Université Mohamed Boudiaf - M'sila

FACULTE DE TECHNOLOGIE

DEPARTEMENT D'ELECTRONIQUE

Numéro de série……

Numéro d'inscription : D.E/3C/05/17

Thèse

Présentée pour l'obtention du diplôme de

DOCTORAT LMD

Filière : Electronique

Spécialité : Electronique et Télécommunications

THEME

Amélioration de la performance des Systèmes d'identification et authentification biométriques par des techniques multimodales avancées

Présentée Par

Abderrahmane Herbadji

Soutenue le : 15 / 04 / 2021

Devant le jury composé de :

Nom & Prénom	Grade	Etablissement	Qualité
SAIGAA Djamel	**Prof.**	**Université de M'sila**	Président
GUERMAT Noubeil	**M.C.A**	**Université de M'sila**	Encadreur
ZIET Lahcene	**Prof.**	**Université de Setif 1**	Co-Encadreur
AMARDJIA Nourredine	**Prof.**	**Université de Setif 1**	Examinateur
LADJAL Mohamed	**M.C.A**	**Université de M'sila**	Examinateur

Année Universitaire : 2020/2021

Université Mohamed Boudiaf - M'sila

FACULTE DE TECHNOLOGIE

DEPARTEMENT D'ELECTRONIQUE

Numéro de série……

Numéro d'inscription : D.E/3C/05/17

Thèse

Présentée pour l'obtention du diplôme de

DOCTORAT LMD

Filière : Electronique

Spécialité : Electronique et Télécommunications

THEME

Improving the performance of Biometric identification and authentication systems using advanced multimodal techniques

Présentée Par

Abderrahmane Herbadji

Soutenue le : 15 / 04 / 2021

Devant le jury composé de :

Nom & Prénom	Grade	Etablissement	Qualité
SAIGAA Djamel	Prof.	Université de M'sila	Président
GUERMAT Noubeil	M.C.A	Université de M'sila	Encadreur
ZIET Lahcene	Prof.	Université de Setif 1	Co-Encadreur
AMARDJIA Nourredine	Prof.	Université de Setif 1	Examinateur
LADJAL Mohamed	M.C.A	Université de M'sila	Examinateur

Année Universitaire : 2020/2021

العنوان : **تحسين أداء أنظمة تحديد الهوية والتوثيق البيومترية باستخدام تقنيات متقدمة متعددة الوسائط**

الأنظمة البيومترية هي تقنية علمية للتعرف على الشخص باستخدام سماته الفيزيائية أو السلوكية أو الكيميائية. تستخدم القياسات الحيوية في الوقت الحاضر على نطاق واسع في العديد من التطبيقات اليومية التي تتراوح من مصادقة مستخدم الأجهزة الذكية إلى عبور الحدود. نظام يستخدم ملف يُعرف المصدر الوحيد للمعلومات الحيوية (على سبيل المثال ، بصمة إصبع واحدة) للتعرف على الأشخاص باسم نظام أحادي أو أحادي القياس. حيث أن النظام الذي يدمج البيانات من مصادر معلومات بيومترية متعددة (مثل الوجه وبصمة الإصبع) يسمى نظام متعدد الوسائط أو متعدد القياسات الحيوية. يمكن للأنظمة متعددة القياسات الحيوية أن تخفف من معدلات الخطأ وبعض نقاط الضعف المتأصلة في أنظمة القياسات الحيوية الأحادية. في هذه الأطروحة ، تم اقتراح مخطط جديد للاندماج على مستوى النقاط يعتمد على المتوسط شبه الحسابي الموزون .(WQAM) على وجه التحديد ، يتم تقدير WQAMs عبر دوال مثلثية مختلفة. يشتمل مخطط الاندماج المقترح على خصائص كل من المتوسط المرجح والمتوسط شبه الحسابي. علاوة على ذلك ، لا يتطلب أي عملية تعلم. تظهر النتائج التجريبية على ثلاث مجموعات بيانات متاحة للجمهور لأنظمة متعددة الوسائط ومتعددة الوحدات ومتعددة الخوارزميات أن خوارزمية اندماج WQAM المقدمة تتفوق على قواعد دمج النقاط المقترحة سابقًا. بالإضافة إلى طريقة WQAM الانصهار متعدد المقاييس الحيوية ، فقد اقترحنا نظامًا متعدد القياسات الحيوية يعتمد على أنماط الوريد (أي أنماط وريد الكف والرسغ .(كان اختيار أنماط الوريد للمصادقة الشخصية لأسباب عديدة مثل المعلومات المستقرة المقدمة على عمر الأشخاص بالإضافة إلى أن هذه السمات البيومترية غير مرئية للعين البشرية (أي أنها تقع داخل الجلد) ، وبالتالي تكتسب مقاومة أكبر للتكرار أو انتحال .في حين تم اقتراح نظام جديد متعدد المقاييس الحيوية لمصادقة المستخدمين استنادًا إلى أنماط إصبعهم الرئيسية باستخدام أربعة أصابع (على سبيل المثال ، صغيرة ، وخاتم ، ووسط ، وفهرس) وقزحية من أجل التغلب على بعض قيود أنظمة القياسات الأحادية.

الكلمات المفتاحية: القياسات الحيوية المتعددة ، دمج نقاط المطابقة ، المتوسط شبه الحسابي الموزون ، المصادقة ، تحديد الهوية ، الأمان ، بصمة الإصبع ، الوجه ، أنماط الوريد ، القزحية ، أنماط الإصبع الرئيسية

Titre : **Amélioration de la performance des Systèmes d'identification et authentification biométriques par des techniques multimodales avancées**

La biométrie est une technologie scientifique permettant de reconnaître une personne en utilisant ses attributs physiques, comportementaux ou chimiques. La biométrie est aujourd'hui largement utilisée dans plusieurs applications quotidiennes allant de l'authentification des utilisateurs d'appareils intelligents au passage des frontières. Un système qui utilise un une source unique d'informations biométriques (par exemple, une seule empreinte digitale) pour reconnaître les personnes est connue sous le nom de système unimodal ou unibiométrique. Alors que le système qui consolide les données de plusieurs sources d'informations biométriques (par exemple, le visage et les empreintes digitales) est appelé système multimodal ou multibiométrique. Les systèmes multi-biométriques peuvent atténuer les taux d'erreur et certaines faiblesses inhérentes aux systèmes uni-biométriques. Dans cette thèse, un nouveau schéma de fusion au niveau des scores basé sur la moyenne quasi-arithmétique pondérée (WQAM) a été proposé. Plus précisément, les WQAM sont estimés via différentes fonctions trigonométriques. Le schéma de fusion proposé englobe les propriétés de la moyenne pondérée et de la moyenne quasi-arithmétique. De plus, il ne nécessite aucun processus d'apprentissage. Les résultats expérimentaux sur trois ensembles de données accessibles au public pour les systèmes multimodaux, multi-unités et multi-algorithmes montrent que l'algorithme de fusion WQAM présenté surpasse les règles de fusion de score proposées précédemment. En plus de la méthode de fusion multi-biométrique WQAM, nous avons suggéré un système multi-biométrique basé sur des modèles de veines (c'est-à-dire des modèles de veines de la paume et du poignet). Le choix des modèles de veines pour l'authentification de la personne était pour de nombreuses raisons telles que les informations stables fournies sur l'âge des personnes ainsi que ces traits biométriques sont invisibles à l'œil humain (c'est-à-dire qu'ils sont situés à l'intérieur de la peau), gagnant ainsi une plus grande résistance à la réplication. ou usurpation d'identité. Tandis que, un nouveau système multi-biométrique pour authentifier les utilisateurs en fonction de leurs principaux modèles de doigts d'articulation en utilisant quatre doigts (c'est-à-dire, petit, anneau, milieu et index) et l'iris est proposé afin de surmonter certaines limites des systèmes uni-biométriques.

Mots clés : Multi-biométrie, fusion Match-score, la moyenne quasi-arithmétique pondérée, authentification, identification, sécurité, empreintes digitales, visage, motifs veineux, iris, principaux motifs de doigts d'articulation

Title : Improving the performance of Biometric identification and authentication systems using advanced multimodal techniques.

Abstract :

Biometrics is a scientific technology to recognize a person using their physical, behavior or chemical attributes. Biometrics is nowadays widely being used in several daily applications ranging from smart device user authentication to border crossing. A system that uses a single source of biometric information (e.g., single fingerprint) to recognize people is known as unimodal or unibiometrics system. Whereas, the system that consolidates data from multiple biometric sources of information (e.g., face and fingerprint) is called multimodal or multi-biometrics system. Multi-biometric systems can alleviate the error rates and some inherent weaknesses of uni-biometrics systems.In this thesis, a novel scheme for score-level fusion based on weighted quasi-arithmetic mean (WQAM) has been proposed. Specifically, WQAMs are estimated via different trigonometric functions. The proposed fusion scheme encompasses properties of both weighted mean and quasi-arithmetic mean. Moreover, it does not require any learning process. Experimental results on three publicly available data sets for multi-modal, multi-unit and multi-algorithm systems show that presented WQAM fusion algorithm outperforms the previously proposed score fusion rules. In addition to WQAM multi-biometric fusion method, we have suggested a multi-biometric system based on vein patterns (i.e., palm and wrist vein patterns). The choice of vein patterns for person authentication was for numerous reasons such as the stable information provided over people age as well as these biometric traits are invisible to the human eye (i.e, they are located inside the skin), thus gaining greater resistance to replicating or spoofing. Whilst, a novel multi-biometric system to authenticate users based on their major knuckle finger patterns using four fingers (i.e., little, ring, middle, and index) and iris is proposed in order to overcome some limitaions of uni-biometric systems.

Key words : Multi-biometrics, Match-score fusion, WQAM, Authentication, Identification, Security, Fingerprint, Face, Vein patterns, Iris, major knuckle finger patterns

Publications

✓ **Abderrahmane Herbadji**, Noubeil Guermat, Lahcene Ziet, Zahid Akhtar, Dipanker Dasgupta "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems," in IET Biometrics, vol. 9, no. 3, pp. 91-99,2020,

✓ **Abderrahmane Herbadji**, Zahid Akhtar, Karaman Siddique, Noubeil Guermat, Lahcene Ziet, Mohamed cheniti, Khan Muhamad: "Combining multiple biometric traits using asymmetric aggregation operators for improved person recognition", Symmetry, 2020, 12, (3), pp. 444

✓ **Abderrahmane Herbadji**, Noubeil Guermat, Lahcene Ziet, Zahid Akhtar, Mohamed cheniti, Djamel Herbadji: "Contactless multi-biometric system using fingerprint and palm-print selfies", Traitement du Signal, 2020 37, (6), pp. 889-897

✓ **Abderrahmane Herbadji**, Noubeil Guermat, Lahcene Ziet, Mohamed cheniti, Djamel Herbadji: "Personal authentication based on wrist and palm vein images", International Journal of Biometrics, 2019, 11, (4), pp. 309-327

✓ Herbadji, D., Derouiche, N., Belmeguenai, A., **Abderrahmane Herbadji**, Boumerdassi, S.: "A tweakable image encryption algorithm using an improved logistic chaotic map", Traitement du Signal, 2019, 36, (5), pp. 407-417

Conferences

✓ **Abderrahmane Herbadji**, Noubeil Guermat, Lahcene Ziet, Mohamed cheniti "Multi-modal Biometric Verification using the Iris and Major Finger Knuckles,"
2019 International Conference on Advanced Electrical Engineering (ICAEE), Algiers, Algeria, 2019, pp. 1-5, doi: 10.1109/ICAEE47123.2019.9014704

Acknowledgements

First and above all, I would like to express my heartfelt gratitude to ALLAH, the merciful, for blessing me with the mental and physical strength and enlightening me on the right path to conclude my PhD studies successfully.

I owe my gratitude to my advisor ***Dr. Noubeil Guermat*** and c-advisor ***Pr. Lahcene Ziet*** for their guidance, supervision, motivation, and support. This excellent support and guidance have indeed helped me find a proper direction in my work.

I would like to express my appreciation to my thesis committee members:

Pr. Djamel Saigaa, Professor at the University of Msila, finds here the expression of my most sincere thanks for having accepted to chair this thesis.

Pr. Noureddine Amardjia, Professor at University of Setif-1, for the interest shown in our work and his participation in the jury as an examiner.

Dr. Mohamed Ladjal, Lecturer A at the University of Msila, for having accepted to be an examiner as well as for his great assistance in the administrative matters.

I am extremely grateful to ***Mr. Mohamed cheniti***, University of Setif1, for his guidance in challenging and exciting fields of pattern recognition and biometrics.

I would like to express my deepest gratitude to ***Dr. Zahid Akhtar***, State University of New York Polytechnic Institute, Utica, USA. His dedication, thirst for novelty, guidance, and commitment to quality were inspirations to honing my research skills in the field of biometrics.

Finally, I would like to express my gratitude and appreciation to all of my family for their support, encouragement, and help.

Abderrahmane HERBADJI
15 April 2021

Contents

List of Figures

List of Tables

Glossary of Important Terms

✓ **BSIF**: Binarised Statistical Image Features

✓ **EER**: Equal Error Rate

✓ **FBI-IAFIS**: Federal Bureau of Investigation-Integrated Automated Fingerprint Identification System

✓ **FAR**: False Acceptance Rate

✓ **FRR**: False Rejection Rate

✓ **ID**: Identification Card

✓ **GAR**: Genuine Acceptance Rate

✓ **GMM**: Gaussian Mixture Model

✓ **HMM**: Hidden Markov Model

✓ **KNN**: k-nearest neighbour

✓ **LDA**: Linear Discriminant Analysis

✓ **LPQ**: Local Phase Quantisation

✓ **LBP**: Local Binary Patterns

✓ **LTP**: Local Ternary Patterns

✓ **MFKP**: Major Finger Knuckle Patterns

✓ **NIST**: National Institute of Standards and Technology

✓ **PIN**: Personnal Identification Number

✓ **PolyU-CHDI**: Hong Kong PolyU Contactless Hand Dorsal Images

✓ **PUT**: Poznan University of Technology

✓ **QDA**: Quadratic Discriminant Analysis

✓ **ROI**: Region Of Interest

✓ **RBF**: Radial Basis Function

✓ **ROC**: Receiver Operating Characteristics

✓ **SVM**: Support Vector Machines

✓ **STD**: standard deviation

✓ **tanh**: tanh-estimators

✓ **t-norms**: Triangular norms

✓ **WQAM**: Weighted Quasi-Arithmetic Mean

Chapter 1

General Introduction

1.1 Introduction

The increase in recent identity theft and global security risks has necessitated trustworthy identity management frameworks. To this aim, biometrics has been proposed as an alternative to traditional identification methods such as "what you have" (e.g., an ID card) or "what you know" (e.g., a password) [8]. Biometrics is an automated measurement and statistical analysis of people's anatomical (e.g., face, fingerprint, iris) or behavioral (e.g., voice, gait, signature) attributes to scientifically recognize or identify them [2]. In fact, biometrics has been widely adopted as an imperative security tool by governments, industries and individuals. For instance, 'US-VISIT' program (i.e., visitors to the US has to provide fingerprint and face images at their port of entry for identification), 'Voice-Fingerprint ID' (i.e., HSBC is providing fingerprint and voice based banking software to access online and phone accounts) [1] and 'Touch ID' (i.e., iPhone 5s is unlocked using fingerprint)....

Biometrics that utilises only single modality is known as unibiometric system [2]. Unibiometric systems suffer from issues like noisy sensor data, non-universality, high interclass similarities, high intraclass variations, low interoperability, and presentation attacks (i.e., fooling biometrics by presenting genuine user's trait artifacts [9]) leading thereby to elevated error rates. Some shortcomings of unimodal biometric systems can be overcome by multibiometric systems, which fuse information from multiple biometric sources to attain improved accuracy [2].

Numerous studies have empirically demonstrated the effectiveness of multi-biometric systems . The information in multi-biometrics can be fused at five different levels sensor-level (i.e. combining raw data acquired from multiple sensors/snapshots), feature-level (i.e. consolidating feature sets obtained from multiple biometrics into a single feature set), score-level (i.e. integrating matching scores output by different biometric matchers to yield a new match score), rank-level (i.e. fusing the ranks produced by the individual subsystems to derive a consensus rank for each identity for final decision) and decision-level (i.e. merging the decision made by individual biometric subsystems.

Biometric fusion at the score-level has been extensively adopted in the literature primarily thanks to straightforwardness in obtaining and integrating the match-scores. The existing score-level fusion methods can normally be grouped into three classes: density-, classifier- and transformation-based techniques . The density- and classifier-based score fusion techniques are remarkably affected by unbalanced training set and score densities (that are usually unknown) estimation, respectively.

1.2 Goals of this Thesis

Transformation-based rules, like product, min, max, and weighted sum rules were observed in the literature to perform weakly, since they failed to take into account the distribution distance of different biometric traits' match-scores. While, classifier-based fusion methods face the problem of unbalanced training set due to the unbalanced authentic and imposter training score sets. Likewise, though density-based approaches can lead to optimal performance, it is hard to estimate the density function of scores accurately because its nature is usually unknown and also limited dataset is available for the same.

In multibiometric based individual recognition, the chosen of the combination rule is very important to attain high accuracy. Generally, the best combination rule is the one that can minimize the imposter matching scores and further maximize the authentic matching scores.

To this end, in this doctoral thesis, we presented a novel economical score level fusion framework based on the weighted quasi-arithmetic mean (WQAM) using different trigonometric functions, which contains properties of both weighted mean and quasi-arithmetic mean. Experiment results for multimodal, multi-unit and multi-algorithm systems on three publicly available databases (i.e. NIST-BSSR1 Multimodal, NIST-BSSR1 Fingerprint and NISTBSSR1 Face) show that the proposed approach is able to outperform existing transformation-, classification- and densitybased score fusion rules

Also, we suggest a multimodal biometric framework to authenticate individuals based on their wrist and palm vein patterns. The choice of wrist and palm vein biometric traits was for numerous reasons. First, the vein images require no cooperation from the individual (i.e., contact-less manner). Second, wrist and palm vein patterns can be simultaneously collected thereby acquisition of these data requires low cost equipment. Third, apart from the stable information provided by wrist and palm vein patterns over people age, these biometric traits are invisible to the human eye, thus gaining greater resistance to replicating or spoofing. Fourth, we have observed that proposed multimodal biometric authentication is able to provide a better security performance than unimodal wrist and palm vein biometrics. Therefore, the use of these two traits allows improving the authentication performance for multimodal biometric system.

1.3 Thesis organisation

The thesis is organised as follows. Chapter 2 discusses the basic issues of biometric systems. Chapter 3 analyzes and reports a critical review of state-of-the-art works on multi-biometric systems and their possible fusion methods. The proposed fusion scheme, which is based on weighted quasi-arithmetic mean (WQAM) are described in chapter 4. In chapter 5, we experimentally evaluated the performance of the proposed score level fusion method, palm and wrist vein based multimodal framework, and iris and major finger knuckles of four fingers. Conclud-

ing remarks, contribution and possible future directions of this research are eventually discussed in Chapter 6

Chapter 2

Overview of Biometric Systems

2.1 Introduction

Biometric is a combination of two Greek words, namely Bio (life) and Metric (to measure). Biometric systems offer reliable, more secure, and natural solution for person recognition. The aim of these systems is automated methods of human identification. The recognition of users in biometric systems is based on their physiological traits (e.g., fingerprint, iris, vein, hand geometry, ear shape) or behaviour characteristics (e.g., gait, signature, keystroke) instead of conventional person authentication that depends on badges, personal identification number (PIN), passwords, these passwords may be words or phrases, ID cards, which are easy to manipulate, stolen, shared, or lost. The physiological traits and behaviour characteristics are generally invariant over time, universal, stable, and unique for every individual [2, 8].

2.2 Operation of a biometric system

A biometric system is essentially a pattern-recognition (pattern matching) system. The identification of a user in a biometric system consists of two main stages, namely enrollment and recognition. During the first phase i.e., enrollment, the biometric data is collected from the person and stored in a database along with his identity. Usually, only the extracted feature set from the biometric data gets stored in the database, while the row biometric data is discarded. During the second stage i.e., recognition, the biometric data is re-collected from the individual and matched against the feature set(s) stored in the database during the first stage to determine the user identity. Therefore, a biometric system can be viewed as having five basic modules, namely, (a) sensor module, (b) quality assessment and feature extraction module, (c) database module, (d) matching module, (e) decision module. The five main modules are discussed below [3]

2.2.1 Sensor module

To attain/measure the raw biometric data of an individual, a suitable biometric sensor is needed. For instance, an optical sensor may be employed to obtain the fingerprint images. In order to acquire a good raw biometric data, the interface (humane-machine) should be easy to use and ergonomic. Besides, the characteristics of the sensor employed play a pivotal role in the acquisition of high quality of biometric samples.

2.2.2 Feature extractor and quality assessment module

The acquired biometric data is typically subjected to further pre-processing before extracting the features. Feature extraction process refers to produce or calculate an expressive digital representation for the input biometric sample, namely template, this template is expected to

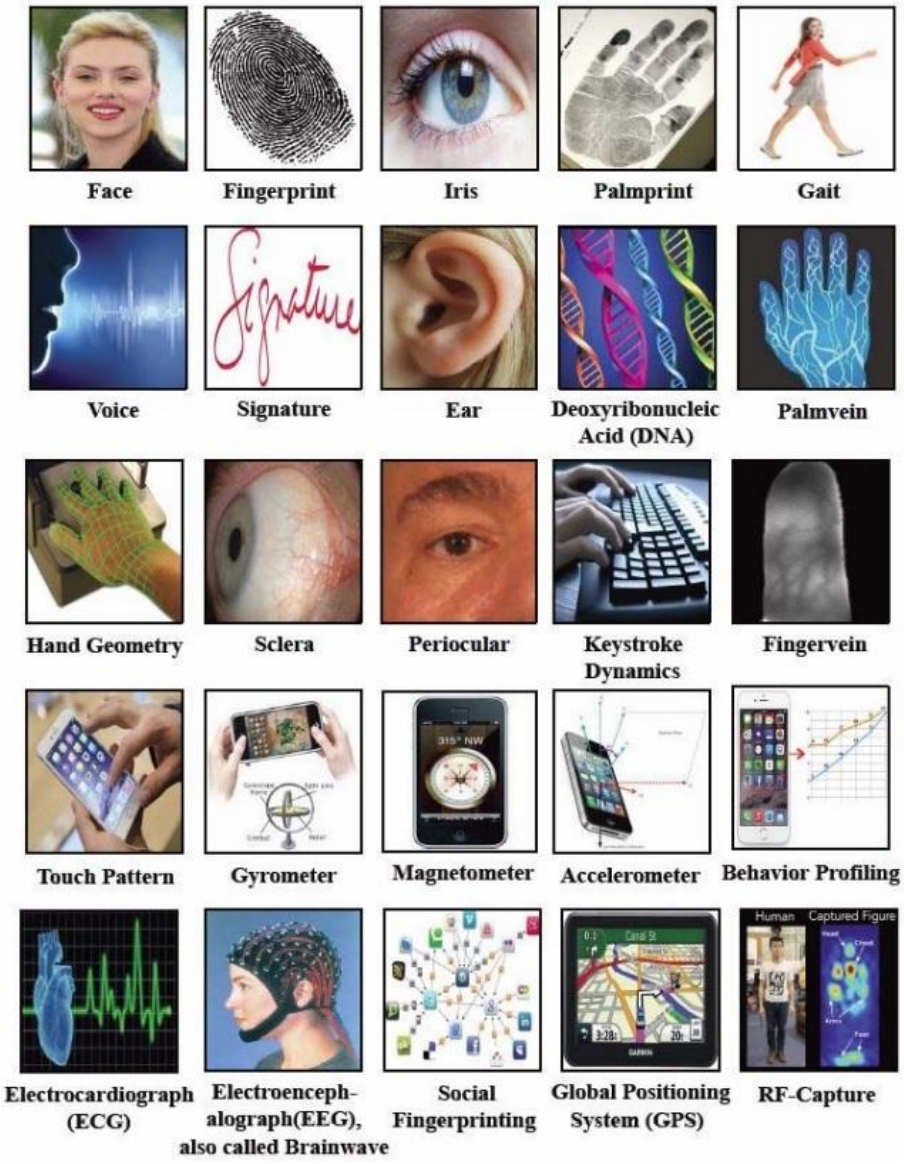

Fig. 2.1 *Examples of attributes that have been proposed and utilised for biometric person recognition [1].*

consist of salient discriminatory information, which is essential for identifying or verifying the person. It is worth noticing that during the enrollment stage the template gets registered either in the central database of the system or stored on a token such as smart card produced for the person.

Owing to the query biometric data (input data) is not always of sufficient quality, a quality assessment algorithm is adopted in the biometric system to determine the suitability of the query data for the subsequent processing. In the case of the quality of the acquired biometric data is not unsuitable, row data is rejected and re-acquired from the user. If the quality assessment algorithm is not incorporated, the quality of the input data is usually improved through subjecting it to signal enhancement algorithm.

2.2.3 Database module

The extracted features from the row biometric data are stored in the system database (i.e., template) besides to some user's biographic information (e.g., Personal Identification Number (PIN), name, address, etc.) that distinguishes him. In order to get a secured biometric templates, these templates should be stored in a central database, which can be secured via physical isolation and through rigorous access control techniques and thereby protect the privacy of innocent users from the malicious individuals that able to abuse their biometric information stored in the database.

2.2.4 Matcher module

The prime aim of the biometric matcher module is to generate match scores by comparing the collected traits' information (query features) with their corresponding template accumulated at the stage of enrollment. The match score determines the amount of similarity between the two feature sets and may be a similarity or a distance. In the case of the matching module produces a similarity score, a larger matching score denotes greater similarity between the stored template and the input biometric sample. Whilst, a greater similarity between the two feature sets is indicated by a smaller distance matching score when the generated scores of the biometric matcher represents a dissimilarity instead of similarity (i.e., distance). Two types of comparison can be made by the matching module, one-to-one for verification and one-to-many for identification purpose.

2.2.5 Decision module

Here, the match scores yielded by the matcher module are utilised with a view to either legitimize the claimed individual's identity in the verification task or to rank the enrolled identities in order to identify a user in identification task. Generally, the match score is compared with a predefined threshold, say τ, that assigns a user as genuine if $S \geq \tau$, otherwise imposter, where in case of similarity scores, the user is authenticated as a genuine $S < \tau$, otherwise as an impostor.

