Efficient Multimodal Biometric Systems Using Face and Palmprint

Mina Farmanbar

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Eastern Mediterranean University
February 2016
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Cem Tanova
Acting Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Prof. Dr. Işık Aybay
Chair, Department of Computer Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Assoc. Prof. Dr. Önsen Toygar
Supervisor

Examining Committee

1. Prof. Dr. Hasan Demirel
2. Prof. Dr. Aytül Erçil
3. Prof. Dr. Adnan Yazıcı
4. Assoc. Prof. Dr. Önsen Toygar
5. Asst. Prof. Dr. Ahmet Ünveren

ABSTRACT

Multimodal biometric systems aim to improve the recognition accuracy by minimizing the limitations of unimodal systems. Fusion of two or more biometric modalities provides a robust recognition system against the distortions of individual modalities by combining the strengths of single biometrics. This thesis proposes different fusion approaches using two biometric systems namely face and palmprint biometrics. These fusion strategies are particularly based on feature level fusion and score level fusion.

In this thesis, face and palmprint biometrics are employed to obtain a robust recognition system using different feature extraction methods, score normalization and different fusion techniques in three different proposed schemes. In order to extract face and palmprint features, local and global feature extractors are used separately on unimodal systems. Then fusion of the extracted features of these modalities is performed on different sets of face and palmprint databases. Local Binary Patterns (LBP) is used as a local feature extraction method to obtain efficient texture descriptors and then Log Gabor, Principal Component Analysis (PCA) and subspace Linear Discriminant Analysis (LDA) are used as global feature extraction methods. In order to increase the performance of multimodal recognition systems, feature selection is performed using Backtracking Search Algorithm (BSA) to select an optimal subset of face and palmprint features. Hence, computation time and feature dimension are considerably reduced while obtaining the higher level of performance. Then, match score level fusion and feature level fusion are performed to show the effectiveness and accuracy of the proposed methods. In score level

fusion, face and palmprint scores are normalized using tanh normalization and matching scores are fused using Sum Rule method.

The proposed approaches are evaluated on a developed virtual multimodal database combining FERET face and PolyU palmprint databases. In addition, a large database is composed by combining different face databases such as ORL, Essex and extended Yale-B database to evaluate the performance of the proposed method against the existing state-of-the-art methods. The results demonstrate a significant improvement compared with unimodal identifiers and the proposed approaches significantly outperform other face-palmprint multimodal systems.

Furthermore, we propose an anti-spoofing approach which utilizes both texture-based methods and image quality assessments (IQA) in order to distinguish between real and fake biometric traits. In the proposed multi-attack protection method, well-known full-reference objective measurements are used to evaluate image quality including, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity (SSIM), Mean Squared Error (MSE), Normalized Cross-Correlation (NXC), Maximum Difference (MD), Normalized Absolute Error (NAE) and Average Difference (AD). The three types of feature extraction approaches namely Local Binary Patterns (LBP), Difference of Gaussians (DoG) and Histograms of Oriented Gradients (HOG) are employed as texture-based methods to perform spoof detection in order to detect texture patterns such as print failures, and overall image blur to detect attacks.

A palmprint spoof database made by printed palmprint photographs using the camera to evaluate the ability of different palmprint spoof detection algorithms was constructed. We present the results of both face and palmprint spoof detection methods using two public-domain face spoof databases (Idiap Research Institute's PRINT-ATTACK and REPLAY-ATTACK databases) and our own palmprint spoof database.

Keywords: multimodal biometrics, face recognition, palmprint recognition, feature level fusion, match score level fusion, Backtracking Search Algorithm, spoofing, face spoofing detection, palmprint spoofing detection, print-attack, replay-attack.

ÖZ

Birden fazla biyometriğin birleştirildiği sistemlerin amacı, tek bir biyometrik kullanıldığında karşılaşılan zorlukları azaltarak insan tanıma performansını arttırmaktır. Birden fazla biyometriğe dayalı sistemler; her bir biyometrik özelliğin sağladığı güçlü yönleri birleştirirken, zayıf yönlerinin de etkisini gösteremeyeceği daha iyi tanıma performansı sağlarlar. Bu tez, yüz ve avuçiçi biyometriklerini birleştiren farklı kaynaşım teknikleri önermiştir. Kullanılan kaynaşım teknikleri özellikle öznitelik düzeyi kaynaşım ve skor düzeyi kaynaşım yöntemleridir.

Bu tezde önerilen, yüz ve avuçiçi biyometriklerine dayalı üç değişik yaklaşım, birçok öznitelik çıkartıcı yöntem, skor normalizasyonu ve değişik kaynaşım teknikleri kullanmaktadır. Yüz ve avuçiçi özniteliklerini çıkarmak için, yerel ve bütünsel öznitelik çıkartıcı yöntemler yüz ve avuçiçi biyometrikleri üzerinde ayrı ayrı kullanılmıştır. Çıkartılan özniteliklerin kaynaşımı yapılmış ve birçok yüz ve avuçiçi veri tabanları üzerinde uygulanmıştır.

Etkili doku tanımlayıcılarını elde etmek için, Yerel İkili Örüntü (LBP) yaklaşımı, yerel öznitelik çıkartıcı olarak kullanılmıştır. Daha sonra, bütünsel öznitelik çıkartıcı yaklaşım olarak da LogGabor, Ana Bileşenler Analizi (PCA) ve alt-uzay Doğrusal Ayırtaç Analizi (LDA) yöntemleri kullanılmıştır. Yüz ve avuçiçi özniteliklerinin en iyilerini seçmek ve biyometrik sistemin performansını arttırmak için Geriye Dönük Arama Algoritması (BSA) kullanılmıştır. Böylece, yüksek performans elde edilirken, hesaplama süresi ve öznitelik vektörlerinin boyutu azaltılmıştır. Daha sonra, önerilen yaklaşımların başarımını göstermek için, eşleşen skor düzeyi kaynaşım ve öznitelik

düzeyi kaynaşım yöntemleri uygulanmıştır. Skor düzeyi kaynaşımında, yüz ve avuçiçi skorlarına tanh normalizasyonu uygulanmış ve eşleşen skorlar Toplam Kuralı ile kaynaştırılmıştır. Önerilen yaklaşımlar, FERET yüz veritabanı ve PolyU avuçiçi veri tabanı üzerinde değerlendirilmiştir. Ayrıca, ORL, Essex ve Yale-B veri tabanlarını birleştiren büyük bir yüz veritabanı kullanılmış ve literatürdeki diğer yaklaşımlarla önerilen yaklaşım karşılaştırılmıştır. Sonuçlar; önerilen yöntemlerin, tekli tanımlayıcılara kıyasla önemli ilerleme kaydettiğini, diğer yüz ve avuçiçi çoklu sistemlere göre de daha iyi olduğunu göstermektedir.

Bu tezde, ayrıca gerçek ve sahte biyometrik verileri ayırt etmek için, dokuya bağlı yöntemler ve görüntü kalitesini ölçen yöntemler kullanılarak yanıltma karşıtı bir yöntem önerilmiştir. Önerilen çoklu saldırı önleme yönteminde, görüntü kalitesini ölçmek için Doruk Sinyal-Gürültü Oranı (PSNR), Yapısal Benzerlik (SSIM), Ortalama Kare Hatası (MSE), Düzgelenmiş Çapraz İlinti (NXC) , Maksimum Fark (MD), Düzgelenmiş Mutlak Hata (NAE) ve Ortalama Fark (AD) kullanılmıştır. Saldırı sezimi için yazdırma hataları ve imge bulanıklığı gibi doku örtülerini kullanan üç çeşit öznitelik çıkarma yaklaşımı kullanılmıştır. Bu dokuya bağlı yöntemler Yerel İkili Örüntü (LBP), Gauss'ların Farkı (DoG) ve Gradient'lere Yönelik Histagramlar (HOG)'dır.

Farklı avuçiçi yanıltma karşıtı algoritmaları karşılaştırmak için, yazdırılmış avuçiçi fotoğrafları kamerayla çekilip avuçiçi yanıltma veritabanı oluşturulmuştur. Idiap Araştırma Enstitüsü'nün yüz yanıltma veritabanları (PRINT-ATTACK ve REPLAY-ATTACK) ve bizim oluşturduğumuz avuçiçi yanıltma veritabanı kullanılarak yapılan yüz ve avuçiçi yanıltma deneylerinin saptama sonuçları bu tezde sunulmuştur.

Anahtar Kelimeler: Çoklu biyometri, yüz tanıma, avuçiçi tanıma, öznitelik düzeyi kaynaşım, eşleşen skor düzeyi kaynaşım, Geriye Dönük Arama Algoritması (BSA), yanıltma, yüz yanıltma saptama, avuçiçi yanıltma saptama, yazdırma saldırısı, tekrar görüntüleme saldırısı.

ACKNOWLEDGMENT

I would never have been able to complete this dissertation without the help of the people who have supported me with their best wishes.

I would like to express my deepest gratitude and thanks to my supervisor, Assoc. Prof. Dr. Önsen Toygar, for her advice, support and guidance throughout my study at Eastern Mediterranean University. I sincerely thank to the committee members of my thesis defense jury for their helpful comments on this thesis.

Last but not least I would also like to thank my dear parents, my brother, and younger sister for their continuous supports in my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS/ ABBREVIATIONS

PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
LBP	Local Binary Patterns
DoG	Difference of Gaussians
HOG	Histograms of Oriented Gradients
HE	Histogram Equalization
MVN	Mean-Variance Normalization
FERET	Face Recognition Technology
BSA	Backtracking Search Algorithm
FFR	False Fake Rate
FGR	False Genuine Rate
HTER	Half Total Error Rate
MSE	Mean Squared Error
PSNR	Peak Signal to Noise Ratio
AD	Average Difference
MD	Maximum Difference
NAE	Normalized Absolute Error
NXC	Normalized Cross-Correlation
SSIM	Structural Similarity Index Measure
IQA	Image Quality Assessments

Chapter 1

INTRODUCTION

1.1 Biometric Systems

Biometrics refers to understanding the distinguishing characteristics of human beings for the purpose of recognition. A biometric system that measures a physical (e.g., palmprint, face, iris, ear, fingerprint) or behavioral (e.g., gait, signature, handwriting, speech) characteristics of a person is called biometric identifiers (or simply Biometrics) for automatically recognizing individuals. An important issue in designing a biometric system is to determine how an individual is identified. The general structure of a biometric system can be either a verification system or an identification system. Identification answers the question, "Who am I?" while Verification answers "Am I who I claim to be?".

A biometric system makes a personal identification by recognizing an individual based on comparing a specific physiological or behavioral characteristic with a match registered template in a database in a one-to-many comparison process. On the other hand, a personal verification that is known as authentication as well, involves confirming or denying a person's claimed identity by comparing the biometric information with the stored template in a database in a one-to-one comparison process. Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system.

A typical biometric system consists of five modules including:

- Data acquisition which captures the biometric data.
- Pre-processing module that extracts the region of interest (ROI) and normalizes the extracted ROI in respect to size.
- Feature extraction module which computes a set of discriminative features.
- Matching (or classification) module to generate match scores;
- Decision module that finally makes a decision.

Several main requirements and properties of a biometric feature to be satisfied for personal recognition can be summarized as follows [1, 2]:

- **Uniqueness:** the feature should be as unique as possible. An identical trait should not appear in two different people.
- **Universality:** the feature should occur in as many people as possible over a population.
- **Permanence**: the feature should be robust enough and non-changeable over a time.
- **Measurability:** the feature should be measurable with simple technical instruments.
- **User friendliness:** It must be easy and comfortable to measure.
- **Acceptability:** the feature should be acceptable in population daily life.

Research on different biometric modalities reports that each biometric trait has its strengths, weaknesses and limitations. Evaluating different modalities shows that a high performance can be achieved in ideal conditions. However, each modality has inherent problems affecting its performance. Therefore, no single biometric is expected to effectively meet the requirements and properties to provide a robust recognition system against the distortions of individual modalities. Figure 1, depicts some example of several biometric traits.

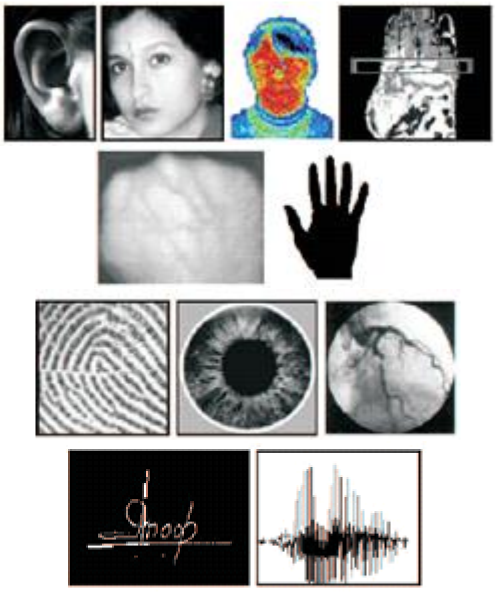

Figure 1: Different Biometric Traits

1.2 Unimodal Biometric Systems

The increasing use of means of identification by recognition of characteristic behavioral and physiological features is an obvious evidence to pay more attention on the security to be only used to describe an individual. Biometric system based on single biometric trait is suffering from limitation such as noisy data, lack of uniqueness and non-universality. For instance, face recognition performance decreases due to changes in illumination, pose and various occlusions [3]. The most common biometric features used for personal recognition are: palmprint, iris, facial thermogram, hand thermogram, hand vein, hand geometry, voice, face, retina, signature, and fingerprint.

In this study, we deal with two modalities namely face and palmprint which are widely used for identification systems. Facial images are probably the most common biometric characteristic used by humans to make personal recognition. On the other hand, human palms contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner [4].

1.2.1 Face Biometric System

In the past few years, one of the most popular biometric modalities was facial recognition. Many algorithms have been proposed in a very wide range of applications. Image pre-processing and normalization, training, testing and matching are important parts of face recognition techniques.

The main objective of image pre-processing techniques is to extract the facial region from the captured image and normalizes it in respect to size and rotation procedure on the facial region is to enhance the discriminative information contained in the facial images. Histogram equalization (HE) and mean-and-variance normalization (MNV) [5] can be used on the face images as pre-processing stage.

The feature extraction methods which extract a set of representative features from the normalized facial region can be applied in the training stage including Principal Component Analysis (PCA) [6], Linear Discriminant Analysis (LDA) [7], kernel methods [8], Eigenface [6], Fisherfaces [9] and support vector machine [10]. The aim of testing stage is to apply the same procedure in the training stage to obtain the feature vectors for test images.

Finally in the last stage, Euclidean distance and Manhattan distance measurements are used to match the feature set extracted from the given face image with the templates stored in the systems database. The details of algorithms used in face recognition are presented in Chapter 2.

1.2.2 Palmprint Biometric System

One of the new physiological biometrics is the palmprint recognition which attracted the researchers due to its stable and unique characteristics. The rich feature information coming from palmprint trait offers one of the powerful means in personal recognition. Compared with other biometrics, the palmprints have several advantages: low-resolution imaging can be employed; low-cost capture devices can be used; it is difficult to fake a palmprint; the line features of the palmprint are stable, etc. [11]. A typical palmprint recognition system consists of five parts: pre-processing, training, testing, feature extraction and matcher. The same strategies are used in palmprint recognition for all stages. The details of algorithms used in palmprint recognition are explained in Chapter 2.

1.3 Multimodal Biometrics

Multimodal biometrics is studied to improve the generalization ability by exploiting two or more modalities. Multimodal biometric systems provide an alternative when a person cannot be recognized because of the noisy sensor data, illumination variations, various occlusions, the prices of biometric traits and susceptibility to spoof attacks [12, 13, 14]. The resultant system is expected to be more robust against the forgeries and distortions of individual modalities. Moreover, complementary information may be provided by different biometrics, leading to a superior identification system. In this thesis, various fusion techniques will be studied on palmprint and face biometrics to improve the recognition performance of individual biometrics systems.

The fusion of two or more biometric systems can be performed at data level, feature level, match score level and decision level [15, 16]. Features extracted from biometric modalities have a rich source of information and fusing features allows classes to be more separable leading to improve the performance. The two most widely used fusion strategies in the literature are feature level and matching score level fusion.

Matching score level has been more used among all fusion levels. Each biometric matcher provides a similarity score such as distances indicating the proximity of the input feature vector with the template feature vector [1]. These scores can be combined to verify the claimed identity. Techniques such as sum rule may be used in order to combine these scores and obtain a new match score which would be used to make the final decision.

Feature level fusion involves the combination of feature sets corresponding to multiple information sources [17]. It can be fused by a simple concatenation of the feature sets extracted from face and palmprint to create a new feature set to represent the individual. The concatenated feature is expected to provide better authentication results than the individual feature vectors.

The matching scores generated by the face and palmprint modalities may not be on the same numerical range. Hence normalization is needed to transform the scores of the individual matchers into a common domain before combining them for matching score level fusion. In this work, the normalized score is obtained by using tanh-normalization method which is reported to be robust and highly efficient [17]. Tanh normalization is represented as:

$$S'_k = \frac{1}{2} \times \left\{ \tanh\left(\frac{0.01(S_k - \mu_{GH})}{\delta_{GH}} \right) + 1 \right\} \tag{1.1}$$

where S_k represents the normalized score for $k = 1, 2, \ldots, n$; μ_{GH} and δ_{GH} are the mean and standard deviation estimates of the genuine score distribution respectively. In this study, the combination of different fusion level schemes at matching score level and feature level are proposed to fuse face and palmprint modalities.

Biometric systems are vulnerable to several types of treats grouped by sensor tampering, database tampering, replay attack, attacking the channel between the database and matching and many other attacks described in [18]. Among the different types of attacks which are often unknown, the literature on spoofing detection systems presents two types of spoofing attacks, namely print and replay attacks. Print attack is based on printed modality images of an identity to spoof 2D recognition systems, while replay attack is carried out by replaying a video sequence of a live identity on a screen that is either fixed or hand-held to evade liveness detection.

Detection of spoofing attacks are still big challenges in the field of spoofing detection and has motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the fingerprint [19, 20], the face [21, 22], the signature [23], or even the gait [24].

In this work we focused on both printed photo and replayed video attacks to unimodal 2D face and palmprint recognition systems separately which are easy to reproduce and has potential to succeed.

1.4 Related Works

Face recognition, as the most successful applications has received more significant attention. Many solutions in the domain of pattern recognition, computer vision and artificial intelligence have been proposed to improve the robustness and recognition. Face recognition based on computing a set of subspace called eigenvectors have been extensively used by researchers in [25, 26, 9, 27, 28]. In [9], a face recognition algorithm is developed which is insensitive to light variation and facial expression. They have used projection directions based on Fisher’s Linear Discriminant to maximize the ratio of between-class scatter. Principal Component Analysis (PCA) s also used for dimensionality reduction.

