BSIF is the applied descriptor, however we did different mergers in different levels for instance fusion in feature extraction level using concatenation, and synchronous fusion in feature extraction and score level using min, max and sum operators.

Keywords: UBS, MBS, FKP, feature extraction, fusion.

ملخص

أصبحت تقنيات القياسات الحيوية أساسًا لمجموعة واسعة من وسائل التحقق من الهوية والتحقق من هوية الموظفين العالية الأمان.

في الوقت الحاضر، يتم تطبيق مجموعة متنوعة من أساليب القياسات الحيوية للتعريف عن الهوية أو التحقق من المستخدم، على سبيل المثال UBS وMBS. لقد اعتمدنا على طريقة مفصل الإصبع المميزة، وقمنا بتصميم نظام مصادقة بيومترية FKP باستخدام صور المفصل من كل من السبابة والإصبع الأوسط. كما قدمنا العديد من التجارب في أطروحتنا مثل خوارزمية التعرف على FKP العالية الفعالية لاستخراج الميزات. BSIF هو الوصف المطبق ، وكذلك قمنا بعمليات اندماج مختلفة في مستويات مختلفة, على سبيل المثال الاندماج في مستوى استخراج الميزات باستخدام التسلسل ، والدمج المتزامن في استخراج الميزات ومستوى النتيجة باستخدام عوامل الحد الأدنى والحد الأقصى والجمع.

كلمات مفتاحية: الدمج، نظام مصادقة بيومترية، الوصف المطبق.

Résumé

Les techniques biométriques sont devenues la base d'une vaste gamme d'outils d'identification et de vérification du personnel hautement sécurisés.

De nos jours, diverses méthodes biométriques sont appliquées pour identifier ou vérifier l'utilisateur, par exemple UBS et MBS. Nous nous sommes appuyés sur l'articulation distinctive du doigt et on avons conçu un système de certification biométrique FKP en utilisant des images de l'articulation de l'index et du majeur. Nous avons également présenté de nombreuses expériences dans notre thèse telles qu'un algorithme de reconnaissance FKP très efficace pour l'extraction de fonctionnalités. BSIF est le descripteur appliquée, ainsi que nous avons fait différentes fusions aux différents niveaux, par exemple la fusion au niveau d'extraction de fonctionnalités en utilisant la séquence, la fusion simultanée dans l'extraction de fonctionnalités et le niveau de score en utilisant des opérateurs min, max et la somme.

Mots-Clés : UBS, MBS, FKP, l'extraction de fonctionnalités, fusion.