2.3 Functionalities of a biometric system

A biometric system may provide to types of recognition, namely, identification and verification (one can use authentication a synonym for verification). Fig. 2.2 depicts the enrollment stage, in which the individual has to present her/his biometric traits (e.g., fingerprint, face, and iris) to the sensor in order to transform it into a reference template and store in the system database The two modes provided by the biometric system are discussed as bellow [2]

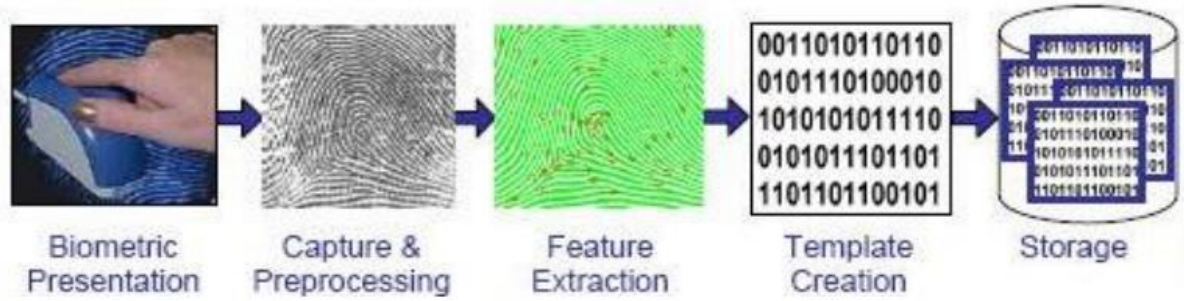

Fig. 2.2 *Biometric enrollment stage.*

2.3.1 Identification

In the identification mode, the biometric system conducts a comparison between the individual's biometric inputs with the templates of all the users enrolled in the database (i.e., one-to-many match) in order to establish the user's identity (see Fig. 2.3). Here, the system's output can be either the identity of the individual whose template has the highest degree of similarity with the input sample presented by the user or a decision indicates that this person is not enrolled in the database. There are many biometric system works in identification mode like US-VISIT IDENT program and the FBI-IAFIS. Owing to the huge number of enrolled users, identification is significantly more challenging than verification. Identification mode can be categorised into two classes:

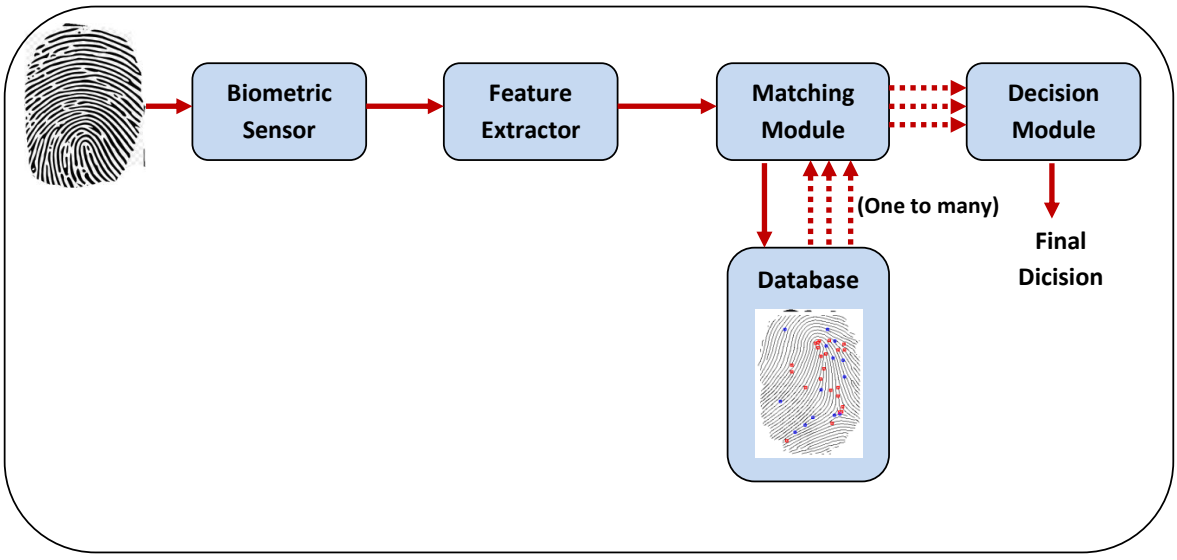

Fig. 2.3 *Biometric identifcation mode.*

• **Positive identification** : In this class, the identity of the person is determined from a known set of identities (i.e., the system answers the question "Are you someone who is known to the

system").

• **Negative identification** : In this class, the user is considered to be concealing his true identity (either explicitly or implicitly) from the system, this kind of identification system is also known as screening and its purpose is to find out "Are you who you say you are not?".

2.3.2 Verification

In the verification mode, the biometric system conducts a comparison only between the individual's query input and her/his own biometric template stored in the database (i.e., one-to-one match) in order to validate the user's claimed identity (see Fig. 2.4). Usually, the identity claim is made through the use of a user name, a token (e.g., smart card), or a PIN (personal identification number). The user is accepted as genuine in the case of the user's query input and template of the claimed identity have high degree of similarity as well as degree of similarity is above a predefined threshold.

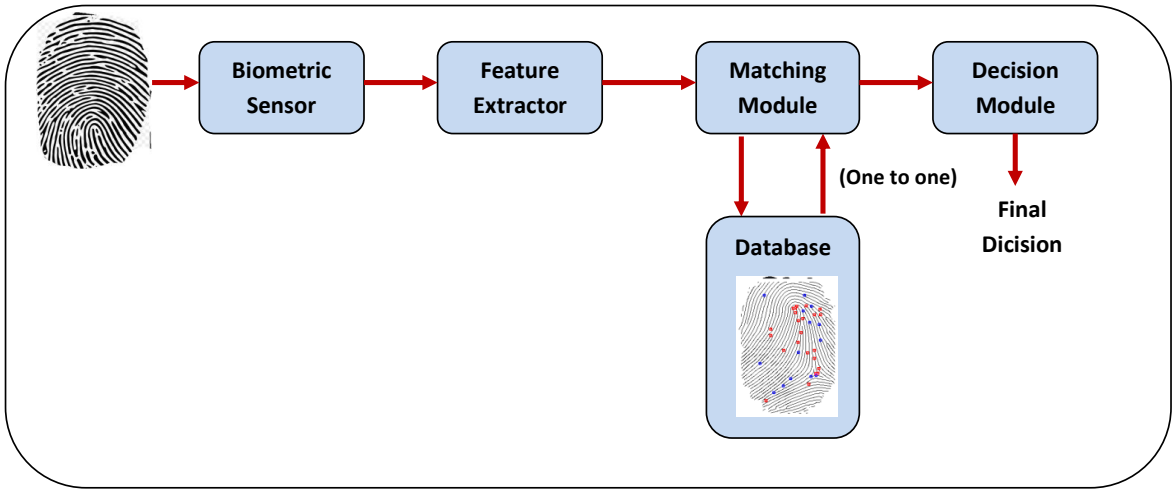

Fig. 2.4 *Biometric verification mode.*

2.4 Selection of biometric modality

Although biometrics is being employed in diffrent daily applications (e.g., border crossing, mobile user authentication, forensics), there is no biometric trait meet all the requirements (e.g., performance, permanence, cost) by these applications, however, a number of them are admissible. Table 2.1 describes the diverse biometric traits against diverse attributes such as collectability, performance, distinct, universal, and permanence. For instance, the fingerprint trait, survey reports medium for universal, high distinctness, high permanence, medium collectability, high performance and medium acceptability.

Table 2.1 *Comparison of biometric traits [3].*
Note: H: high, M: medium, L: low.

Biometric trait	Universal	Uniqueness	Permanence	Collectability	Performance	Acceptability
Face	H	L	M	H	L	H
Fingerprint	M	H	H	M	H	M
Ear	H	L	M	H	L	H
Iris	H	H	H	M	M	L
Gait	M	L	L	H	L	H
Hand vein	M	M	M	M	M	M
Hand Geometry	M	M	M	H	M	M
Retina	H	H	M	L	H	L
Signature	L	L	L	H	L	H
Voice	M	L	L	M	L	H
DNA	H	H	H	L	L	L

Several biometric traits have been utilised to verify human identity such as fingerprint, face, voice, palmprint, etc. Each biometric trait has its pros and cons and, therefore, the choice of a biometric trait depends on many factors besides its accuracy performance [3]. The factors of determining the suitability of a biometric trait for a particular application can be expressed as follows [2, 7, 6]

2.4.1 Universality

This factor means that each user has to possess the required biometric trait. It is worth noticing that universality factor determines the failure to enroll rate.

2.4.2 Uniqueness

In order to avoid the false match rate (FAR) of a biometric system, the given biometric trait should lead to differ between the users.

2.4.3 Permanence

In order to attain a high recognition rate of a biometric system, the user's trait should be sufficiently invariant over a period time. Otherwise, it will lead to a high false non-match rate (FRR).

2.4.4 Collectability

Collectability or measurability means that the biometric modality must be appropriate for capture, and should be comfortable for the individual to present to the biometric sensor

2.4.5 Performance

This fatcor refers to accuracy, speed, and robustness of the system. Accuracy of biometric systems is usually defined by their false accept and false reject rates. Accuracy is influenced in the data collection process by environmental (e.g., lighting, shadows, background noise).

2.4.6 Resistance to circumvention

It determinates the degree of resistance against spoofing attack [10, 11]. Spoofing is the process by which a fraudulent user can subvert or attack a biometric system by masquerading as registered user and thereby gaining illegitimate access and advantages.

2.4.7 Acceptability

It indicates the degree of public acceptance and approval for a given biometric trait. Thus, individuals should be willing to present their biometric trait to the system. This is a significant factor because user acceptance is critical to the success of any biometric implementation.

2.5 Comparison of biometric traits and its applications

In fact, biometrics has been widely adopted as an imperative security tool in numerous applications in our vastly interconnected society (see Table 2.3). Questions like "Is she really who she claims to be?", "Is this person authorized to use this facility " or " Is he on the watch list posted by the government " are routinely being posed in a variety of scenarios ranging from issuing a driver's license to gaining entry into a country (see Fig. 2.5). The applications of biometrics can be divided into three main sectors (i.e., Government sector, Commercial sector, and Forensic sector). [2, 8, 7]. The behavioral and psychological biometric traits along with their characteristics are shown in table 2.2. while, the different applications of each biometric trait are tabulated in Table 2.3.

Fig. 2.5 *Government and commercial applications that employ biometrics to recognize person* ***(a)*** *The US-VISIT program* ***(b)*** *the Schiphol Privium program,* ***(c)*** *Unique Identity (UID) Card project , and* ***(d)*** *a product by Fujitsu captures the palm vein pattern [2].*

2.6 Unimodal Biometric Systems

A system that uses a single source of biometric information (e.g., single fingerprint) to recognize people is known as unimodal or uni-biometrics system; this systems are not adequate in tackling issues like noisy input data, non-universality, lack of individuality and spoofing, which lead to lower accuracy. Some issues associated with unimodal systems are discussed as follows [2, 9].

Table 2.2 *Biometric modalities and their characteristics [2, 6, 7]*

Biometric modality	Advantages	Limitations
Face	✓ physical contact is not required ✓ Convenient, less complex statistics ✓ Fast recognition process ✓ 3D offers increased precision	✓ For the twins, differences may not be clear ✓ With age facial traits may change ✓ Potential privacy concerns ✓ Lighting and variations in pose can reduce accuracy
Fingerprint	✓ Generally uses small, low-cost readers ✓ Reliable and highly accurate ✓ Fast matching process ✓ An effective biometric for large-scale systems ✓ Widely accepted forensic tool	✓ Not considered hygienic ✓ Twists, cuts or dirt may create obstacles
Iris	✓ High accuracy and more protective ✓ High stability of characteristics over time ✓ Moderate data storage requirements ✓ Works well with either verification or identification applications	✓ Small sample size ✓ Diseases may affect the accuracy ✓ Challenges at a large distance
Ear	✓ Identification process is fast ✓ Most stable and less computational complexity ✓ Less computational complexity	✓ Identification process is fast ✓ Uncomfortable as it requires direct contact
Hand geometry	✓ Operates well in challenging environments ✓ Widely used ✓ Less processing	✓ Not accurate for moderate to large populations ✓ Unhygienic ✓ Injuries and jewels may harm the results
Palmprint	✓ Large variety of features ✓ High reliability and permanent ✓ Good recognition even with low resolution scanners	✓ Unhygienic ✓ Injuries may create obstacles
Retina	✓ Among the most accurate of biometrics ✓ Moderate storage requirements for templates	✓ Special hardware is required ✓ Expensive
Vein pattern	✓ Highly private ✓ Very accurate ✓ Difficult to circumvent ✓ Near contactless, hygienic	✓ not yet widely used ✓ Can be impacted by bright ambient light
Voice	✓ Easy implementation ✓ Less expensive ✓ convenient to employ ✓ High public acceptance	✓ Throat disease can affect the accuracy ✓ Generally large storage requirements for templates ✓ Not sufficiently distinctive for identification over large databases
Lip motion	✓ Different and unchangeable ✓ Template's size is small ✓ User interaction is not required	✓ Lack of accuracy
Keystroke dynamics	✓ Easy implementation and use ✓ Additional hardware is not required	✓ Only useful for applications require keyboarding
Gait	✓ Easy to capture the image ✓ Convenient to use ✓ No distance problem	✓ Computationally expensive ✓ Lack of accuracy
Signature	✓ More accuracy ✓ Less false acceptance rate ✓ Low storage require	✓ Can be forged ✓ Changes based on emotional and medical condition of person
DNA	✓ highly unique feature ✓ High performance ✓ Its universality is very high	✓ More storage required ✓ Not automatic technique ✓ More informative so privacy issues

Table 2.3 *Application of biometric traits [7, 2]*

Biometric trait	Applications
Face	Criminal Identification Access Control Verification Human Computer Interaction Surveillance
Fingerprint	License and Visa Authentication Access Control Verification Human Computer Interaction Law Enforcement Forensics
Retina	Security agencies such as FBI, CIA, and NASA
Ear	Law Enforcement Forensics Surveillance
Iris	Identification as Aadhaar card in India Access Control
Lip motion	Criminal Police training Forensic Professional
Voice	Web based transactions Voice Response based health and banking systems.
Gait	Chiropractic Medical diagnose
Vein pattern	Financial systems and Banks Door Security system, Travel and Transportation
palmprint	Personal Identification Blood relation Identification Medical Diagnosis Selection of athletes
Signature	Banking system

2.6.1 Non-universality

Universality is one of the basic needs for a biometric modality, which means that every person accessing the biometric system have to present the respective biometric trait for recognition.

Fig. 2.6 *fingerprints' failure to enroll caused by poor quality ridges due to extreme finger dryness [3]*

Meaningful biometric data are not always extracted from a subset of users. For instance, NIST has reported that it is not possible to extract correct minutia features from the fingerprints of two percent of the population due to some issues like handrelated disabilities or cuts and bruises on fingertips because of the poor quality of the ridges [9], leading thereby to boost in the failure to enroll (FTE) rate as shown in Fig.2.6.

Fig. 2.7 *Example of a noisy fingerprint image.*

2.6.2 Noisy sensor data

Noise in biometric data is typically produced by unfavorable ambient conditions or improperly maintained sensors. For example, the presence of dirt on the sensor of a fingerprint scanner may result in a noisy fingerprint image (see Fig. 2.7), which leads to be inccorectly matched with their respective templates in the database. Hence, accuracy reduction is expected.

2.6.3 Lack of individuality

This issue refers to the hardness to make distinction between users of the biometric system. There may be large inter-class similarities in the feature sets used to represent these traits. Note that lack of individualty can be occured with all biometric traits, e.g., the facial appearance of a son and his father or twins' facial may be quite similar as displayed in Fig. 2.8. The lack of

uniqueness (Inter-class similarities) in the biometric feature set leads to an increase in the false acceptance rate (FAR) of the system.

Fig. 2.8 *Face images of a pair of twins [2].*

2.6.4 Intra-class variation

Intra-class variations in biometric samples are typically occurs when the collected biometric data during enrrolment stage are very different to the data acquired from the same user during recognition stage, thereby affecting the matching process. It is worth noting that this variation are typically produced by the user's poor interaction with the sensor as shown in Fig 2.9, changes in sensor characteristics during the verification phase, inherent changes in the biometric trait, and changes in the environmental conditions (e.g., illumination changes).

Fig. 2.9 *Intra-class variation associated with an individual's face image [4]*

2.6.5 Spoof attacks

Spoof attacks or susceptibility to circumvention occurs when an impostor attempt to provide a fake biometric sample of a legitimate (genuine) enrolled user in order to circumvent the system [1, 3, 9]. Generally, Behavioral biometric traits like signature and voice are susceptible to spoof attacks than physiological ones. However, physical traits are also susceptible to circumvention e.g., it is possible to construct an artificial iris or fingerprint and use them to circumvent a biometric recognition system as shown in Fig. 2.10. It si worth noting that spoof physical triats requires the help of a legitimate enrolled user.

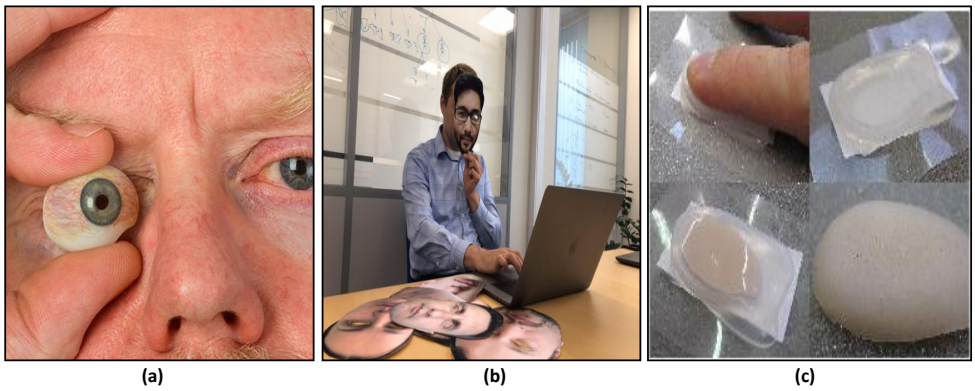

Fig. 2.10 *Examples of Biometrics spoofing: (a) iris spoofing; (b) face spoofing; (c) fingerprint spoofing*

2.7 Conclusion

Traditional authentication methods based on passwords and identity cards still face several challenges such as passwords can be forgotten or identity cards can be faked. Some of the limitations can be addressed by biometrics, which employes human anatomical or behavioural (e.g., gait, signature, keystroke analysis) characteristics ,e.g, iris, fingerprint, face, gait, etc., to establish the identity. In this chapter, we discussed the architecture and types of a biometric recognition system, pros and cons of each biometric modality as well as the limitations of unimodal systems that use only one trait for indentification. Thereby, these systems are not sufficient to meet the variety of requirements such as matching performance, required by various large-scale verification systems; to address this issue and other drawbacks, multi-biometrics can be viewed as one of the standard solutions where it will be discussed in the next chapter.

Chapter 3

Multi-biometric Systems

3.1 Introduction

Though unibiometric systems based on single biometric marker are widely used for person recognition, these systems imposed some vulnerabilities and limitations when used in real applications that cover a massive number of users, i.e., becoming inefficient due to several drawbacks such as spoof attacks, noisy data, distortion, non-universality, interclass similarities and others. Examples of such applications include the US-VISIT program and the Unique Identification (UID) system in India, where identities of a very large number of individuals (hundreds of millions) need to be resolved.

The drawbacks imposed by unimodal biometric systems can be overcome by combining multiple biometrics information (i.e., multimodal biometric systems) in order to achieve better authentication accuracy and robustness. Multi-biometric systems are able to alleviate the aforementioned troubles inherent to unibiometric. They use multiple sensors and/or modalities (multiple sources of biometric information) instead of a single modality; thereby it is very difficult for an impostor to spoof physical quality and behaviour characteristic of a genuine user simultaneously.

Accuracy improvement, which is the primary motivation for using multi-biometric systems, happens due to two reasons. Firstly, the fusion of multiple biometric sources effectively increases the dimensionality of the feature space and reduces the overlap between the feature distributions of different users. Secondly, noise, imprecision, or inherent drift (caused by factors like aging) in a subset of the biometric sources can be compensated by the discriminatory information provided by the remaining sources.

Although multi-biometric systems achieve numerous advantages, they are usually more expensive than uni-biometric systems due to the need for additional hardware (computational or storage resources) and larger enrollment and recognition times. Thus, it is essential to carefully analyze the tradeoff between the added cost and the benefits accrued when making a business case for the use of multi-biometrics in a specific application.

In order to design a multi-biometric system, we need to address the following four design issues: information sources, mode of operation, Level of fusion, and the Fusion approach. [2].

3.2 Biometric modality analysis (matching)

In the literature, most common biometric modalities adopted are fingerprint and face [1], which are also considered in this phd thesis.

3.2.1 Fingerprint matching algorithms

The fingerprint matching algorithms can be categorised into three categories [8]:

- **Correlation-based matching** : The correlation between two fingerprint images are measured to indicate the degree of similarity by utilising the intensities of pixels [2]. For instance, Kumar et al. [12] proposed the use of advanced correlation filters.

- **Minutiae-based matching** : Minutiae-based fingerprint matching is the most popular and widely utilised technique. The algorithms use the number of matching minutiae pairs between two fingerprints images [13]. Maio and Maltoni [14] proposed a technique where the ridge lines are followed to extract minutiae directly from the grey-scale images.

- **Minutiae-based matching** :Fingerprint systems utilising the non-minutiae features has got much attention during the last decade. Non-minutiae-based matching algorithms can be roughly schematised as (a) Gabor filter-based descriptors, e.g. Jain et al. [15] extracted texture features using Gabor filter around each core point; (b) local image descriptors, e.g. Kumar et al. [16] proposed use of local Gaussian pattern and fuzzy local directional pattern for fingerprint matching; (c) the transform-based descriptors, e.g. authors in [17] proposed a local texture analysis scheme using discrete cosine transform for fingerprint matching; (d) machine/ deep learning-based methods, e.g. Yang and Park [18] employed invariant moment features with non-linear back propagation neural network (BPNN) for fingerprint verification; (e) hybrid systems, e.g. Nanni and Lumini [19] proposed a scheme that used minutiae and local binary patterns features.

3.2.2 Face matching algorithms

Existing face matching schemes can be divided into four main categories [2]:

- **Local, holistic and hybrid systems:** In this category, local, holistic and hybrid (i.e. combination of local and holistic) features with similarity measures are used. For instance, Ahonen et al. [20] proposed using local binary pattern with Chi-square distance as matching technique.

- **Appearance- and model-based systems:** Appearance- and model-based methods use an image as a point in a highdimensional vector space and a model of the face for recognition, respectively. For example, Turk and Pentland [21] devised an algorithm that uses eigenfaces based on principal component analysis.

- **Geometry- and template-based systems:** Geometry-based techniques analyse geometric relationships of local features. While template-based methods define a face as a function to compare the input image with a template set. For example, Wiskott et al. [22] developed a biologically inspired algorithm using elastic bunchgraph matching

- **Template-matching, statistical and neural networks systems:** Template-matching, statistical, and neural networks techniques are based on patterns with similarity measure/correlation, patterns with a discriminant function, and patterns representation and matching using neural networks, respectively. For instance, Taigman et al. [23] proposed a face representation system built on a nine-layer deep convolution neural network.

3.3 Research on vein pattern recognition

Several biometric traits have been utilised to verify human identity such as fingerprint, face, voice, palm-print, etc. Recently, the use of vein patterns (i.e., finger vein, wrist vein, palm vein, palm-dorsa vein) as a biometric trait has emerged in biometric applications [6]. The vein patterns are characterised by rich and stable information, which leads to differentiate between people . However, there is lack literature on the integration of wrist and palm vein for multi-modal biometric authentication.

3.3.1 Previous works in wrist vein recognition

One of the promising biometric traits, becoming important for researchers, is wrist vein pattern, it provides numerous advantages compared to other biometric modalities. Automated authentication of wrist vein has invited some attention in the literature. Cheniti et al. [24] investigated a multi-biometric verification based on 2D correlation to authenticate a user from his left and right wrist vein patterns. Kurban et al. [25] used an ordinary 5 MP mobile phone camera instead of specific sensors to capture the wrist vein images. Nikisins et al. [26] proposed wrist vein recognition based on fast cross-correlation with rotation and translation compensation. FernÃ¡ndez Clotet and Findling [27] investigated a mobile wrist vein verification system applying a scale invariant feature transform (SIFT) and obtained 0.072% of EER. Das et al. [28] extracted wrist vein features with local binary patterns (LBPs). Hartung et al. [29] performed the minutia cylinder-codes (MCC) on wrist vein images, while using correlation to compute matching scores. Uriarte-Antonio et al. [30] proposed wrist vein biometric recognition utilising a minutiae feature extraction method. A summary of the most representative studies in wrist vein recognition is presented in Table 3.1.

3.3.2 Previous works in palm vein recognition

Numerous works focused on palm vein-based unimodal biometric recognition have been proposed in the literature. Pan and Kang [31] proposed a palm vein recognition based on three local invariant feature extraction approaches: speeded-up robust features (SURF), SIFT and affine-scale invariant feature transform (ASIFT). Lee [32] extracted palm vein features with 2D

Table 3.1 *Overview of previous works in the field of wrist vein-based biometric recognition*

Reference	Feature extraction	Database	Size	Performance	Year
[30]	Crossing number-based minutiae	UC3M	29	EER = 15.75%	2011
[29]	Minutia cylinder-codes	UC3M	29	EER = 0.31%	2013
[28]	Local binary patterns	PUT	29	EER = 0.79%	2014
[25]	Fast Fourier transform-based low-pass filtering with PCA	Private	34	Acc = 94.11%	2016
[24]	Private algorithm	PUT	50	EER = 0.00%	2017
[27]	Scale invariant feature transform	Private	30	EER = 0.15%	2017
[26]	Fast cross-correlation with rotation and translation compensation	PUT	50	Acc = 96.25%	2018

Gabor filter and achieved 0.4% of EER. Wang et al. [33] investigated a biometric identification system based on thermal palm vein images, while Gabor wavelet transform was applied for feature extraction. Athale et al. [34] proposed a hardware palm vein authentication system and 92% accuracy has been obtained utilising PCA algorithm. While, Cancian et al. [35] developed an embedded standalone palm vein recognition system by combining the Gabor filters and histograms calculations to create the biometric templates. Piciucco et al. [36] applied a high dynamic range (HDR) on palm vein authentication systems and employed the local derivative pattern (LDP) and LBP to extract features from palm vein images. A summary of the most representative studies in palm vein recognition is presented in Table 3.2.

3.4 Sources of Multiple Evidence

Some shortcomings of unimodal biometric systems can be overcome by multi-biometric systems, which fuse information from multiple biometric sources to attain improved accuracy. There are five possible scenarios that can provide multiple sources of biometric (see Fig. 3.1).

Depending upon the sources of fusion, multi-biometric systems can be classified into multimodal, multi-instance, multi-algorithm, multi-sensor, and multi-sample systems.