On the other hand, palmprint recognition has been widely studied due to containing distinctive features such as principal lines, wrinkles, ridges and valleys on the surface of the palm. Compared with other biometrics modalities, palmprint has become important to personal identification because of its advantages such as low resolution, low cost, non-intrusiveness and stable structure features [29, 30].

In [31], a palmprint recognition method based on eigenspace technology is proposed. The original palmprint images are transformed into eigenpalms, which are the eigenvectors of the training set and can represent the principle components of the palmprint quite well. Then, the features are extracted using projecting a new palmprint image by the eigenpalms.

The use of biometrics, level of fusion and method of integration of the multiple biometrics have been studied by many researchers in the literature [32, 15, 33, 34, 35, 36, 37, 38, 39]. A number of studies have shown the effectiveness and power of the multi-biometric systems based on fusion prior to matching (Feature Level Fusion) and fusion after matching (Match Score Level Fusion). Numerous identification systems based on different modalities have been proposed which utilize feature level fusion and score level fusion.

Fusion of palmprint and face biometrics is employed in several studies to improve the performance of a unimodal system by combining the features extracted from both face and palmprint modalities. Shen et. al in [40] developed a feature code named FPcode to represent the features of both face and palmprint. The experimental results of the feature level and score level fusion are significantly improved compared to unimodal biometrics. In their work, a fixed length of coding scheme is used which is very efficient in matching. Rokita et. al in [41] applied a Gabor filter on the face and palmprint to construct feature vector of the images. Then a support vector machine (SVM) is applied to verify the identity of a user. One SVM machine is built for each person in the database to distinguish that person from the others. The proposed algorithm is carried on their own database containing face and hand images taken by a cell phone camera.

A unified representation of the recognition scores is proposed in [42]. The corresponding quality and reliability value into a single complex number provides simplification and speedup for the fusion of multiple classifiers. A new approach based on score level fusion is presented in [43] to obtain a robust recognition system by concatenating face and iris scores of several standard classifiers. The features from face and iris are extracted using local and global feature extraction methods such as PCA, subspace LDA, spPCA, mPCA and LBP. A combined database using ORL and BANCA face databases together with CASIA and UBIRIS iris databases is formed in their experiments.

On the other hand, Ross and Jain in [44] presented various possible scenarios in multimodal biometric systems. Additionally, the levels of fusion and the integration strategies are discussed. In [45], the problem of information fusion in biometric verification systems is addressed by combining information at the matching score level. The recognition rate of the system is improved by the fusion of three biometric modalities such as face, hand and fingerprint geometry. Their experiments indicate that the sum rule performs better than the decision tree and linear discriminant classifiers.

A feature level fusion scheme has been proposed in [46] to improve multimodal matching performance. They used fusion at the feature level in three different scenarios: fusion of PCA and LDA of face; fusion of LDA coefficients corresponding to the R, G, B channels of a face image; fusion of face and hand modalities. Ross and Govindarajan in [47], proposed a novel fusion strategy for personal identification using face and palmprint biometrics. Both Principal

Component Analysis (PCA) and Independent Component Analysis (ICA) are considered in this feature vector fusion strategy.

Recently, Seshikala et. al in [48] proposed a feature level fusion of face and palmprint by taking the curvelet transform of bit quantized images. The k-nearest neighbor (KNN) classifier is used to determine the final biometric classification. The experimental results demonstrate that the proposed approach outperforms the unimodal systems and the proposed nearly Gaussian fusion (NGF) strategy has a better performance compared to the other fusion rules.

In addition, several multimodal systems have been reported in which PSO algorithm is extensively used to select the features from modality sources [15, 36]. Two efficient fusion schemes are designed for multimodal biometric systems using face and palmprint [15]. The face and palmprint modalities are coded using Log-Gabor transformation with 4 different scales and 8 different orientations resulting in high dimensional feature space. In order to improve the recognition rate, several schemes such as feature level and score level fusion are also proposed. Moreover, Particle Swarm Optimization (PSO) algorithm is implemented to significantly reduce the dimension by selecting the optimal features coming from different fusion schemes. Fusion results report a significant improvement in performance of the proposed systems. Xu et al.

In [32] a multimodal system with feature level fusion is proposed in which two biometrics are used as the real and imaginary part of the complex matrix. They proposed a novel method named MCPCA and tested on a palmprint-based personal identification system, with bimodal biometrics using palmprint and face images and with bimodal biometrics using ear and face images. Jing et al. explored a multimodal biometric system in which different projection methods are used to extract the features from the biometric images [33].

Yao et al. [34] proposed a multimodal biometric recognition system in which Gabor filters and principle component analysis methods have been used to extract the features from face and palm-print modalities. A multimodal system has been reported in which Gabor filtered images were fused at pixel level and kernel discriminative common vectors- radial basis function (KDCV-RBF) is used to classify the subjects [35].

In [36], Gabor-Wigner transformation (GWT) is utilized for feature extraction using face and palmprint multimodal systems. A binary PSO is then used to select the dominant features as well as reducing the dimension. In their proposed multimodal biometric systems, the face and palmprint modalities are integrated using feature level and score level fusion. Performance of the proposed hybrid biometric system shows that PSO is able to significantly improve the recognition rate of the system with reduced dimension of the feature space.

In [38], both matching score level and feature level fusion are employed to obtain a robust recognition system based on face-iris biometric systems using several standard feature extractors and Particle Swarm Optimization. Local texture descriptor methods achieve high accuracies, and they are robust to variations such as illumination, facial expression and partial occlusions in face recognition [49, 50, 51].

The objective of feature selection is to search in a very large dimension space and remove irrelevant features and retain only relevant ones. Feature selection methods have been shown to be efficient in optimizing the feature selection process [15, 36, 52].

Recently, different type of countermeasures based on motion and texture analysis have been considered for face anti-spoofing. Micro-texture analysis has been widely used for spoofing detection from single face images [53, 54, 55, 56]. Face spoofing detection from single images using micro-texture analysis was implemented in [54] to emphasize the differences of micro texture in the feature space. A simple LBP+SVM method is proposed which achieved a comparable result both on NUAA and Idiap databases. In order to extract high frequency information from the captures images, DoG and LTV algorithms are used in [57]. More specially, LBP-Top-based dynamic texture analysis has been used to demonstrate the effectiveness of the texture features [58, 59, 60]. A number of comparative studies have been reported to suggest motion information that can cover a wide range of attacks targeting the 2D face recognition systems.

In [61], an efficient face spoof detection algorithm based on Image Distortion Analysis (IDA) is proposed. Specular reflection, blurriness, chromatic moment, and color diversity features are extracted to form the IDA feature vector. In order to extract facial dynamic information, Santosh et. al in [21] modified Dynamic Mode Decomposition (DMD) to capture the complex dynamics of head movements, eye-blinking, and lip movements found in a typical video sequence containing face images. The use of image quality assessment for liveness detection has been studied in previous works for image manipulation detection [62, 63, 64, 65]

A novel software-based fake detection method is presented in [66] to detect different types of fraudulent access attempts. The proposed approach used 25 general image quality features extracted from one image distinguish between real and impostor samples.

1.5 Research Contributions

The contribution of this PhD thesis is to use face and palmprint modalities for person identification by several hybrid multimodal biometric approaches. The proposed hybrid approaches are based on both feature level and match score level fusion of the human face and palmprint. The proposed methods concatenate features extracted by Local Binary Patterns (LBP) and Log Gabor followed by dimensionality reduction using Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) algorithms. Backtracking Search Algorithm (BSA) as a feature selection method is used to improve the performance by selecting the optimal set of face and palmprint features. Sum Rule is then performed on tanh normalized scores of each modality. Finally the matching module is performed using Nearest Neighbor Classifier to compute the recognition accuracy. The general contributions of this thesis can be summarized as:

- Applying feature extraction methods for face and palmprint recognition by fusing local and global discriminant features to get a large feature vector in order to enhance the recognition performance.
- Removing redundant information coming from face and palmprint feature vectors by selecting the optimized features.

- Solving the problem of time and memory computation by concatenating the face and palmprint matched scores to decrease overall complexity of the system.
- Selecting the most effective and discriminant features by applying a proper feature selection method in order to reduce the high dimensionality of the feature space.

1.6 Outline of the Dissertation

The rest of the thesis is organized as follows. Chapter 2 presents the details of feature extraction methods applied on face and palmprint biometrics. The employed databases in order to test the performance of the proposed multimodal biometric systems are described in Chapter 3. A hybrid approach for person identification using palmprint and face biometrics (proposed scheme 1 and scheme 2) are detailed in Chapter 4. Feature selection for the fusion of face and palmprint (proposed scheme 3) is explained in Chapter 5. The proposed spoof detection approach on face and palmprint biometrics is described in Chapter 6. Finally, we conclude this study in Chapter 7.

Chapter 2

FEATURE EXTRACTION METHODS REVIEW

2.1 General Information

Features play a very important role in the area of image processing and classification. Hence, finding efficient feature extraction methods to be used in the selection and classification is one of the concerns. In pattern recognition we extract relevant data about an object by applying feature extraction methods and those features which are likely to assist in discrimination are selected and used in the classification of an object. General features such as texture, color, shape can be used to describe the content of the images. According to the abstraction level, they can be divided into [67]:

- Pixel-level features: Features calculated at each pixel, e.g. color, location.
- Local features: Features calculated over the results of subdivision of the image band on image segmentation or edge detection.
- Global features: Features calculated over the entire image or just regular sub-area of an image.

Sub-pattern based and holistic methods have been used in many applications. The facial images can be divided into equal size non-overlapped partitions in sub-pattern based methods. In order to obtain local features these partitions are individually experimented. Then, the extracted features of each partition will be concatenated to provide an overall feature vector of the original image. Sub-pattern based methods can be implemented with different number of partitions.

On the other hand, holistic methods use the entire area of an original image as the input of classification task. These methods extract features, reduce the dimension and then categorize them accordingly. However, there may be redundant data in the extracted features which will affect the overall classification performance. Appropriate statistical techniques are needed in order to overcome this problem.

In this study, we used both local and global feature extraction methods on face and palmprint images to extract the features in face-palmprint multimodal biometric systems. All these local and global feature extractors discussed in this work are implemented on Matlab7. The system is Windows XP professional with 2.39 GHz CPU and 8 GB RAM.

Global feature extraction methods such as PCA [68], subspace LDA [9] and Log Gabor [69] are used for both face and palmprint images, while LBP [49] is a local feature approach for extracting the texture features. LBP is a simple but efficient operator to describe local image patterns. It provides several local descriptions of a face and palmprint images and then combines them into a global description. In order to have equal size for each subimage all the images are resized before partitioning. The number of eigenvectors used in PCA and LDA methods are selected experimentally as the maximum number of nonzero eigenvectors. In the following sections details of the methods are presented.

2.2 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is one of the known statistical techniques used in many applications such as face and palmprint recognition [31, 70, 71, 68]. The main role of PCA is to operate directly on the whole patterns to extract global features which will be used for subsequent classification. It uses a set of previously found projections from a given training subset. PCA can be also used to reduce the dimensions of a multi-dimensional data set down into its basic components excluding any unnecessary information. It transforms uncorrelated component from the covariance matrix of the original data into a projection vector by maintaining as many variances as possible. It can be performed by using only the first few principal components so that the dimensionality of the transformed data is reduced [68]. The steps required to perform PCA algorithm are summarized in the following subsections [72]:

2.2.1 PCA Algorithm

Step 1: Read images

All the images $I_i = [I_1, I_2, \dots, I_N]$ in the dataset are supposed to be a set of N data vectors $V_i = [V_1, V_2, \dots, V_N]$, where each image is converted into a single vector of size L. The resulting $N \times L$ dimension matrix is referred to as X.

Step 2: Calculate the mean of images

Calculate the mean m of each stored image vector V_i. The result is a single column vector with the size $L \times 1$. Then, subtract the mean image from each image vector using equation (2.1), where m is the mean image and is obtained from equation (2.2).

$$Y_i = I_i - m \tag{2.1}$$

$$m = \frac{1}{N}\sum_{i=1}^{N} I_i \qquad (2.2)$$

Step 3: Calculate the covariance matrix

Calculate the covariance matrix of the obtained matrix from previous step according to the following equation (2.3).

$$C = \frac{1}{N}\sum_{i=1}^{N} Y_i Y_i^T \qquad (2.3)$$

Step 4: Calculate the eigenvectors and eigenvalues of the covariance matrix

Determine the matrix V of eigenvalues of the covariance matrix C using equation (2.4), which contains useful information about the data.

$$CW = \lambda W \qquad (2.4)$$

Where W is the set of eigenvectors related to the eigenvalues λ.

Step 5: Sort the eigenvectors and eigenvalues

Sort the eigenvectors and corresponding eigenvalues in descending order. It gives the components in order to significance. The eigenvectors with the highest eigenvalues is the principal component of the data set. The final dataset is supposed to have less dimensions than original due to leaving some components out.

Step 6: Projection

Project every centered training image into the created eigenspace based on a new ordered orthogonal basis by considering the first eigenvectors with a largest variance of the data using equation (2.5).

$$P_{ik} = W_k^T \,.\, Y_i \quad \forall\, i, k \qquad (2.5)$$

Where k varies from 1 to λ and W_k is the matrix of eigenvectors corresponding to the λ significant eigenvectors having the largest corresponding eigenvalues of C.

Step 7: Recognition

Consider the similarity score between a test image and every training image projection in the matrix P. Project each test image I_{test} into the same eigenspace using equation (2.6).

$$P_{test} = W_k^T (I_{test} - m) \tag{2.6}$$

2.3 Linear Discriminant Analysis (LDA)

Linear Discriminant Analysis (LDA) is a linear supervised method used in statistics and pattern recognition to classify objects [73]. It is similar to PCA and mainly aims to discriminate the input data. LDA is also used for dimensionality reduction before data classification while preserving as much of the class discriminatory information as possible [27, 74]. In order to project the high dimension input data into a lower dimension space, LDA tries to find the best projection by discriminating data as much as possible. The goal of LDA is to maximize the between-class scatter matrix measure while minimizing the within-class scatter matrix measure. Within class scatter matrix measures the amount of scatter between items in the same class.

In this work, LDA is used on face and palmprint images. Generally, we apply PCA method to reduce the dimension by generalizing the input data and then LDA can be performed to classify the data. The common steps of LDA algorithm are described as follows:

2.3.1 LDA Algorithm

Step 1: Read images

Collecting all the images $x_i = [x_1, x_2, \dots, x_N]$ in the dataset. Each is converted into a single vector of size L. The resulting $N \times L$ dimension matrix is referred to as X.

Step 2: Take the PCA projection

Calculate the mean m and the covariance matrix C by applying PCA on the stored vectors to take the projection matrix to LDA as input data.

Step 3: Fine the within-class scatter matrix

Calculate the within-class scatter matrix using the following equations (2.7) and (2.8). It will be obtained by calculating the sum of the covariance matrices of the centered images in the class.

$$S_i = \sum_{x \in X_i} (x - m_i)(x - m_i)^T \tag{2.7}$$

$$S_w = \sum_{i=1}^{L} S_i \tag{2.8}$$

where m_i is the mean of i^{th} class.

Step 4: Fine the between-class scatter matrix

Calculate the between-class scatter matrix using the following equation (2.9). It is the covariance of data set whose members are the mean vectors of each class.

$$S_b = \sum_{i=1}^{C} (m_i - m)(m_i - m)^T \tag{2.9}$$

where C is the number of classes.

Step 5: Compute the eigenvectors of the projection matrix

Compute the eigenvectors of the projection matrix by using equation (2.10).

$$W = eig\ (S_w^{-1} S_b) \tag{2.10}$$

Step 6: Projection

Project every centered training image by using the projection matrix as equation (2.11).

$$M = W \times P \tag{2.11}$$

Step 7: Recognition

Consider the similarity score between a test image projection matrix and every training image projection matrix.

2.4 Log Gabor

Gabor filters have attracted lots of attention in biometrics research community, mainly due to its orientation selectivity, spatial localization and spatial frequency characterization. Firstly proposed by Dennis Gabor in 1946 [75], the canonical coherent states of the Gabor filters are different versions of a Gaussian-shaped window shifted in time/space and frequency variables. However, these filters present a limitation in bandwidth.

Log-Gabor filters were proposed by Field in 1987 [69] to overcome the bandwidth limitation in traditional Gabor filters. These Log-Gabor filters always have null dc component and desirable high-pass characteristics.

The main characteristics of Gabor wavelets are described as follows [76, 77] :

- Construction by a linear combination.
- Energy preservation in transform domain (Parseval's theorem).
- Non-orthogonally but an unconditional basis, a frame [78].
- Symmetry of the Fourier domain.

- Time/space and frequency shift-invariance.
- Localization: monomodal and isotropic.
- Regularity: smooth and infinitely derivable.

The design of a Gabor filter bank is a complex task. In texture classification, in particular, Gabor filters show a strong dependence on a certain number of parameters, the values of which may significantly affect the outcome of the classification procedures.

Many different approaches to Gabor filter design, based on mathematical and physiological consideration, are documented in literature [79]. However the effect of each parameter, as well as the effects of their interaction, remain unclear. On the linear frequency scale, the transfer function of the Log-Gabor transform has the form:

$$G(\omega) = \exp\{\frac{-\log(\frac{\omega}{\omega_0})^2}{2 * log(\frac{k}{\omega_0})^2}\} \tag{2.12}$$

where ω_0 is the filter center frequency, ω is the normalized radius from center and k is the standard deviation of angular component. In order to obtain a constant shape filter, the ratio $(\frac{k}{\omega_0})$ must be held constant for varying values of ω_0. Gabor and Log-Gabor filtering are one of the most popular methods in the field of image processing and texture analysis [80, 81, 82, 83, 84].

2.4.1 Log Gabor Algorithm

Step 1: Read images

Collecting all the images in the dataset.

Step 2: Create the filter

Defining the five input parameters such as theta, lambda, gamma, sigma and psi. A filter bank consisting of Gabor filters can be viewed with various scales and rotations. The image at scale 1 is the original, higher scales result from applying a gaussian blur.

Step 3: Apply the created above log Gabor filter to the input image

Each image is analyzed using $x = scale \ \times orientation$ different Log-Gabor filters resulting in x different filtered images. A 2D image of $x \times x$ will produce a 1D vector with size of $1 \times x \ \times x$ after concatenating x filtered images.

Step 4: Classification

Then, the produced vector of training images is used to the classification task.

2.5 Local Binary Patterns (LBP)

Texture has been one of the most important characteristic which has been used to classify and recognize objects and has been used in finding similarities between images in databases. Local binary patterns (LBP) is one of the sub-pattern based operators that is firstly introduced by Ojala et al. [85, 86]. It is able to provide a simple and effective way to represent patterns by assigning a label to every pixel of an image by thresholding the 3×3 neighborhood of each pixel with the center pixel value. The result will be a binary number.