Table 3.2 *Overview of previous works in the field of palm vein-based biometric recognition*

Reference	Feature extraction	Database	Size	Performance	Year
[31]	Scale invariant feature transform speeded-up robust features ASIFT	Private PolyU multispectral palmprint	100 500	EER = 2.20% EER = 0.4%	2011
[32]	2D Gabor filter	Private	207	EER = 0.44%	2012
[33]	Gabor wavelet	Private	178	Acc = 98.88%	2012
[34]	Principal component analysis	Private	60	Acc = 92%	2015
[37]	Template matching	Private	62	Acc = 93.54%	2015
[35]	Gabor filters and histograms	Private	21	EER = 1.45%	2017
[36]	Local binary pattern and local derivative pattern	Private	86	EER = 3.81% EER = 3.81%	2017

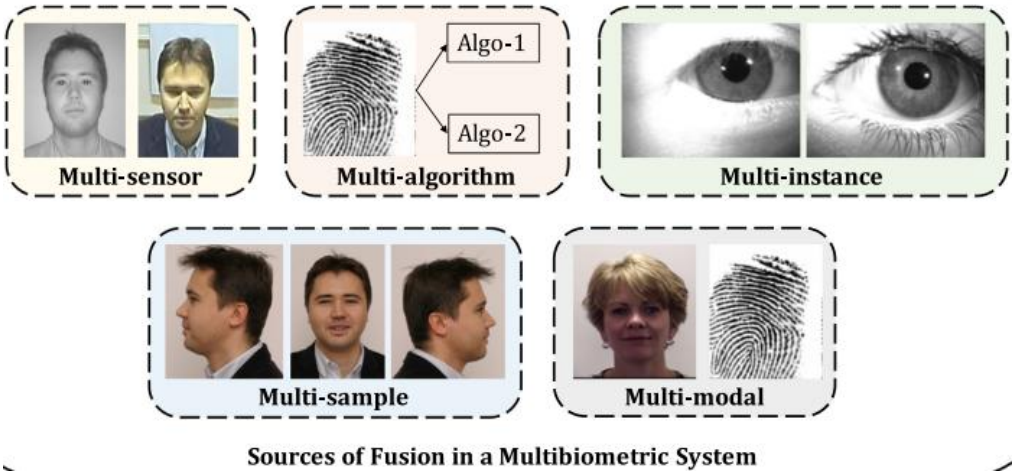

Fig. 3.1 *multi-biometric systems utilise information from multiple biometric sources to establish an identity [5].*

3.4.1 Multimodal systems

These systems utilise data presented by different body traits in order to recognize an individual. Some of the earliest multimodal biometric systems utilised face and voice features to establish

the identity of an individual. Since the different biometric traits of an individual are expected to be uncorrelated (e.g., fingerprint and iris), use of multimodal biometric systems generally leads to greater improvement in performance compared to other types of multi-biometric systems [2, 8]. The cost of deploying multimodal biometric systems is substantially more due to the requirement of multiple sensors and, consequently, the development of appropriate user interfaces.

Researchers have presented numerous studies to demonstrate the effectiveness of multimodal systems, e.g., face, fingerprint, and iris modalities , face, fingerprint, and speech modalities [38], and iris and periocular modalities [39, 40]. Besides, some works focused on fusing different traits for evaluating speaker recognition, e.g., audio, lip motion, and lip texture [41] and audio and lip motion [42].

Multi-modal systems are also useful in scenarios when an individual cannot provide data for a particular biometric modality (say injured fingerprints), but can provide data pertaining to another one (say face) [2]. Though integrating data from various biometric modalities further enables extraction of distinctive features, often resulting in boosted biometric verification accuracy, performance may be degraded if some biometric traits with lower accuracy are included.

3.4.2 Multi-instance (mult-unit) systems

These systems utilise data presented by multiple instances of the same body trait and are also sometimes referred to as multi-unit systems. In the case of iris recognition, left and right irides of a person can be employed to recognize his identity, thus resulting in multi-unit system [43]. Besides the multi-unit system based on the tow irides, both left and right wrist vein also have explored for person recognition [24]. Similarly, in the case of a fingerprint or palm-print recognition system, a multi-instance system can utilise data captured from the ten fingers or both palms [44, 45]

Multi-instance systems are easier to implement, because they do not require the introduction of new sensors nor do they entail the development of new feature extraction and matching algorithms. Nevertheless, a new sensor arrangement might be necessary in order to facilitate the simultaneous collect of the multiple units/instances. In addition to the easier implemetion of multi-instance systems, they are especially beneficial for individuals whose biometric traits cannot be reliably acquired due to inherent issues. For instance, the fusion of evidence across multiple fingers may serve as a good discriminator better than a single finger in case of a person with dry finger skin.

Multi-instance systems are often necessary in applications where the size of the system database is very large (e.g., the FBI's IAFIS database currently has more than 60 million ten-print images) and all ten fingers lead to additional discriminatory information that is required for high recognition performance [2].

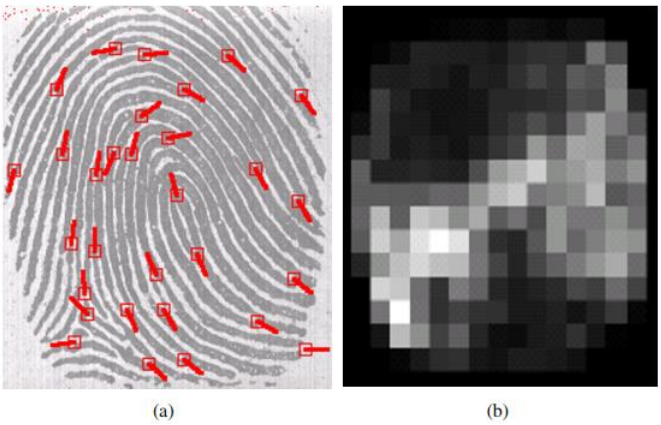

Fig. 3.2 *Extracting different sets of features from the same fingerprint image. (a) Minutia features, (b) texture features [2].*

3.4.3 Multi-algorithm systems

These systems utilise numerous algorithms in order to process an input sample. Data is collected from a biometric modality using a single sensor; however, multiple algorithms are used to process it. For instance, a fingerprint recognition system operating on minutiae- and ridge-based matchers in order to extract diverse feature sets which can improve the performance of the biometric system (see Fig. 3.2).

Multi-algorithm systems are cost-effective because these kind of systems do not require new sensors to acquired the biometrics information. Furthermore, since the user is not required to interact with multiple sensors, thereby, the biometric traits are collected without any inconvenience to users.

3.4.4 Multi-sample systems

This kind of systems utilise multiple samples derived from the same biometric trait acquired by a single sensor in order to account for the variations that can occur in the trait as well as to obtain a more complete representation of the biometric trait. Here, each of the samples are processed using the same algorithm, and then fuse them to obtain an overall recognition result. For instance, in a fingerprint system equipped with a sensor with a small sensing area, various dab prints of person's finger may be acquired with a view to capture numerous regions of the fingerprint; these fingerprint images are combined together in order to attain a complete representation of the fingerprint, which will lead to providing a massive number of minutiae (you can add an image). Likewise, in the case of face recognition system; this system may collect and store the frontal image of a individual's face along with the left and right profile images in order to account for variations in the facial pose.

In multi-sample systems, it is important to determine the number of samples of biometric

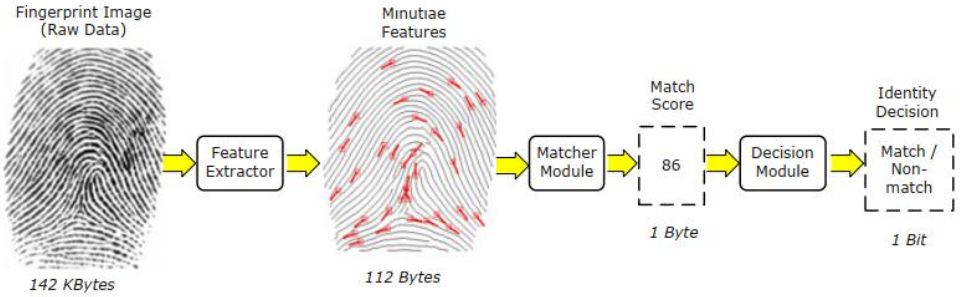

Fig. 3.3 *Different levels of fusion possible in a multi-biometric system. Raw data is the richest source of information, while the final decision (in a verification scenario) contains just a single bit of information [2].*

trait that should be collected. The acquired samples have to represent the variability as well as the typicality of the individual's biometric data with a view to avoid poor performance due to the slack properties of sample if only one sample is used.

3.4.5 Multi-sensor systems

Multi-sensor systems utilise multiple sensors to image a single biometric trait of an individual in order to extract a varied data. Although, multi-sensor systems rely on a single modality for recognition, it captures diverse information from the same biometric modality employing multiple sensors. For example, a face recognition module could utilise RGB data captured using a visible spectrum camera, along with depth information captured using a 3D camera [46]. In this case, the introduction of a new sensor to measure the facial surface variation increases the cost of the multi-biometric system.

In addition to the cost of multi-sensor multi-biometric system, the user is required to interact with the multiple sensors, and thereby leading to larger enrollment and recognition times.

3.5 Levels of fusion

Fusion play an important role in multi-biometrics, the main reason behind the success of multi-biometric systems is totally depends on how we apply fusion strategies in an effective manner. In multi-biometric systems, combination of information can be done through using the data provided in any of the four biometric modules, i.e., sensor, feature extractor, matcher, and decision modules (see Fig. 3.3).

Fig. 3.4 depicts the different levels at which fusion can be incorporated, namely, (i) sensor-level, (ii) feature-level, (iii)score-level, (iv) rank-level, or (v) decision-level. Biometric fusion can be broadly categorised into (a) fusion prior to matching (i.e., the first two levels) and (b)

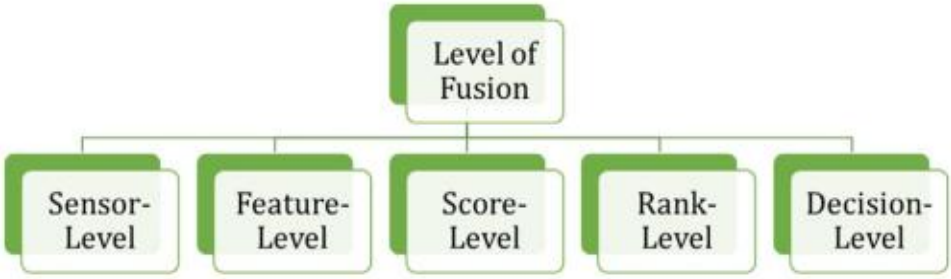

Fig. 3.4 *Data fusion can be carried out at numerous levels in multi-biometric systems.*

fusion after matching (the rest levels). Note that rank-level fusion is typically applicable to only identification systems. Each of these levels of fusion are explained in detail below.

3.5.1 Sensor-level fusion

In this category, the raw data collected by the sensors are combined immediately after its acquisition in sensor level fusion. That is, information integration is accomplished prior to feature extraction, directly on the raw data (see Fig. 3.5). For instance, a small fingerprint sensor may capture more one impression of an individual's fingerprint and create a composite fingerprint image that reveals a more complete ridge structure (see Fig. 3.6). This process, known as mosaicing, is particularly useful in sweep-sensors in which each image slice represents only a small portion of the fingerprint and thereby an appropriate stitching algorithm is required in order to fuse the different slices to form the complete fingerprint image nd hence improved the accuracy of the systems. Likewise, In case of a face recognition system, various face images can be collected with pose variations such as frontal, left profile, or right profile, and mosaicing technique may be employed to integrate the samples with a view to obtaining a combined face representation [47]. It is worth noting that sensor level fusion can be applied only for multi-sensor and multi-sample systems.

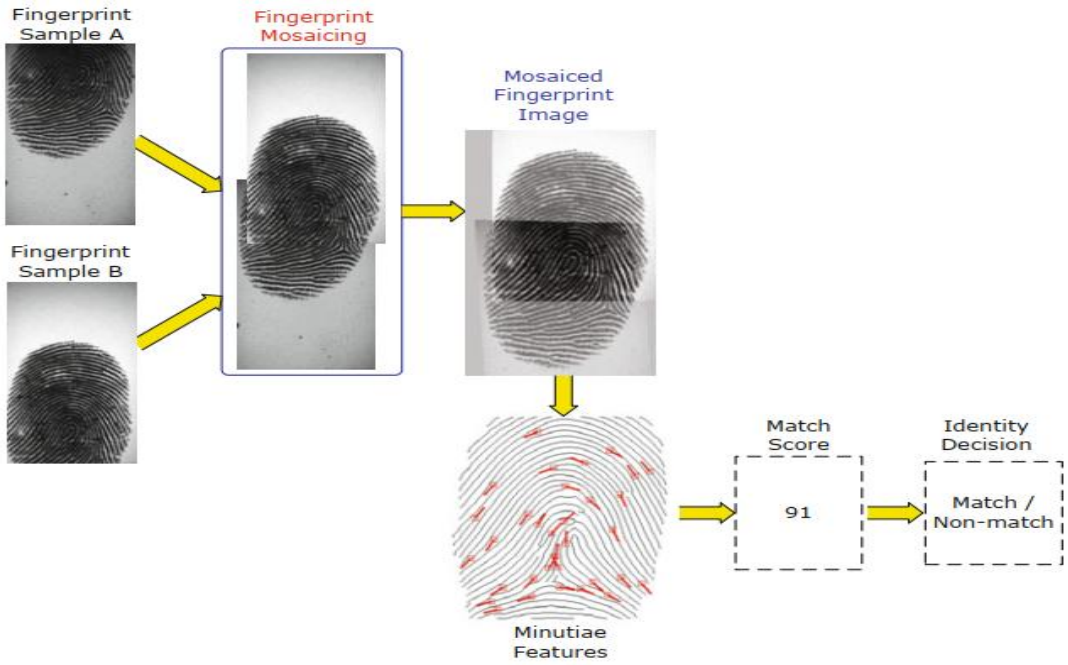

Fig. 3.6 *Combination of various impressions of the same user's finger utilising the mosaicing process to obtain a composite fingerprint image (i.e., Sensor-level fusion)*

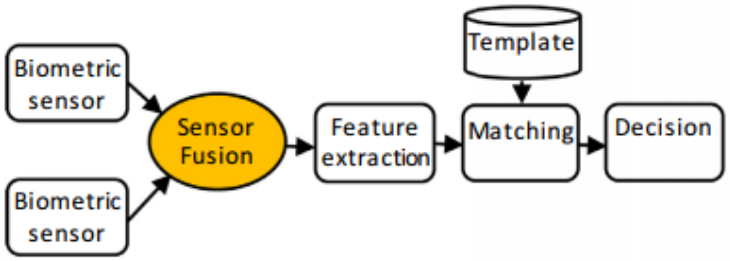

Fig. 3.5 *Block diagram of sensor level fusion in multi-biometric systems*

3.5.2 Feature-level fusion

In this fusion scheme, different feature vectors extracted from the same or multiple biometric traits of the same person are consolidated together to obtain a single feature vector (see Fig. 3.7). It should be noted that the obtained feature vector usually has large dimensions. Feature-level combination algorithms can be classified into two broad classes, namely, homogeneous and heterogeneous. One can use homogeneous feature fusion method when the feature sets are obtained employing the same algorithm for feature extraction to multiple samples of the same biometric trait (e.g., minutia sets from two impressions of the same finger). Note that this level

of fusion is applicable to multi-sensor and multi-sample biometric systems. Heterogeneous feature fusion methods are required when the component feature sets are originated from samples of different biometric traits or from different feature extraction algorithms.

Feature sets in this level have richer information about the raw biometric data than score and decision level fusion, thus, the best performance is expected in this level of fusion, but it is difficult to achieve in practice due to some reasons such as features set of different biometric modalities may be incompatible as well as the large dimensionality of feature vectors due to fusing feature sets from different modalities.

Consider a multi-biometric user recognition system where fixed-length feature vectors from two biometric sources are available; this vectors may be exhibit significant differences in their range as well as form (i.e., distribution) and thus feature normalization procedure is applied in order to map them into a common domain. Commonly, the min-max normalization scheme is used, which converts the features values into the range [0,1], irrespective of their original values.

The purpose of feature fusion is to generate a new feature vector by concatenating the two feature sets, which would better represent the biometric sample of a user. Owing to the large dimensionality of the yielded feature vector, feature selection or transformation techniques can be applied. Feature selection is a dimensionality reduction scheme that entails choosing a minimal feature set of size d, $d < (d1 + d2)$; d1 represents the size of vector one and d2 is the size of feature vector two [2]. Examples of feature selection algorithms include sequential forward selection (SFS), sequential backward selection (SBS), sequential forward floating search (SFFS), sequential backward floating search (SBFS), etc [2].

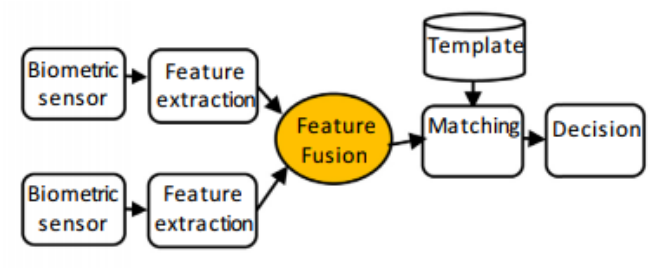

Fig. 3.7 *Block diagram of feature level fusion in multi-biometric systems*

3.5.3 Score-level fusion

In this fusion category, the different match score yielded by different matchers are combined into a single match score, and that can be subsequently used by verification and identification modules in order to arrive at a final identity decision (see Fig. 3.8). Multi-biometrics fusion at the match score-level has been widely employed due to ease in accessing, fusing and attaining

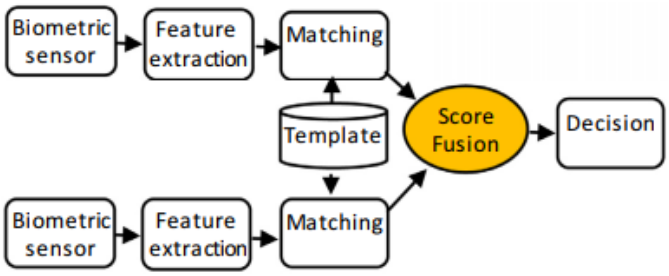

Fig. 3.8 *Block diagram of score level fusion in multi-biometric systems*

great accuracy. Scores obtained by different biometric matchers may be dissimilarity (a smaller distance indicates a better match) while another may output a similarity measure (a larger similarity value indicates a better match). Besides, match scores can be on different numerical scale. Therefore, fusion at score level is a challenging problem.

Many score fusion schemes have been proposed in the literature. The score fusion rules can be categorised into three broad groups: classifier-based fusion techniques, density-based fusion techniques and rule-based fusion techniques, as shown in Fig. 3.9.

- **Classifier-based fusion techniques** In this category, the matching scores acquired via multiple matchers are joined to construct a single vector of features, which then is fed to a fitting classifier with the view to obtain the concluding label if the user is legitimate or imposter. For instance, Fahmy *et al.* [48] proposed to use the support vector machine (SVM) as a fusion tool for iris and fingerprint multi-biometric system. While Bayesian inference based fingerprint, face and on-line signature fusion system was presented in [49]. Nguyen *et al.* [50] showed that the multi-biometric recognition problem can be modeled using Dempster' Shafer theory. Dynamic Bayesian network-based continuous person authentication was developed in [51] that utilised face and keystrokes patterns. A maximum entropy model was proposed in [52] to combine IR face, ear and iris for surveillance applications. From the machine learning perspective, the classifier-based fusion techniques can also be classified as generative and discriminative models. For instance, SVM is a discriminative model, while Bayesian inference is a generative model.

- **Density-based fusion techniques** In this category, the distributions of legitimate and imposter match-scores are first approximated, then usually likelihood ratio (LLR) test is applied to obtain the final output. For instance, in [44] authors proposed estimating the legitimate and imposter score distributions like a restricted Gaussian mixture model (GMM) with LLR. Reported results in [44] demonstrated that use of GMM yields better results than the results yielded by the use of kernel probability function approximator on WVU and XM2VTS data sets. In turn, Fathima *et al.* [53] and Raghavendra *et al.* [54] have proposed multi- biometrics

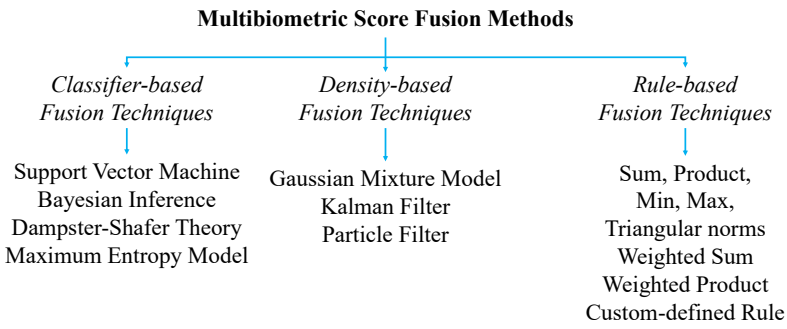

Fig. 3.9 *Categorisation of multi-biometric score fusion methods*

fusion based on Kalman and particle filters, respectively

- **Rule-based fusion techniques** In this category, the biometric matching scores are generally first converted into the same domain via normalisation schemes such as min-max, z-score, tanh [55], or double sigmoid [56], then they are combined either by fixed or trained rule [57]. The fixed rules do not demand any particular learning approach, e.g. sum, product, min, max and triangular norms rules [58].The trained rules require training or learning procedures to estimate the model parameters through the training samples to be subsequently utilised in the testing stage, e.g. weighted sum, weighted product [4]. The representative studies of fixed rules are [58, 59]. Specifically, authors in [58] presented score-level integration scheme based on diverse *t*-norms such as Frank, Yager, Hammcher, and Schweizer-Sklar to integrate hand vein, palmprint and finger knuckle modalities. While in [59] min and max rules were used to fuse the information originated from 2D and 3D palmprints. The representative studies of trained rules are [60, 61]. Artabaz *et al.* [60] proposed a multi-biometrics score fusion scheme by utilising quality-based weights and evolutionary genetic algorithm. Kabir *et al.* [61] devised score reliability-based weighting method for biometric score fusion such that the reliability (weight) is estimated using the distance of score from the mean.

A summary with relevant biometric attributes of some representative works in multi-biometric score level fusion systems is presented in Table 3.3.

3.5.4 Decision-level fusion

This type of fusion can be viewed as a particular case of the score-level fusion, where the scores are converted into a binary (match/non-match) before fusion as shown in Fig. 3.10 [5, 65]. Decision fusion is very beneficial when only the decisions output by the individual biometric matchers are available [2]. Techniques proposed in the literature for decision-level fusion include majority voting, weighted majority voting [**?**], "AND" and "OR" rules [66, 67], Bayesian decision fusion [68], the Dempster-Shafer theory of evidence. Note that this level has least complexity, it is too rigid, because only limited information is available at this level.

Table 3.3 *Previous works on score level fusion based multibiometric authentication systems. GAR: Genuine Acceptance Rate, EER: Equal Error Rate.*

Study	Modalities	Fusion Techniques	Database	Database Size	Performance	Year
Nandakumar *et al.* [62]	Face and left and right index fingerprints	Likelihood-ratio SVM	NIST Multimodal	517	GAR = 98.8%	2008
	Left and right index fingerprints	Likelihood-ratio SVM	NIST Fingerprint	6000	GAR = 91.4%	2008
	Face matchers C and G	Likelihood-ratio SVM	NIST Face	3000	GAR = 77.2%	2008
Hanmandlu *et al.* [58]	Palmprint, hand veins and hand geometry	Frank t-norm	IIT Delhi	100	GAR = 100%	2011
	Knuckles of index and middle fingers and Palmprint	Hamacher t-norm	Hong Kong PolyU	165	GAR = 100%	2011
Peng *et al.* [63]	Finger vein, fingerprint, finger shape and finger knuckle print	Sugeno-Weber t-norm	Hong Kong PolyU Finger	100	ERR = 3.19e-04	2014
Chaa *et al.* [59]	2D and 3D palmprints	EER based Sum Weighting Score (WHT)	Hong Kong PolyU	260	EER = 0.00%	2017
Hezil *et al.* [64]	Ear and plamprint	KNN classifier	IIT Delhi-2 Ear and IIT Delhi Palmprint	221	GAR = 100%	2017

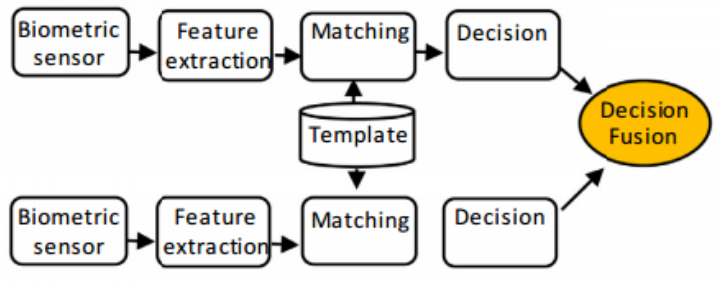

Fig. 3.10 *Block diagram of decision level fusion in multi-biometric systems*

3.5.5 Rank-level fusion

Rank level fusion is carried out in identification systems, where each matcher associates a rank with each enrolled user's identity. The main purpose rank-level fusion methods is to merge all the ranks in order to derive a consensus rank for each identity. Techniques proposed in the literature for rank-level fusion include Highest Rank Method, Borda Count Method, and Logistic Regression Method [2].

3.6 Performance evaluation

The biometric system's performance can be influenced by two factors, the first one is environmental (i.e., at the acquisition) such as the temperature, illumination conditions, and humidity, whilst the second factor is related on performance e.g., quality of the sensor, composition of target user population, and robustness of recognition. In order to measure the accuracy of a biometric system, False Non-Match Rate (FNMR) and False Match Rate (FMR) are usually utilised. FNMR refers to the expected probability that two mate samples (samples of the same biometric trait obtained from the same user) will be falsely declared as a non-match. FMR is the expected probability that two non-mate samples will be incorrectly recognized as a match. For instance, A FNMR of 2(pecent) means that on average, 2 in 100 authentication attempts by genuine users will not succeed. A FMR of 0.02(pecent) indicates that on average, 1 in 5,000 authentication attempts by random impostors are likely to succeed [2].

3.6.1 Verification's accuracy evaluation

In the context of biometric verification, FNMR and FMR are generally referred to as False Reject Rate (FRR) and False Accept Rate (FAR), respectively. A match score is categorised as a genuine if it measures the similarity between two mate samples and imposter score indicates the similarity between two non-mate samples. Since the same biometric system can be operated at different thresholds depending on the changing security level or different requirements

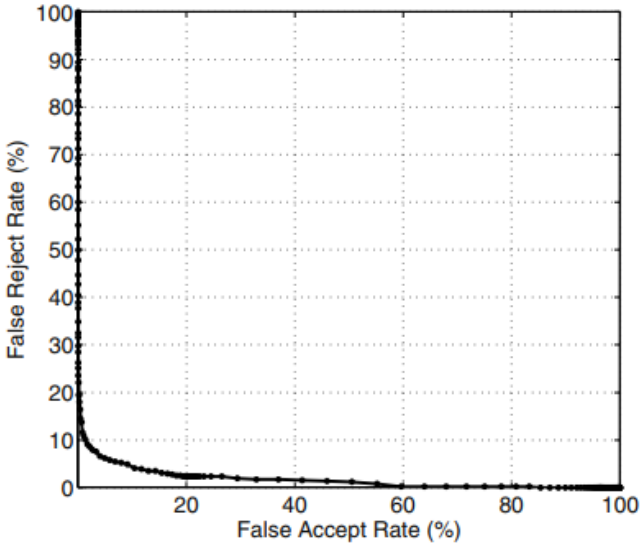

Fig. 3.11 *An ROC curve which plots FRR against FAR in the linear scale*

of different applications, the FAR and FRR at different values of threshold are measured and summarized into different curves.

• **ROC and DET curves** One of The best ways to compare the performance of two biometric systems is to examine their ROC (Receiver Operating Characteristics) curves. The ROC curve is obtained by plotting Genuine Acceptance Rate (GAR) vs. False Acceptance Rate (FAR), where GAR = 1 - FRR. The FRR (False Rejection Rate) is the proportion at which genuine individuals are rejected by the system as imposters, FAR (False Acceptance Rate) is the proportion at which imposter individuals are accepted by the system as genuine users, and GAR is the rate of the genuine users accepted over the total of enrolled individuals (see Fig. 3.11 and Fig. 3.12). Another way to evaluate verification rate of biometric system is DET (Detection Error Tradeoff) curve. The DET curve is obtained by plotting the FRR against the FAR at various thresholds (see 3.13).

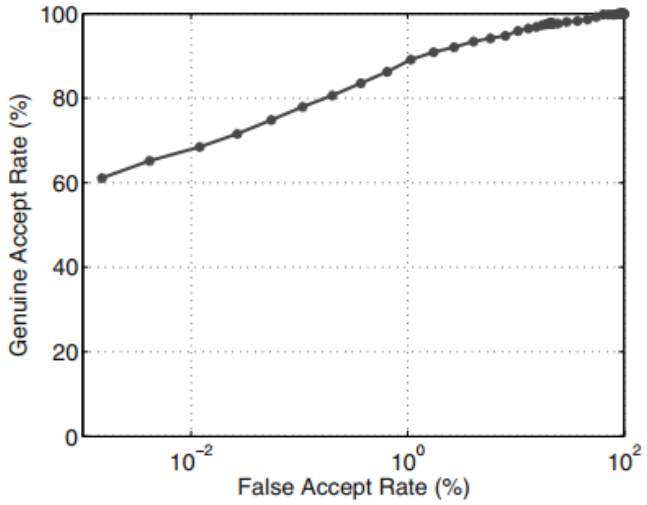

Fig. 3.12 *An ROC curve which plots GAR against FAR, where FAR is in logarithmic scale*

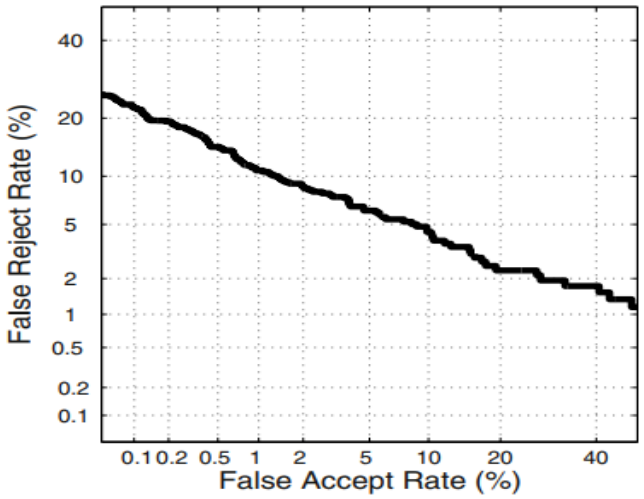

Fig. 3.13 *DET curve which plots FRR against FAR in the normal deviate scale*

• **Equal Error Rate** The performance of a biometric system can be reported using other single-valued measures such as the Equal Error Rate (EER). The EER refers to that point in a DET (or ROC) curve where the FAR equals the FRR as shown in Fig. 13. Here, for better performance, EER should be lower.

• **Decidability index (d')** In addition to above motioned measures for biometric performance, one can adjudge the performance using d', Its value gives the separation between the means of the genuine and impostor probability distributions in standard deviation units. d prime is defined as

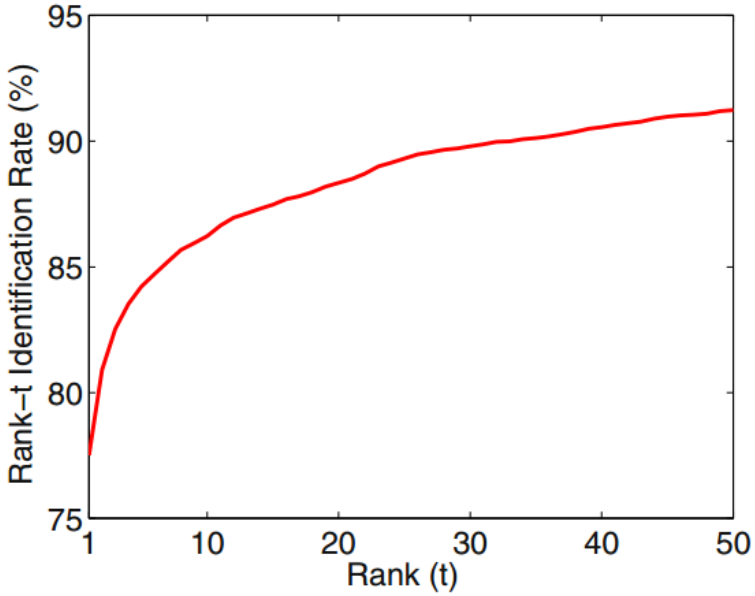

Fig. 3.14 *CMC curve for the Face-G matcher in NIST-BSSR1 multimodal database [2]*

$$d' = \frac{|\mu_1 - \mu_0|}{\sqrt{\frac{\sigma_1^2 + \sigma_0^2}{2}}} \tag{3.1}$$

where mu_1 (mu_0) and σ_1 (σ_0) are the mean and standard deviation, respectively, of the genuine (impostor) score distributions. The greater *d'* value is, the more separable the two distributions become (in this case, the EER becomes smaller and the consequent accuracy of the biometric system increases in general)

3.6.2 Identification's accuracy evaluation

In Identification type, the user is identified by comparing his/her biometric input with the templates of all users enrolled in the database i.e., conducting a one-to-many comparison. Here, the performance is evaluated using Cumulative Match Characteristic (CMC) curve.

3.6.2.1 CMC curve

The rank-t identification rate for different values of t can be summarized using the Cumulative Match Characteristic (CMC) curve as displayed in Fig. 3.14, which plots R_t against t for $t = 1, 2, ..., N$, where N is the number of enrolled users [2, 69].

Table 3.4 *Multimodal biometric databases.*

Reference	Name	Biometric modalities	Number of users	Year
[73]	WVU	Face, Iris, Fingerprint, Palmprint, Voice, Hand Geometry	270	2007
[74]	BiosecurID	Face, Iris, Voice, Signature, Keystroking, Handwritting, Hand	400	2010
[75]	SDUMLA-HMT	Face, Iris, Gait	106	2011
[76]	MOBio	Face, Speech	150	2012
[77]	MMU GASPFA	Gait, Speech, Face	82	2013
[78]	MobBIO	Face, Iris, Voice	105	2014
[79]	LEA	Face, Iris, Fingerprint	18000	2015

3.7 Multimodal Benchmark databases

he availability of benchmark databases is crucial to evaluate new biometric systems. In fact, most of first multimodal data sets were synthetically produced by defining a ?chimeric user? obtained combining biometric modalities acquired from different users. Some researchers [70] observed a large discrepancy between performances evaluated with real and chimeric multimodal databases and claim that ignoring the influence of feature dependency can have negative impact on the performance of the fusion schemes [71] and can produce misleading system performance evaluation results.

Recently a relatively significant number of real multimodal biometric databases have appeared [72], some of the most recent ones are summarized in Table 3.4.

3.7.1 WVU data set

WVU [73] is is a multi-modal data set that was produced by West Virginia University in 2007. It contains face, voice, fingerprint, palmprint, hand geometry, and iris images from 270 subjects. Each subject has multiple samples. The database is already divided into three subsets: (1) initial training (40% of the total database), (2) online learning, and (3) testing. Note that this data set also contains soft biometric information such as weight, height, gender, and ethnicity.

3.7.2 BiosecurID data set

BiosecurID [74] is a large multimodal dataset (large variety of biometric traits and subjects) which was collected in various Spanish University in the framework of the Biosecure project in 2010. It includes eight biometric traits i.e., iris, face images,, face videos, signature, handwritten text, speech, palmprint, fingerprints (collected with two different sensors), hand contour-geometry and keystroking from 400 subjects. It is worth noticing that the acquisition of biometric modalities was in four different sessions distributed in a 4 month time span.

3.7.3 SDUMLA-HMT data set

SDUMLA-HMT [75] is a medium size database, the biometric traits were captured from 106 young subjects (age between 17 and 31) at Shandong University, Jinan, China. Each traits has many images: fingerprint images capttured via 5 different sensors, finger vein images of 6 fingers, ace images from 7 view angles, gait videos from 6 view angles, and iris images from an iris sensor. It is worth mentioning that the collection of this database was done in a single session and controlled background

3.7.4 MOBIO data set

The MOBIO database [76] was collected over a period of 18 months from six sites across Europe from August 2008 until July 2010.It consists of over 61 h of audio-visual data of 150 subjects. Among them, 51 are females and 99 males. face videos were collected using a hand-held mobile device (i.e., the Nokia N93i).

3.7.5 MMU GASPFA data set

MMU GASPFA data set [77] is a medium size multimodal database; this database contains face images, speech and gait video form 82 subjects. The traits were collected in in a single acquisition session utilising commercial off-the-shelf equipment such as smart phones, digital camera, and digital voice recorder. The data set can be interested for researchers because it allow to combine gait recognition and face/speech biometric modalities.

3.7.6 MobBIO data set

MobBIO [78] is a multimodal database which includes biometric data (i.e., ace, iris and voice) acquired from 105 subjects using an Asus EeePad Transformer tablet. The nationalities of the volunteers is mainly Portuguese and the subjects were in the age group 14 to 58 years.

3.7.7 LEA data set

LEA [79] is a large multimodal database consists of three biometric traits namely fingerprint, face, and iris which have been collected in unconstrained real world conditions with uncooperative users. this database has been created by a Law Enforcement Agency. Its main characteristic, besides the large number of subjects (i.e., 18,000 individual) is is noisy, has both good and poor quality images,.

3.8 Conclusion

Multi-biometric systems which merge information from multiple biometric sources are able to overcome the inherent limitations of unibiometrics such as non-universality problem, noisy sensor data as well as helps to decrease the failure to enroll rate. In this chapter, we have presented the advantages of multimodal systems, different level of fusion, the evaluation of performance and finally we have discussed diffrent real multimodal benchmark databases. The following chapter presents the proposed score level fusion method, which is based on the weighted quasiarithmetic mean (WQAM).

Chapter 4

WQAM fusion scheme

4.1 Introduction

Multi-biometric systems fuse information from multiple biometric sources, where different evidences (traits) usually compensate for the inherent limitations of the other ones, thereby leading to higher performance, reliability and robustness against attacks compared to uni-biometrics. Aggregation is the process of combining several values into a single value. Mathematical functions which provide a mechanism for doing so are called aggregation functions. In this chapter, we discus the main classes and general properties of aggregation functions. Thent, we prsent an overview of weighted quasi-arithmetic means (WQAM) which have been applied for match-score combination.

4.2 Aggregation function

An aggregation function is a function of $n > 1$ arguments that maps the (n-dimensional) cube onto an interval $I = [a,b]$, $f : I^n \longrightarrow I$, with the properties:

1. $\underbrace{f(a,a,...,a)}_{n\text{-times}} = a$ and $\underbrace{f(b,b,...,b)}_{n\text{-times}} = b$.
2. $\mathbf{x} \leq \mathbf{y}$ implies $f(x) \leq f(y)$ for all $x, y \in I^n$.

4.3 Extended Aggregation function

An extended aggregation function is a mapping :

$$F : \bigcup_{n\in\{1,2,...\}} I^n \longrightarrow I \tag{4.1}$$

Such that the restriction of this mapping to the domain In for a fixed n is an n-ary aggregation function f , with the convention $F(x) = x$ for $n = 1$.

Table 4.1 presents some examples of aggregation functions.

4.4 Fuzzy logic and rule based systems

In fuzzy set theory [80], membership of objects in fuzzy sets is numbers from [0, 1]. Fuzzy sets allow one to model vagueness and uncertainty which are very often present in natural languages. For instance, the set ”ripe bananas” is fuzzy, as there are obviously different degrees of ripeness. Similarly, the sets of ”high blood pressure” and ”tall people” are fuzzy because there is no clear cutoff which discriminates objects between those that are in the set and those that are not. An object may simultaneously belong to a fuzzy set and its complement.

Table 4.1 *Examples of aggregation functions*

Aggregation function	Formula
Arithmetic mean	$f_n(\mathbf{x}) = \frac{1}{n}(x_1 + x_2 + ... + x_n)$
Geometric mean	$f_n(\mathbf{x}) = \sqrt[n]{x_1 x_2 ... x_n}$
Harmonic mean	$f_n(\mathbf{x}) = \frac{1}{\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n}}$
Minimum	$min(\mathbf{x}) = min\{x_1, ..., x_n\}$
Bounded sum	$(f_n\mathbf{x}) = min\{1, \sum_{i=1}^{n} x_i\}$

A fuzzy set F defined on a set of X is represented by a membership function $\mu_F : X \to [0,1]$, in such a way that for any object $x \in X$ the value $\mu_F(x)$measures the degree of membership of x in the fuzzy set F. The fuzzy sets' classical operations of, union and intersection, are based on the maximum and minimum, i.e., $\mu_{A\cup B} = max\{\mu_A, \mu_B\}$, $\mu_{A\cap B} = min\{\mu_A, \mu_B\}$. Nowadays a large class of conjunctive and disjunctive functions, the triangular norms, grouping and overlap functions are employed to model fuzzy set union and intersection.

Fuzzy set theory has proved to be extremely useful for solving many real world problems, in which the data are imprecise, e.g., [81, 82, 83, 84, 85] . Fuzzy control in consumer electronics and industrial systems is considered as a notable example of the practical applications of fuzzy logic.

4.5 Classification and General Properties of aggregation functions

4.5.1 Main Classes

There are numerous semantics of aggregation, and the main classes are defined using these semantics. In some cases we need that low and high inputs average each other, in other cases aggregation functions model logical connectives (disjunction and conjunction), thus, the inputs reinforce each other, and sometimes the behavior of aggregation functions depends on the inputs. The aggregation functions can be categorised into four main classes as follows [82, 86, 87]:

- Conjunctive,
- Disjunctive,
- Averaging,
- Mixed.

• **Conjunctive aggregation** An aggregation function f has conjunctive behavior if for every $\mathbf{s} \in \boldsymbol{I}^n$ it is bounded by

$$f(\mathbf{s}) \leq min(\mathbf{s}) = min(s_1, s_2, ..., s_n) \tag{4.2}$$

• **Disjunctive aggregation** An aggregation function f has disjunctive behavior if for every $\mathbf{s} \in \boldsymbol{I}^n$ it is bounded by

$$f(\mathbf{s}) > max(\mathbf{s}) = max(s_1, s_2, ..., s_n) \tag{4.3}$$

• **Averaging aggregation** An aggregation function f has averaging behavior if for every $\mathbf{s} \in \boldsymbol{I}^n$ it is bounded by

$$min(\mathbf{s}) \leq f(\mathbf{s}) < max(\mathbf{s}) \tag{4.4}$$

• **Mixed aggregation** An aggregation function f is mixed if it does not belong to any of the above classes, i.e., it exhibits different types of behavior on different parts of the domain.

4.5.2 Main Properties

• **Idempotency** An aggregation function f is called idempotent if for every input $\mathbf{s} = (t,t,...,t)$, $t \in \mathbf{I}$ the output is $f(t,t...,t) = t$. Arithmetic and geometric means (Eq. 4.5 and Eq. 4.6) are examples of averaging (idempotent) aggregation function

$$f_n(\mathbf{s}) = \frac{1}{n}(s_1 + s_2 + ... + s_n) \tag{4.5}$$

$$f_n(\mathbf{s}) = \sqrt[n]{s_1 s_2 ... s_n} \tag{4.6}$$

Due to monotonicity of f, idempotency is equivalent to averaging behavior. The aggregation functions min and max are the only two functions that are at the same time conjunctive (disjunctive) and averaging, and thereby idempotent.

• **Symmetry** An aggregation function f is called symmetric, if its value does not depend on the permutation of the arguments, i.e.,

$$f(s_1, s_2, ..., s_n) = f(s_{P(1)}, s_{P(2)}, ..., s_{P(n)}), \tag{4.7}$$

for every **s** and every permutation $P = (P(1), P(2), ..., P(n))$ of $(1, 2, ..., n)$.

Examples of the symmetric aggregation functions are the arithmetic and geometric means and the product. While that weighted arithmetic mean (Eq. 4.8) with non-equal weights $w_1, w_2, ..., w_n$, that are non-negative and add to one is not symmetric.

$$f(\mathbf{s}) = \sum_{i=1}^{n} w_i s_i = w_1 s_1 + w_2 s_2 + ... + w_n s_n \tag{4.8}$$

Permutation of arguments is very important in aggregation, as it helps express symmetry, as well as to define other concepts. A permutation of $(1, 2..., 5)$ is just a tuple like $(5, 3, 2, 1, 4)$. There are $n! = 1 \times 2 \times 3 \times ... \times n$ possible permutations of $(1, 2, ..., n)$.

- **Strict monotonicity** An aggregation function is strictly monotone increasing if $\mathbf{x} \leq \mathbf{y}$ but $\mathbf{x} \neq \mathbf{y}$ implies $f(\mathbf{x}) < f(\mathbf{y})$for every $\mathbf{x}, \mathbf{y} \in \mathbf{I}^n$. Strict monotonicity is a rather restrictive property. Note that there are no strictly monotone conjunctive or disjunctive aggregation functions because every conjunctive function coincides with $min(\mathbf{x})$ for those $\mathbf{x}$ that have at least one zero component, and min is not strictly monotone (similarly, disjunctive aggregation functions coincide with $max(\mathbf{x})$ for those $\mathbf{x}$ that have at least one component $x_i = 1$).

- **Neutral element** An aggregation function f has a neutral element $e \in \mathbf{I}$, if for every $t \in I$ in any position it holds $f(e, ..., e, t, e, ..., e) = t$. For extended aggregation functions, we have a stronger version of this property, which relates aggregation functions with a different number of arguments. The are many aggregation functions which have a neutral element, e.g., the min and product functions have neutral element $e = 1$, whilst the max function has neutral element $e = 0$.

- **Absorbing element (annihilator)** An aggregation function f has an absorbing element $a \in [0, 1]$ if

$$f(s_1, ..., s_{i-1}, a, s_{i+1}, ..., s_n) = a, \tag{4.9}$$

for every s such that $s_i = a$ with a in any position. It is worth noting that Any conjunctive aggregation function has absorbing element $a = 0$. Any disjunctive aggregation function has absorbing element $a = 1$.

- **Zero divisor** An element $a \in]0, 1[$ is a zero divisor of an aggregation function f if for all $i \in \{1, ..., n\}$ there exists some $s \in]0, 1]^n$ such that its $i - th$ component is $s_i = a$, and it holds $f(s) = 0$, i.e., the equality

$$f(s_1,...,s_{i-1},a,s_{i+1},...,s_n) = 0, \tag{4.10}$$

can hold for some $\mathbf{s} > 0$ with a at any position.

Note that, if a is a zero divisor, then all values $b \in]0,a]$ are also zero divisors due to the monotonicity of function f.

• **One divisor** An element$a \in]0,1[$ is a one divisor of an aggregation function f if for all $i = 1,...,n$ there exists some $s \in [0,1[^n$ such that its i-th component is $s_i = a$ and it holds $f(s) = 1$, i.e., the equality

$$f(s_1,...,s_{i-1},a,s_{i+1},...,s_n) = 1, \tag{4.11}$$

can hold for some $\mathbf{s} < 1$ with a at any position.

• **Associativity** A two-argument function f is associative if $f\,(f(s_1,s_2),s_3) = f(s_1,f(s_2,s_3))$ holds for all s_1,s_2,s_3 in its domain. The important role of associativity is to simpler calculation of aggregation functions, and it effectively allows one to easily aggregate any number of inputs Examples of associative aggregation functions are minimum, maximum and the product functions while the arithmetic mean is not associative.

• **Bisymmetry** An extended aggregation function F is bisymmetric if for all $m,n = 1,2,...$ and for all $s \in [0,1]^{mn}$:

$$f_{mn}(\mathbf{s}) = f_m(f_n(s_{11},...,s_{1n}),...,f_n(s_{m1},...,s_{mn})) = f_n(f_m(s_{11},...,s_{m1}),...,fm(s_{1n},...,s_{mn})) \tag{4.12}$$

• **Shift-invariance** An aggregation function $f : [0,1]^n \to [0,1]$ is shift-invariant (or stable for translations) if for *all* $\lambda \in [-1,1]$ and for all $(s_1,...,s_n) \in [0,1]^n$ it is

$$f(s_{1+\lambda},...,s_{n+\lambda}) = f(s_1,...,s_n) + \lambda \tag{4.13}$$

whenever $(s_1+\lambda,...,s_{n+\lambda}) \in [0,1]^n$ and $f(s_1,...,s_{n+\lambda}) \in [0,1]$

• **Homogeneity** An aggregation function $f : [0,1]^n \to [0,1]$ is homogeneous if for *all* $\lambda \in [0,1]$ and for all $(s_1,...,s_n) \in [0,1]^n$ it is

$$f(\lambda s_1,...,\lambda s_n) = \lambda f(s_1,...,s_n). \tag{4.14}$$

Aggregation functions which are both shift-invariant and homogeneous are known as linear aggregation functions. Note that, due to the boundary conditions $f(0,...,0) = 0$ and $f(1,...,1) = 1$,

either shift-invariant, homogeneous or linear aggregation functions are necessarily idempotent, and thus they can only be found among averaging functions, e.g., arithmetic mean 4.5.

4.5.3 Duality

The concept of a dual aggregation function helps with mapping most properties of conjunctive aggregation functions to disjunctive ones. Therefore, one should study conjunctive functions, and obtain the corresponding results for disjunctive functions by duality. Besides, some aggregation functions are self-dual. In order to study the duality of aggregation function, we should first to define the concept of negation.

- **Strict negation** A univariate function N defined on $[0,1]$ is called a strict negation, if its range is also $[0,1]$ and it is strictly monotone decreasing. Example of negation is $N(t) = 1 - t^2$

- **Strong negation** A univariate function N defined on $[0,1]$ is called a strong negation, if it is strictly decreasing and involutive (i.e., $N(N(t)) = t$ for all $t \in [0,1]$). Example of strong negation is $N(t) = 1 - t$.

- **Dual aggregation function** Let $N : [0,1] \to [0,1]$ be a strong negation and $f : [0,1]^n \to [0,1]$ an aggregation function. Then the aggregation function fd given by

$$f_d(s_1,...,s_n) = N(f(N(s_1),N(s_2),...,N(s_n))) \tag{4.15}$$

is called the dual of f with respect to N, or, for short, the N-dual of f. When using the standard negation, f_d is given by

$$fd(s_1,...,s_n) = 1 - f(1-s_1,...,1-s_n) \tag{4.16}$$

and we will simply say that $f_d$is the dual of f.

- **Self-dual aggregation function** Given a strong negation N, an aggregation function f is self-dual with respect to N (for short, N-self-dual), if

$$f(\mathbf{s}) = N(f(N(\mathbf{s}))) \tag{4.17}$$

where $N(\mathbf{s}) = (N(s_1),...,N(s_n))$. For the standard negation we have $f(s) = 1 - f(1-s)$, and it is simply said that f is self-dual. Example of self-dual aggregation function is the arithmetic mean **??**.

4.5.4 Comparability

In order to compare different aggregation functions and establish a certain order among them, we have to compare aggregation functions for every $\mathbf{s} \in [0,1]^n$. Note that all aggregation functions are comparable. One can say that an aggregation function f is stronger than another aggregation function of the same number of arguments g, if for all $\mathbf{s} \in [0,1]^n : g(\mathbf{s}) \leq f(\mathbf{s})$. It is expressed as $g \leq f$. When f is stronger that g, it is equivalently said that g is weaker than f. For instance, The strongest conjunctive aggregation function is the *min*, and the weakest disjunctive aggregation function is the *max*. It is worth mentioning that any disjunctive aggregation function is stronger than an averaging function, whilst any averaging function is stronger than a conjunctive one.

4.5.5 Continuity and stability

In continuous aggregation functions, a small change in the input leads to a small change in the output. Although there are some interesting aggregation functions which are discontinuous, continuity is very important because it helps to produce a stable output. The following definition puts a bound on the actual change in value due to changes in the input.

- **Lipschitz continuity** An aggregation function f is called Lipschitz continuous if there is a positive number M, such that for any two vectors $\mathbf{x}, \mathbf{y}$ in the domain of definition of f:

$$|f(\mathbf{x}) - f(\mathbf{y})| \leq Md(\mathbf{x}, \mathbf{y}) \tag{4.18}$$

where $d(\mathbf{x}, \mathbf{y})$ is a distance between $\mathbf{x}$ and $\mathbf{y}$. The smallest such number M is called the Lipschitz constant of f. Usually, the distance is the Euclidean distance (Eq. 4.19) between vectors.

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + ... + (x_n - y_n)^2} \tag{4.19}$$

but it can be chosen as any norm $d(\mathbf{x}, \mathbf{y}) = ||\mathbf{x} - \mathbf{y}||$; typically it is chosen as a p-norm. A p-norm, $p \geq 1$ is a function defined as:

$$||\mathbf{x}||_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{\frac{1}{p}} \tag{4.20}$$

for finite p, and $||\mathbf{x}||_\infty = max_{i=1...,n}|x_i|$

Therefore, if the change in the input is $\delta = ||\mathbf{x} - \mathbf{y}||$, then the output will change by at most $M\delta$. Here Mcan be interpreted as the upper bound on the rate of change of a function. Note that all differentiable functions are necessarily Lipschitz-continuous, but not vice versa.

• **p-stable aggregation functions** Given $p \geq 1$, an aggregation function is called p-stable if its Lipschitz constant in the p-norm $||.||_p$ is 1

• **1-Lipschitz aggregation functions** An aggregation function f is called 1-Lipschitz if it is p-stable with $p = 1$, i.e., for all $\mathbf{x}, \mathbf{y}$:

$$|f(\mathbf{x}) - f(\mathbf{y})| \leq |x_1 - y_1| + |x_2 - y_2| + \cdots + |x_n - y_n|. \tag{4.21}$$

• **1-Kernel aggregation functions** An aggregation function f is called kernel if it is p-stable with $p = \infty$, i.e., for all $\mathbf{x}$, $\mathbf{y}$:

For kernel aggregation functions, the error in the output cannot exceed the largest error in the input vector. Note that the arithmetic mean is p-stable for any p, whilst min, max and the product are p-stable extended aggregation functions for any p. Although geometric mean (4.6) is continuous, it is not Lipschitz.

4.6 Weighted Quasi-Arithmetic Mean

In fuzzy logic and fuzzy set theory, the most popular and widely utilised aggregation functions *min* and *max* functions because they are the only two operations consistent with a number of set-theoretical properties, and in particular mutual distributivity [**ref 33 of the book**]. These connectives model fuzzy set intersection and union (or conjunction and disjunction).