Later, the basic LBP operator is extended to so-called uniform LBP [87]. Different patterns are produced by the operator LBP to describe the texture of images. It contains at most two bitwise transitions of 0 and 1. For instance, 00000000, 01111111, and 01110000 are some samples of uniform pattern with 0,1 and 2 transitions respectively, and 11001001 and 01010011 are some samples of non-uniform patterns with 4 and 5 transitions. LBP is a good texture descriptor and it is shown that this method achieves high accuracies on face recognition [88, 89, 90, 91, 51, 92, 50].

2.5.1 LBP Algorithm

Step 1: Read images

Collecting all the images in the dataset.

Step 2: Divide the image into local partitions

Dividing each image into several non-overlapped blocks with equal size.

Step 3: Assign labels to each pixel

In order to extract the local features, LBP texture descriptors are performed on each block separately. LBP is checking a local neighborhood surrounding a central point R which is sampled at P points and tests whether the surrounding points are greater than or less than the central point to classify textures. If the pixel value of the center is greater than its neighbor, then it assigns 1 otherwise assigns 0 to the neighbor's pixels. The LBP value of the center pixel in the P neighborhood on a circle of radius R is calculated by:

$$LBP_{(P,R)} = \sum_{p=0}^{p-1} S\left(g_p - g_c\right) 2^p \qquad (2.13)$$

$$S(x) = f(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \qquad (2.14)$$

Step 4: Calculate the histogram

Then, for each block a histogram is extracted to hold information related to the patterns on a set of pixels.

Step 5: Concatenate the features

Finally, the extracted features of each block will be directly concatenated to produce a single global feature vector.

Step 6: Recognition

Comparing training and test images using the global descriptor.

Chapter 3

DESCRIPTION OF DATABASES

3.1 Face Databases

In order to investigate the performance of our unimodal and multimodal systems, a set of experiments are performed using different subsets of face. Face databases employed in this thesis are FERET [93], ORL [94], Yale-B [95] and Essex [96]. Subsections have a brief overview on each face database separately.

3.1.1 FERET Face Database

The Facial Recognition Technology (FERET) Database ran from 1993 through 1997 in 15 sessions. Sponsored by the Department of Defense's Counterdrug Technology Development Program through the Defense Advanced Research Products Agency (DARPA). The final corpus, used here, consists of 14126 face images from 1564 sets of images involving 1199 subjects and 365 duplicate sets of images [93]. Duplicate sets captured in different days covering the second image sets of the same individuals. There was a 2 years gap for taking the images of the same individual in duplicate sets. Image dimension is considered as 256×384. The naming convention based on different categories for the FERET imagery including frontal images and pose angles is shown in Figure 2: Naming Convention of FERET Database.

Two letter code	*Pose Angle (degrees)*	*Description*	*Number in Database*	*Number of Subjects*
Fa	0 = frontal	Regular facial expression	1762	1010
Fb	0	Alternative facial expression	1518	1009
ba	0	Frontal "b" series	200	200
bj	0	Alternative expression to ba	200	200
bk	0	Different illumination to ba	200	200
bb	+60		200	200
bc	+40	Subject faces to his left which is	200	200
bd	+25	the photographer's right	200	200
be	+15		200	200
bf	-15		200	200
bg	-25	Subject faces to his right which	200	200
Bh	-40	is the photographer's left	200	200
bi	-60		200	200
ql	-22.5	Quarter left and right	763	508
qr	+22.5		763	508
hl	-67.5	Half left and right	1246	904
hr	+67.5		1298	939
pl	-90	Profile left and right	1318	974
pr	+90		1342	980
Ra	+45	Random images. See note	322	264
Rb	+10	below. Positive angles indicate	322	264
Rc	-10	subject faces to photographer's	613	429
Rd	-45	right	292	238
Re	-80		292	238

Figure 2: Naming Convention of FERET Database

In this work, a subset of 235 subjects were used after cropping the images into 80×64 pixels. The images in this dataset have different illumination conditions (right-light, center-light and left-light), regular and alternative facial expressions (happy, normal, sleepy, sad), a wide range of poses (both frontal and oblique views) and they are with or without glasses. Sample images of an individual in FERET face database are shown in Figure 3.

Figure 3: Sample Images of FERET Dataset

3.1.2 ORL Face Database

AT&T database of faces formerly known as the ORL face database is a standard face database that contains a set of face images taken between April 1992 and April 1994 at the lab. ORL database was used in the context of a face recognition project carried out in collaboration with the Speech, Vision and Robotics Group of the Cambridge University Engineering Department [94]. It contains 10 different images of each of 40 distinct subjects. There were taken at different times, varying the lighting, facial expressions such as open and closed eyes, smiling and not smiling and facial details with and without glasses having a dark homogeneous background. The size of each image is 92x112 pixels. A subset of all 40 subjects are used in this study to validate the proposed unimodal and multimodal systems. Sample set of face images from ORL database is depicted in Figure 4.

Figure 4: Sample Images of ORL Dataset

3.1.3 Extended Yale-B Face Database

The extended database as opposed to the original Yale Face Database B with 10 subjects was first reported by Kuang-Chih Lee and Jeffrey Ho [97]. All images stored in the database are manually aligned, cropped, and then re-sized to 168×192 images [97]. It contains 16128 images of 38 human subjects under 9 poses and 64 illumination conditions. Some images from Extended Yale-B Database are shown in Figure 5.

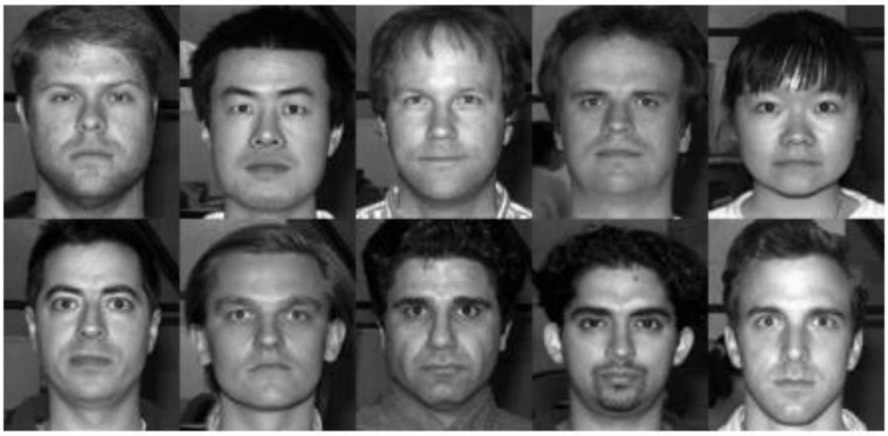

Figure 5: Sample Images of Extended Yale-B Database

3.1.4 Essex Face Database

Essex Face Database contains total number 7900 images from 395 individuals. Each subject providing 20 face images. Image resolution is 196×196 pixels. All images were captured under artificial lighting, mixture of tungsten and fluorescent overhead. It Contains images of male and female subjects with various racial origins. The images are mainly of first year undergraduate students, so the majority of individuals are between 18-20 years old but some older individuals are also present. A wide range of poses with or without glasses and with and without beards is demonstrated in this database. Some images from Extended Yale-B Database are shown in Figure 6.

Figure 6: Sample Images of Essesx Database

3.2 Palmprint Database

Palmprint modality experiments are performed on PolyU database provided by the Hong Kong Polytechnic University [98]. PolyU is a large database which contains 7752 grayscale images corresponding to 386 different palms in BMP image format. Around twenty samples from each of these palms were collected in two sessions, where 10 samples were captured in the first session and the second session, respectively. The average interval between the first and the second collection was two months. The size of the original images is 150×150 pixels [99]. Samples of the cropped images in PolyU palmprint database are demonstrated in Figure 7.

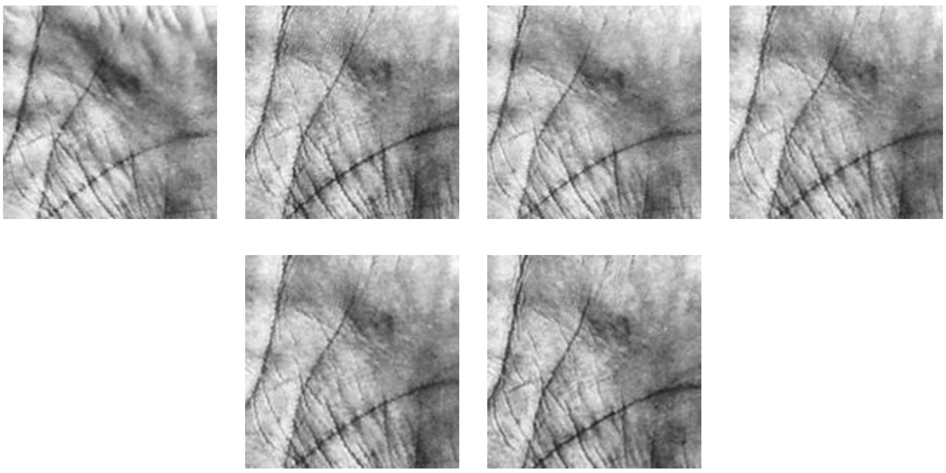

Figure 7: Samples of the Cropped Images of a Specific User in PolyU Palmprint Database

3.3 Multimodal Database

There is no available face-palmprint multimodal database collection including face and palmprint images of the same subject. Thus, all experiments are carried out on a virtual multimodal database combining face and palmprint coming from two independent unimodal databases. In order to investigate the performance, we choose FERET database for face modality and PolyU database for palmprint modality which are widely used databases for benchmarking. For example face image a from FERET database and palmprint image a' from PolyU database belong to the same person. Some more samples of virtual multimodal database are shown in Figure 8.

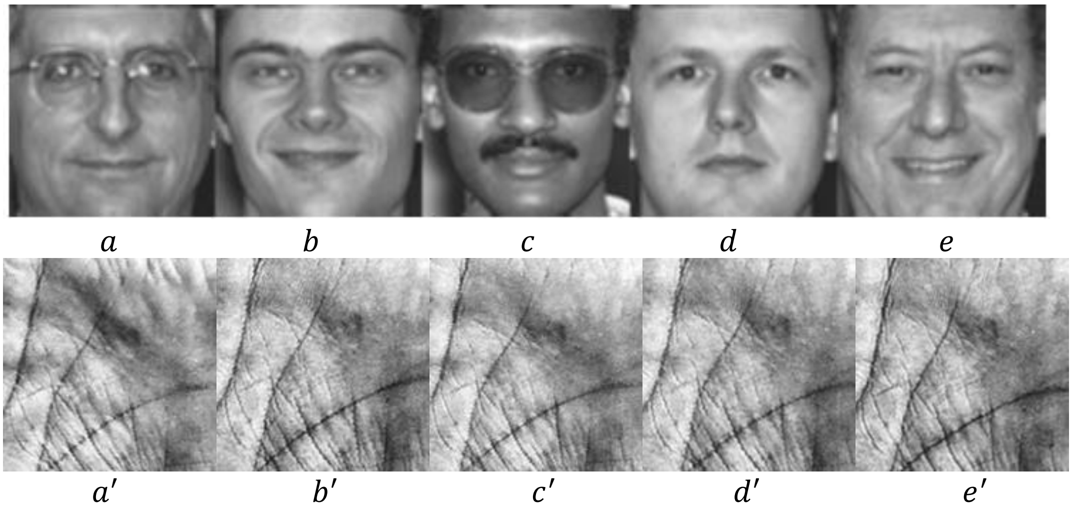

Figure 8: Sample Images from Virtual Multimodal Database

Chapter 4

A HYBRID APROACH FOR PERSON IDENTIFICATION USING PALMPRINT AND FACE BIOMETRICS

4.1 Description of Proposed Scheme 1 and Scheme 2

Fusion of face and palmprint have been studied in the literature, using Gabor and Log Gabor filters and Independent Component Analysis (ICA). The contribution of these studies is to apply different fusion techniques on the fusion stage followed by NN, KNN and SVM classifiers [41, 48]. In order to get high recognition accuracy, different local and global feature extraction methods were investigated to find the most appropriate method for face and palmprint recognition separately.

Face and palmprint modalities have their own limitations such as illumination variation, the palmprint bulkier scanners, and low quality palmprint images which does not take the advantage of textural or visual features of face. These limitations can be solved for each modality before the fusion stage. In that case, the features from each modality will be extracted separately to overcome the individual limitations which are decreasing the single model system performance.

In the first two proposed approaches, scheme 1 and scheme 2, face and palmprint biometrics are employed to provide a robust recognition system by using efficient feature extraction methods, score normalization and fusion strategies. The concentration of this study, is to improve the recognition performance for the fusion of face and palmprint biometrics using local and global feature extractors.

In the following subsections, two different proposed schemes, proposed scheme1 and proposed scheme2, that use feature level and score level fusion are described. In the first scheme, local binary patterns (LBP) method is employed to extract the local features of the face and palmprint images. In the second scheme, PCA and LDA projections are used to select the most effective and discriminant features on the features resulting from local binary pattern. The feature concatenation and score matching are then performed for classification.

4.1.1 Proposed Scheme 1

This section describes our first proposed hybrid system which concatenates features of face and palmprint extracted by Local Binary Patterns (LBP). Both feature level and score level fusion techniques are employed to improve the recognition accuracy of the proposed system.

The following is the detailed stages employed in the first proposed method for face and palmprint identification.

Step 1: Image preprocessing is performed on both face and palmprint biometrics separately using different techniques. Following this process, all images are histogram equalized (HE) and then normalized to have zero mean and unit variance (MVN) in order to spread energy of all pixels to produce image with equal amount of energy.

Step 2: All the entire images are then filtered with Local Binary Patterns. It divides the image into several blocks and performs filter on 8 neighbors in radius 2. Each palm divided into 4 × 4 and face into 5 × 5 blocks to produce 16 and 25 blocks separately.

Step 3: LBP histogram features are extracted from face and palmprint images.

Step 4: The texture features of left-palm and right-palm are concatenated to produce a single feature vector as shown in Figure 9.

Step 5: The scores of the individual biometrics (face and palmprint) are normalized using tanh normalization before the fusion.

Step 6: Sum Rule is applied to combine the normalized face and palmprint scores**.**

Step 7: The similarity between test and train images is measured using Euclidean distance measure in the classification step. Euclidean distance measurement is represented in equation (5.1), where X and Y denote the feature vectors of length n.

$$d_{(X,Y)} = \sqrt{\sum_{i=0}^{n}(X_i - Y_i)^2} \tag{5.1}$$

Step 8: The final decision is obtained in this last stage. The experimental results of the proposed system in the next section demonstrate that using LBP facial feature extractor and utilizing both feature level and score level fusion has an improved recognition accuracy compared to the unimodal systems. The block diagram of the first proposed fusion scheme is shown in Figure 10.

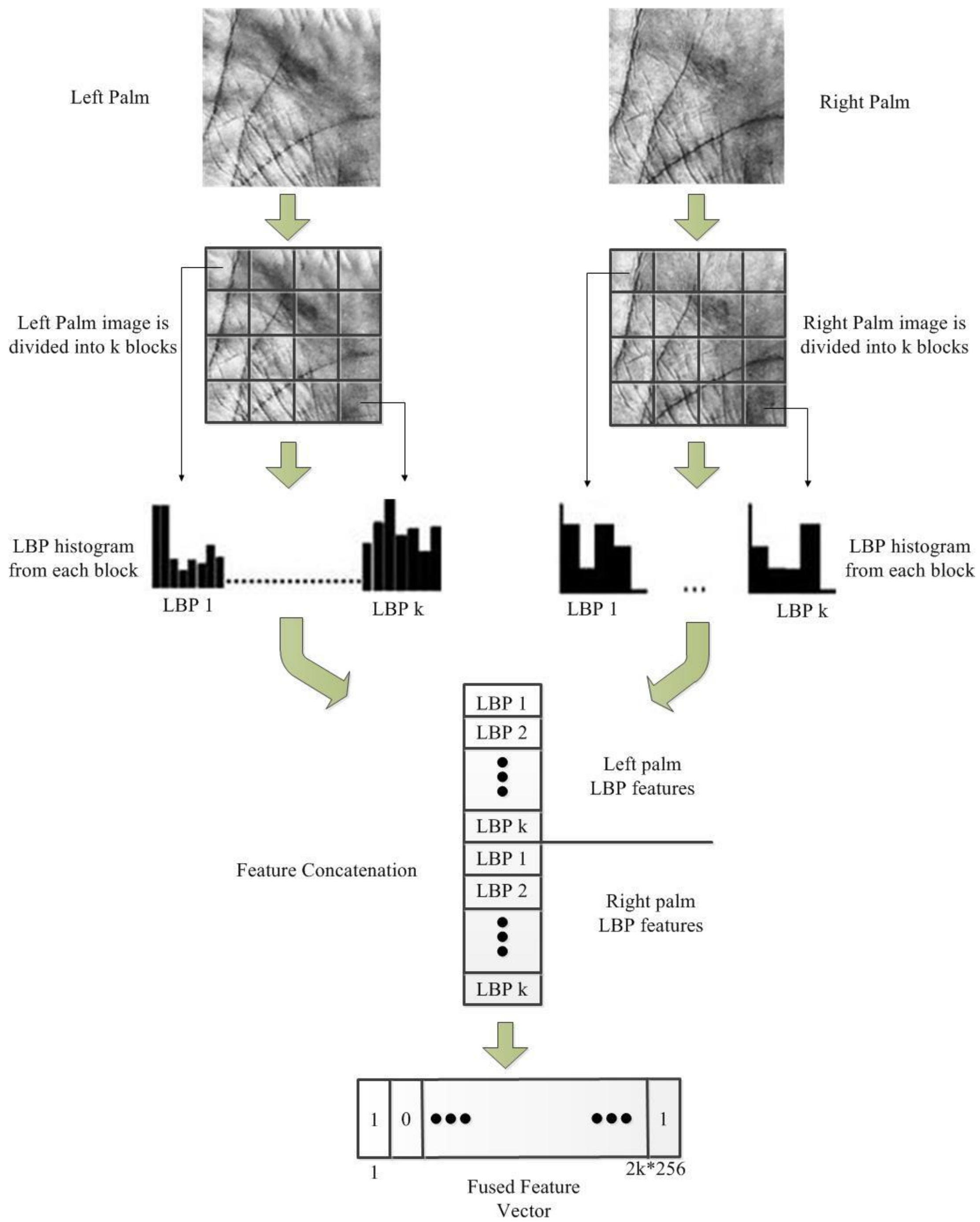

Figure 9: Feature concatenation of left-palm and right-palm

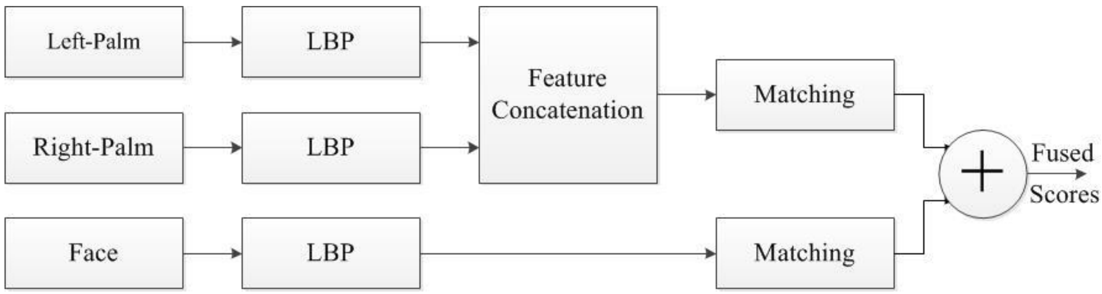

Figure 10: Proposed scheme of feature level and score level fusion (scheme 1)

The information fusion of two modalities can be performed at four levels: sensor level, feature level, match score level and decision level. In this proposed method, we applied integration of the face and palmprint scores based on the Sum Rule to fuse the normalized scores. Two of the simplest fusion techniques are Sum Rule and Product Rule to apply on the matching distances of unimodal classifiers. In that case, equal weights for each modality are used in the fusion process. Generally, the results of Sum Rule demonstrated that it is more efficient compared to Product Rule. The sum of the scores is shown in equation (5.2), where S_f corresponds to face matchers and S_p corresponds to palmprint matchers.

$$S = S_{f+}S_p \tag{5.2}$$

4.1.2 Proposed Scheme 2

This section describes our second proposed hybrid system which concatenates features of face and palmprint extracted by Local Binary Patterns (LBP) followed by dimensionality reduction using Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) algorithms. Feature level and score level fusion strategies are used to provide the robust recognition system.