In addition to *min* and *max* function which were used in fuzzy logic, Means also have been employed as an aggregation functions. Means are averaging aggregation functions. Mathematically, a mean is simply a function f with following property

$$min(x) \leq f(x) \leq max(x) \tag{4.22}$$

4.6.1 Arithmetic Mean

The arithmetic mean (Eq. (4.23)) or the operator modeling the average is strictly monotone increasing aggregation function, besides being continuous, symmetric, linear, additive, etc.

$$M(s_1, \ldots, s_n) = \frac{1}{n} \sum_{i=1}^{n} s_i \tag{4.23}$$

Since M is properly defined for any number of arguments, it is an extended aggregation function

• **Main proprieties of Arithmetic Mean**

1. The arithmetic mean M is a strictly increasing aggregation function.
2. M is a symmetric function.
3. M is an additive function, i.e., $M(s_1+s_2)=M(s_1)+M(s_2)$ for all $s1,s2\in[0,1]^n$ such that $s_1+s_2\in[0,1]^n$.
4. M is a homogeneous function, i.e.,$M(\lambda s)=\lambda M(s)$ for all s$\in \mathbf{I}^n$ and for *all* $\lambda\in\mathbf{R}$.
5. The orness measure orness $(M)=1/2$.
6. M is a Lipschitz continuous function.

4.6.2 Weighted Arithmetic Mean

The demand of merging the weights (i.e., importance) into arithmetic means has lead to the class of weighted arithmetic mean (WAM) (as given in Eq. 4.24):

$$M_w(s_1,...,s_n)=\sum_{i=1}^{n} w_i s_i=\langle \mathbf{w},\mathbf{s}\rangle \tag{4.24}$$

- **Main proprieties of Weighted Arithmetic Mean**

1. WAM is a strictly increasing aggregation function, if all $w_i>0$; WAM is a strictly increasing aggregation function, if all $w_i>0$;
2. WAM is an asymmetric(unless $w_i=1/n$for all $i\in 1,\cdots,n$) idempotent function;
3. WAM is an additive function i.e., $M_w(s_1+s_2)=M_w(s_1)+M_w(s_2)$ for all $s_1,s_2\in[0,1]^n$ such that $s_1+s_2[0,1]^n$;
4. WAM is a homogeneous function i.e., $Mw(\lambda s)=\lambda Mw(s)$ for all $s\in[0,1]^n$ and for all $\lambda\in\mathbf{R}$;
5. WAM is a Lipschitz continuous function, in fact it is a kernel aggregation function

4.6.3 WQAM description

For a given strictly monotone continuous function $g:[0,1]\to[-\infty,\infty]$, the quasi-arithmetic mean is a function defined as:

$$M_g(s_1,...,s_n)=g^{-1}\left(\frac{1}{n}\sum_{i=1}^{n} g(s_i)\right) \tag{4.25}$$

Thus, Weighted Quasi-Arithmetic Mean (WQAM) is a combination of both weighted mean and quasi-arithmetic mean approaches, where these approaches act as generalization of arithmetic mean. In particular, the WQAM is defined as an aggregation operator $M_{w,g} : U_{n\in N}[0,1]^n \to [0,1]$, which is expressed as [88]:

$$M_{w,g}(s) = g^{-1}\left(\sum_{i=1}^{n} w_i g(s_i)\right) \tag{4.26}$$

Where $g : [0,1] \to [-\infty,\infty]$ is the generating function, g^{-1} is its inverse function and w is a weight vector. Note that $w_i \in [0,1]$ and $\sum_{i=1}^{n} w_i = 1$. In the case of $\sum_{i=1}^{n} w_i \neq 1$, the WQAM is expressed as [88]:

$$M_{w,g}(s) = g^{-1}\left(\frac{1}{W}\sum_{i=1}^{n} w_i g(s_i)\right) \tag{4.27}$$

where $W = \sum_{i=1}^{n} w_i$.

4.6.3.1 Main proprieties of WQAM

The basic properties of WQAM can be expressed as follows [88, 89]:

1. Each WQAM is a bisymmetric aggregation function
2. WQAMs are strictly monotone increasing on $]0,1[^n$ when all weights w_i are strictly positive and Ran $g \subset R$.
3. WQAMs are continuous when $Ran(g) \neq [-\infty,\infty]$ [90]. Note that if $Ran(g) = [-\infty,\infty]$, then we have the summation $-\infty+\infty$ or $+\infty-\infty$ if $s_i = 0$ and $s_j = 1$ for some $i \neq j$. When this occurs, a convention, such as $-\infty+\infty = +\infty-\infty = -\infty$, is adopted, and continuity of WQAM is lost.
4. WQAMs are N-self-dual if and only if N is the strong negation generated by g, i.e., if N(t) = $g^{-1}(g(0)+g(1)-g(t))$ for any $t \in [0,1]$. This implies, in particular:
   - WQAMs, such that $g(0) = \pm\infty$ or $g(1) = \pm\infty$ are never N-self-dual;
   - Weighted arithmetic means are always self-dual (i.e., N-self-dual with respect to the standard negation $N(t) = 1-t$);
5. The generating function is not defined uniquely, but up to an arbitrary linear transformation, i.e., if $g(t)$ is a generating function of some WQAM, then $ag(t)+b, a, b \in R, a \neq 0$ is also a generating function of the same mean, provided $Ran(g) \neq [-\infty,\infty]$;
6. Weighted power means are the only homogeneous WQAM

7. In WQAMs , there are no neutral element. They may have an absorbing element only when all the weights are strictly positive and $g(a) = \pm\infty$ or $g(b) = \pm\infty$, and in such cases the corresponding absorbing elements are, respectively, a and b.

4.6.3.2 The utilsed types of WQAM

In this paper, we have evaluated five types of WQAMs. The first is the weighted power mean and its generating function is given by [88]:

$$g(n) = \begin{cases} s^r & \text{if } r \neq 0 \\ log(s) & \text{if } r = 0 \end{cases}. \tag{4.28}$$

The second used type of WQAM is weighted exponential mean, the generating function of this type is given by

$$g(n) = \begin{cases} r^s & \text{if } r \neq 1 \\ s & \text{if } r = 1 \end{cases}. \tag{4.29}$$

The third used type of WQAM is weighted radical mean, the generating function of this type is given by

$$g(s) = r^{1/s} \tag{4.30}$$

with $r > 0$ and $\neq$

The fourth used type of WQAM's generating function is given by

$$g(s) = e^{-\left(\frac{r}{s}\right)} \tag{4.31}$$

The fifth used type of WQAM is the weighted trigonometric mean with three generating function as [88]:

$$\begin{cases} g_1(s) = sin(\frac{\pi}{2}s) \\ g_2(s) = cos(\frac{\pi}{2}s) \\ g_3(s) = tan(\frac{\pi}{2}s) \end{cases}. \tag{4.32}$$

For a given continuous strictly monotone function $g : [0,1] \to [-\infty,\infty]$ and $w \in]0,1[$, the corresponding bivariate WQAM is the function [88] presented as:

$$M_{w,g}(s_1,s_2) = g^{-1}[(1-w)g(s_1) + wg(s2)] \tag{4.33}$$

For $g = \log(s)$, the the bivariate WQAM is defined as:

Table 4.2 *Examples of WQAMs with their generating functions g.*

$g(s)$	$g^{-1}(s)$	WQAM
$\tan(\frac{\pi}{2}s)$	$\frac{2}{\pi}\arctan(s)$	$\frac{2}{\pi}\arctan\left(\sum_{i=1}^{n} w_i \tan(\frac{\pi}{2}s_i)\right)$
$\sin(\frac{\pi}{2}s)$	$\frac{2}{\pi}\arcsin(s)$	$\frac{2}{\pi}\arcsin\left(\sum_{i=1}^{n} w_i \sin(\frac{\pi}{2}s_i)\right)$
$\cos(\frac{\pi}{2}s)$	$\frac{2}{\pi}\arccos(s)$	$\frac{2}{\pi}\arccos\left(\sum_{i=1}^{n} w_i \cos(\frac{\pi}{2}s_i)\right)$
s^r	$s^{\frac{1}{r}}$	$\left(\sum_{i=1}^{n} w_i (s_i)^r\right)^{\frac{1}{r}}$
$\log(s)$	$\exp(s)$	$\exp\left(\sum_{i=1}^{n} w_i \log(s_i)\right)$
$\left(\cos(\frac{\pi}{2}s)\right)^r$	$\left(\frac{2}{\pi}\arccos(s)\right)^{\frac{1}{r}}$	$\left(\frac{2}{\pi}\arccos\sum_{i=1}^{n} w_i \cos(\frac{\pi}{2}s_i)\right)^{\frac{1}{r}}$
r^s	$\log_r(s)$	$\log_r\left(\sum_{i=1}^{n} w_i r^{s_i}\right)$
$r^{1/s}$	$\frac{\log(r)}{\log(s)}$	$\left(\log_r\left(\sum_{i=1}^{n} w_i r^{1/s_i}\right)\right)^{-1}$
$e^{-(r/s)}$	$\frac{-r}{\log(s)}$	$\frac{-r}{\log_r\left(\sum_{i=1}^{n} w_i e^{-(r/s)}\right)}$

$$M_w(s_1, s_2) = s_1^{1-w} s_2^w \tag{4.34}$$

Table 4.2 tabulates the used WQAMs, i.e., the weighted trigonometric and power means using various of generating function.

A good biometric score fusion technique is expected to maximise the genuine scores and minimise the impostor scores in order to have higher genuine acceptance rate (GAR) and lower false acceptance rate (FAR). Towards this aim, WQAM (using sin, cos and tan etc.) is presented that can simultaneously maximise the genuine scores and minimise the imposter scores, which can be seen in Figs. 4.1, 4.2, 4.3. Moreover, a large number of functions can be easily adopted in the proposed fusion scheme in different biometric systems

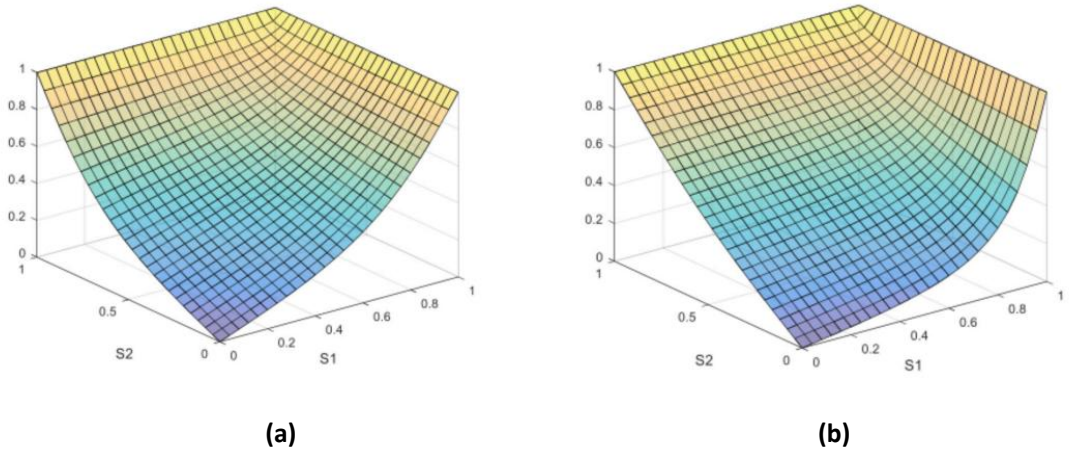

Fig. 4.1 *Match-score plots using WQAM with tan function (a) w1 = 0.5 for match score S1 and w2 = 0.5 for match score S2, (b) w1 = 0.2 for match score S1 and w2 = 0.8 for match score S2*

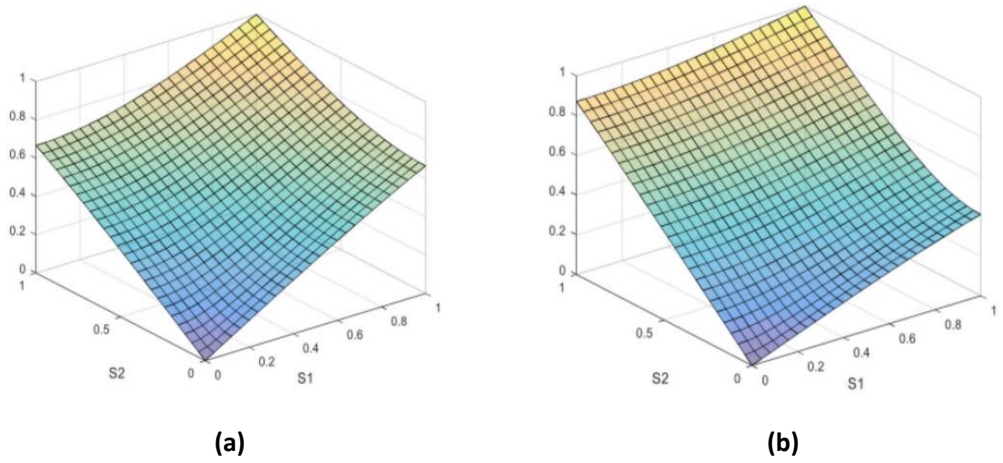

Fig. 4.2 *Match-score plots using WQAM with cos function (a)* $w1 = 0.5$ *for match score S1 and* $w2 = 0.5$ *for match score S2, (b)* $w1 = 0.2$ *for match score S1 and* $w2 = 0.8$ *for match score S2*

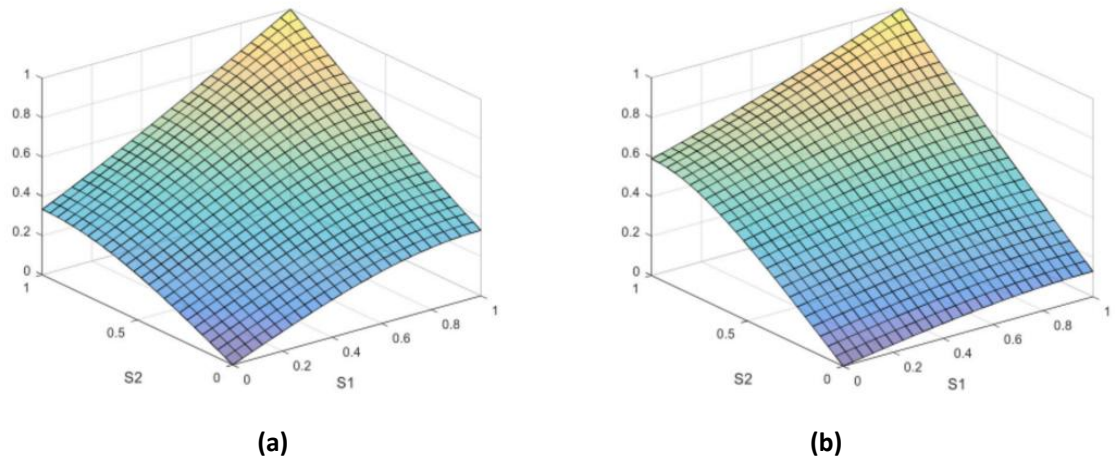

Fig. 4.3 *Match-score plots using WQAM with sin function (a) w1 = 0.5 for match score S1 and w2 = 0.5 for match score S2, (b)w1 = 0.2 for match score S1 and w2 = 0.8 for match score S2*

4.7 Conclusion

In this chapter, we presented the proposed method for score level fusion in multimodal biometric verification systems. In particular, we focused on a aggregation functions and fuzzy logic based systems, specifically, weighted quasi-arithmetic mean. This chapter has defined and discused the main classes (e.g, conjunctive, disjunctive, averaging) and general properties (e.g., associativity, bisymmetry, strict monotonicity) of aggregation functions. Then we described the main proprieties of WQAM and show how this method could be applied for score fusion as well as the types of WQAMs and their generating functions that have been used in this thesis. The following chapter discusses the results obtained through applying this fusion method.

Chapter 5

Experimental results

5.1 Introduction

Biometrics is now being principally employed in many daily applications ranging from border crossing to mobile user authentication. In high security scenarios, biometrics require stringent accuracy and performance criteria. Towards this aim, multi-biometric systems that fuse evidences from multiple sources of biometric have exhibited to diminish the error rates and alleviate inherent frailties of the individual biometric systems. In this thesis, a novel scheme for score-level fusion based on Weighted Quasi-Arithmetic Mean (WQAM) has been proposed. Specifically, WQAMs are estimated via different trigonometric functions. The proposed fusion scheme encompasses properties of both weighted mean and quasi-arithmetic mean. Moreover, it does not require any leaning process. Experimental results on three publicly available datasets (i.e., NIST-BSSR1 Multimodal, NIST-BSSR1 Fingerprint, and NIST-BSSR1 Face) for multi-modal, multi-unit and multi-algorithm systems show that presented WQAM fusion algorithm outperforms the previously-proposed score fusion rules based on transformation (e.g., t-norms), classification (e.g., support vector machines) and density estimation (e.g., likelihood ratio) methods.

One of the newest promising biometrics researched today is the vein pattern recognition. In this chapter we propose a multimodal biometric system to identify people using their left and right palm and wrist vein images. Besides, a novel multi-biometric user authentication framework based on their major knuckle finger patterns using four fingers (i.e., little, ring, middle, and index) and iris has been proposed.

5.2 Proposed WQAM-based multi-biometric authentication method

Fig. 5.1 depicts the representational figure of the proposed score-level fusion utilising WQAM. In a verification setting, each user provides her biometric traits to the respective sensors, and claims her identity. Next, the framework separately matches the captured traits against their corresponding features (i.e., templates) in the data-base accumulated at the time of enrollment, and yields a vector of matching score $S = [S_1, S_2, ?, S_N]$, where S_i is match-score produced via ith modality corresponding to ith sensor. Since the matching scores provided by different matchers are generally heterogeneous, score normalization is required to transform these matching scores into a common domain prior to fusion. In order to normalize the matching scores into the domain $[0,1]$, two normalization methods (i.e., tanh-estimator and min-max) were employed in this paper as follows:

$$S' = \frac{S - \min(S)}{\max(S) - \min(S)} \tag{5.1}$$

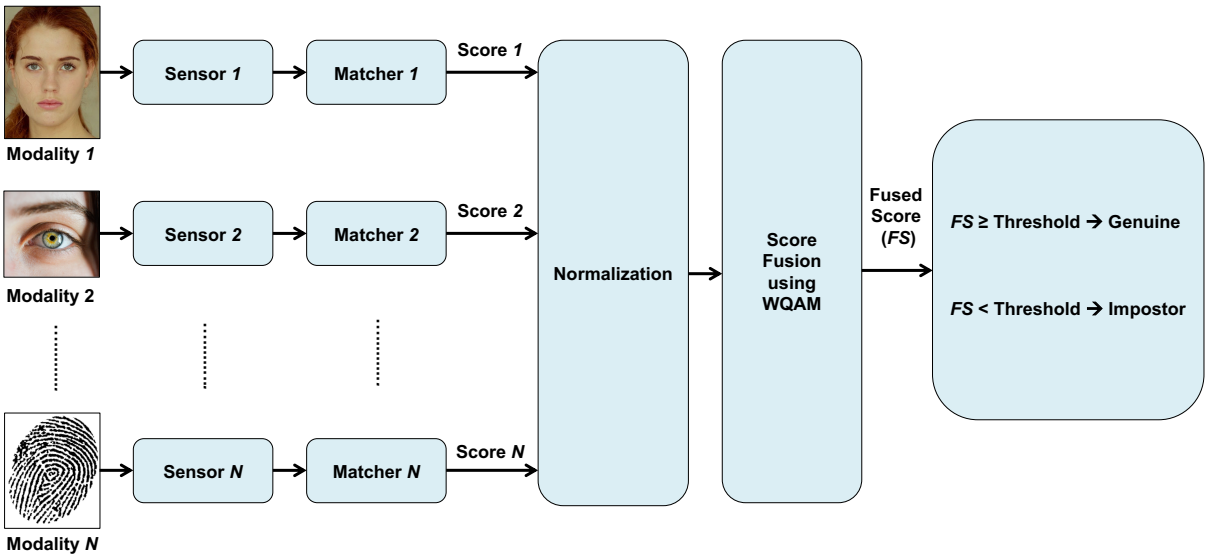

Fig. 5.1 *Proposed framework for score level fusion utilising WQAM.*

Eq. 5.1 represents the min-max normalization techniques [8], where S' and S, respectively, are normalized and match scores through a particular matcher, and

$$S' = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{S-\mu}{\sigma}\right)\right)+1\right\} \tag{5.2}$$

Eq. 5.2 depicts tanh-estimator normalization scheme [8], where S', σ and μ are normalized score, standard deviation and mean estimates of match-score distribution obtained via Hampel estimators, respectively. Finally, the normalized scores are fused utilising the WQAM. If the fused score FS is greater than or equals to a specified threshold (τ), the user is categorised as a genuine user, otherwise, it is categorised as an impostor.

The procedure is summarized in the form of pseudo code in Algorithm 1.

5.2.1 Experiments

Here, we present an experimental evaluation of the proposed fusion scheme on three publicly available databases.

5.2.1.1 Databases

The proposed score-level integration framework has been evaluated on three individual partitions of the NIST-BSSR1 dataset. The three partitions are NIST-Multimodal dataset, NIST-Fingerprint dataset and NIST-Face dataset [91]. Note that the face and fingerprint raw images of the subject are not available, but only match scores. Also, information about the face and fingerprint matching techniques is not provided by the NIST.

Algorithm 1 WQAM-based score level fusion framework.

Input : A training and a testing data set.
A set of matchers.
A set of generating functions $g(s)$.
Output: The system's performance (namely, decision of match/un-match).
1. Compute the empirical threshold τ using training data set.
2. **for each** user do
3.Compute the match score S_1 from the first modality using matcher 1.
4. Compute the match score S_2 from the second modality using matcher 2.
...
5. Compute the match score $(S_n)$from the nth modality using matcher n.
6. Normalise the match-scores (using either min-max (Eq. 5.1) or tanh-estimator (Eq. 5.2)).
7. Select a generating function $g(s)$ and compute a weight vector W // $w_i \in [0,1]$ and $\sum_{i=1}^{n} w_i = 1$.
8. Compute fused matched score using Eq. 4.26. Let FS be the fused score.
9. Compute the decision by comparing FS with the threshold τ.
10. Return the performance of the system.
11. **end for**

• **NIST-Multimodal dataset** NIST-multimodal dataset is composed of four subsets of match-scores. Two fingerprint match-scores are procured from the right and left forefingers. While, two face match-scores are acquired via two different face matchers indicated as C and G. The face and fingerprint samples were collected from 517 subjects. In each subset, there are 517 and 266,772 (517 $\times$ 516) genuine and imposter match-scores, respectively.

• **NIST-Fingerprint dataset** NIST-fingerprint dataset encompasses two subsets of match-scores acquired through the right and left index fingers belonging to same person. The samples were collected from 6000 subjects. In this study, 6000 and 35,994.000 (6000 $\times$ 5999) genuine and imposter match-scores were used.

• **NIST-Face dataset** NIST-face database is made-up of two subsets of match-scores procured through the C and G face matchers. The face data was captured from 3000 subjects. This study used 6000 (two scores per subject) and 17,994.000 (6000 $\times$ 2999) genuine and imposter match-scores for each face matcher.

5.2.2 Experimental Results

We have tested the proposed WQAM-based score fusion method on mutli-modal-, multi-unit-, and multi-algorithm-biometric systems. In particular, the performances of proposed fusion scheme are analyzed utilising ROC (receiver operating characteristic) curve. A ROC curve is a plot of FAR versus GAR. GAR, FAR and FRR are genuine acceptance rate such as GAR = 1

– FRR (i.e., ratio of legitimate users accepted as genuine), false acceptance rate (i.e., ratio of impostors accepted as legitimate) and false rejection rate (i.e., ratio of legitimate users rejected as impostors), respectively. We also used equal error rate (EER), where FRR and FAR are equal to evaluate performance of the system. Note that in each weighted fusion experiment, we empirically estimated the weight values using training data subset. Namely, the weight values were computed by maximising the system performance. In particular, during training, the values of weights were varied from 0 to 1 and selected the ones that yielded highest system performance

5.2.2.1 Performance of WQAM based fusion scheme on multi-modal systems

A biometric multi-modal system combines evidences of multiple biometric traits of the same person to attain enhanced accuracy. In this study, the multimodal system was composed of two modalities, i.e. face and fingerprint. More specifically, the matchingscores from right and left index fingerprints and two face matchers C and G were employed

The match-scores from face matchers C and G as well as right and left index fingerprints are first normalized using tanh-estimator normalization technique as in Eq. 5.2. Let S_1, S_2, S_3 and S_4 be the normalized match-scores of face matcher G, face matcher C, right fingerprint and left fingerprint, respectively, which are fused via WQAM with corresponding weight W_1, W_2, W_3 and W_4 to yield fused score for final decision.

The performances of individual face C, face G, right fingerprint, and left fingerprint systems and multi-modal biometric system using WQAM is reported in Fig. 5.2 in terms of ROCs. In particular, the individual systems were combined utilising WQAM trigonometric function $\cos(\frac{\pi}{2}s)$ with weights $W_1 = 0.57$, $W_2 = 0.18$, $W_3 = 0.17$ and $W_4 = 0.08$. It is easy to see in Fig. 5.2 that 68.0%, 74.3%, 85.3% and 77.2% of GARs are attained, respectively, for face matcher G, face matcher C, right index fingerprint and left index fingerprint using FAR = 0.01% as the operating point. Whereas, 99.8% of GAR is procured using the proposed WQAM based on $\cos(\frac{\pi}{2}s)$ with 0.01% FAR as the operating point.

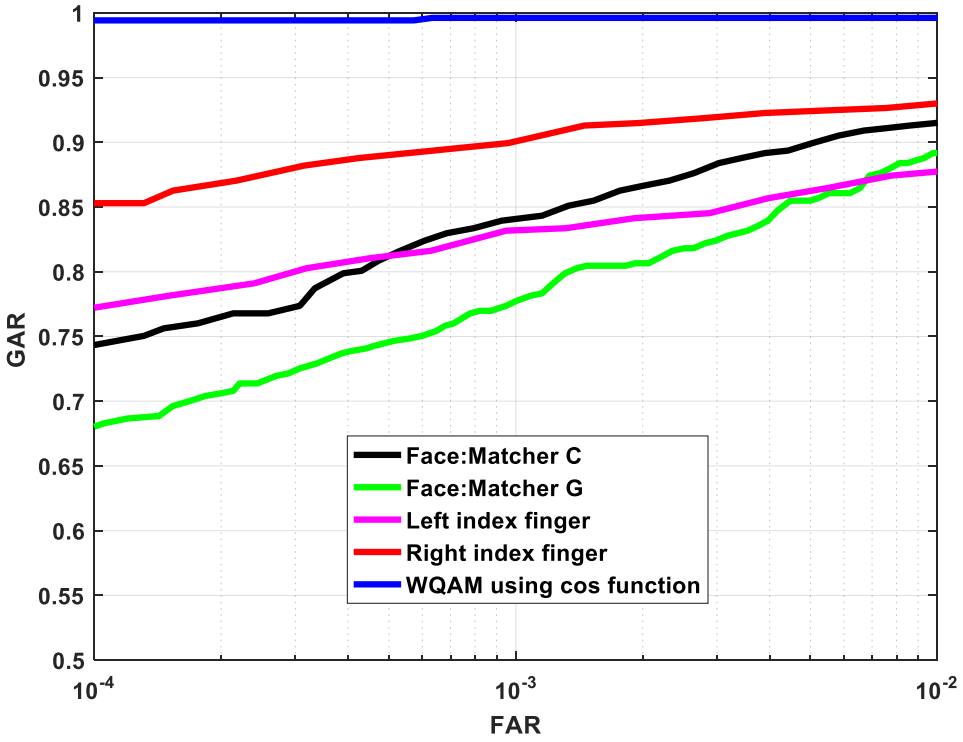

Fig. 5.2 *ROC curves of individual modalities (i.e., face matcher G, face matcher C, right index finger and left index finger) and their integration using WQAM based fusion framework.*

In Table 5.1, we report the results of proposed WQAM fusion (using sin, tan, $\left(cos\left(\frac{\pi}{2}s\right)\right)^r$ and s^r) together with existing score fusion based on the likelihood ratio and SVM (proposed in [62], both requiring learning and training), Frank and Harmacher t-norms [58], EER based weighted sum [59], and min and max rules. The results clearly point out that proposed WQAM fusion scheme outperforms prior multi-biometric score fusion rules.

5.2.2.2 Performance of WQAM based fusion scheme on multi-unit systems

A multi-unit biometric system utilises multiple instances of the same body trait. In this study, the right and left index fingers were employed to constitute a multi-unit system.

For multi-unit multi-biometric system, the match-scores of right and left index fingers were normalized using min-max procedure as depicted in Eq. 5.1, then they were integrated using WQAM based on $\cos\left(\frac{\pi}{2}s\right)^r$ with weights $W_1 = W_2 = 0.5$. Fig. 5.3 depicts ROCs of individual left and right fingers and their multi-biometric system. The WQAM fusion scheme improves the performance of uni-biometric systems, as GARs of right and left forefingers are 83.5% and 75.5% at FAR = 0.01%, respectively, whereas GAR equals to 91.6% when WQAM-based generating function $\cos\left(\frac{\pi}{2}s\right)^r$ with $r = 11$ is used at the same operating point.

Table 5.1 *Comparison of multi-modal fusion via different techniques on NIST face and fingerprint databases.*

Score-level fusion method for FAR = 0.01 %	GAR, %	EER, %
WQAM using cos function	**99.42**	**0.38**
WQAM using sin function	**99.34**	**0.38**
WQAM using tan function	**99.42**	**0.38**
WQAM using s^r function with$r = 2$	**99.42**	**0.38**
WQAM using $(\cos)^r$ function with$r = 3$	**99.33**	**0.38**
WQAM using r^s function with$r = 6$	**99.42**	**0.38**
WQAM using $r^{\frac{1}{s}}$ function with$r = 0.1$	**99.37**	**0.38**
WQAM using $exp(\frac{-1}{s})$ function with$r = 2$	**99.28**	**0.38**
Max rule [59]	91.70	0.85
Min rule [59]	78.00	7.03
Hammcher t-norm [58]	96.89	0.60
Frank t-norm with $p = 1.3$ [58]	96.92	0.84
EER based Sum Weighting Score (WHT) [59]	93.41	1.60
LLR [62]	99.10	0.61
SVM [62]	98.80	0.82
exponential product [92]	96.62	0.62
tan-hyperbolic product [93]	96.65	0.46
entropy using Frank t-norm with p = 0.01 [58]	96.62	0.61

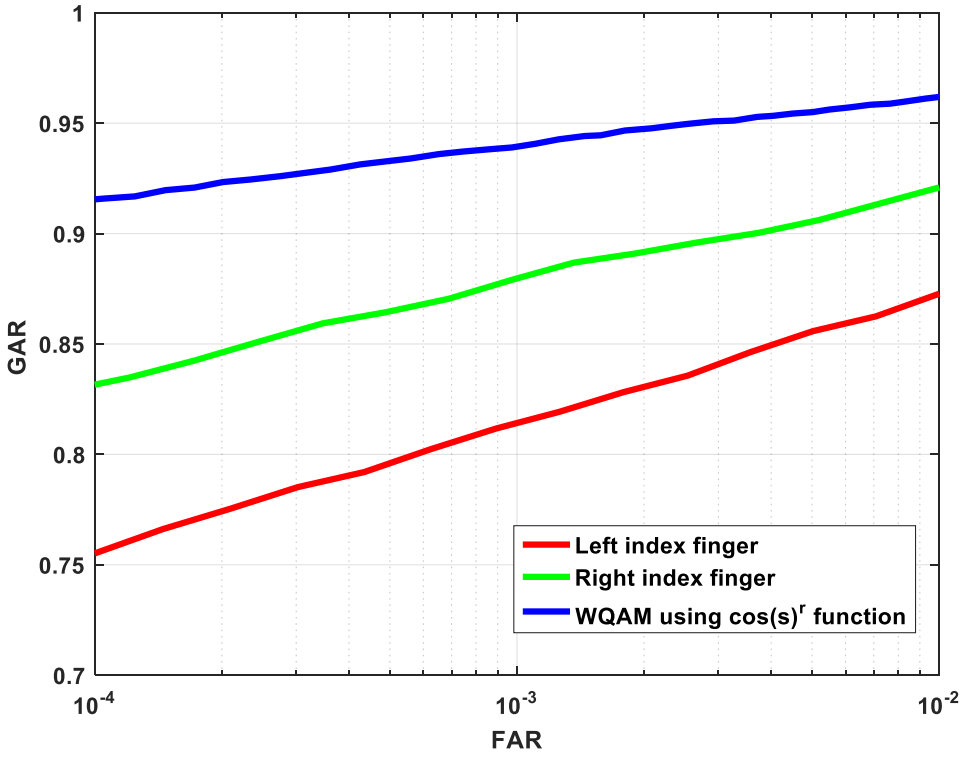

Fig. 5.3 *ROCs of individual biometric modalities (left index finger and right index finger) and their fusion using WQAM on the NIST-fingerprint database.*

In Table 5.2, we report results of proposed WQAM fusion with different functions as well as previously proposed multi-biometric fusion strategies. We can observe in Table 5.2 that performance obtained using proposed WQAM-based score fusion with sin, cos, $(\cos)^r$, tan, and s^r functions are very competing with respect to the ones attained by Likelihood ratio and SVM [62] based fusion methods. Furthermore, we can notice that the proposed framework is capable of achieving better accuracy than widely adopted systems depending on min [59], max [59], Harmacher t-norms [58], Frank t-norms [58] and EER based weighted sum [59] fusion rule.

5.2.2.3 Performance of WQAM based fusion scheme on multi-algorithm systems

A multi-algorithm biometric system uses multiple matching algorithms on the same biometric trait to improve the performance. In this work, the multi-algorithm biometric system applied two face matching algorithms.

For multi-algorithm multi-biometric systems experiments, two sets of similarity scores originated from two face authentication algorithms/matchers, labeled as C and G, were utilised. The scores were normalized by the tanh-estimator normalization technique as in Eq. 5.2. We report the performance in terms of ROCs of individual face matcher C and G along with proposed WQAM score fusion framework for multi-algorithm system with weights $W_1 = 0.57$ and $W_2 = 0.43$ in Fig. 5.4. As in case of multi-modal and multi-unit fusion experiments, the proposed WQAM scheme (here, multi-algorithm multi-biometric system) improves the perfor-

Table 5.2 *Comparison of multi-unit fusion on NIST fingerprint databases.*

Score-level fusion method for FAR = 0.01 %	GAR, %	EER, %
WQAM using cos function	**91.50**	**2.82**
WQAM using sin function	**91.17**	**2.84**
WQAM using tan function	**91.29**	**3.00**
WQAM using s^r function with $r = 2$	**91.52**	**2.87**
WQAM using $(\cos)^r$ function with $r = 11$	**91.60**	**2.78**
WQAM using r^s function with $r = 5$	**91.23**	**2.91**
WQAM using $r^{\frac{1}{s}}$ function with $r = 0.01$	**90.40**	**2.91**
WQAM using $exp(\frac{-1}{s})$ function with $r = 0.2$	**91.41**	**2.93**
Max rule [59]	90.30	2.84
Min rule [59]	79.60	7.00
Hammcher t-norm [58]	85.36	5.00
Frank t-norm with $p = 1.3$ [58]	88.04	14.00
EER based Sum Weighting Score (WHT) [59]	90.90	2.90
LLR [62]	91.40	2.30
SVM [62]	91.40	3.20
exponential product [92]	91.20	3.02
tan-hyperbolic product [93]	88.90	9.65
entropy using Frank t-norm with p = 0.01 [58]	87.87	3.77

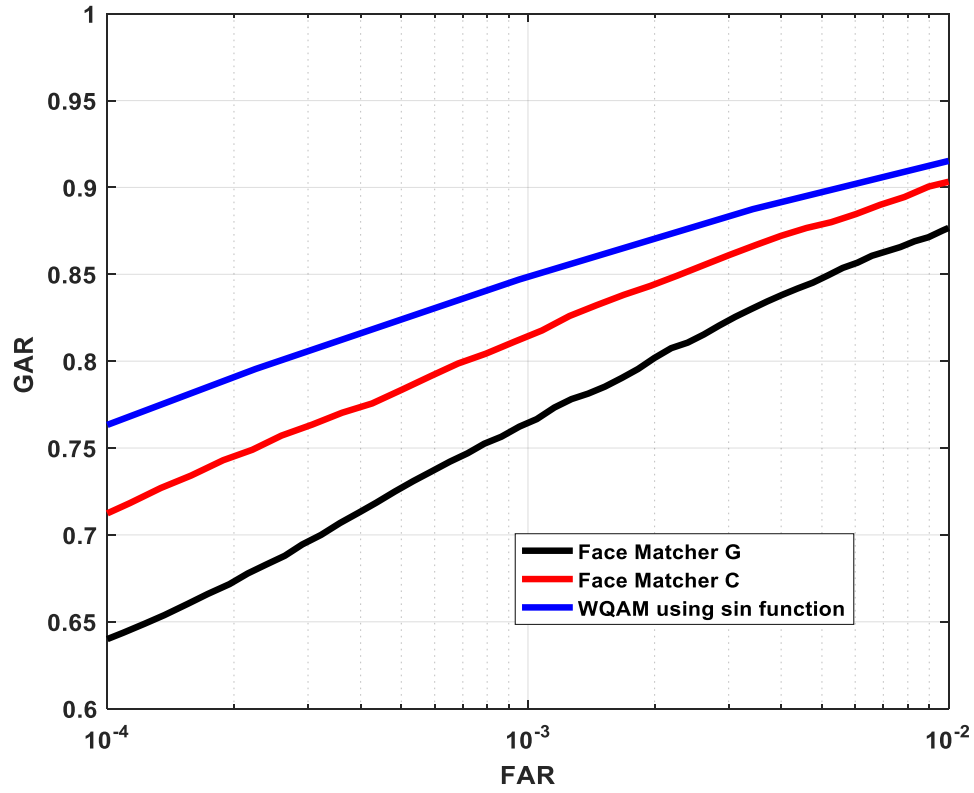

Fig. 5.4 *ROCs of individual biometric algorithms (face matcher C and face matcher G) and their fusion using WQAM on the NIST-face database.*

mances of individual system (here, face matchers). For instance, it is easy to see in Fig. 5.4 that at FAR = 0.01% operating point, the GARs of face matcher G, face matcher C, and multi-algorithm system using WQAM with sin function are 64.0% , 71.2% and 76.34%, respectively.

The results of both proposed WQAM-based multi-algorithm fusion with sin, tan, $\left(cos\left(\frac{\pi}{2}s\right)\right)^r$ and s^r functions and existing person recognition systems using min, max, t-norms, EER based weighted sum, likelihood ratio and SVM are presented in Table 5.3 in terms of GAR (%). We can observe in Table 5.3 that the proposed WQAM fusion method with sin function outperformed not only other WQAM fusion with cos and tan functions but also min [59], max [59], Harmacher t-norms [58], Frank t-norms [58] and EER based weighted sum [59] fusion rule. While, the multi-algorithm systems developed in [62] via likelihood ratio and SVM have shown to achieve results inline with those by the proposed WQAM based systems.

To sum up, our results provide evidence that proposed WQAM fusion scheme is efficient in enhancing accuracy of uni-biometric systems under multimodal (i.e., based on different multiple biometric traits), multi-unit (i.e., based on multiple samples of the same biometric trait) and multi-algorithm (i.e., based on numerous feature extraction and/or matching techniques on the same biometric trait) scenarios.

Table 5.3 *Comparison of multi-algorithm fusion on NIST-face databases.*

Score-level fusion method for FAR = 0.01 %	GAR, %	EER, %
WQAM using cos function	**76.17**	**5.10**
WQAM using sin function	**76.34**	**5.10**
WQAM using tan function	**76.20**	**5.00**
WQAM using s^r function with $r = 10$	**76.26**	**5.00**
WQAM using $(\cos)^r$ function with $r = 2$	**76.28**	**5.20**
WQAM using r^s function with $r = 2$	**76.20**	**5.07**
WQAM using $r^{\frac{1}{s}}$ function with $r = 10$	**76.15**	**5.20**
WQAM using $exp(\frac{-1}{s})$ function with $r = 15$	**76.18**	**4.64**
Max rule [59]	71.50	4.10
Min rule [59]	73.15	6.10
Hammcher t-norm [58]	75.90	5.30
Frank t-norm with $p = 1.3$ [58]	75.80	5.20
EER based Sum Weighting Score (WHT) [59]	74.90	5.40
LLR [62]	77.20	3.70
SVM [62]	77.00	4.80
exponential product [92]	75.80	5.20
tan-hyperbolic product [93]	75.87	5.20
entropy using Frank t-norm with p = 0.01 [58]	75.86	5.20

5.3 The proposed palm and wrist vein multi-biometric system

Fig. 5.5 illustrates the block diagram of the proposed multimodal biometric authentication using wrist and palm vein images. Specifically, two frameworks are proposed, for the first, the information originating from a single hand is integrated using t-norms. While, four sources of information coming from two hands are combined in the second framework. In a verification setting, the user has to present his wrist and palm to the sensor, and declares his identity. First, the wrist and palm vein images are resized to 250×250 pixels and converted to gray scale. After that, the median filter is applied for noise reduction purpose. Then, the system individually matches the wrist and palm vein images with corresponding templates stored in the database during the enrolment phase to yield the wrist and palm vein matching scores.

In this work, we have utilised four local texture descriptors namely LPQ [94], LBP [95], BSIF [96] and LTP [97] to extract the wrist and palm vein features. These local texture descriptors proved its effectiveness in real-world conditions more than global image descriptors that extract the features directly from the entire images.

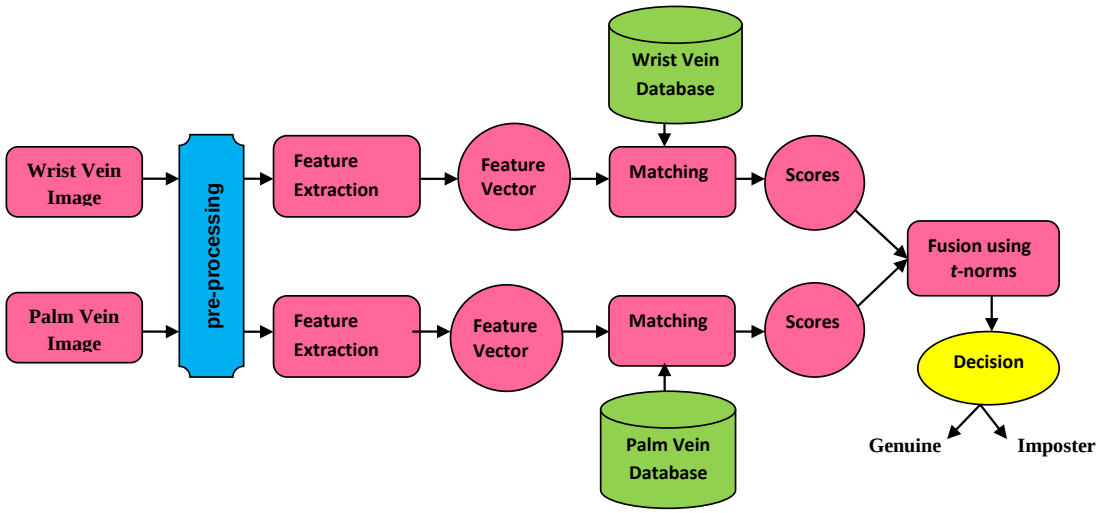

Fig. 5.5 *A schematic diagram of wrist and palm vein based verification framework..*

Fig. 5.6 shows normalised wrist and palm vein images of (left palm, right palm, left wrist, right wrist) and the corresponding LBP, LTP, LPQ and BSIF textural descriptors.

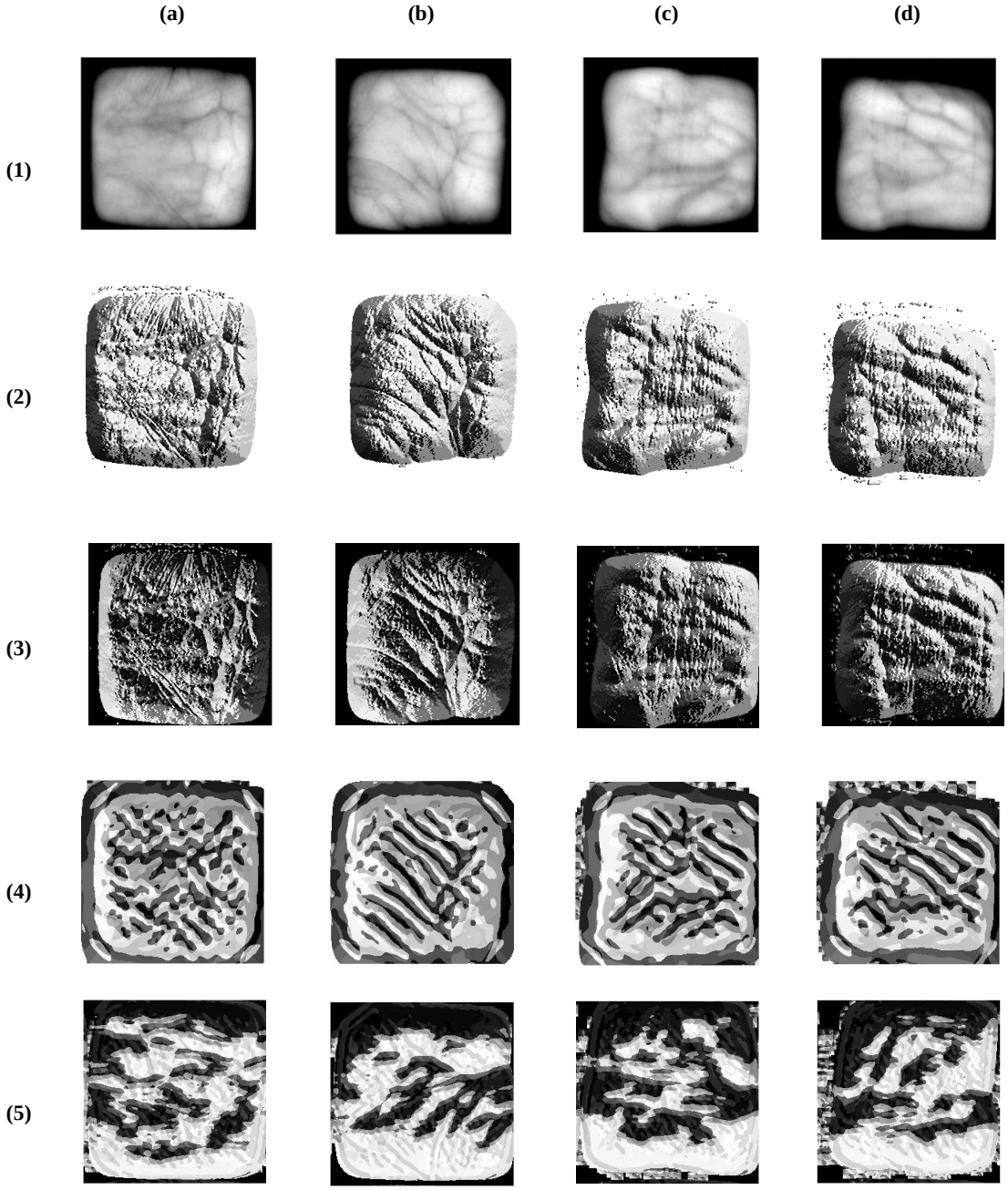

Fig. 5.6 *(a) Left palm vein (b) Right palm vein (c) Left wrist vein (d) Right wrist vein (1) Normalised palm and wrist vein images (2) LBP (3) LTP (4) LPQ (5) BSIF features codes.*

Table 5.4 *Some t-norms that have been used for matching score combination*

T-norms	Function
Hamacher	$\frac{xy}{x+y-xy}$
Schweizer-Sklar ($p>0$)	$(max(x^p+y^p-1,0))^{(\frac{1}{p})}$
Yager ($p>0$)	$max(1-((1-x^p)+(1+y^p))^{(\frac{1}{p})},0)$
Schweizer-Sklar ($p<0$)	$(x^p+y^p-1)^{(\frac{1}{p})}$
Dombi ($p>0$)	$\frac{1}{1+\left(\left(\frac{1-x}{x}\right)^p+\left(\frac{1-y}{y}\right)^p\right)^{\frac{1}{p}}}$
Aczel-Alsina ($p>0$)	$e^{-((-\ln x)^p+(-\ln y)^p))^{\frac{1}{p}}}$

5.3.1 Matching score fusion using t-norms

Triangular norms ($t-$norms) and t-conorms [58] are the most general families of binary functions that satisfy the requirements of the conjunction and disjunction operators. A t-norm function $T(S_1,S_2):[0,1]\times[0,1]\rightarrow[0,1]$ maps the unit square into the unit interval and satisfies the following conditions:

1 *Commutativity:* $T(S_1,S_2)=T(S_2,S_1)$.

2 *Associativity:* $T(S_1,T(S_2,S_3))=T(T(S_1,S_2),S_3)$.

3 *Monotonicity:* $T(S_1,S_2)\leq T(S_3,S_4)$ if $S_1\leq S_2$ and$S_3<S_4$.

4 *Boundary conditions:* $T(0,0)=0$ and $T(S_1,1)=S_1$.

The used t-norms in this paper are tabulated in Table 5.4.

5.3.2 Experimental results and analysis

5.3.2.1 Database

The proposed multimodal biometric system has been tested on a publicly available dataset called PUT vein pattern database [98], this database contains 2,400 images, which is composed from two sections "Wrist" and "Palm were captured from 50 volunteers from both left and right wrist and palm vein. Twelve samples per-subject are available, we have randomly selected six samples for generating enrolled template and six samples as a testing set. Here, each image of the testing set is matched with the six images of enrolled template for each person. Therefore, we have $1,800(6\times6\times50)$ genuine scores and $88,200(6\times6\times49\times50)$ imposter scores from

each of the modalities.

5.3.2.2 Experimental results

In our multi-biometric system, the performance is tested via the indicator receiver operating characteristics (ROC). Besides, the decidability index (Eq. 5.3) was also used to evaluate the proposed multi-biometric systems, which appears the extent of overlap between the distribution scores of the genuine and the imposter and given by

$$d' = \frac{|\mu_{gen} - \mu_{imp}|}{\sqrt{\frac{\sigma_{gen}^2 + \sigma_{gen}^2}{2}}} \tag{5.3}$$

Where μ_{gen} and μ_{imp} represent the means of the two distributions, σ_{gen} and σ_{imp}^2 represent the variances of the two distributions. The higher d' value indicates that the distributions between the genuine and the imposter scores are more separated.

- **Performance of proposed multi-biometric system based on a single hand** In this first set of experiments, we propose a multimodal biometric system to recognise users using wrist and palm vein images; this system is based on a single hand (i.e., left or right hand).

As mentioned above, the texture descriptors (i.e., LPQ, BSIF, LBP, and LTP) have been extracted from the wrist and palm vein images that contain rich information. Figs. 5.7(a)−5.7(b)

Table 5.5 *Comparison of fusion using different approaches of both left and right hand images*

Score-level fusion method for FAR = 0.01 %	GAR, % *Left hand*	GAR , % *Right hand*
Max rule	85.84	81.95
Min rule	96.02	96.65
Sum rule	97.03	97.25
Hammcher t-norm	**100.00**	98.66
Schweizer-Sklar t-norm with $p = 3$	99.66	98.66
Yager t-norm with $p = 0.7$	99.83	98.74
Dombi t-norm with $p = 1.5$	99.42	99.00
Aczel-Alsina t-norm with $p = 1.2$	99.67	98.80

displays the score distribution of wrist and palm vein biometric traits (i.e., LPQ features for wrist vein and BSIF features for palm vein based on left hand). We can see in these figures that there is some overlap between the distributions of genuine and imposter scores. For better security performance, these distributions should be more separable. Fig 5.7(c) displays the score distribution where scores of two biometric traits are integrated using Hamacher t-norm. From this figure, we can observe that there is no overlap between the distributions of genuine and imposter scores thus achieving good accuracy. Fig. 5.8 displays ROC's of unimodal biometric systems and integrated traits by employing the score level fusion based on Hamacher t-norm. At FAR equals 0.01%, the GAR's of left wrist vein and left palm vein are 85.85%, 96.18%, respectively. While, with Hamacher t-norm, GAR of 100% is achieved at 0.01% FAR operating point. Table 3 shows other t-norms like Schweizer-Sklar, Yager, Dombi, and Aczel-Alsina, which we have also tested for score level fusion. In addition, sum rule, min and max rules were presented. Also, the obtained performances using right hand were reported as well. From Table 5.5, we can observe that Dombi t-norm outperforms the other t-norms for right hand, where GAR of 99.00% is obtained at FAR equals 0.01%.