Biometric systems employ a set of steps and it is common to start with a given set of features and then attempt to derive an optimal subset of features leading to high classification performances. Hence, we need to find a way to select the most discriminant features that keep the complementary information by reducing the dimensionality of the fused features. PCA and LDA are employed to extract the most effective features and to reduce the dimensionality of the feature space before performing the classification.

The following is the detailed stages employed in the second proposed method for face and palmprint identification.

Step 1: Image preprocessing is performed on both face and palmprint biometrics separately same as procedure done in scheme 1. All images are histogram equalized (HE) and then normalized to have zero mean and unit variance (MVN).

Step 2: All the entire images are then filtered with Local Binary Patterns with 4×4 blocks for each palm and 5×5 blocks of face images separately.

Step 3: LBP histogram features of the face and palmprint are initially extracted in this scheme.

Step 4: Then PCA and LDA are employed to reduce the dimensionality of the feature space.

Step 5: The features of the left and right palms are then concatenated to produce a single feature vector of the palmprint. This process is also repeated for all face images.

Step 6: Then using tanh normalization technique, the scores of face and palmprint are normalized.

Step 7: The normalized scores of face and palmprint are used in the classification step using Nearest Neighbor Classifier. The block diagram of the second proposed fusion scheme is shown in Figure 11.

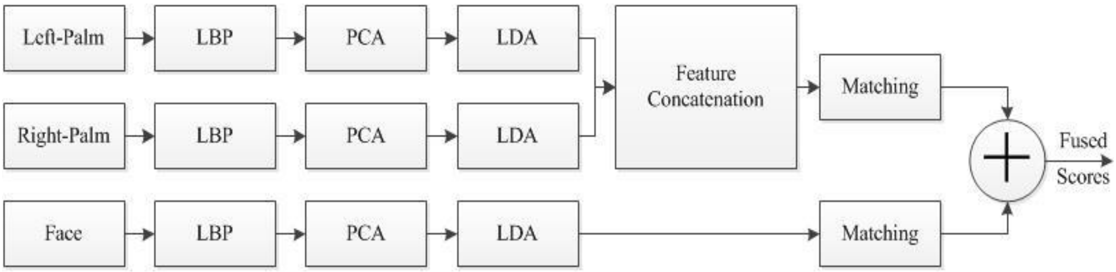

Figure 11: Proposed scheme of feature level and score level fusion (scheme 2)

4.2 Experimental Results of Proposed Scheme 1 and Scheme 2

A set of experimental results of different biometric systems are presented using PolyU and FERET databases in the proposed hybrid systems. All methods discussed in this chapter are implemented on Matlab7. The system is Windows XP professional with 2.39 GHz CPU and 8 GB RAM. The matching scores generated by the face and palmprint modalities may not be on the same numerical range. Hence normalization is needed to transform the scores of the individual matchers into a common domain before combining them for matching score level fusion. In this work, the normalized score is obtained by using tanh-normalization method which is reported to be robust and highly efficient.

4.2.1 Databases

All experiments are carried out on a virtual multimodal database combining face and palmprint data coming from two different unimodal databases due to the unavailability of a real multimodal database.

Palmprint modality experiments are performed on PolyU database provided by the Hong Kong Polytechnic University [98]. PolyU is a large database which contains gray-scale palmprint images from 235 palms (each user providing 5 different palm images). In this study, for each user, 3 training samples were randomly selected and the rest 2 were used as test samples. The size of the original images is 150×150 pixels and due to high computational cost, the pre-processing module resizes the original images to 50×50.

On the other hand, the FERET database was used for facial image experiments [93]. A subset of this database were used after cropping the images into 80×64 pixels by using Torch3Vision software [100]. The images in this dataset have different illumination conditions (right-light, center-light and left-light), regular and alternative facial expressions (happy, normal, sleepy, sad), a wide range of poses (both frontal and oblique views) and they are with or without glasses.

Recognition experiments were performed on the training and test subsets which were repeated 10 times without any overlapping between the sample images in these subsets. Therefore, there are 705 training samples and 470 testing samples. Hence, in our virtual multimodal biometric database, each user has 10 samples of palm and face images.

4.2.2 Results

The first set of experiments analyz the results of the implementation of different unimodal recognition systems. Furthermore, the performance of different fusion techniques at feature level and matching score level are presented in the second set of experiments. In order to compare the proposed methods with the other unimodal and multimodal systems, a set of experiments is conducted which is described below.

All methods used in the experiments employ the same distance measure which is Euclidean distance. In this research, fusion is conducted by using 50 most significant eigenvectors in both PCA and LDA. The Log-Gabor transform used in our experiments has four different scales and eight orientations. Thus, each image is analyzed using 8×4 different Log-Gabor filters resulting in 32 different filtered images. Due to memory issue in using Log-Gabor filter; in the preprocessing stage, all the gray scale face and palmprint images are cropped to a size of 32×32. A 2D image of 32×32 will produce a $1D$ vector with size of 1×32768 after concatenating 32 filtered images. This vector is used to compute the covariance matrix in the following PCA and LDA dimensionality reduction stage. In order to test the effectiveness of the proposed methods, we examined both unimodal and multimodal biometrics fusion results separately.

Table 1, Table 2 and Table 3 present a comparison of the recognition rates between unimodal and multimodal biometrics; and fusion results of face and palmprint using the same procedures, respectively.

Table 1: Comparison of recognition rates for different unimodal systems

Methods	Avg. Recognition Rate (%)	Min-Max Interval
Leftpalm-PCA,LDA	88.70 ± 1.85	[85.74; 91.49]
Leftpalm-LogGabor,PCA,LDA	90.45 ± 1.41	[87.87; 92.55]
Leftpalm-LBP	**94.02 ± 0.92**	**[92.55; 95.74]**
Face-PCA,LDA	79.79 ± 9.71	[70.21; 94.04]
Face-LogGabor,PCA,LDA	78.34 ± 9.69	[69.36; 94.26]
Face-LBP	**83.21 ± 7.87**	**[74.68; 96.17]**
Rightpalm-PCA,LDA	89.96 ± 1.91	[87.23; 92.77]
Rightpalm-LogGabor,PCA,LDA	91.57 ± 1.42	[89.79; 93.40]
Rightpalm-LBP	**94.30 ± 0.90**	**[93.19; 95.74]**

Table 2: Comparison of recognition rates for different leftpalm-face multimodal systems

Methods	Avg. Recognition Rate (%)	Min-Max Interval
LeftpalmFace-PCA,LDA-Feature Level Fusion	93.87 ± 3.50	[89.57; 98.94]
LeftpalmFace-PCA,LDA-Score Level Fusion	97.01 ± 1.61	[94.04; 99.36]
LeftpalmFace-LogGabor,PCA,LDA-Feature Level Fusion	96.85 ± 1.44	[94.26; 98.94]
LeftpalmFace-LogGabor,PCA,LDA-Score Level Fusion	96.89 ± 1.76	[93.19; 99.15]
LeftpalmFace-LBP-Feature Level Fusion	90.98 ± 4.81	[85.32; 98.94]
LeftpalmFace-LBP-Score Level Fusion	**97.49 ± 0.96**	**[95.96; 99.15]**

Table 3: Comparison of recognition rates for different rightpalm-face multimodal systems

Methods	Avg. Recognition Rate (%)	Min-Max Interval
RightpalmFace-PCA,LDA-Feature Level Fusion	94.34 ± 3.41	[89.57; 98.72]
RightpalmFace-PCA,LDA-Score Level Fusion	97.30 ± 1.61	[94.47; 99.36]
RightpalmFace-LogGabor,PCA,LDA-Feature Level Fusion	97.11 ± 1.49	[94.68; 99.15]
RightpalmFace-LogGabor,PCA,LDA-Score Level Fusion	97.74 ± 1.60	[95.32; 99.57]
RightpalmFace-LBP-Feature Level Fusion	91.23 ± 4.49	[86.38; 98.72]
RightpalmFace-LBP-Score Level Fusion	**97.94 ± 1.01**	**[96.81; 99.79]**

The highest recognition rates achieved by unimodal systems are 94.02%, 83.21% and 94.30% on left-palm, face and right-palm, respectively as shown in Table 1. These results are achieved when local binary patterns feature extraction is employed. The min-max interval of the recognition rates and the standard deviation of each method are also demonstrated.

The second set of experiments are performed on multimodal systems in order to show the effect of fusion on face and palmprint biometrics. As shown in Table 2, it is evident that the feature level fusion with PCA-LDA increases the recognition accuracy by 1.11%; and score level fusion achieves 1.14% improvement compared to unimodal face and unimodal palmprint systems.

Furthermore, 1.14% improvement in feature level fusion and 1.15% improvement in score level fusion is achieved in Log Gabor-PCA-LDA fusions. The score level fusion is increased around 1.17% in LBP fusion compared to the corresponding unimodal systems. The highest recognition rates are obtained once we used score level fusion of leftpalm-face and rightpalm-face with LBP algorithm which are 97.49% and 97.94%, respectively.

The proposed hybrid methods demonstrated in Table 4 present the effectiveness and the advantages of the combination of feature and score level fusion approaches since face and palmprint biometric features are rich and suitable for fusion. The proposed hybrid fusion schemes improve the classification rate up to 99.06%.

Table 4: Comparative results showing recognition rate of the proposed schemes

Methods	Avg. Recognition Rate (%)	Min-Max Interval
Hybrid Fusion of scheme I	**98.75** ± 0.67	[97.45; 100]
Hybrid Fusion of scheme II	**99.06** ± 0.93	[97.45; 100]

The presented hybrid methods, namely proposed scheme 1 and scheme 2, achieve an improvement of 0.81% and 1.12%, respectively compared to the other multimodal systems considered for the fusion of palmprint and face biometrics. In addition, compared to the unimodal left palmprint, face and right palmprint systems, the proposed hybrid fusion scheme 2 achieves a performance improvement of 5.04%, 5.85% and 4.76%, respectively. This is a significant improvement over the state-of-the-art unimodal biometrics systems and the improvement over the other multimodal systems is also encouraging.

4.3 Conclusion of Scheme 1 and Scheme 2

The proposed multimodal systems present a hybrid multimodal system based on feature level and score level fusion of face and palmprint biometrics. First of all, unimodal and multimodal recognition systems using feature extraction methods such as LBP, Log Gabor, PCA and LDA are considered in this study. The experiments are conducted on face, left palm and right palm, separately to show the accuracy of the unimodal systems.

The proposed hybrid systems using a combination of left palm, right palm and face features are applied using LBP features with and without PCA and LDA for dimensionality reduction. The experimental results of the proposed schemes show a significant performance improvement over the other multimodal systems considered in this study for the fusion of palmprint and face biometrics. Additionally, there is a big improvement achieved by the proposed schemes compared to the state-of-the-art unimodal face and palmprint systems.

Chapter 5

FEATURE SELECTION FOR THE FUSION OF FACE AND PALMPRINT BIOMETRICS

5.1 Description of Proposed Scheme 3

In this chapter, we propose a hybrid multimodal biometric system based on face and palmprint using Local Binary Patterns (LBP) feature extraction method and Backtracking Search Algorithm (BSA) as a feature selection method to improve the performance by selecting the optimal set of face and palmprint features.

The proposed scheme is further extended to model face and palmprint data to provide a robust multimodal biometric system at matching score level fusion. Sum Rule is then performed on tanh normalized scores of each modality. Finally the matching module is performed using Nearest Neighbor Classifier to compute the recognition accuracy.

The number of independent runs is taken as 30, and the enrollment and testing phases are repeated *n* times (where $n = 10$) without any overlapping between these two sets. The experiments are carried out on a large virtual database combining face and palmprint data coming from two different unimodal databases over 235 subjects. Extensive analysis is performed on unimodal and multimodal face-palmprint biometric systems. The performance of different fusion systems are tested on FERET face and PolyU palmprint databases. Further, the experiments are carried out independently to analyze the performance achieved by the proposed hybrid multimodal system.

The contribution of the proposed system is to improve the recognition rate by using Local Binary Patterns facial feature extraction and reducing computation time by using Backtracking Search Algorithm which selects the proper set of features. The motivation of the proposed hybrid system is to use Local Binary Patterns as a simple but efficient operator to describe local image patterns. The optimal features are then selected using Backtracking Search Algorithm to overcome the high computational time as shown in Figure 12 and Figure 13. These figures are described in the next subsections in detail.

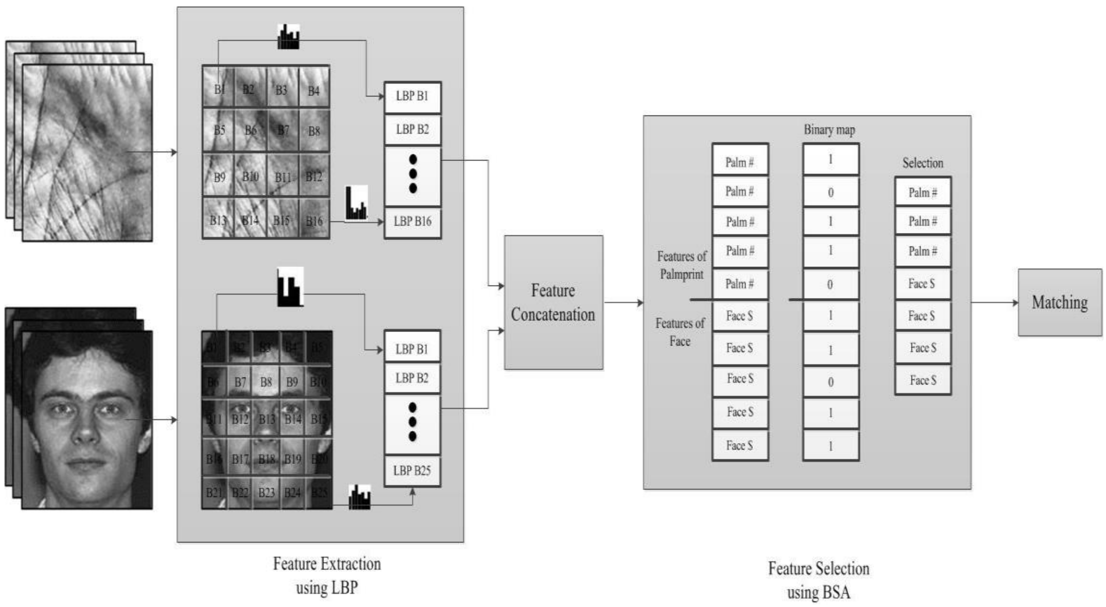

Figure 12: Block diagram of feature extraction and feature selection stages of the proposed scheme

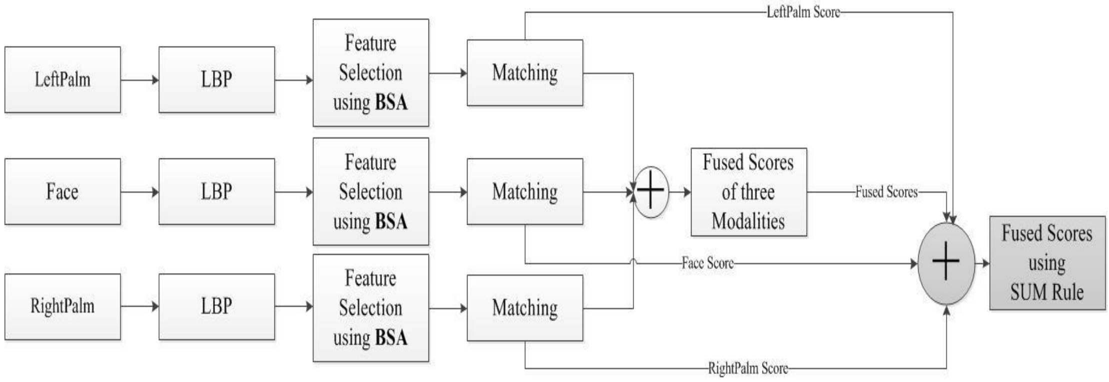

Figure 13: Proposed scheme of score level fusion

5.2 Feature Selection Using BSA

Backtracking Search Algorithm (BSA) is a novel population based iterative evolutionary algorithm that has been proposed by Civicioglu [101]. BSA is designed to search for the local and global optimum for an optimization problem. BSA uses a unique mechanism that includes three basic genetic operators such as selection, mutation and crossover to generate trial individuals. A random mutation strategy is employed in BSA. It uses only one direction for each target individual. BSA randomly chooses the direction of individual from individuals of a randomly chosen previous generation. BSA uses a non-uniform crossover strategy that is much more complex than other traditional crossover strategies used in many genetic algorithms.

5.2.1 Principle of BSA

Many feature selection algorithms have been used to perform feature selection of multimodal biometrics features. In this study, we employ BSA which has a simple structure that is effective for solving multimodal problems. The binary BSA is used to perform a selection of face and palmprint concatenated features. BSA is a dual population algorithm and the old populations that may include efficient individuals are well used based on randomly selected previous generation while PSO does not use previous generation populations.

The objective of feature selection is to perform search in very large dimension space to remove irrelevant features and retain only relevant ones. We mainly focus on the optimization problem of reducing the dimension of face and palmprint features, while it has never been applied to large scale biometric feature selection so far.