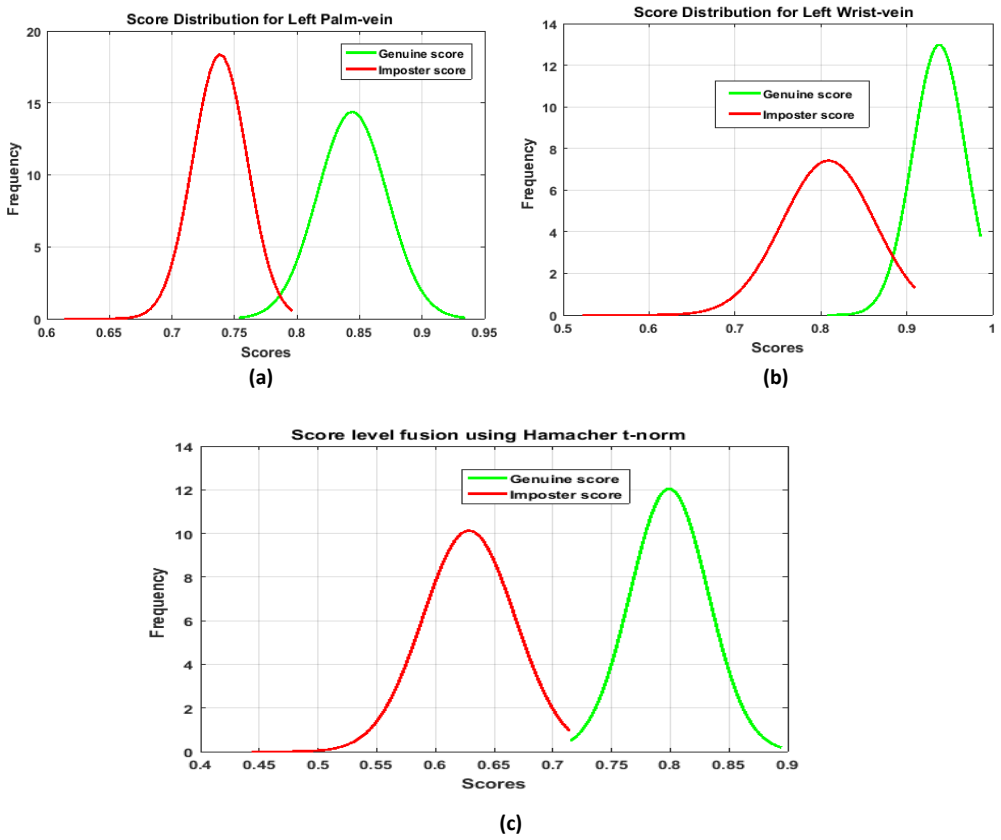

Fig. 5.7 *Score distribution of (a) left palm vein, (b) left wrist vein and (c) score level fusion using Hamacher t-norm.*

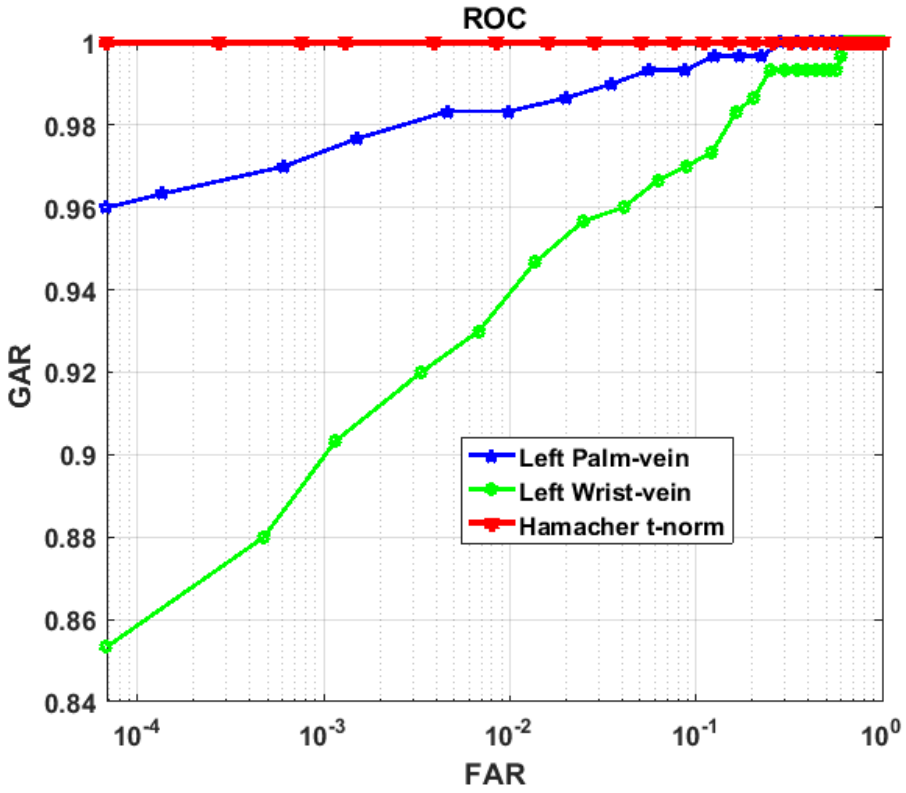

Fig. 5.8 *Comparison of ROC's of individual modalities with score level fusion of left hand using Hamacher t-norm.*

In Tables5.6 and 5.7 , we present the performances of the proposed multimodal biometric authentication that integrates wrist and palm vein images of a single human hand using homogeneous features (i.e., applying the same descriptor for the two biometric modalities). As can be seen from Table 5.6 , the BSIF descriptor achieves better recognition rate than all remaining descriptors (i.e., LPQ, LBP, and LTP). At FAR equals 0.01%, the GARs of left wrist and left palm vein are 89.35% and 96.18%, respectively, whereas GAR equals 99.06% is obtained at the same operating point with Hamacher t-norm-based score fusion method.

Table 5.6 *GAR of both unimodal and multi-biometric systems of left hand using different descriptors*

Descriptors	*Left wrist vein*	*Left palm vein*	*Fusion using Hamacher t-norm*
LPQ	85.85%	92.58%	98.73%
LBP	68.17%	70.33%	84.36%
LTP	65.47%	70.90%	84.35%
BSIF	89.35%	96.18%	99.06%

We can see in Table 5.7, different results obtained using LPQ, LBP, LTP, and BSIF for right human hand. It is easy to observe that BSIF descriptor achieves better accuracy compared to other previously mentioned descriptors. At FAR of 0.01%, the GARs of right wrist and right palm vein are 88.76% and 97.15% respectively. But with Hamacher t-norm GAR of 98.90% is achieved at the same FAR.

Table 5.7 *GAR of both unimodal and multi-biometric systems of right hand using different descriptors*

Descriptors	*Right wrist vein*	*Right palm vein*	*Fusion using Hamacher t-norm*
LPQ	81.57%	91.26%	96.91%
LBP	58.10%	71.40%	79.14%
LTP	56.26%	68.37%	79.70%
BSIF	88.76%	97.15%	98.90%

To sum up, the results clearly shown that multimodal biometric framework using a single hand (i.e., left hand) based on LPQ and BSIF descriptors for wrist and palm vein images outperforms the multi-biometric based on right hand as well as systems that utilise homogeneous features for both left and right human hand.

- **Performance of proposed multi-biometric system based on both left and right hand images** In this second set of experiments, we present a multi-biometric user authentication system that utilises both left and right hand, particularly combining left wrist vein, right wrist vein, left palm vein, and right palm vein patterns. Figure 5.9 shows ROC's of individual biometric traits (i.e., using LPQ features) and of fused traits by using Schweizer and Sklar t-norm

on PUT vein database. At FAR equals 0.01%, the GARs of left wrist vein, left palm vein, right wrist vein, and right palm vein are: 85.85%, 92.58%, 81.57%, and 91.26%, respectively. While, with Schweizer and Sklar t-norm-based score fusion method, GAR of 100% is obtained at 0.01% FAR operating point. Table 5.8 compares the authentication results obtained using different local descriptors (i.e., LPQ, BSIF, LBP, and LTP) as well as previously mentioned score fusion approaches. From Table 6, it is easy to observe that LPQ and BSIF descriptors achieve good results better than multi-biometric systems utilising LBP and LTP features.

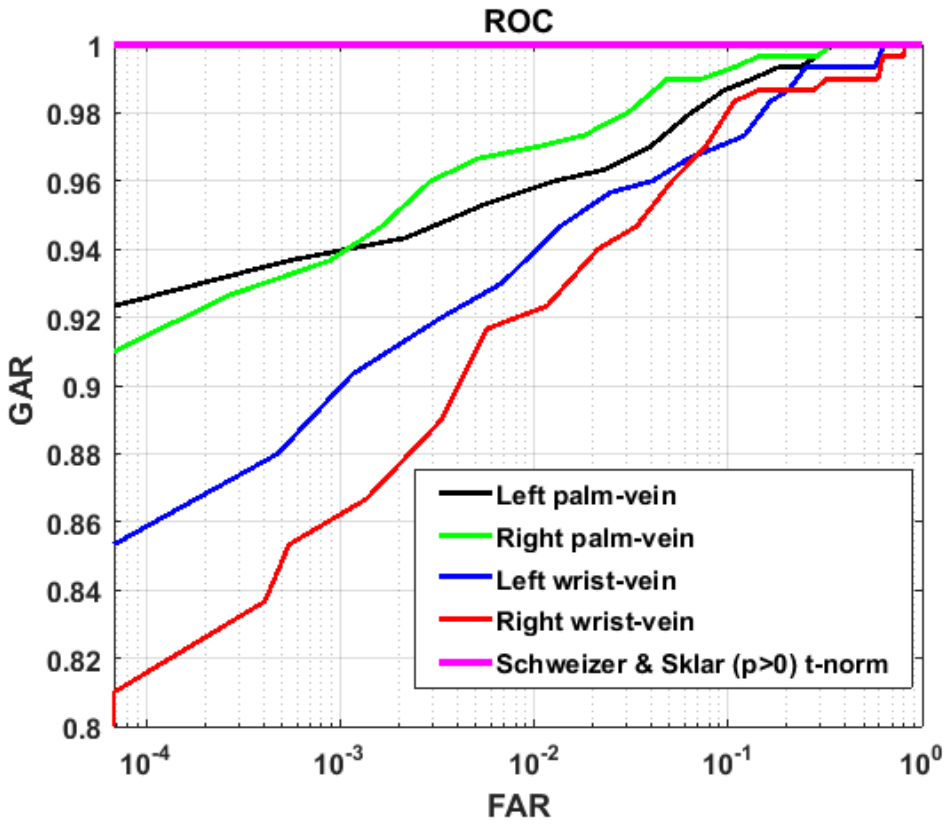

Fig. 5.9 *Comparison of ROC's of individual biometric traits with score level fusion using Schweizer-Sklar t-norm.*

Furthermore, we can indicate that fusion using t-norms outperforms the other strategies (i.e., min, max and sum rules) thus making them superior. In addition, we have also evaluated the proposed multimodal biometric system using decidability index (d'), where the greater d' value indicates that the genuine and imposter distributions are more separated thereby the recognition rate of the biometric system boosts in general. The d' values of each biometric modality and their combination-based different score fusion strategies, i.e., t-norms, min, max, and sum rules utilising previously mentioned local textural descriptors are reported in Tables 5.9 and 5.9, respectively. From these tables, it is easy to observe that score level fusion using Schweizer-Sklar t-norm (i.e., LPQ features) performs and achieves a greater d' value compared to other

t-norms and fixed rule as well as the unimodal biometric systems, this leads to accurate person recognition.

Table 5.8 *Comparison of fusion using different approaches of both left and right hand images*

Score-level fusion method for FAR = 0.01 %	GAR, % *LPQ*	GAR , % *BSIF*	GAR , % *LBP*	GAR , % *LTP*
Max rule	100.00	94.00	90.00	90.00
Min rule	90.93	91.70	63.20	64.19
Sum rule	99.50	98.10	87.28	87.73
Hammcher t-norm	**100.00**	**100.00**	91.15	91.24
Schweizer-Sklar t-norm with $p = 0.9$	**100.00**	**100.00**	94.22	94.42
Yager t-norm with $p = 2.2$	**100.00**	**100.00**	93.96	94.02
Dombi t-norm with $p = 0.5$	**100.00**	**100.00**	94.59	94.55
Aczel-Alsina t-norm with $p = 0.7$	**100.00**	**100.00**	93.55	95.42

Table 5.9 *d' values of unimodal palm and wrist vein biometric systems*

Biometrics modality	*d'(LPQ)*	*d'(BSIF)*	*d'(LBP)*	*d'(LTP)*
Left palm vein	3.7392	4.2459	92.5875	2.5822
Right palm vein	3.9416	4.3900	2.6891	2.6718
Left wrist vein	2.9418	3.4878	2.2620	2.2451
Right wrist vein	3.0317	3.3645	2.2749	2.2668

Table 5.10 *Comparison of different fusion methodologies in terms of d'*

Score-level fusion methodology	*d'(LPQ)*	*d'(BSIF)*	*d'(LBP)*	*d'(LTP)*
Max rule	5.8710	4.5600	3.5709	3.5538
Min rule	3.0162	3.5004	2.4106	2.3986
Sum rule	5.0093	4.3336	3.3176	3.2949
Hammcher t-norm	5.2907	5.5865	3.4269	3.4188
Schweizer-Sklar t-norm with $p = 0.9$	4.5054	6.2835	4.5049	4.4793
Yager t-norm with $p = 2.2$	**12.5119**	5.8750	3.7721	3.7647
Dombi t-norm with $p = 0.5$	4.9785	5.5095	2.8522	2.8757
Aczel-Alsina t-norm with $p = 0.7$	5.7393	5.1886	2.9617	2.4234

To sum up, the performances attained using wrist and palm vein images from both left and right hand prove that fusion of these four biometric modalities is capable to enhance the recognition rate compared to unimodal systems as well as the multimodal systems that depend on a single hand images, especially those utilising homogeneous features for both wrist and palm vein images

• **Performance of proposed multi-biometric system based on classifier fusion using t-norms** In this section, we aim to evaluate three classifier-based t-norms for score level fusion, which are KNN, linear discriminant analysis (LDA) and quadratic discriminant analysis (QDA). To generate the training and testing sets, half of genuine and imposter scores were randomly selected for each set. In this work, we have considered the average of obtained GARs through 20 test runs as a performance measure. Firstly, we assessed the performance of the fusion of information originating from both wrist and palm vein images utilising a single hand (i.e., left or right hand)-based classifier fusion. The LPQ and BSIF textural descriptors were used to extract features from wrist and palm vein images, respectively. Secondly, the three classifiers are tested for the second proposed multimodal biometric system that merging wrist and palm vein of both left and right hand, the performance was tested using LPQ, BSIF, LBP and LTP features for each modality. Table 5.11 reports GARs of the KNN, QDA and LDA classifiers-based t-norms, we can observe that QDA and LDA classifiers perform better than KNN classifier. The GAR = 100% was obtained at FAR = 0.01% by QDA and LDA classifier at all used t-norms, min and

Table 5.11 *Comparison of fusion using different approaches of both left and right hand images*

Score-level fusion methodology for FAR = 0.01%	GAR, % *Left hand*			GAR , % *Right hand*		
Classifier	KNN	QDA	LDA	KNN	QDA	LDA
Classifier via Max rule	94.62	**100.00**	**100.00**	97.46	**100.00**	**100.00**
Classifier via Min rule	84.72	**100.00**	**100.00**	83.14	**100.00**	**100.00**
Classifier via Hamacher	95.70	**100.00**	**100.00**	98.72	**100.00**	**100.00**
Classifier via Yager t-norm $p = 0.2$	98.92	**100.00**	**100.00**	97.06	**100.00**	**100.00**
Classifier via Dombi t-norm with $p = 0.2$	99.87	**100.00**	**100.00**	97.30	**100.00**	**100.00**
Classifier via Aczel-Alsina t-norm with $p = 1.5$	98.20	**100.00**	**100.00**	96.38	**100.00**	**100.00**

max rules for each hand. Whereas, KNN classifier-based Dombi t-norm with p = 0.2 has given better performance for left hand in comparison to all used t-norms, where GAR = 99.7% was obtained.

Table 5.12 presents the GARs value of the LPQ and BSIF-based classifier. From this table, we can indicate that almost all classifier employed for this fusion give a GAR of 100% at FAR = 0.01%. From Table 5.13, it is clear to observe that classifier-based fusion using LBP and LTP textural descriptors achieves a better significant improvement compared to transformation-based score fusion, especially the LDA and QDA. For example, the multi-biometric recognition utilising the LBP and LTP features with Hamacher t-norm fusion rule yield GAR of 91.15% and 91.24%, respectively. But, GAR equals to 100% is obtained when LDA and QDA classifiers-based t-norms is used.

Table 5.12 *Comparison of different classifier fusion using t-norms of both left and right hand with LPQ and BSIF features*

Score-level fusion methodology for FAR = 0.01%	GAR, % *LPQ*			GAR , % *BSIF*		
Classifier	KNN	QDA	LDA	KNN	QDA	LDA
Classifier via Max rule	92.54	**100.00**	**100.00**	91.63	**100.00**	**100.00**
Classifier via Min rule	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**
Classifier via Hamacher	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**
Classifier via Yager*t*-norm $p = 0.2$	95.68	**100.00**	**100.00**	97.59	**100.00**	**100.00**
Classifier via Dombi t-norm with $p = 0.2$	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**
Classifier via Aczel-Alsina t-norm with $p = 4$	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**

Table 5.13 *Comparison of different classifier fusion using t-norms of both left and right hand with LBP and LTP features*

Score-level fusion methodology for FAR = 0.01%	GAR, % *Left hand*			GAR , % *Right hand*		
Classifier	KNN	QDA	LDA	KNN	QDA	LDA
Classifier via Max rule	61.90	**100.00**	**100.00**	65.30	**100.00**	**100.00**
Classifier via Min rule	89.702	**100.00**	**100.00**	87.70	**100.00**	**100.00**
Classifier via Hamacher	95.76	**100.00**	**100.00**	97.74	**100.00**	**100.00**
Classifier via Yager t-norm $p = 0.2$	67.40	**100.00**	**100.00**	71.53	**100.00**	**100.00**
Classifier via Dombi t-norm with $p = 0.2$	95.80	**100.00**	**100.00**	96.91	**100.00**	**100.00**
Classifier via Aczel-Alsina t-norm with $p = 1.5$	93.32	**100.00**	**100.00**	96.97	**100.00**	**100.00**

5.4 The proposed Iris and Major Finger Knuckles multi-biometric system

The purpose of this study is to explore the possibility of fusing Major Finger Knuckle Patterns (MFKPs) of four fingers, i.e., index, middle, ring, and little along with iris, for automated human authentication. It may be noted that MFKPs of four fingers can be acquired simultaneously without any nuisance to individuals, also at lower cost. Therefore it is important to invest the acquisition of five biometric traits using only two sensors. The proposed multi-biometric

system was performed using the score level fusion. The features from MFKPs and iris have been extracted applying the same local texture descriptor namely binarised statistical image features (BSIF). Thus, homogeneous features were extracted.

Figure 5.10 shows an architecture illustrating the overall procedure of the proposed multi-biometric system verification that integrates information from MFKPs and iris biometric sources. To ascertain the claimed identity of an individual, the individual should present his hand and iris to the corresponding sensor. First, hand and iris are processed to extract the region of interest. Then, the segmented images are matched with respective templates stored during the enrolment stage in the database to find the similarity between each two feature vectors. The matching scores obtained from deferent biometric matchers should be first normalized into the same range [0, 1] via min-max normalisation (5.2) prior to integrating them. After that, the normalized scores of five individual matchers (iris, major knuckle from little finger, from ring finger, from middle finger, and from index finger) are combining using grouping function. Let $S = G(x,y)$ denotes the combination of two scores based on the proposed grouping function. Let S'_1, S_2, S_3, S_4, and S_5 the normalized match-scores for the five biometric traits. The two scores S'_1 and S'_2 are first fused to yield $G(S'_1, S'_2)$ which is in turn integrated further with S'_3 to yield $G(G(S'_1, S'_2), S'_3)$ until all normalized match-scores are fused. Thus, the fused match-score F can be given as : $F = G(G(G(G(S'_1, S'_2), S'_3), S'_4), S'_5)$

Finally, the combined match-score F is compared with a threshold τ, which assigns an unknown user as genuine if $F > \tau$, otherwise the user is classified as an imposter

5.4.1 Score level fusion using Grouping Function

Aggregation is the process of integrating numerous values into a single one, which has been employed in many experimental sciences. The function that maps a vector of input values into a single output value is called aggregation function. In this work, we explore matching scores combination using an aggregation function namely grouping function to integrate major knuckle patterns and iris.

The concept of grouping functions was introduced by H. Bustince [99]. These functions are complement of the concept of overlap functions. Grouping functions are a type of binary functions that are employed as a rule of grouping for fuzzy sets. In particular, grouping function is a mapping $G : [0,1] \times [0,1] \to [0,1]$ which satisfies the following conditions:

(a) G is *commutative*.

(b) G is *continuous*.

(c) G is *nondecreasing*.

(d) $G(1,1) = 1$.

(e) $G(0,0) = 0$.

The grouping function (Eq. 5.4)utilised in this study is expressed as follows:

$$G(S_1,S_2) = \frac{max(S_1,S_2)}{max(S_1,S_2) + \sqrt{(1-S_1)(1-S_2)}} \tag{5.4}$$

Where S_1 and S_2 are two normalized matching scores.

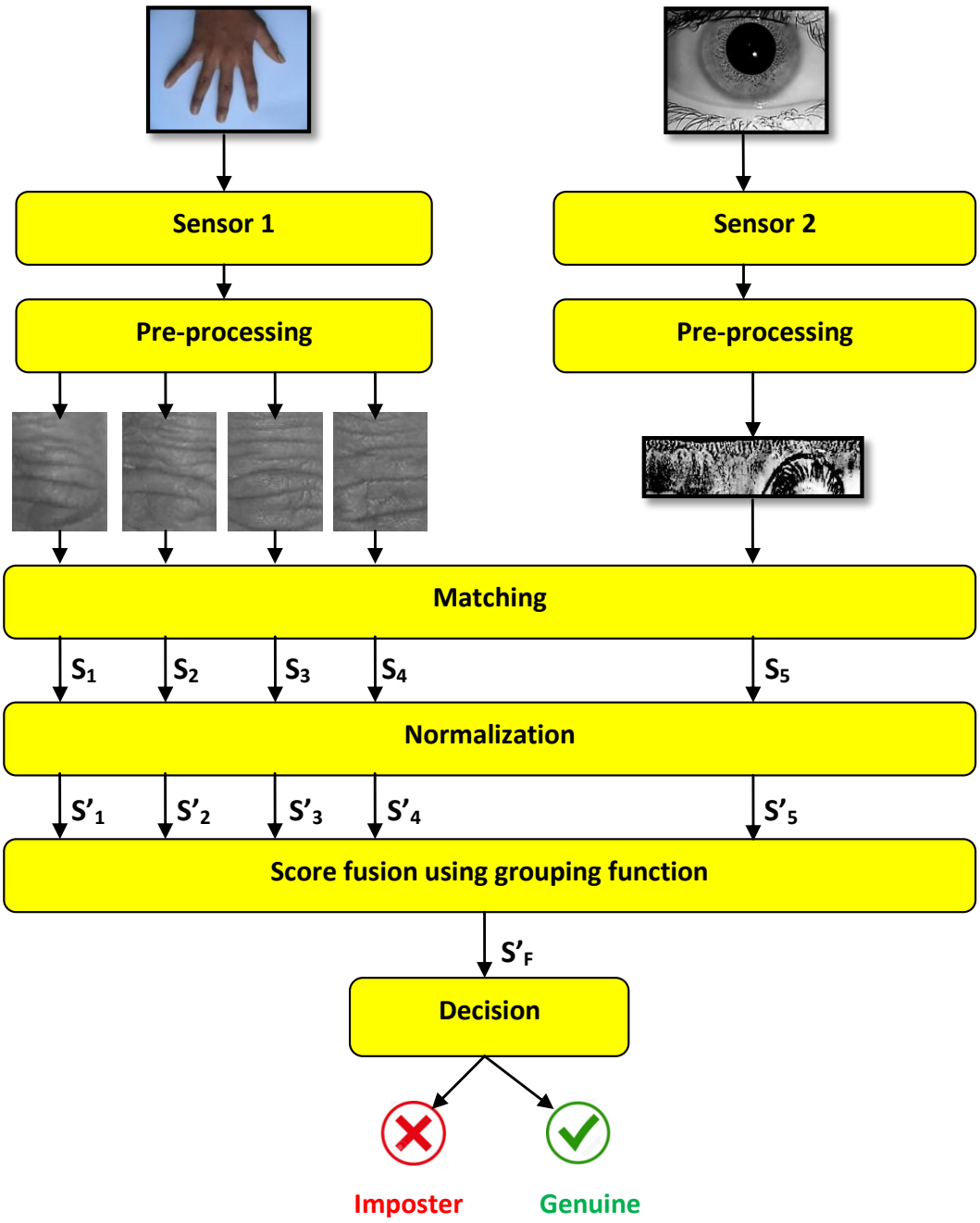

Fig. 5.10 *Architecture of proposed Iris and Major Finger Knuckle multimodal biometric authentication framework.*

5.4.2 Databases

The performance of proposed multi-biometric system was evaluated on our own chimeric database due to the lack of MKFPs-iris multimodal database. To construct the chimeric database, we have used the iris images from IIT Delhi-1 iris datasbase [100]. The images were collected from the staff and students at IIT Delhi campus, India. The 2240 images were acquired from 224 different users, i.e., 176 males and 48 females aged 14-55 years. It may be noted that all iris images were acquired in the indoor environment with resolution of 320x240 pixels. The Majority of these images were acquired from the left eye except some images were acquired from right eye. In addition to the iris original images, 432x48 pixels normalized iris images are also included.

The second used database in our experiments is the Hong Kong Polytechnic University Contactless Hand Dorsal Images Database [101]. The images were collected in the Hong Kong polytechnic university campus, in IIT Delhi campus, and in some villages in India. The database contains images of 712 subjects. Besides, segmented and norma-lized images of minor, second, and major knuckle of little, ring, middle, and index fingers along with resized dorsal images are also included. we only used images for major knuckle.

5.4.3 Experimental Results

The grouping function based-biometric score fusion scheme is evaluated based on a virtual multimodal biometric dataset that consists from little, ring, middle, and index finger's major knuckles of 224 users and the irises of another 224 users of iris. Thereby the dataset has virtually 224 users, 2 images per-user, out of which one image to build the enrolled template and one image for testing in order to investigate the combination of these modalities in more realistic scenarios, when only one enrolled template is available for each person. Therefore we have 224 genuine scores and 49952(224×223) imposter scores for each of the biometric trait considered.

The performance evaluation of the proposed biometric-based authentication is reported in Receiver Operating Characteristics (ROC) curves. Figure 5.11 displays ROC's of unimodal biometric authentication and of their integration by using grouping function at score level fusion on proposed virtual multimodal dataset. At FAR equals 0.01 percent, the GARs of iris, index's major knuckle, middle's major knuckle, ring's major knuckle, and little's major knuckle are: 89.23%, 40.00%, 45.50%, 51.40%, and 14.00% respectively. But with grouping function GAR of 95.54% is achieved with the same FAR. The performance achieved by score level integration strategy using symmetric sum proposed in [102] was reported. In addition, we also report the results attained by using Schwizer & Sklar and Einstein product t-norms [58], min and max rules [103] , and weighted sum [100]. From table 5.14, we can observe that proposed score level fusion using grouping function outperforms the existing popular approaches in the literature.

Table 5.14 *Comparison of fusion using different approaches of both left and right hand images*

Score-level fusion method for FAR = 0.01 %	GAR , %
Max rule [103]	43.30
Min rule [103]	62.30
Weighted Sum [100]	93.42
Schweizer-Sklar t-norm with $p = 0.5$ [58]	83.80
Einstein product t-norm [58]	84.00
S-sum using max rule [102]	85.75
S-sum using min rule [102]	93.70
Proposed Grouping Function	**95.54**

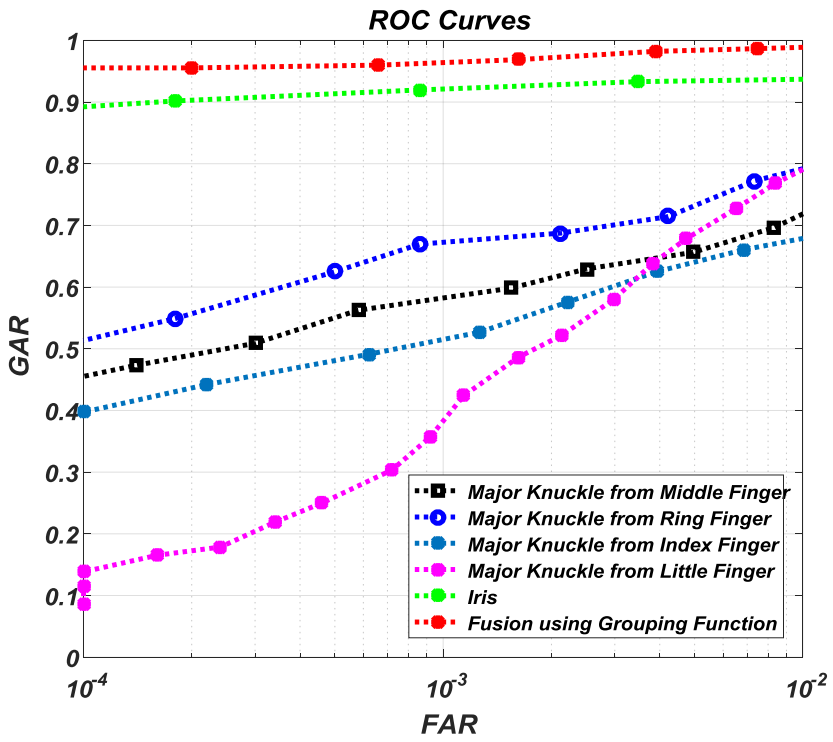

Fig. 5.11 *ROCs of unimodal systems (iris, index's major knuckle, middle's major knuckle, ring's major knuckle, and little's major knuckle) and their fusion using grouping function.*

5.5 Conclusion

This chapter presents a new score level fusion approach for a multi-biometric system based on WQAM. The proposed score level fusion algorithm incorporates properties of both weighted mean and quasi-arithmetic mean. These WQAMs do not require any learning procedure, thus making our system simple, efficient and computationally less expensive. The presented experimental results are performed on NIST-BSSR1 data set, which demonstrate that our approach outperforms the prior proposed score combination approaches (i.e. min, max rules, t-norms, LLR). In addition to WQAM-based fusion approach, we have prsented a novel multi-modal biometric framework for recognising individuals based on their palm and wrist vein patterns. The experimental analysis on a publicly available PUT data set shows that the presented vein pattern based multi-biometric system leads to acheive high verifiction rate.

Finally, a multimodal biometric framework for ascertaining the identity of users based on their iris and major finger knuckle patterns using four fingers has been presented, where the match-scores are integrated via grouping function.

Chapter 6

General conclusion and future works

6.1 General Conclusion

A widespread technology known as biometrics was employed as an alternative to these conventional recognition mechanisms due to the growth of threats in identity management and security tasks.This technology is based on human anatomical (e.g., fingerprint, face, iris, palmprint) or behavioural (e.g., gait, signature, keystroke analysis) characteristics. Besides, biometric traits are inherently possessed by a human thereby it is comparatively difficult to forge or steal it. Thus, biometric attributes constitute a robust link between a human and his identity. Moreover, unlike knowledge-based and token-based strategies for person recognition, biometric traits are able to guaranty that no user is able to assume more than one identity. Biometric-based automated person authentication systems have become pervasive, which are being used not only by individuals but also governments at large scales, e.g., at border crossing.

Among the newest biometric traits, vein pattern gained wide acceptance especially in authentication applications, since it is located inside the skin, therefore it makes very difficult for a malicious user to fraud this pattern. Moreover, vein patterns have an important merits, stable over time compared to some biometric marker that can be changed under the impact of ageing such as face. The collection of vein images is easily obtained compared to other biometric techniques: in the IRIS case for example, it is necessary to proceed by several training. Thus, it provides a user-friendly recognition.

Multibiometrics, which reconciles the evidence presented by several sources of biometric information, have illustrated to enhance recognition accuracy as well as robustness against attacks. However, unimodal biometrics (i.e., utilizing only one biometric trait) are not adequate in tackling issues like noisy input data, non-universality, low interoperability and spoofing [6], which lead to lower accuracy. To alleviate some of these limitations, integration of two or more biometric traits offers many advantages compared to unimodal authentication Some of the advantages are attaining improvement in the overall accuracy, ensuring a larger population coverage, addressing the issue of non-universality, and providing greater resistance to spoofing. Information fusion in multi-biometrics can be classified into five levels, namely, sensor level, feature level, matching score level, decision level, and rank level.

6.2 Author's contributions

In this thesis, we presented a novel multi-biometric scheme for score-level fusion based on Weighted Quasi-Arithmetic Mean (WQAM) computed via different trigonometric functions. The proposed score level fusion algorithm incorporates properties of both weighted mean and quasi-arithmetic mean. In addition, it does not entail any training/learning strategy, thereby making the proposed system computationally inexpensive, simple and competent. Experimental analysis using three publicly available datasets (i.e., NIST-BSSR1 Multimodal, NIST-BSSR1

Fingerprint, and NIST-BSSR1 Face) for multimodal, multi-units and multi-algorithms systems demonstrates that the proposed WQAMs fusion framework is capable of outperforming the prior proposed score fusion rules in the literature

Two frameworks focused on a palm and wrist vein-based multimodal authentication system are proposed. For the first framework, wrist and palm traits of the same hand are fused, whilst four biometric markers are combined in the second framework using texture descriptors such as local phase quantisation (LPQ), local binary patterns (LBPs), binarised statistical image features (BSIF) and local ternary patterns (LTP). In addition, two approaches of score level fusion are applied: 1) transformation-based using sum rule, min-max rules and t-norms; 2) classifier-based via t-norms.

Also, we presented a multimodal biometric framework for ascertaining the identity of users based on their iris and major finger knuckle patterns. The experiments on a chimeric database (i.e., the iris images have been selected from IIT Delhi-1 iris database, whereas MFKPs have been selected from the contactless hand dorsal images of PolyU database) confirmed that proposed multibiometric framework using grouping function achieves better recognition compared to unimodal iris and MFKPs biometrics as well as their combination using other existing biometric score fusion methods.

6.3 Future works

The future studies can be summarised as follows:

- We aim to study the proposed framework (WQAM-based biometric score fusion) under big data and wide-ranging scenarios, including smartphone behavioural biometric traits, such as scrolling patterns, phone movement.
- We will evaluate the robustness of the presented method against spoofing attacks.
- Also, we plan to study palm and wrist vein recognition based on deep learning, which can give vein patterns recognition another good choice.

Finally, It is hoped that the proposed biometric fusion schemes will be exploited and explored for the development of information fusion systems in this field as well as in different domains.

Bibliography

[1] Akhtar, Z., Hadid, A., Nixon, M., Tistarelli, M., Dugelay, J., Marcel, S.: 'Biometrics: In search of identity and security (Q & A)', *IEEE MultiMedia*, 2018, pp. 1–10

[2] Jain, A.K., Ross, A.A., Nandakumar, K.: 'Introduction to biometrics'. (Springer Science & Business Media, 2011)

[3] Jain, A.K., Ross, A., Prabhakar, S.: 'An introduction to biometric recognition', *IEEE Transactions on circuits and systems for video technology*, 2004, **14**, (1), pp. 4–20

[4] Ding, C., Tao, D.: 'Pose-invariant face recognition with homography-based normalization', *Pattern Recognition*, 2017, **66**, pp. 144–152

[5] Singh, M., Singh, R., Ross, A.: 'A comprehensive overview of biometric fusion', *Information Fusion*, 2019, **52**, pp. 187–205

[6] Wilson, C.: 'Vein pattern recognition: a privacy-enhancing biometric'. (CRC press, 2010)

[7] Dargan, S., Kumar, M.: 'A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities', *Expert Systems with Applications*, 2020, **143**, pp. 113114

[8] Bhanu, B., Govindaraju, V.: 'Multibiometrics for Human Identification'. (Cambridge University Press, 2011)

[9] Akhtar, Z.: 'Security of multimodal biometric systems against spoof attacks', *PhD thesis, Department of Electrical Electronic Engineering, University of Cagliari, Italy*, 2012,

[10] Ghiani, L., Hadid, A., Marcialis, G.L., Roli, F.: 'Fingerprint liveness detection using local texture features', *IET Biometrics*, 2016, **6**, (3), pp. 224–231

[11] Hadid, A., Evans, N., Marcel, S., Fierrez, J.: 'Biometrics systems under spoofing attack: an evaluation methodology and lessons learned', *IEEE Signal Processing Magazine*, 2015, **32**, (5), pp. 20–30

[12] Kumar, B.V., Savvides, M., Xie, C., Venkataramani, K., Thornton, J., Mahalanobis, A.: 'Biometric verification with correlation filters', *Applied Optics*, 2004, **43**, (2), pp. 391–402

[13] Fierrez.Aguilar, J., Chen, Y., Ortega.Garcia, J., Jain, A.K. 'Incorporating image quality in multi-algorithm fingerprint verification'. In: International Conference on Biometrics. (Springer, 2006. pp. 213–220

[14] Maio, D., Maltoni, D.: 'Direct gray-scale minutiae detection in fingerprints', *IEEE transactions on pattern analysis and machine intelligence*, 1997, **19**, (1), pp. 27–40

[15] Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S.: 'Filterbank-based fingerprint matching', *IEEE transactions on Image Processing*, 2000, **9**, (5), pp. 846–859

[16] Kumar, R., Chandra, P., Hanmandlu, M. 'Local directional pattern (ldp) based fingerprint matching using slfnn'. In: 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013). (IEEE, 2013. pp. 493–498

[17] Tachaphetpiboon, S., Amornraksa, T. 'A fingerprint matching method using dct features'. In: IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005.. vol. 1. (IEEE, 2005. pp. 461–464

[18] Yang, J.C., Park, D.S.: 'Fingerprint verification based on invariant moment features and nonlinear bpnn', *International Journal of Control, Automation, and Systems*, 2008, **6**, (6), pp. 800–808

[19] Nanni, L., Lumini, A.: 'Local binary patterns for a hybrid fingerprint matcher', *Pattern recognition*, 2008, **41**, (11), pp. 3461–3466

[20] Ahonen, T., Hadid, A., Pietikainen, M.: 'Face description with local binary patterns: Application to face recognition', *IEEE transactions on pattern analysis and machine intelligence*, 2006, **28**, (12), pp. 2037–2041

[21] Turk, M., Pentland, A.: 'Eigenfaces for recognition', *Journal of cognitive neuroscience*, 1991, **3**, (1), pp. 71–86

[22] Wiskott, L., Krüger, N., Kuiger, N., Von.Der.Malsburg, C.: 'Face recognition by elastic bunch graph matching', *IEEE Transactions on pattern analysis and machine intelligence*, 1997, **19**, (7), pp. 775–779

[23] Taigman, Y., Yang, M., Ranzato, M., Wolf, L. 'Deepface: Closing the gap to human-level performance in face verification'. In: Proceedings of the IEEE conference on computer vision and pattern recognition. (, 2014. pp. 1701–1708

[24] Mohamed, C., Akhtar, Z., Eddine, B.N., Falk, T.H. 'Combining left and right wrist vein images for personal verification'. In: 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA). (IEEE, 2017. pp. 1–6

[25] Kurban, O.C., Nıyaz, Ö., Yildirim, T. 'Neural network based wrist vein identification using ordinary camera'. In: 2016 International Symposium on INnovations in Intelligent SysTems and Applications (INISTA). (IEEE, 2016. pp. 1–4

[26] Nikisins, O., Eglitis, T., Anjos, A., Marcel, S. 'Fast cross-correlation based wrist vein recognition algorithm with rotation and translation compensation'. In: 2018 International Workshop on Biometrics and Forensics (IWBF). (IEEE, 2018. pp. 1–7

[27] Fernández, P., Findling, R.D. 'Mobile wrist vein authentication using sift features'. In: EUROCAST. (, 2017. p. 140

[28] Das, A., Pal, U., Ballester, M.A.F., Blumenstein, M. 'A new wrist vein biometric system'. In: 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM). (IEEE, 2014. pp. 68–75

[29] Hartung, D., Tistarelli, M., Busch, C. 'Vein minutia cylinder-codes (v-mcc)'. In: 2013 International Conference on Biometrics (ICB). (IEEE, 2013. pp. 1–7

[30] Uriarte.Antonio, J., Suarez.Pascual, J.E., Garcia.Lorenz, M., Sanchez.Reillo, R. 'Parametrical study of a vascular biometric system'. In: 2011 International Conference on Hand-Based Biometrics. (IEEE, 2011. pp. 1–6

[31] Pan, M., Kang, W. 'Palm vein recognition based on three local invariant feature extraction algorithms'. In: Chinese Conference on Biometric Recognition. (Springer, 2011. pp. 116–124

[32] Lee, J.C.: 'A novel biometric system based on palm vein image', *Pattern Recognition Letters*, 2012, **33**, (12), pp. 1520–1528

[33] Wang, R., Wang, G., Chen, Z., Liu, J., Shi, Y. 'An improved method of identification based on thermal palm vein image'. In: International Conference on Neural Information Processing. (Springer, 2012. pp. 18–24

[34] Athale, S.S., Patil, D., Deshpande, P., Dandawate, Y.H.: 'Hardware implementation of palm vein biometric modality for access control in multilayered security system', *Procedia Computer Science*, 2015, **58**, pp. 492–498

[35] Cancian, P., Di.Donato, G.W., Rana, V., Santambrogio, M.D. 'An embedded gabor-based palm vein recognition system'. In: 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI). (IEEE, 2017. pp. 405–408

[36] Piciucco, E., Maiorana, E., Campisi, P.: 'Palm vein recognition using a high dynamic range approach', *Iet Biometrics*, 2018, **7**, (5), pp. 439–446

[37] Shah, G., Shirke, S., Sawant, S., Dandawate, Y.H.: 'Palm vein pattern-based biometric recognition system', *International Journal of Computer Applications in Technology*, 2015, **51**, (2), pp. 105–111

[38] Jain, A.K., Hong, L., Kulkarni, Y. 'A multimodal biometric system using fingerprint, face and speech'. In: 2nd Int'l Conf. AVBPA. vol. 10. (, 1999.

[39] Woodard, D.L., Pundlik, S., Miller, P., Jillela, R., Ross, A. 'On the fusion of periocular and iris biometrics in non-ideal imagery'. In: 2010 20th International Conference on Pattern Recognition. (IEEE, 2010. pp. 201–204

[40] Zhang, Q., Li, H., Sun, Z., Tan, T.: 'Deep feature fusion for iris and periocular biometrics on mobile devices', *IEEE Transactions on Information Forensics and Security*, 2018, **13**, (11), pp. 2897–2912

[41] Çetingül, H.E., Erzin, E., Yemez, Y., Tekalp, A.M.: 'Multimodal speaker/speech recognition using lip motion, lip texture and audio', *Signal processing*, 2006, **86**, (12), pp. 3549–3558

[42] Wark, T., Sridharan, S.: 'Adaptive fusion of speech and lip information for robust speaker identification', *Digital Signal Processing*, 2001, **11**, (3), pp. 169–186

[43] Rathgeb, C., Busch, C.: 'Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters', *Computers & Security*, 2014, **42**, pp. 1–12

[44] Nandakumar, K., Jain, A.K. 'Multibiometric template security using fuzzy vault'. In: 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems. (IEEE, 2008. pp. 1–6

[45] Uhl, A., Wild, P.: 'Single-sensor multi-instance fingerprint and eigenfinger recognition using (weighted) score combination methods.', *IJBM*, 2009, **1**, (4), pp. 442–462

[46] Goswami, G., Vatsa, M., Singh, R.: 'Rgb-d face recognition with texture and attribute features', *IEEE Transactions on Information Forensics and Security*, 2014, **9**, (10), pp. 1629–1640

[47] Singh, R., Vatsa, M., Ross, A., Noore, A.: 'A mosaicing scheme for pose-invariant face recognition', *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 2007, **37**, (5), pp. 1212–1225

[48] Fahmy, M.S., Atyia, A.F., Elfouly, R.S. 'Biometric fusion using enhanced svm classification'. In: 2008 international conference on intelligent information hiding and multimedia signal processing. (IEEE, 2008. pp. 1043–1048

[49] Gonzalez.Rodriguez, J., Fierrez.Aguilar, J., Ramos.Castro, D., Ortega.Garcia, J.: 'Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems', *Forensic science international*, 2005, **155**, (2-3), pp. 126–140

[50] Nguyen, K., Denman, S., Sridharan, S., Fookes, C.: 'Score-level multibiometric fusion based on dempster–shafer theory incorporating uncertainty factors', *IEEE Transactions on Human-Machine Systems*, 2014, **45**, (1), pp. 132–140

[51] Muncaster, J., Turk, M. 'Continuous multimodal authentication using dynamic bayesian networks'. In: Proceedings of the 2nd Workshop on Multimodal User Authentication. (, 2006. pp. 1–8

[52] Hanmandlu, M., et al.: 'Multimodal biometric system built on the new entropy function for feature extraction and the refined scores as a classifier', *Expert Systems with Applications*, 2015, **42**, (7), pp. 3702–3723

[53] Fathima, A.A., Vasuhi, S., Babu, N., Vaidehi, V., Treesa, T.M.: 'Fusion framework for multimodal biometric person authentication system.', *IAENG International Journal of Computer Science*, 2014, **41**, (1)

[54] Raghavendra, R., Dorizzi, B., Rao, A., Kumar, G.H.: 'Designing efficient fusion schemes for multimodal biometric systems using face and palmprint', *Pattern Recognition*, 2011, **44**, (5), pp. 1076–1088

[55] Jain, A., Nandakumar, K., Ross, A.: 'Score normalization in multimodal biometric systems', *Pattern recognition*, 2005, **38**, (12), pp. 2270–2285

[56] Rattani, A., Tistarelli, M. 'Robust multi-modal and multi-unit feature level fusion of face and iris biometrics'. In: International Conference on biometrics. (Springer, 2009. pp. 960–969

[57] Kumar, A., Kanhangad, V., Zhang, D.: 'A new framework for adaptive multimodal biometrics management', *IEEE transactions on Information Forensics and Security*, 2010, **5**, (1), pp. 92–102

[58] Hanmandlu, M., Grover, J., Gureja, A., Gupta, H.M.: 'Score level fusion of multimodal biometrics using triangular norms', *Pattern recognition letters*, 2011, **32**, (14), pp. 1843–1850

[59] Chaa, M., Boukezzoula, N.E., Attia, A.: 'Score-level fusion of two-dimensional and three-dimensional palmprint for personal recognition systems', *Journal of Electronic Imaging*, 2017, **26**, pp. 12–26

[60] Artabaz, S., Sliman, L., Dellys, H.N., Benatchba, K., Koudil, M. 'Multibiometrics enhancement using quality measurement in score level fusion'. In: International conference on intelligent systems design and applications. (Springer, 2016. pp. 260–267

[61] Kabir, W., Ahmad, M.O., Swamy, M. 'Score reliability based weighting technique for score-level fusion in multi-biometric systems'. In: 2016 IEEE Winter Conference on Applications of Computer Vision (WACV). (IEEE, 2016. pp. 1–7

[62] Nandakumar, K., Chen, Y., Dass, S.C., Jain, A.: 'Likelihood ratio-based biometric score fusion', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2008, **30**, (2), pp. 342–347

[63] Peng, J., El.Latif, A.A.A., Li, Q., Niu, X.: 'Multimodal biometric authentication based on score level fusion of finger biometrics', *Optik - International Journal for Light and Electron Optics*, 2014, **125**, (23), pp. 6891 – 6897

[64] Hezil, N., Boukrouche, A.: 'Multimodal biometric recognition using human ear and palmprint', *IET Biometrics*, 2017, **6**, (5), pp. 351–359

[65] Lumini, A., Nanni, L.: 'Overview of the combination of biometric matchers', *Information Fusion*, 2017, **33**, pp. 71–85

[66] Hanmandlu, M., Kumar, A., Madasu, V.K., Yarlagadda, P. 'Fusion of hand based biometrics using particle swarm optimization'. In: Fifth International Conference on Information Technology: New Generations (itng 2008). (IEEE, 2008. pp. 783–788

[67] AlMahafzah, H., Sheshadri, H., Imran, M. 'Multi-algorithm decision-level fusion using finger-knuckle-print biometric'. In: Emerging Research in Electronics, Computer Science and Technology. (Springer, 2014. pp. 39–47

[68] Kumar, A., Zhang, D.: 'Personal authentication using multiple palmprint representation', *Pattern Recognition*, 2005, **38**, (10), pp. 1695–1704

[69] Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W. 'The relation between the roc curve and the cmc'. In: Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05). (IEEE, 2005. pp. 15–20

[70] Yang, W., Hu, J., Wang, S., Chen, C.: 'Mutual dependency of features in multimodal biometric systems', *Electronics Letters*, 2015, **51**, (3), pp. 234–235

[71] Nandakumar, K., Ross, A., Jain, A.K. 'Biometric fusion: Does modeling correlation really matter?'. In: 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems. (IEEE, 2009. pp. 1–6

[72] Ríos.Sánchez, B., Arriaga.Gómez, M.F., Guerra.Casanova, J., de Santos.Sierra, D., de Mendizábal.Vázquez, I., Bailador, G., et al.: 'gb2sμmod: A multimodal biometric video database using visible and ir light', *Information Fusion*, 2016, **32**, pp. 64–79

[73] Crihalmeanu, S., Ross, A., Schuckers, S., Hornak, L. 'A protocol for multibiometric data acquisition, storage and dissemination'. In: Technical Report, WVU, Lane Department of Computer Science and Electrical Engineering. (, 2007.

[74] Fierrez, J., Galbally, J., Ortega.Garcia, J., Freire, M.R., Alonso.Fernandez, F., Ramos, D., et al.: 'Biosecurid: a multimodal biometric database', *Pattern Analysis and Applications*, 2010, **13**, (2), pp. 235–246

[75] Yin, Y., Liu, L., Sun, X. 'Sdumla-hmt: a multimodal biometric database'. In: Chinese Conference on Biometric Recognition. (Springer, 2011. pp. 260–268

[76] McCool, C., Marcel, S., Hadid, A., Pietikäinen, M., Matejka, P., Cernockỳ, J., et al. 'Bimodal person recognition on a mobile phone: using mobile phone data'. In: 2012 IEEE International Conference on Multimedia and Expo Workshops. (IEEE, 2012. pp. 635–640

[77] Ho, C.C., Ng, H., Tan, W.H., Ng, K.W., Tong, H.L., Yap, T.T.V., et al.: 'Mmu gaspfa: a cots multimodal biometric database', *Pattern Recognition Letters*, 2013, **34**, (15), pp. 2043–2050

[78] Sequeira, A.F., Monteiro, J.C., Rebelo, A., Oliveira, H.P. 'Mobbio: a multimodal database captured with a portable handheld device'. In: 2014 International Conference on Computer Vision Theory and Applications (VISAPP). vol. 3. (IEEE, 2014. pp. 133–139

[79] Bharadwaj, S., Bhatt, H.S., Singh, R., Vatsa, M., Noore, A.: 'Qfuse: Online learning framework for adaptive biometric system', *Pattern Recognition*, 2015, **48**, (11), pp. 3428–3439

[80] Zadeh, L.A.: 'Fuzzy sets', *Information and control*, 1965, **8**, (3), pp. 338–353

[81] Dubois, D.J.: 'Fuzzy sets and systems: theory and applications'. vol. 144. (Academic press, 1980)

[82] Dubois, D., Prade, H.: 'Fundamentals of fuzzy sets'. vol. 7. (Springer Science & Business Media, 2012)

[83] Yager, R.R., Filev, D.P.: 'Essentials of fuzzy modeling and control', *New York*, 1994, **388**

[84] Zadeh, L.A.: 'Fuzzy sets as a basis for a theory of possibility', *Fuzzy sets and systems*, 1978, **1**, (1), pp. 3–28

[85] Zimmermann, H.J.: 'Fuzzy set theory and its applications'. (Springer Science & Business Media, 2011)

[86] Calvo, T., Kolesárová, A., Komorníková, M., Mesiar, R. 'Aggregation operators: properties, classes and construction methods'. In: Aggregation operators. (Springer, 2002. pp. 3–104

[87] Dubois, D., Prade, H.: 'On the use of aggregation operations in information fusion processes', *Fuzzy sets and systems*, 2004, **142**, (1), pp. 143–161

[88] Beliakov, G., Pradera, A., Calvo, T.: 'Aggregation functions: A guide for practitioners'. vol. 221. (Springer, 2007)

[89] Calvo, T., Mayor, G., Mesiar, R.: 'Aggregation operators: new trends and applications'. vol. 97. (Physica, 2012)

[90] Komorníková, M.: 'Aggregation operators and additive generators', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2001, **9**, (02), pp. 205–215

[91] NIST: 'National institute of standards and technology: NIST biometric scores set', *https://wwwnistgov/itl/iad/ig/biometricscores*, 2004,

[92] Akhtar, Z., Alfarid, N. 'Secure learning algorithm for multimodal biometric systems against spoof attacks'. In: Proc. international conference on information and network technology (IPCSIT). vol. 4. (, 2011. pp. 52–57

[93] Toh, K.A., Yau, W.Y.: 'Combination of hyperbolic functions for multimodal biometrics data fusion', *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 2004, **34**, (2), pp. 1196–1209

[94] Ahonen, T., Rahtu, E., Ojansivu, V., Heikkila, J. 'Recognition of blurred faces using local phase quantization'. In: 2008 19th international conference on pattern recognition. (IEEE, 2008. pp. 1–4

[95] Ahonen, T., Hadid, A., Pietikäinen, M. 'Face recognition with local binary patterns'. In: European conference on computer vision. (Springer, 2004. pp. 469–481

[96] Kannala, J., Rahtu, E. 'Bsif: Binarized statistical image features'. In: Proceedings of the 21st international conference on pattern recognition (ICPR2012). (IEEE, 2012. pp. 1363–1366

[97] Tan, X., Triggs, B.: 'Enhanced local texture feature sets for face recognition under difficult lighting conditions', *IEEE transactions on image processing*, 2010, **19**, (6), pp. 1635–1650

[98] Kabacinski, R., Kowalski, M.: 'Vein pattern database and benchmark results', *Electronics Letters*, 2011, **47**, (20), pp. 1127–1128

[99] Bustince, H., Pagola, M., Mesiar, R., Hullermeier, E., Herrera, F.: 'Grouping, overlap, and generalized bientropic functions for fuzzy modeling of pairwise comparisons', *IEEE Transactions on Fuzzy Systems*, 2011, **20**, (3), pp. 405–415

[100] Kumar, A., Passi, A.: 'Comparison and combination of iris matchers for reliable personal authentication', *Pattern recognition*, 2010, **43**, (3), pp. 1016–1026

[101] Kumar, A., Xu, Z.: 'Personal identification using minor knuckle patterns from palm dorsal surface', *IEEE Transactions on Information Forensics and Security*, 2016, **11**, (10), pp. 2338–2348

[102] Cheniti, M., Boukezzoula, N.E., Akhtar, Z.: 'Symmetric sum-based biometric score fusion', *IET Biometrics*, 2017, **7**, (5), pp. 391–395

[103] Bharadi, V.A., Pandya, B., Nemade, B. 'Multimodal biometric recognition using iris & fingerprint: By texture feature extraction using hybrid wavelets'. In: 2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence). (IEEE, 2014. pp. 697–702