The steps of BSA can be summarized as follows:

Step 1: BSA initializes the population with

$$P_{i,j} \sim U(low_i, up_j) \tag{7.1}$$

where U is the uniform distribution, N and D are the population size and the problem dimension, respectively, and each $P_{i,j}$ is a target individual in the population P $for\ i = 1, 2, \ldots, N$ and $j = 1, 2, \ldots, D$.

Step 2: BSA's Selection-I stage analyses the population, and determines the old population $oldP$ in equation (7.2) according to the beginning of each iteration through the if-then rule in equation (7.3) .

$$oldP_{i,j} \sim U(low_i, up_j) \tag{7.2}$$

$$\text{if a} < \text{b then oldP} := \text{P} \mid \text{a, b} \sim \text{U}(0, 1) \tag{7.3}$$

where $:=$ is the update operation. Equation (7.2) ensures that BSA generates a population belonging to a randomly selected previous generation as the old population and remembers this old population until it is changed.

Step 3: BSA mutation and crossover processes generate the new off spring from the current population and old population during each generation by using equation (7.4) as follows:

T = P + (map .* F).* (oldP - P) (7.4)

where map is a binary integer-valued matrix of size $N \times D$ and F is the scale control factor that controls the amplitude of the search-direction matrix. The initial value of the trial population is calculated by using the advantages of the old population experiences from previous generation. In the crossover process step, a binary integer-valued matrix (map) is generated that indicates the individuals of T to be manipulated by using the relevant individuals of P.

Step 4: BSA Selection-II stage is performed after one generation is finished. It compares the fitness value of each trial population with the fitness value of initial population. If the fitness value of any trial population is better than the fitness value of the individual population, the fitness value of the trial population is assigned to the fitness value of initial population and the coordinates of it are assigned to initial population coordinates.

Step 5: BSA determines the current best fitness value in the whole newly generated population and its coordinates in the current iteration.

Step 6: The iteration repeats steps 2-5 until a stopping criterion is met. Then the global best value and its coordinates become the output as the optimal solution to the problem as shown in Figure 14.

```
//Initialization
Initialization of binary population P and old population oldP randomly generated
by U (0,1)

//Initial fitness value of P
for each individual S in P do
        apply S on all the images in the database
        calculate fitness value of the corresponding S (recognition rate)
end for
while stopping criteria are not met do
// Selection-I
        update oldP by taking the advantages of P using U (0,1) OR permuting
        arbitrary changes in position of individuals in oldP

//Generation of Trial-population
        perform mutation and crossover strategies to generate trial population T
        using initial-map matrix

//Selection-II
for each individual S in T do
        apply S on all the images in the database
        calculate fitness value of the corresponding S (recognition rate)

 if fitness-value of any S in T is better than fitness-value in P then
        take current value of S and its coordinates as new individual
 end if
        update P
end for

//Export global optimum value
choose best fitness value among all individuals in current iteration, and keep it in the
global optimum value fitnessP_best and its coordinates in P_best

end while
```

Figure 14: BSA Algorithm used in the proposed method [101]

5.2.2 Representation of Populations

In this work, we start the initialization process by generating the binary initial population and old population of size $D \times N$ using uniform distribution function $U(0; 1)$, where D and N are the dimension of the features and the population size, respectively. Each solution is then represented as a binary bit string consisting of 0’s and 1’s. The value of `1` indicates that the feature is selected for the next step while `0` means that the feature is not selected.

5.2.3 Fitness Function

In order to evaluate each candidate solution in all feature selection algorithms, an appropriate fitness function is needed. In our classification problem, the main objective of fitness function is to maximize the recognition rate. In that case, fitness function is computed as the distance of all training samples with the given test sample using Euclidean distance measurement. Then, we select the one that has the lowest distance value with the test sample. We evaluate whether they belong to the same class or not. We repeat it for all the testing samples and count the number of acceptance and rejection. The fitness function is defined as follows:

$$\text{Recognition Rate}=\frac{N_{accepted}}{N_{test}} \tag{7.5}$$

where $N_{accepted}$ is the number of successful recognition and N_{test} is the number of all testing images in the database.

5.2.4 Control Parameters of the Algorithm

BSA parameters have been chosen experimentally in our study. The maximum number of iterations is taken as 50. We experimentally used different size of populations from 5 to 40 in steps of 5 for each of the fitness functions. Finally we fixed the population size as 30 since any further improvement is not provided. A default value of scale factor $F = 3.randn$ is suggested in the literature for general approach in [101] where $randn \sim N(0,1)$ (N is the standard normal distribution). However, in our experiments we found better results with the value $F = 1$.

5.3 Description of Proposed Scheme 3

In a multimodal biometric system, an effective fusion method is needed for combining information from various single modality systems. The score level fusion is the best due to its simplicity and rich source of information.

This section describes our proposed method in detail (Proposed scheme 3) which involves match score level fusion by utilizing the scores provided by face and palmprint modalities in two different stages. In order to fuse face and palmprint scores, first we performed Local Binary Patterns (LBP) due to its discriminative power to extract the features which lead to increase feature space dimension. Then, Backtracking Search Algorithm (BSA) is applied as a feature selection method to select an optimized subset of features from original sets by removing the irrelevant data. The block diagram of the proposed hybrid fusion scheme is shown in Figure 13.

The following is the detailed stages employed in the proposed method for face and palmprint identification:

Step 1: Image preprocessing is performed on face and palmprint images separately. Each palm and face image is resized to 50×50 and 80×64, respectively. Following this stage, all images undergo Histogram Equalization technique and then normalized with Mean Variance Normalization.

Step 2: Each modality is then filtered using LBP to be divided into several blocks. The number of partitions used in palm and face is 16 and 25 respectively, with $P = 8$ neighbors and radius $R = 2$ (each palm is divided into 4×4 and face into $5 \times$

5 partitions). LBP histogram features are extracted from each biometric image to produce a global feature vector of each modality.

Step 3: Due to high dimension feature space, before producing the scores, BSA is applied to find a proper feature subset of each biometric source by removing irrelevant and redundant information as demonstrated in Figure 12.

Step 4: The matching scores generated by the face and palmprint modalities may not be on the same numerical range. In order to avoid degradation in fusion accuracy, they have to be transformed into a unique domain before fusing the match scores. In this study, the normalized scores are obtained by using tanh-normalization method which is reported to be robust and highly efficient [17]. In order to fuse the scores of the proposed scheme, Sum Rule technique is employed.

Step 5: The fused scores of three biometrics coming from Step 4 are considered and score fusion with each biometrics resource scores is performed to have a single scale score.

Step 6: Euclidean distance measure is used to measure the similarity between test and train images. Nearest Neighbor Classifier is employed to classify the individuals after the fusion of their normalized face and palmprint scores.

5.4 Experimental Results of Proposed Scheme 3

This section presents the experimental results of unimodal systems, multimodal systems and the proposed fusion strategy on different modalities. There is no available face-palmprint multimodal database collection including face and palmprint images of the same subject. Thus, all experiments are carried out on a virtual multimodal database combining face and palmprint coming from two independent unimodal databases. In order to investigate the performance, we choose FERET database for face modality and PolyU database for palmprint modality which are widely used databases for benchmarking.

PolyU database is provided by Hong Kong Polytechnic University with 235 segmented subjects [98]. Different number of images from each subject, from each of the left and right hand, are acquired in varying hand pose variations. In addition, all the original images of size 150×150 pixels are cropped and resized to 50×50. In this study, a subset of 235 users (each user providing 5 different palm images) is used. For each user, 3 images are randomly assigned as training and the rest 2 images as testing samples. On the other hand, face images of size 80×64 in FERET database have been captured under semi-controlled conditions such as illumination conditions (right-light, left-light and center-light), a wide range of poses (frontal and oblique views), different expression (happy, sad, normal and sleepy) and with or without glasses [93]. In our multimodal system, 235 subjects, each with 10 samples of palm and face images are considered. Hence, 705 training samples and 470 testing samples are collected. Recognition test was performed 10 times using randomly selected testing and training sets and an average result was calculated. The images selected in the training set were not used in the testing set.

Hence, experiments are performed without any overlapping between the sample images in these two subsets. In order to evaluate the effectiveness of the proposed hybrid system, we examined both unimodal and multimodal biometrics fusion results separately. It is noticed that all methods used in the experiments employ the same distance measure which is Euclidean distance.

5.4.1 Unimodal Biometric Systems

The first experiments analyze the results of the implementation of different unimodal recognition systems s,uch as right-palm, left-palm and face. The experimental results are demonstrated in Table 5 using the local feature extractor LBP. In particular, we have used LBP(8,1), LBP(8,2), LBP(16,1) and LBP(16,2) for palmprint in order to test different LBP operators. As it is illustrated in Table 6, the best result is achieved with the operator LBP(8,2). In addition, according to the results investigated in [102, 103], we decided to use LBP(8,2) for face and palmprint recognition.

Table 5: Recognition rates for different unimodal systems.

Methods	Left-palm		Face		Right-palm	
	Avg. Performance (%)	Min-Max Interval	Avg. Performance (%)	Min-Max Interval	Avg. Performance (%)	Min-Max Interval
LBP	94.02 ± 0.92	[92.55; 95.74]	83.21 ± 7.87	[74.68; 96.17]	94.30 ± 0.90	[93.19; 95.74]

Table 6: Comparison of different LBP operators for palmprint recognition.

LBP Operator	Grid				
	3*3	4*4	5*5	6*6	10*10
LBP(8,1)	91.53	92.57	92.30	91.96	89.69
LBP(8,2)	93.36	**94.02**	92.53	91.40	88.74
LBP(16,1)	44.94	63.62	73.64	78.40	86.40
LBP(16,2)	56.74	68.74	75.43	78.28	83.79

5.4.2 Multimodal Biometric Systems

Using the multimodal face and palmprint database, two sets of experiments are performed to demonstrate the performance of secured fusion methods. The first experiment (Experiment 1) is performed to analyze the performance of feature level fusion as shown in Figure 15. It involves the combination of feature sets corresponding to face and palmprint data. It is performed by a simple concatenation of the extracted features. On the other hand, concatenated face and palmprint features obtained from LBP feature extractor can be reduced by performing BSA feature selection as shown in Figure 16 with the block diagram of match score level fusion for face-palmprint biometric system (Experiment 2).

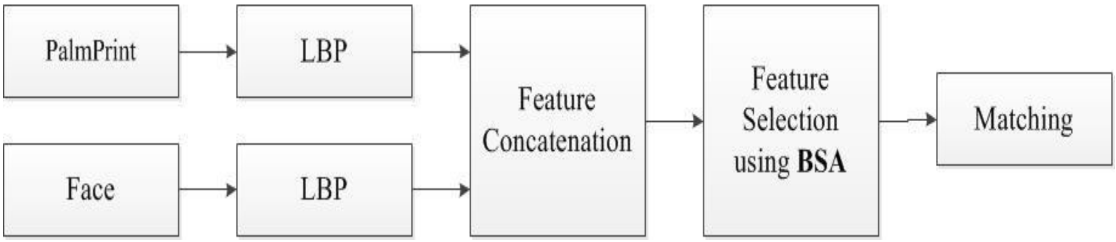

Figure 15: Block diagram of feature level fusion for face-palmprint biometric system (for Experiment 1)

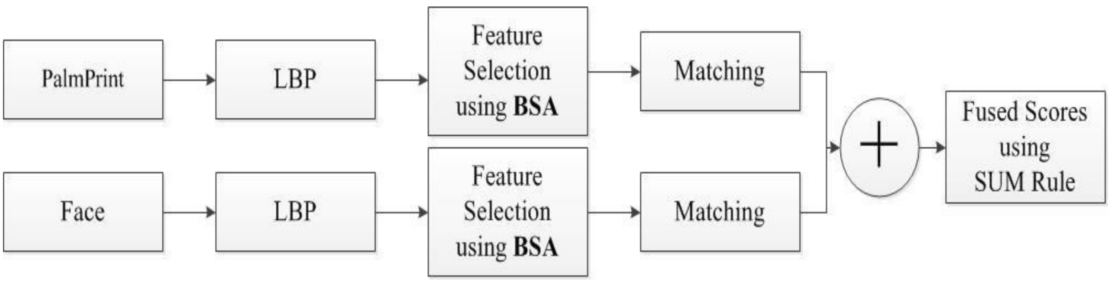

Figure 16: Block diagram of match score level fusion for face-palmprint biometric system (for Experiment 2)

The result of the multimodal systems with and without BSA are carried out for the analysis of match score level fusion. Each biometric modality generates matching scores which are normalized using tanh-normalization technique to obtain a single score. Finally, we employed the Sum Rule to perform the fusion of face and palmprint biometrics. On the other hand, BSA feature selection is performed on the extracted features coming from each biometric model before fusing the scores.

Table 7: Fusion methods for palmprint-face multimodal recognition system

Methods	without (BSA)		**with (BSA)**	
	Average Performance (%)	Min-Max Interval	Average Performance (%)	Min-Max Interval
LeftPalm-Face,LBP (feature-level fusion)	90.98 ± 4.81	[85.32; 98.94]	**93.60** ± 2.72	[88.17; 98.95]
LeftPalm-Face,LBP (score-level fusion)	97.49 ± 0.96	[95.96; 99.15]	**97.88** ± 0.81	[96.31; 99.29]
RightPalm-Face,LBP (feature-level fusion)	91.23 ± 4.50	[86.38; 98.72]	**94.25** ± 2.29	[90.31; 98.36]
RightPalm-Face,LBP (score-level fusion)	97.94 ± 1.01	[96.81; 99.79]	**98.10** ± 0.88	[96.53; 99.59]

Accordingly, all the results obtained using the system in Figure 16 are the average values over 30 independent runs. It can be observed from Table 7 that using BSA helps to achieve an improvement over the other methods. Fusion methods with BSA increase the recognition accuracy of feature-level fusion and score-level fusion by 1.02% and 1.002%, respectively compared to using fusion methods without applying BSA. Table 8 reports the computation complexity (for test phase on the whole database) and the number of selected features after applying BSA.

Table 8: Computation time and related number of features with and without BSA feature selection.

Methods	Computation time in sec		Number of features used	
	without (BSA)	with (BSA)	without (BSA)	with (BSA)
LeftPalm-Face,LBP (feature-level fusion)	543	170	10469	5441
LeftPalm-Face,LBP (score-level fusion)	544	213	10469	5271
RightPalm-Face,LBP (feature-level fusion)	542	170	10469	5233
RightPalm-Face,LBP (score-level fusion)	543	210	10469	5037

It is shown in Table 8 that BSA feature selection reduces the feature space by 40% and 50% in score-level and feature-level fusion, respectively. Hence, computation time is considerably reduced while obtaining higher level of performance.

Table 9: Recognition rate of the proposed method.

Method	Avg. Performance (%)	Min-Max Interval
Proposed method (LBP + BSA)	**99.17 ± 0.41**	[98.42; 99.87]

5.4.3 Comparison of the Proposed Method Results with the Existing Unimodal and Multimodal Systems

The proposed face-palmprint based personal identification system tries to improve the identification results of single biometric systems based on facial and palmprint features by integrating them using fusion at the matching-score level. It is demonstrated that fusing LBP scores coming from Leftpalm-Rightpalm-Face using BSA and Sum Rule in two separate stages improves the recognition accuracy that outperforms most of the methods considered in this study. In fact, a high recognition performance such as **99.17%** is achieved as shown in Table 9 by applying BSA on LBP algorithm with Sum Rule fusion strategy.

On the other hand, in order to evaluate the performance of the proposed method against the existing state-of-the-art methods, experiments are carried out over the same databases reported in [36]. Hence, a large database is composed by combining different face databases such as ORL [94], Essex [96] and extended Yale-B database [97, 95]. A subset of 40 subjects, 38 subjects and 72 subjects are taken from ORL, extended Yale-B and Essex database, respectively.

The whole database consists of 900 images over 150 subjects with six images per subject. The palmprint database is taken from PolyU which also consists of 150 subjects each with six images. All the images are resized to 50×50 pixels. Images from face and palmprint databases are randomly paired to obtain a virtual multimodal database. Additionally, experimental conditions and the number of training and test samples are also taken as the ones used in the corresponding references, so that the fairness is guaranteed for comparative evaluations.

Table 10: Comparison of the proposed multimodal system with the state-of-the-art methods.

Methods	Face	Palmprint	Multimodal
Gabor-PCA [34]	52.57	62.72	90.73
Gabor-KDRC [35]	71.28	63.81	94.40
Two-step MCPCA [32]	59.70	89.60	92.50
Log Gabor+KDDA+PSO [15]	83.78	87.23	98.62
KSDA-GSVD [33]	93.87	91.64	99.44
GWT+PSO [36]	95.12	91.15	98.34
Proposed method (LBP + BSA)	**85.00**	**94.64**	**98.12**

A comparable result is obtained in comparison to the state-of-the-art systems [32, 34, 35, 36] as shown in Table 10. The performance of our proposed system is significantly better than some of the proposed multimodal systems. It achieves 5.62%, 7.39%, 3.72% improvement compared to three methods in [32, 34, 35], respectively. It is clearly observed that our proposed multimodal system performs well compared to the proposed methods based on face and palmprint biometrics and it has comparable performance with [32], [15]and [34].

Considering the performance of [32] for multimodal system, one can see that [33] has achieved better accuracy in which many linear and non-linear techniques are used to improve the recognition rate. It uses multiple projection extensions which increases the computational complexity.

On the other hand, Log Gabor is employed in [15] which increases the cost of memory usage due to filtering images with multiple orientations and scales. Both KDDA and PSO are used to reduce the large feature space dimension which increase the computational time. The performance of [15], [33] and [36] are slightly better than the proposed method. The difference between the proposed method and these three methods is only 0.50%, 1.32% and 0.22%, respectively.

5.4.4 Conclusion of Scheme 3

This chapter presents a multimodal personal identification system utilizing face and palmprint biometric systems using match score level fusion technique. The unimodal and multimodal identifiers utilize feature extraction method such as Local Binary Patterns (LBP) and feature selection method such as Backtracking Search Algorithm (BSA). The experiments are conducted on face, left-palm and right-palm separately to demonstrate the accuracy of the unimodal and combined multimodal systems.

The experimental results of the proposed scheme using FERET face and PolyU palmprint databases demonstrate considerable improvement in recognition results compared to other multimodal systems and unimodal identifiers. A comparison of the proposed multimodal system with the state-of-the-art systems shows that the proposed approach is better than some of the state-of the art methods and is comparable with the best performing methods in the literature.

Chapter 6

SPOOF DETECTION ON FACE AND PALMPRINT BIOMETRICS

6.1 Introduction

In the last decades, the increasing interest in security and the evaluation of the robustness of biometric systems has shown to be a major field of research. Most of the biometric systems are based on pattern-recognition systems that are usually designed to only recognize identities without concern whether the identity is real or not. Spoofing attacks are a major concern to biometric systems. In these attacks, a person tries to masquerade as someone else by presenting some type of synthetically produced artifact such as printed photograph, mask or 3D model of a targeted person in front of the camera to fraudulently gaining illegitimate access to the biometric system.

In order to counter spoofing in 2D face and palmprint recognition systems, techniques are generally divided into motion, liveness and texture analysis [104]. Texture analysis techniques mainly detect texture patterns such as print failures, and overall image blur to detect attacks. The printing process and the paper structure that produce texture features can differentiate those printed images from real face images. Motion analysis refers to motion features such as optimal flow and are used to get over the dependency on certain texture patterns [105, 106]. However, motion analysis meet some limitations when there is low motion information due to changing behavior of the user, high noisy images and low resolution. Motion analysis might also failed when spoof attacks is performed using more sophisticated methods, just like 3D sculpture face model [107].

On the other hand, liveness cues depend on the vitality signs of a biometric trait by analyzing spontaneous movements that cannot be detected in photographs. Eye blinking, lips movement and changes in facial expression can be considered as these cues for 2D face recognition. Cue-based methods impose extra requirements on the recognition system, and hence have a narrower application range. As a result, one solution may not always be generalized to other attack methods.

Furthermore, the quality of digital images could visibly degrade, since they are subject to distortions during acquisition, capturing, processing, transmission and reproduction. For example, palmprint images captured from a printed paper are more likely to present local acquisition artifact such as spots and patches; face images captured from an electronic device will probably be over or underexposed. Recently, a significant amount of research has gone into the development of quality assessment methods that take advantage of known characteristics of the human visual system. Therefore, using a wide range of image quality methods (IQM) should detect the quality differences between real and fake samples.

6.1.1 Contributions

The contribution of this thesis in face and palmprint spoof detection can be summarized as follows:

- In order to counter both printed photo and replayed video attacks, different texture-based and IQA-based methods are proposed.
- We constructed a palmprint spoof database including 50 subjects made by printed palmprint photo using the camera. It allows us to evaluate the ability of different palmprint spoof detection algorithms.
- We present the results of both face and palmprint spoof detection methods using two public-domain face spoof databases (Idiap PRINT-ATTACK and REPLAY-ATTACK) and our own palmprint spoof database.

6.2 Texture-based Methods

Texture-based methods focus on textural differences between the live and counterfeit biometric images. The key idea is to detect the structure and the dynamics of the biometric traits micro-textures that characterize only real faces. Texture-based methods have achieved significant success on different face, iris, fingerprint databases [53, 58, 108, 109].

In this work, Local Binary Patterns (LBP), Difference of Gaussians (DoG) and Histograms of Oriented Gradients (HOG) have been implemented for analyzing and measuring the texture quality and determining whether degradations occurred due to recapturing process.

6.2.1 Difference of Gaussians

Difference of Gaussians (DoG) band pass pyramids approach was originally proposed by [110, 111] and is very widely used in artificial vision. In order to increase detailed information presented in a digital image, DoG removes high frequency components by constructing a Gaussian pyramid from the input image. It repeats smoothing and subsampling, and a Difference of Gaussians pyramid will be computed from the differences between the adjacent levels in the Gaussian pyramid. Then, interest points are obtained from the points at which the DoG values assume extrema with respect to both the spatial coordinates in the image domain and the scale level in the pyramid.

6.2.2 Histograms of Oriented Gradients

Histograms of Oriented Gradients (HOG) approach is a feature descriptor used in image processing and computer vision for the purpose of object detection. The technique counts occurrences of gradient orientation in localized portions of an image [112]. It divides the image window into small regions. Regions can be either rectangle or radial. Each region accumulating a weighted local 1D histogram of gradient directions over the pixels of the region. Finally, the combined histogram features coming from each region provide a single feature vector.

6.3 Image Quality Assessment Metrics

Image quality metrics can be classified according to the availability of an original (distortion-free) image, with which the distorted image is to be compared. Most existing techniques are known as full-reference (FR), meaning that the quality of a test image is evaluated by comparing it with a reference image that is assumed to have perfect quality. No-reference (NR) metrics try to assess the quality of a test image without any reference to the original one.

In this thesis, the well-known full-reference objective measurements are used to evaluate image quality including, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity (SSIM), Mean Squared Error (MSE), Normalized Cross-Correlation (NXC), Maximum Difference (MD), Normalized Absolute Error (NAE) and Average Difference (AD). Our main goal is to investigate the statistical discriminative power of several quality measures to distortion due to compression, additive noise and blurring.

6.3.1 Pixel Difference Measures

These features compute the distortion between two images on the basis of their pixel wise differences. In this work, we include Mean Squared Error (MSE) [112], Peak Signal to Noise Ratio (PSNR) [113], Average Difference (AD) [114], Maximum Difference (MD) [114] and Normalized Absolute Error (NAE) [114] in which the equations for each measure are shown below, where, x is the original image of size $M \times N$ which is assumed to have a high quality and y is the distorted image.

$$MSE\ (x, y) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{(i,j)} - y_{(i,j)})^2 \tag{9.1}$$

$$PSNR = 10log_{10}\frac{(2^n - 1)^2}{\sqrt{MSE}} \tag{9.2}$$

$$AD\ (x, y) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{(i,j)} - y_{(i,j)}) \tag{9.3}$$

$$MD(x, y) = MAX\left|x_{(i,j)} - y_{(i,j)}\right| \tag{9.4}$$

$$NAE\ (x, y) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|x_{(i,j)} - y_{(i,j)}\right|}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|x_{(i,j)}\right|} \tag{9.5}$$

6.3.2 Structural Similarity Measures

The distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones. Structural Similarity Index Measure (SSIM) [115], has the simplest formulation as shown below and has gained widespread popularity in a broad range of practical applications.

$$SSIM(x,y) = \frac{(2\times\ \bar{x}\times\ \bar{y} + C1)(2\ \times \sigma_{xy} + C2)}{\left(\sigma_x^2 + \sigma_y^2 + C2\right)\times((\overline{x})^2 + (\overline{y})^2 + C1)} \tag{9.6}$$

where $C1$ and $C2$ are constants and $\bar{x}$, $\bar{y}$, σ_x^2, σ_y^2 and σ_{xy} are given as:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9.7}$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{9.8}$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2 \tag{9.9}$$

$$\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \bar{y})^2 \tag{9.10}$$

$$S\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \tag{9.11}$$

6.3.3 Correlation-based Measures

The similarity between two digital images can be quantified in terms of the correlation function such as Normalized Cross-Correlation (NXC) [114] in which the equation of this measure is shown below.

$$NXC\ (x,y) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\ x_{(i,j)} \times y_{(i,j)}}{\sum_{i=1}^{M}\sum_{j=1}^{N} x_{(i,j)}} \tag{9.12}$$

6.4 Proposed Anti-spoofing Framework

This section presents the proposed anti-spoofing approaches which utilize both texture-based methods and image quality assessments (IQA) in order to distinguish between real and fake biometric traits. The proposed protection system may not be capable under different biometric systems and a very high performance may not be obtained for diverse spoofing attacks, but they provide a good level of security against printed photo and replayed video face and palmprint spoofing attacks. The pipeline of our proposed system is represented which consist of two different types of local feature extractors such as LBP histograms and HOG, two global feature extractors PCA and LDA and a simple Nearest Neighbor Classifier.

The following is the detailed stages employed in the proposed methods for face and palmprint spoof detection:

Step 1. Image preprocessing is performed on face and palmprint images separately. First, a video frame of face samples in Idiap databases is decomposed to single frames in order to produce single-image inputs. Then, all produced palm and face images are resized to 60×60 prior to the anti-spoofing experiments. Following this stage, all images undergo Histogram Equalization technique and then normalized with Mean Variance Normalization.

Step 2. All the images are then filtered with LBP or HOG which obtained the best results in REPLAY-ATTACK and PRINT-ATTACK databases, and divided into several blocks (each image divided into 5×5 blocks) to produce 25 blocks. Features are extracted from each biometric image to produce a global feature vector of each modality.

Step 3. Due to high dimension feature space, before producing the scores, PCA and LDA are employed to find a proper feature subset of each biometric source by removing irrelevant and redundant information.

Step 4. In order to avoid degradation in accuracy, the matching scores have to be transformed into a unique domain before classification. In this study, the normalized scores are obtained by using tanh-normalization method which is reported to be robust and highly efficient.

Step 5. Euclidean distance measure is used to measure the similarity between real and fake images. The classification is performed using Nearest Neighbor Classifier.

Step 6. On the other side, the original images are used prior to the computation of the IQ features. Normalized Absolute Error (NAE) is then used as the best Image Quality Assessment metric in order to provide a general quality score. This has allowed us to compare the image quality between a genuine images and fake one by considering the minimum error of a real or fake test sample with all real and fake images stored in training set.

Step 7. In **Step 5** and **Step 6**, each classifier is applied separately (but no decision is taken). The final decision is postponed to the end of the fusion process in order to take advantage of each algorithm. In the fusion step, the results provided by different texture-based methods in **Step 5** and image quality assessment metric in **Step 6** are aggregated using logical OR operator which returns the decision real if either or both decisions are real and returns fake otherwise. Figure 17, presents our proposed anti-spoofing approach.

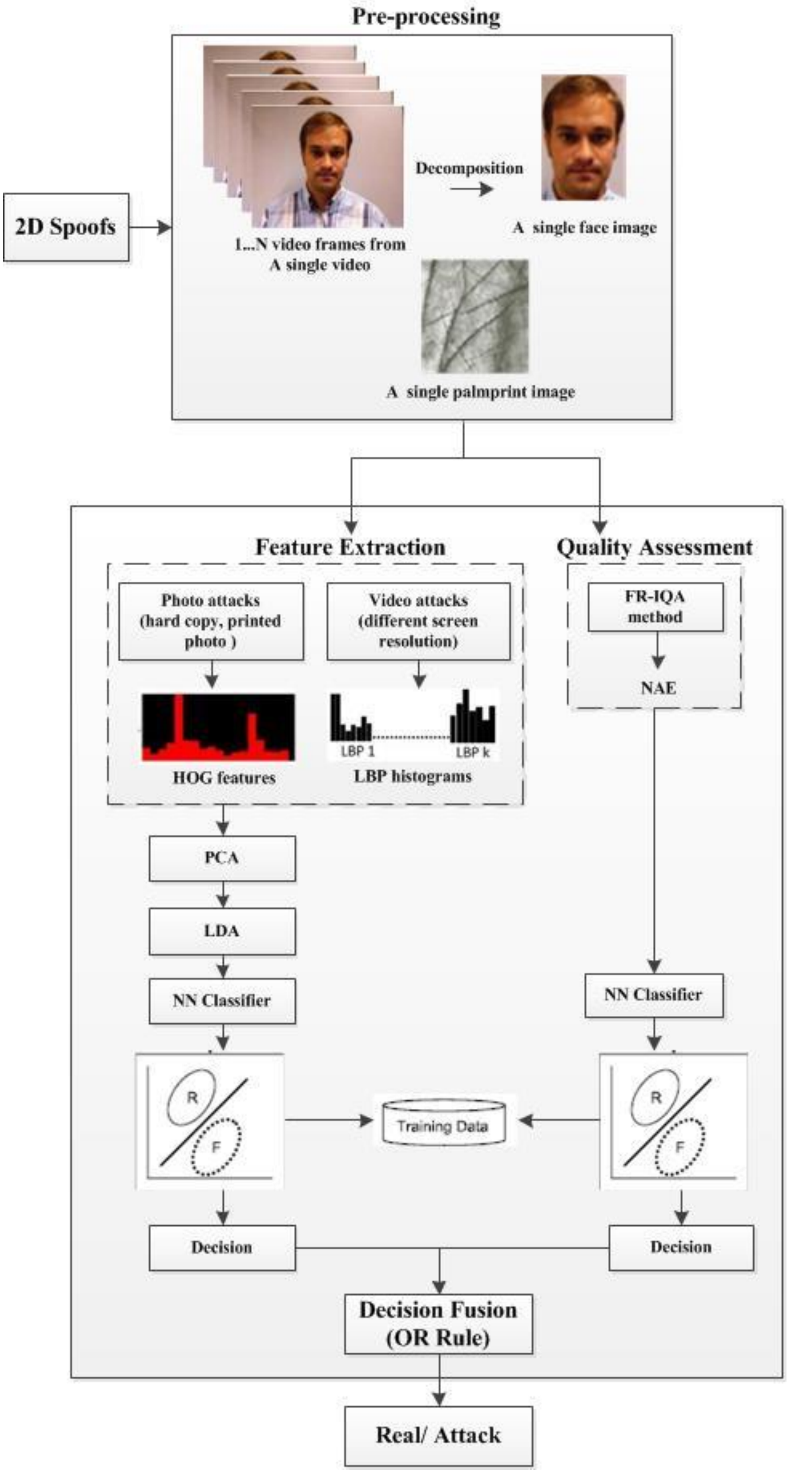

Figure 17: The Proposed Anti-spoofing Approach

6.5 Experimental Result

This section presents our experimental analysis on the proposed hybrid protection system and single texture-based and IQA-based method using the PRINT-ATTACK, REPLAY-ATTACK face databases and our palmprint spoof database. These experiments are performed to demonstrate the robustness of the proposed scheme against spoofing attacks. The results are presented on the tables for both evaluated schemes (using LBP, DoG and HOG) with and without performing PCA and LDA on the images. In addition, we examined the effect of image quality toward anti-spoofing accuracy.

A biometric spoofing detection system is subject to two types of errors. The False Genuine Rate (FGR), which is the number of false samples that are incorrectly classified as real, and the False Fake Rate (FFR), which is the number of genuine samples being considered as fake. The widely used performance measure is Half Total Error Rate (HTER), defined as half of the sum of the False Genuine Rate (FGR) and False Fake Rate (FFR). Hence, in all cases, performance of the palmprint spoof detection system has been reported in terms of FFR, FGR and HTER error rates (in percentage).

6.5.1 Palmprint Spoof Attack-printed Photo Database

Experiments are performed on PolyU database provided by the Hong Kong Polytechnic University. All the original gray-scale images of size 150×150 pixels are cropped and resized to 50×50. Due to non-availability of spoof palmprint database, we constructed a spoof database made by printed paper. In order to generate a printed photo for attack, KONICA MINOLTA 554eSeriesPCL printer 1200×600dpi is used to print subject’s palmprint on a plain A4 paper from PolyU database. Canon 6D camera is then used to capture a HD picture of size 5472×3648, which is then stored in spoof palmprint database. The average standoff for the printed photo attack is ~50cm. Figure 18 shows example images of genuine and spoof palmprint of one subject in the PolyU database. In this study, we prepared a palmprint dataset using 50 individuals, each including 10 real samples and 10 attack samples randomly selected from left and right hands. In general, for validating the performance under spoofing attacks the whole database of 50 individuals is divided into two sets. The general distribution of the database in the train and test is specified in Table 11. In this case attacker is assumed not to have previous knowledge about recognition algorithm and tries to access by only displaying printed palmprint photograph of the attacked person to the input camera. Furthermore, a printed palmprint image which is directly injected to the communication channel before the feature extraction step, will most likely lack some of the properties found in natural images.

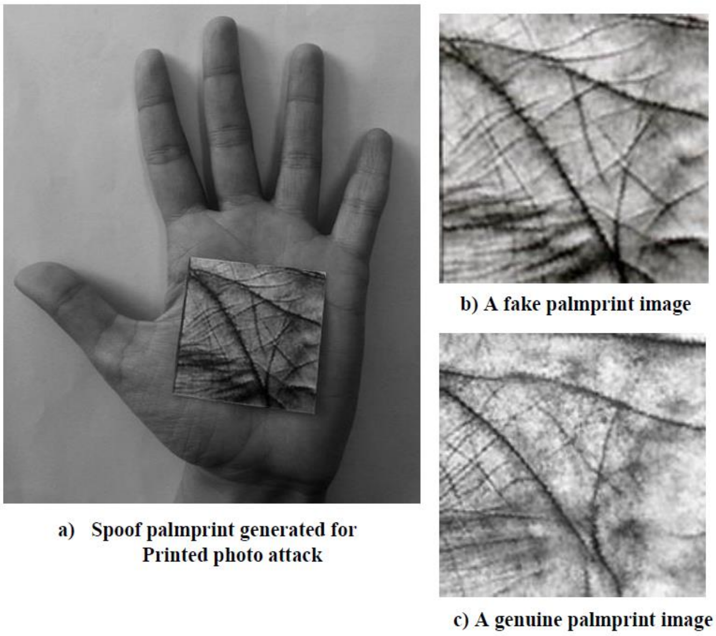

Figure 18: Samples of palmprint images.

Table 11: Number of Samples available in each real and fake subset in PolyU

PolyU Palmprint DB			
Train (Real/ Fake)		Test (Real/ Fake)	
# Individuals	# Samples	# Individuals	# Samples
15	300	35	700

6.5.2 Face Spoof Database

In this section, we provide a brief summary of two face spoof databases: Idiap PRINT-ATTACK and REPLAY-ATTACK databases which are publicly available from the Idiap Research Institute [22, 53]. These datasets consist of 200 short video clips of printed-photo and 1300 video clips of photo and video attack attempts recordings for both valid-access and attack attempts of 50 different subjects under different lighting conditions. Each video captured with a 320×240 resolution webcam of an Apple 13-inch MacBook Laptop with at least 240 frames each. The recordings were carried out under two different conditions: 1) controlled, with a uniform background and artificial lighting; and 2) adverse, with natural illumination and non-uniform background.

In addition, access attempts in the three attack subsets (print, mobile and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (paper, mobile phone or tablet): 1) hand-based and 2) fixed-support. The total set of videos is divided into 3 subsets for training, development and testing. Identities for each subset were chosen randomly without any overlap. In this study, the whole database has been split into training set (containing 15 subjects from training subset) and the grandtest (containing 35 subjects coming from development and testing subsets).

We evaluated our experiments on face databases only when the face regions are considered and the background is not included. For this reason, the input face image is first aligned based on two eyes locations and then is detected by Viola-Jones face detection algorithm which is widely used for face detection [117]. We extracted the live and fake face images from the corresponding videos. In particular, for each subject, we extracted 10 live face images and 10 spoofed face images collected in grandtest set.

In the grandtest experiments the protection method is trained using data from the print, mobile and highdef scenarios, and tested on three type of attacks in test set. This is probably the most realistic attack case while we cannot know a priori the type of artifact (paper, mobile phone or tablet) that the attacker will use to try to break into the system. Some typical images (frames extracted from the videos) from real and fake (print, mobile and highdef) access attempts are shown in Figure 19.

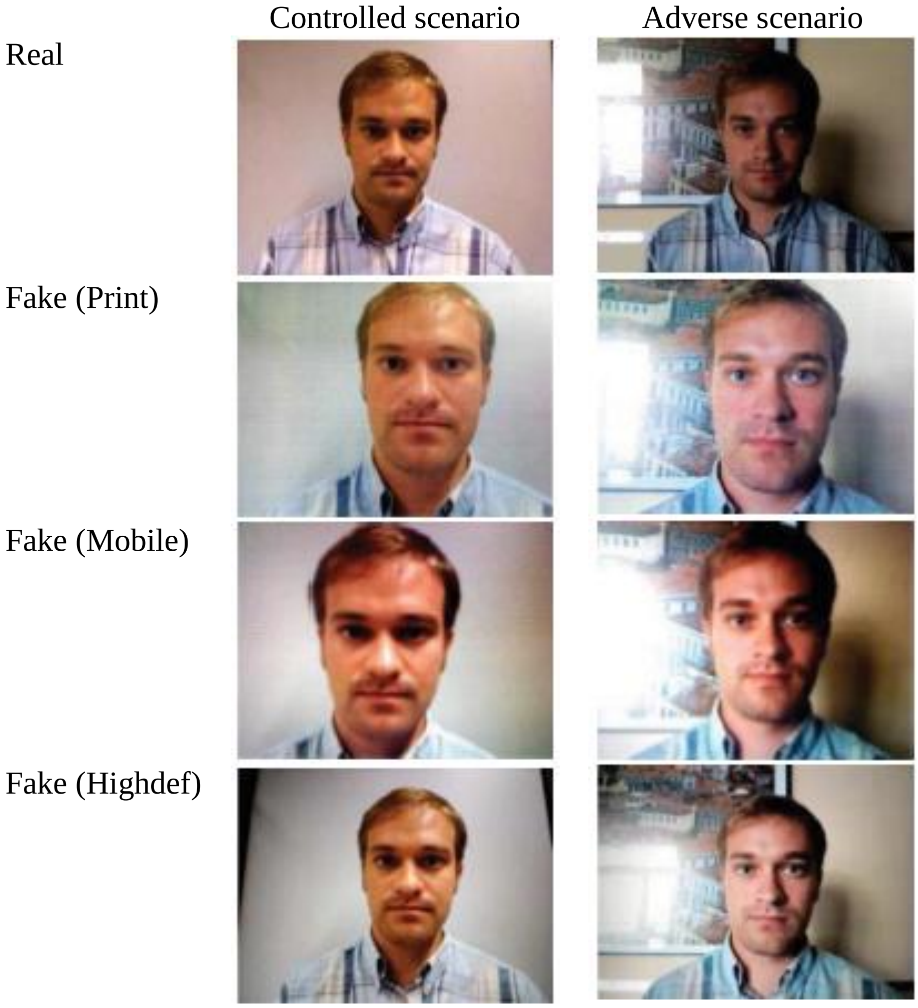

Figure 19: Examples of real and fake (print, mobile and highdef) face images available in REPLAY-ATTACK databases

6.5.3 Texture-based Protection Systems

The first experiments analyze the results of the implementation of three types of spoof detection feature vectors such as LBP, DoG and HOG with and without PCA and LDA for dimensionality reduction. In Table 12, we show the results obtained on the constructed spoof palmprint test set by the proposed LBP, DoG and HOG texture-based methods using a standard classifier based on Principle Analysis Component (PCA) and Linear Discriminant Analysis (LDA). The results for LBP, DoG and HOG using PCA-LDA features give an HTER of 45.1%, 16.9% and 11.1% respectively.

Similar experimental set up has been followed for print-attack database and the results are listed in Table 13. LBP+PCA-LDA and DoG+PCA-LDA features recorded an HTER of 81.6% and 50% while HOG+PCA-LDA recorded an HTER of 8.9%.

The results of the HOG feature extractor with PCA-LDA for the cut photo attacks on palmprint and face databases clearly show significantly better classification performance with the lower classification error rate.

Table 12: Results in HTER % on PolyU spoof database for texture-based methods

Methods	Without (PCA, LDA)			With (PCA, LDA)		
	FFR	FGR	HTER	FFR	FGR	HTER
LBP	42%	54%	48.4%	64.9%	25.4%	45.1%
DoG	8.2%	88.8%	48.5%	15.4%	18.3%	16.9%
HOG	37.1%	62.5%	49.8%	11.7%	10.6%	**11.1%**

Table 13: Results in HTER % on PRINT_ATTACK database for texture-based methods

Methods	Without (PCA, LDA)			With (PCA, LDA)		
	FFR	FGR	HTER	FFR	FGR	HTER
LBP	60%	35.7%	47.8%	72.3%	90.9%	81.6%
DoG	56.2%	61.4%	58.8%	0%	100%	50%
HOG	40%	43.7%	41.8%	0%	17.7%	**8.9%**

As in the palmprint and print-attack experiments, we have also conducted experiments at frame level. Results of the texture-based methods on Replay-Attack database are demonstrated in Table 14. In the case of Replay-Attack scenario, LBP+PCA-LDA has obtained the best classification accuracy recorded an HTER of

8.9%. Hence, it can be an appropriate protection approach to increase the security of biometric system.

Table 14: Results in HTER % on REPLAY_ATTACK database for texture-based methods

Methods	Without (PCA, LDA)			With (PCA, LDA)		
	FFR	FGR	HTER	FFR	FGR	HTER
LBP	52.5%	35.4%	44%	17.7%	0%	**8.9%**
DoG	42%	72.8%	57.4%	0.5%	86%	43.5%
HOG	42%	40%	41%	99.1%	0%	49.5%

6.5.4 Image Quality Assessment for Fake Biometric Detection

The second set of experiments are performed on a multi-attack protection method using 7 general image quality measures which aims to evaluate different image quality assessment (IQA) metrics in order to overcome certain type of spoofs. IQA-based method is based on a single-image input. Hence, each frame of the videos in the PRINT-ATTACK and REPLAY-ATTACK databases is considered as an independent input sample. Therefore, classification of real or fake is done on a frame-by-frame basis and not per video. Our experiments on Print-Attack and Replay-Attack databases also show the strength of the employed image quality assessments metrics.

As shown in Table 15 and Table 16, it is evident that the PSNR, SSIM and NAE methods have achieved better results rather than other methods. For both Print-Attack and Replay-Attack datasets, NAE produces the minimum error rate by HTER of 9% which is consistently selected as the best feature set for all the measured scenarios in the whole group of 7 quality measures.

Table 15: Comparison of HTER (%) on the grandtest protocol of the PRINT-ATTACK DB for the proposed IQA methods

Method	FFR	FGR	HTER
PSNR	8%	11.7%	9.8%
SSIM	6%	15%	10%
NAE	**15%**	**3%**	**9%**
MSE	15.7%	53.4%	34.5%
MD	23.4%	52.8%	38.1%
AD	66.5%	34.8%	50.7%
NXC	15.7%	53.4%	34.5%

Table 16: Comparison of HTER (%) on the grandtest protocol of the REPLAY-ATTACK DB for the proposed IQA methods

Method	FFR	FGR	HTER
PSNR	7.4%	14.5%	10.9%
SSIM	10%	54%	32%
NAE	**12%**	**6%**	**9%**
MSE	16%	50.5%	33.25
MD	27.1%	50.5%	38.8%
AD	51.1%	49.4%	50.2%
NXC	16%	50.5%	33.25

We have repeated the same experiments on our palmprint database in order to test the widely used general image quality approaches showing performance for different applications. The lowest detection error rate is obtained once we used MSE by recorded HTRE of 7.1%. In addition, PSNR, SSIM and NAE have also reported good performances by HTER of 27.9%, 23.6% and 27.9%, respectively.

Table 17: Comparison of HTER (%) on the grandtest protocol of the our constructed palmprint for the proposed IQA methods

Method	FFR	FGR	HTER
PSNR	48.8%	7.1%	27.9%
SSIM	20.5%	26.8%	23.6%
NAE	49.4%	6.5%	27.9%
MSE	7.1%	7.1%	7.1%
MD	98%	0.2%	49.5%
AD	0.0%	92.5%	46.2%
NXC	48.8%	37.1%	42.9%

In order to further improve the overall performance, the proposed protection system employs Normalized Absolute Error (NAE) as the best performing feature subset, and Histograms of Oriented Gradients (HOG) and Local Binary Patterns (LBP) as the best local feature descriptors. A comparable result is obtained in comparison to the state-of-the-art systems as shown in Table 18. Our proposed anti-spoofing approach which utilizes the fusion of both texture-based method and image quality assessment (IQA), namely proposed scheme 4, achieves an improvement by HTER of 5% and 1.2%, respectively compared to the single model systems considered for the texture-based methods and image quality assessments metrics on Print-Attack and Replay-Attack datasets.

Table 18: Comparative results showing classification error rate HTER (%) of the proposed scheme on Print-Attack and Replay-Attack databases

Method	**PRINT-ATTACK (HOG + NAE)**			**REPLAY-ATTACK (LBP + NAE)**		
	FFR	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**
Proposed scheme	0%	1%	**5%**	2.5%	0%	**1.2%**

On the other hand, compared to the results of texture-based and IQA-based algorithms on palmprint spoof database, the proposed fusion approach achieves a performance improvement as reported in Table 19. HOG+NAE recorded HTER of 5.8%, HOG+MSE recorded HTER of 5.8% and HOG+SSIM recorded 3.5%.

Table 19: Comparative results showing classification error rate HTER (%) of the proposed scheme on our own palmprint database

Method	**Palmprint (HOG + NAE)**			**Palmprint (HOG + SSIM)**			**Palmprint (HOG + MSE)**		
	FFR	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**
Proposed scheme	**11.4%**	**0.2%**	**5.8%**	**11.4%**	**0.2%**	**5.8%**	**5.4%**	**1.7%**	**3.5%**

On the other hand, in order to demonstrate the effectiveness of the proposed protection approach, a comparison is presented with the state-of-the-art methods. Similar experimental protocol with the protocol used in the state-of-the-art methods is followed and the results are shown in Table 20 that are obtained by different texture-based detection methods on the face compared to the performance of our proposed method.

Table 20: Comparison Results in HTER(%) on Replay-Attack and Print-Attack Databases for Different State-of-the-art Methods.

Method	**Replay-Attack**		**Print-Attack**	
	Dev	**Test**	**Dev**	**Test**
DMD+SVM [21]	8.50	7.50	0.00	0.00
DMD+LBP+SVM [21]	5.33	3.75	0.00	0.00
PCA+SVM [21]	20.00	21.50	16.25	15.11
PCA+LBP [21]	11.67	17.50	9.50	5.11
DMD+LBP+SVM [21]	0.50	0.00	0.00	0.00
PCA+LBP+SVM [21]	21.75	20.50	11.50	9.50
$\boldsymbol{LBP_{3*3}^{U2}}$**+ LDA** [53]	19.60	17.17	-	-
$\boldsymbol{LBP_{3*3}^{U2}}$**+SVM** [53]	14.84	15.16	-	-
LBP+SVM [54]	13.90	13.87	-	-
LBP-TOP+SVM [58]	7.88	7.60	-	-
$\boldsymbol{LBP_{8,1}^{U2}}$**+SVM** [118]	10.00	14.87	5.00	3.12
$\boldsymbol{LBP_{8,2}^{U2}}$**+SVM** [118]	11.66	14.37	5.00	2.50
$\boldsymbol{LBP_{16,2}^{U2}}$**+SVM** [118]	8.50	12.87	5.00	3.12
$\boldsymbol{LBP_{8,1}^{U2}+LBP_{8,2}^{U2}+LBP_{16,2}^{U2}}$**+SVM** [118]	8.50	11.75	3.33	5.60
Proposed pipeline	**1.60**	**1.00**	**4.30**	**4.70**
	Grandtest		**Grandtest**	
IQA-based [66]	15.2		-	
LBP-based [53]	15.2		-	
LBP-based [54]	13.9		-	
Proposed pipeline	**1.2**		**5**	

It is observed that an HTER of 1.6% was recorded on the development set of the Replay-Attack dataset and an HTER of 1% on the test set. For the Print-Attack dataset, we recorded an HTER of 4.3% and 4.7% on development and test sets, respectively. The performance of our proposed system is significantly better than most of the proposed spoof detection systems. Furthermore, different LBP-based anti-spoofing approaches were tested following the same protocol used in the present study. A comparison between texture-based and IQA-based protection methods is also presented in Table 20 in which all results are reported on the grandtest scenario. These results also show the effectiveness of the proposed method compared to the state-of-the-art systems.

Chapter 7

CONCLUSION AND FUTURE WORKS

This thesis presents several multimodal personal identification systems utilizing face and palmprint biometric systems using feature level and match score level fusion techniques. The unimodal and multimodal identifiers utilize feature extraction method such as LBP, Log Gabor, PCA and subspace LDA. A feature selection method namely Backtracking Search Algorithm (BSA) is also used in order to improve the performance by selecting the optimal set of face and palmprint features.

In the first and second proposed schemes, fusion of face and palmprint biometrics using local and global feature extractors in both feature level and match score level is presented. The experiments are conducted on face, left-palm and right-palm separately to show the accuracy of the unimodal systems. The proposed hybrid systems using a combination of left-palm, right-palm and face features are applied using LBP features with and without PCA and LDA for dimensionality reduction.

The experimental results of the proposed schemes using PolyU palmprint and FERET face databases show a significant performance improvement over the other mulimodal systems considered in this thesis for the fusion of face and palmprint biometrics. Additionally, there is a big improvement achieved by the proposed schemes compared to the state-of-the-art unimodal face and palmprint systems.

In the proposed scheme 3, the unimodal and multimodal identifiers utilize feature extraction method such as Local Binary Patterns (LBP) and feature selection method such as Backtracking Search Algorithm (BSA). The experiments are conducted on face, left-palm and right-palm separately to demonstrate the accuracy of the unimodal and combined multimodal systems.

The experimental results of the proposed scheme using FERET face and PolyU palmprint databases demonstrate considerable improvement in recognition results compared to other multimodal systems and unimodal identifiers. A comparison of the proposed multimodal system with the state-of-the-art systems shows that the proposed approach is better than some of the state-of-the art methods and is comparable with the best performing methods in the literature.

In order to counter spoofing in 2D face and palmprint recognition systems, a novel protection method is also proposed. Different texture-based and IQA-based methods are evaluated to counter both printed photo and replayed video attacks. For this purpose, we considered three types of spoof detection feature vectors such as LBP, DoG and HOG with and without PCA and LDA for dimensionality reduction.

Additionally, feature space of seven complementary image quality measures are considered. We have combined texture-based algorithms and IQA metrics with simple classifier to detect real accesses and fraudulent attacks. The proposed fusion protection scheme is able to generalize well to different databases and scenarios. It is able to adopt to different types of attacks. It is also able to perform at a high level of security for different biometrics traits.

We also constructed a palmprint spoof database including 50 subjects made by printed palmprint photo using the camera to evaluate the ability of different palmprint spoof detection algorithms. We presented results of both face and palmprint spoof detection methods using two public-domain face spoof database (Idiap PRINT-ATTACK and REPLAY-ATTACK) and our own palmprint spoof database.

Further works are planned to use the proposed spoof detection approach consisting of a liveness detection method, texture-based descriptor and analyzing different classifiers. Various texture based and motion based methods will be implemented and fused to propose a new method to differentiate live subject against fake one in constraint and unconstraint environments.

In addition, further research is planned to extend the proposed systems on any other biometrics like iris, fingerprint, etc to be investigated and fused to provide a robust multimodal biometric system. It includes improving the biometrics accuracy and working on its forgery resistance.

REFERENCES

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol,* 14, 4-20.

[2] Jain, A. K., Ross, A., & Prabhakar, S. (2006). Biometrics: A Tool for Information Security. *IEEE Transaction on Information Forensis and Security,* 1, 125-143.

[3] Liau, H. F., & Isa, D. (2011). Feature selection for support vector machine-based face-iris multimodal biometric system. *Expert Systems with Applications,* 38(9), 11105–11111.

[4] Zhang, D., & Shu, W. (1999). Two novel characteristic in palmprint verification: Datum point invariance and line feature matching. *Pattern Recognit.*, 32(4), 691–702.

[5] Pujol, P., Macho, D., & Nadeu, C. (2006). On Real-Time Mean-and-Variance Normalization of Speech Recognition Features. *Acoustics, Speech and Signal Processing, ICASSP 2006 Proceedings. 2006 IEEE International Conference on*, 1.

[6] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of*

Cognitive Neuroscience. 3(1), 71-86.

[7] Tu, H., & Yang, J. (2001). A direct LDA algorithm for high dimensional data-with application to face recognition. *The Journal of Pattern Recognition*, 34, 2067-2070.

[8] Penev, P., & Atick, J. (1996). A General Statistical Theory for Object Representation. *Network Computation in Neural Systems*, 7.

[9] Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces versus fisherfaces: Recognition using class specific linear projection. *IEEE Trans. Pattern Anal. Mach. Intell*, 19(7).

[10] Huang, J. X., & Wechsler, H. (1998). Face Pose Discrimination Using Support Vector Machines (SVM). *Proceeding of 14 th conference on pattern Recognition, (ICPR 98)*.

[11] Zhan, D., Jing, X., & Yang, J. (2006). Biometric Image Discrimination Technologies. *Computational Intelligence and Its Application Series, Idea Group Publishing*, 80-95.

[12] Chen, Z., Chang, C., Han, X., & Wang, K. (2014) .Illumination processing in face recognition. *International Journal of Pattern Recognition and Artificial Intelligence*, 28.

[13] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security Privacy Mag*, 1, 33-42.

[14] Jain, A. K., Bolle, M., & Pankanti, S. (1999). Biometrics: Personal Identification in Networked Society.

[15] Raghavendra, R., Dorizzi, B., Rao, A., & Kumar, G. H. (2011). Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. *Pattern Recogn*, 44, 1076-1088.

[16] Eskandari, M., & Toygar, Ö. (2015). Selection of optimized features and weights on face-iris fusion using distance images. *Computer Vision and Image Understanding.*

[17] Jain, A. K., Nandakumara, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition*, 38, 2270-2285.

[18] Nalini, K. R., Jonathan, H. C., & Ruud, M. B. (2001). An analysis of minutiae matching strength. *Springer*, 2091, 223-228.

[19] Javier, G., Raffaele, C., Alessandra, L., Guillermo, G. G., Davide, M. F., Julian, O., & Dario, M. (2010). An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. *Pattern Recognit. Lett.*, 31, 725-732.

[20] Marcos, M., Julian, F., Javier, G., & Javier, O. (2011). An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognit. Lett.,* 32, 1643-1651.

[21] Santosh, T., Norman, P., David, W., Aamo, I., Nik, S., & Anthony, T. S. H. (2015). Detection of Face Spoofing Using Visual Dynamics. *IEEE Transaction on Information Forensics and Security,* 10, 762-777.

[22] Anjos, A., Chakka, M. M., & Marcel, S. (2014). Motion-based countermeasures to photo attacks in face recognition. *Biometrics*, 3, 147-158.

[23] Jean, H., Renato, L., Andreas, H., & Rolf, I. (2007). A new forgery scenario based on regaining dynamics of signature. *Advances in Biometrics, Springer Berlin Heidelberg,* 366-375.

[24] Abdenour, H., Mohammad, G., Vili, K., & Matti, P. (2012). Can gait biometrics be spoofed. *Pattern Recognition (ICPR), 2012 21st International Conference on,* 3280-3283.

[25] Zhong, H., Qing-Huan, Z., & Ming-hui, D. (2006). Face Recognition using PCA on Enhanced Image for Single Training Images. *Machine Learning and Cybernetics, International Conference on,* 3218-3221.

[26] Daoqiang, Z., & Zhi-Hua, Z. (2005). (2D) 2PCA: Two-directional two-

dimensional PCA for efficient face representation and recognition. *Neurocomputing,* 69(3), 224–231.

[27] Martinez, A. M., & Kak, A. C. (2001). PCA versus LDA. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 23, 228-233.

[28] Nicolas, M., Frederic, A., Insaf, H., & Thomas, E. (2007). A Comparative Implementation of PCA Face Recognition Algorithm. *Electronics, Circuits and Systems, ICECS 2007. 14th IEEE International Conference on,* 865-868.

[29] Duta, N., Jain, A. K., & Mardia, K. V. (2002). Matching of palmprint. *Pattern Recognition Lett.,* 23, 477–485.

[30] You, J., Li, W., & Zhang, D. (2002). Hierarchical palmprint identification via multiple feature extraction. *Pattern Recognition,* 35, 847–859.

[31] Guangming, L. U., David, Z., & Kuanquan, W. (2003). Palmprint recognition using eigenpalms features. *Pattern Recognition Letters,* 24, 1463–1467.

[32] Zhang, X., & Yang, J. Y. (2010). A feature extraction method for use with bimodal biometrics. *Pattern Recogn,* 43, 1106-1115.

[33] Jing, X. Y., Li, S., Li, W. Q., Yao, Y. F., Lan, C., Lu, J. S., & Yang, J. Y. (2012). Palmprint and face multi-modal biometric recognition based on SDA-

GSVD and its kernelization. *Sensors*, 12(5), 5551-5571.

[34] Yao, Y. F., Jing, X. Y., & Wong, H. S. (2007). Face and palmprint feature level fusion for single sample biometrics recognition. *Neurocomputing,* 70(9), 1582-1586.

[35] Jing, X. Y., Yao, Y. F., Zhang, D., Yang, J. Y., & Li, M. (2007). Face and palmprint pixel level fusion and Kernel DCV-RBF classifier for small sample biometric recognition. *Pattern Recogn,* 40, 3209-3224.

[36] Nirmala, S., & Aloka, S. (2014). Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction. *Pattern Analysis and Applications,* 18(4), 921-932.

[37] Eskandari, M., & Toygar, Ö. (2014). Fusion of face and iris biometrics using local and global feature extraction methods. *Signal, Image and Video Processing*, 8, 995-1006.

[38] Eskandari, M., Toygar, Ö. & Demirel, H. (2014). Feature extractor selection for face-iris multimodal recognition. *Signal, Image and Video Processing*, 8(6), 1189-1198.

[39] Gohalm, M. S., Mansoor, A. B., Masood, H., & Mumtaz, M. (2011). Personal identification using feature and score level fusion of palm- and fingerprints.

Signal, Image and Video Processing, 5(4), 477-483.

[40] Shen, L., Bai, L., & Ji, Z. (2011). Fpcode: An efficient approach for multi-modal biometrics. *International Journal of Pattern Recognition and Artificial Intelligence*, 25(2).

[41] Rokita, J., Krzyzak, A., & Suen, C. Y. (2008). Multimodal biometrics by face and hand images taken by a cell phone camera. *International Journal of Pattern Recognition and Artificial Intelligence*, 22(3).

[42] Barra, S., Marsico, M., Nappi, M., & Riccio, D. (2014). Complex numbers as a compact way to represent scores and their reliability in recognıtion by multi-biometric fusion. *International Journal of Pattern Recognition and Artificial Intelligence*, 28.

[43] Eskandari, M., Toygar, Ö., & Demirel, H. (2013). A new approach for face-iris multimodal biometric recognition using score fusion. *International Journal of Pattern Recognition and Artificial Intelligence*, 27.

[44] Ross, A., & Jian, A. K. (2004). Multimodal biometrics: An overview. *Proc. 12th European Signal Processing Conference (EUSIPCO)*, 1221-1224.

[45] Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. *Pattern Recognition Letters*, 24, 2115-2125.

[46] Feng, G., Dong, K., Hu, D., & Zhang, D. (2004). When faces are combined with palmprints:a novel biometric fusion strategy. *First International Conference on Biometric Authentication (ICBA*).

[47] Ross, A., & Govindarajan, R. (2004). Feature level fusion using hand and face biometrics. *Proceedings of SPIE Conference on Biometric Technology for Human Identification,* 196-204.

[48] Seshikala, G., Kulkarni, U. P., & Prasad, G. (2014). Feature fusion of palm and face based on curvelet transform. *IJCSN International Journal of Computer Science and Network,* 3, 2277-5420.

[49] Ahonen, T., Hadid, A., & Pietikainen, M. (2006). Face description with local binary patterns: application to face recognition. *IEEE Trans. Pattern Anal. Mach. Intell,* 28(12), 2037-2041.

[50] Wei, Y., Lin, G., Sha, Y., Yonggang, D., Pan, J., Jun, W., & Shijun, L. (2014). An improved LBP algorithm for texture and face classifcation. *Signal, Image and Video Processing,* 8, 155-161.

[51] Anbarjafari, G. (2013). Face recognition using color local binary pattern from mutually independent color channels. *EURASIP Journal on Image and Video Processing.*

[52] Izadpanahi, S., & Toygar, Ö. (2014). Human age classification with optimal geometric ratios and wrinkle analysis. *International Journal of Pattern Recognition and Artificial Intelligence*, 28.

[53] Chingovska, I., Anjos, A., & Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoofing. *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG Proceedings of the International Conference of the,* 1-7.

[54] Maatta, J., Hadid, A., & Pietikainen, M. (2011). Face Spoofing Detection From Single images Using Micro-texture Analysis. *Proc. International Joint Conference on Biometrics (UCB 2011), Washington, D.C., USA*, 1-7.

[55] Jiamin, B., Tian, N., Xinting, G., & Yun, S. (2010). Is physics-based liveness detection truly possible with a single image?. *Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on*, 3425-3428.

[56] Tiago, D. F. P., Jukka, K., Andre, A., Jose, M. D. M., Abdenour, H., Matti, P., & Sebastien, M. (2014). Face liveness detection using dynamic texture. *EURASIP Journal on Image and Video Processing*.

[57] Xiaoyang, T., Yi, L., Jun, L., & Lin, J. (2010). Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. *Computer Vision ECCV*, 6361, 504-517.

[58] Tiago, D. F. P., Andre, A., Jose, M. D. M., & Sebastien, A. (2012). LBP−TOP based countermeasure against face spoofing attacks. *Proc. ACCV Workshops,* 121-132.

[59] Jukka, K., Abdenour, H., & Matti, P. (2012). Face Spoofing Detection Using Dynamic Texture. *Computer Vision ACCV 2012 Workshops*, 7728, 146-157.

[60] Guoying, Z., & Matti, P. (2007). Dynamic texture recognition using local binary patterns with an application to facial expressions. *IEEE Transactions on Pattern Analysis and machine Intelligence,* 29, 915-928.

[61] Di, W., Hu, H., & Jain, A. K. (2015). Face Spoof Detection with Image Distortion Analysis. *IEEE Transactions on Information Forensics and Security,* 10(4), 746-761.

[62] Siwei, L., & Farid, H. (2006). Steganalysis using higher-order image statistics. *IEEE Transactions on image processing*, 1(1), 111-119.

[63] Sevinc, B., Ismail, A., Bulent, S., & Nasir, M. (2006). Image manipulation detection. *Journal of Electronic Imaging*, 15(4), 041102-1–041102-17.

[64] Avcibas, I., Memon, N., & Sankur, B. (2003). Steganalysis using image quality metrics. *IEEE Transactions on Image Processing*, 12(2), 221-229.

[65] Matthew, C. S., & Ray, K. J. (2010). Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints. *IEEE Transactions on Information Forensics and Security,* 5(3), 041102-1–041102-17.

[66] Javier, G., Sebastien, M., & Julian, F. (2014). Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. *IEEE Transactions on Image Processing,* 23(2), 710-724.

[67] Ryszard, S. (2007). Image Feature Extraction Techniques and Their Applications for CBIR and Biometrics Systems. *International Journal of Biology and Biomedical Engineering,* 1(1), 6-16.

[68] Jolliffe, I. T. (2002). Principal Component Analysis, Springer Series in Statistics. *Springer Series in Statistics.*

[69] Field, D. J. (1984). Relations between the statistics of natural images and the response properties of cortical cells. *Journal of the Optical Society of America (JOSA),* 4, 2379-2394.

[70] Wu, D., Zhang, D., Wang, K., & Huang, B. (2004). Palmprint classification using principal lines. *Pattern Recognition,* 37, 1987-1998.

[71] Morchid, M., Dufour, R., Bousquet, P. M., Linares, G., & Torres-Moreno, J. M. (2014). Feature selection using Principal Component Analysis for massive

retweet detection. *Pattern Recognition Letter*, 49, 33-39.

[72] Wendy, Y. (2000). Analysis of PCA-based and Fisher Discriminant-based Image Recognition Algorithms. *Colorado State University, Master Thesis, Fort Collins, Colorado.*

[73] Zhao, H., Yuen, P. C., & Yang, J. (2005). Optimal subspace analysis for face recognition. *International Journal of Pattern Recognition and Artificial Intelligence*, 19, 375-393.

[74] Wang, H., Wang, Z., Leng, Y., Wu, X., & Li, Q. (2007). PCA plus F-LDA: A new approach to face recognition. *International Journal of Pattern Recognition and Artificial Intelligence*, 21, 1050-1059.

[75] Gabor, D. (1964). Theory of Communication. *Journal of Inst. Electr. Eng.*, 93, 429-457.

[76] Kamarainen, J. K., Kyrki, V., & Kälviäinen, H. (2006). Invariance properties of Gabor filter based features - overview and applications. *IEEE Transactions on Image Processing*, 15(5), 1088-1099.

[77] Fischer, S., Redondo, R., & Cristóbal, G. (2009). How to construct log-Gabor Filters?. *Instituto de Optica (CSIC), Serrano 121, 28006 Madrid, Spain*.

[78] Daubechies, I. (1992). *Ten lectures on wavelets*. SIAM, Philadelphia, PA.

[79] Francesco, B., & Antonio, F. (2007). Evaluation of the effects of Gabor filter parameters on texture classification. *Pattern Recognition*, 40(12), 3325–3335.

[80] He, G., Tang, Y. Y., Fang, B., & Wang, P. S. P. (2011). Bionic face recognition using gabor transformation. *International Journal of Pattern Recognition and Artificial Intelligence*, 25, 391-402.

[81] Karar, S., & Parekh, R. (2013). Palmprint recognition using phase symmetry. *International Journal of Scientific and Research Publications,* 3.

[82] Malviya, R., Kumar, R., Dangi, A., & Kumawat, P. (2011). Verification of palm print using log gabor filter and comparison with ICA. *International Journal of Computer Applications in Engineering Sciences, I*, 222-227.

[83] Raghavendra, R., & Busch, C. (2014). Novel image fusion scheme based on dependency measure for robust multispectral palmprint recognition. *Pattern Recognition*, 47, 2205-2221.

[84] Shojaeilangari, S. S., Yau, W. Y., & Teoh, E. K. (2014). A novel phase congruency based descriptor for dynamic facial expression analysis. *Pattern Recognition Letter,* 49, 55-61.

[85] Ojala, T., Pietikainen, M., & Harwood, D. (1996). A comparative study of texture meature with classification based on feature distibution. *Pattern recognition*.

[86] Ojala, T., Pietikainen, M., & Harwood, D. (1994). Performance evaluation of texture measures with classification based on kullback discrimination of distributions. *Proceedings of the 12th IAPR International Conference on Pattern Recognition.*

[87] Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 24(7), 971-987.

[88] Nanni, L., Lumini, A., & Brahnam, S. (2012). Survey on LBP based texture descriptors for image classification. *Journal of Expert Systems with Applications,* 39, 3634-3641.

[89] Heikkila, M., Pietikainen, M., & Schmid, C. (2009). Description of interest regions with Local Binary. *Patterns, Pattern Recognition,* 42, 425-436.

[90] Pietikainen, M., Hadid, A., Zhao, G., & Ahonen, T. (2011). Computer vision using local binary patterns. *Computational Imaging and Vision,* 40.

[91] Chen, H. X., Tang,, Y. Y., Fang, B., & Wang, P. S. P. (2011). A multi-layer

contrast analysis method for texture classification based on lbp. *International Journal of Pattern Recognition and Artificial Intelligence,* 25.

[92] Sanchez, J., & Redolfib, J. (2015). Exponential family Fisher vector for image classification. *Pattern Recognition Letters*, 59, 26-32.

[93] FERET database, Department of Defense's Counterdrug Technology Development Program. (1993-1997). Retrieved from http://www.itl.nist.gov/iad/humanid/feret

[94] ORL face database, AT&T Laboratories, Cambridge University, UK. Retrieved from http://www.uk.research.att.com/facedatabase.html

[95] Exteded Yale Face Database B, University of Yale, Retrieved from http://vision.ucsd.edu/ leekc/ExtYaleDatabase/ExtYaleB.html

[96] Essex face database, vision group, University of Essex, UK. Retrieved from http://cswww.essex.ac.uk/mv/allfaces/index.html

[97] Lee, K. C., Ho, J., & Kriegman, D. (2005). Acquiring Linear Subspaces for Face Recognition under Variable Lighting. *IEEE Trans. Pattern Anal. Mach. Intelligence*, vol. 27(5), 684-698.

[98] PolyU palmprint Database, Retrieved from http://www.comp.polyu.edu.hk/

biometrics

[99] David, Z., Wai, K., Jain, Y., & Michael, W. (2003). On-line palmprint identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9), 1041-1050.

[100] Marcel, S., & Rodriguez, Y. (2007) Torch3vision - the vision package of touch3, Retrieved from www.torch.ch

[101] Civicioglu, P. (2013). Backtracking Search Optimization Algorithm for numerical optimization problems. *Applied Mathematics and Computation.*, 219, 8121-8144.

[102] Shan, C., & Braspenning, R. (2010). Recognizing Facial Expressions Automatically from Video. *Handbook of Ambient Intelligence and Smart Environments*, 7441, 479-509.

[103] Ramon, E., Lorenzo, J., & Castrillon, M. (2012). Gender Classification in Large Databases. *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, *Lecture Notes in Computer Science*.

[104] Chakka, M. M., Anjos, A., Marcel, A., & Tronci, R. (2011). Competition on counter measures to 2-D facial spoofing attacks. *Biometrics (IJCB), 2011 International Joint Conference on*, 1-6.

[105] Kollreider, K., Fronthaler, H., & Bigun, J. (2005). Evaluating liveness by face images and the structure tensor. *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on,* 75-80.

[106] Kollreider, K., Fronthaler, H., & Bigun, J. (2008). Verifying liveness by multiple experts in face biometrics. *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on,* 1-6.

[107] Saptarshi, C., & Dhrubajyoti, D. (2014). An Overview of Face Liveness Detection. *International Journal on Information Theory (IJIT),* 3(2), 11-25.

[108] Jianwei, Y., Zhen, L., Shengcai, L., & Li, S. Z. (2013). Face Liveness Detection with Component Dependent Descriptor. *Biometrics (ICB), 2013 International Conference on,* 1-6.

[109] Freitas, T., Anjos, A. J., Martino, M., & Marcel, S. (2013). Can face anti-spoofing countermeasures work in a real world scenario?. *Biometrics (ICB), 2013 International Conference on,* 1-8.

[110] Peter, J. B., & Edwars, H. A. (1983). The Laplacian pyramid as a compact image code. *IEEE Transactions on Communications,* 9, 532-540.

[111] Crowley, J. L., & Stern, R. M. (1984). Fast computation of the difference of low pass transform. *IEEE Transactions on Pattern Analysis and Machine*

Intelligence, 6, 212-222.

[112] Navneet, D., & Bill, T. (2005). Histograms of Oriented Gradients for Human Detection. *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on,*. 1, 886-893.

[113] Avcibas, I., Sankur, B., & Sayood, K. (2002). Statistical evaluation of image quality measures. *J. Electron. Imag.*, 11(2), 206–223.

[114] Huynh, Q., & Ghanbari, M. (2008). Scope of validity of PSNR in image/video quality assessment. *Electron. Lett.*, 44(13), 800-801.

[115] Eskicioglu, A. M. & Fisher, P. S. (1995). Image quality measures and their performance. *IEEE Trans. Commun,* 43(12), 2959–2965.

[116] Wang, Z. Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Process.,* 13(4), 600-612.

[117] Pual, V., & Michael, J. J. (2004). Robust real-time face detection. *International journal of computer vision,* 57(2), 137-154.

[118] Bharadwaj, S., Dhamecha, T. J., Vatsa, M., & Singh, R. (2013). Computationally Efficient Face Spoofing Detection with Motion

Magnification. *Computer Vision and Pattern Recognition Workshops (CVPRW), 2013 IEEE Conference on*, 105-110.

[119] Demirel, H., & Anbarjafari, G. (2008). Pose Invariant Face Recognition using Probability Distribution Functions in Different Color Channels. *IEEE Signal Processing Letters,* 15(537).

[120] Cao, N. T., Ton, A. H., & Choi, H. I. (2014). Facial expression recognition based on local binary pattern features and support vector machine. *International Journal of Pattern Recognition and Artificial Intelligence,* 28.

[121] Yurtkan, K., & Demirel, H. (2014). Entropy-based feature selection for improved 3D facial expression recognition. *Signal, Image and Video Processing*, 8, 267-277.

[122] Hadid, A., Dugelay, J., & Pietikainen, M. (2011). On the use of dynamic features in face biometrics: recent advances and challenges. *Signal, Image and Video Processing.,* 5(4), 495-506.

[123] Ross, A., Nandakumar, K., & Jain, A. K. (2006). Handbook of Multibiometrics.

[124] Georghiades, A. S., Belhumeur, P. N., & Kriegman, D. J. (2001). From Few to Many: Illumination Cone Models for Face Recognition under Variable

Lighting and Pose. *IEEE Trans. Pattern Anal. Mach. Intelligence,* 23(6), 643-660.

[125] Belhumeur, P. N., Hespanha, J., & Kriegman, D. J. (1997). Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. *IEEE Transactions On Pattern Analysis And Machine Intelligence,* 19, 711-720.

[126] Lu, G., Zhang, D., & Wang, K. (2003). Palmprint recognition using eigenpalms features. *Pattern Recognition,* 24, 1463-1467.

[127] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. *Springer.*