Multi-Biometric Systems: A State of the Art Survey and Research Directions

Ramadan Gad
Computer Science and Engineering,
Faculty of Electronic Engineering, Menoufia University,
Egypt.

AYMAN EL-SAYED
Computer Science and Engineering,
Faculty of Electronic Engineering, Menoufia University,
Egypt.

Nawal El-Fishawy
Computer Science and Engineering,
Faculty of Electronic Engineering, Menoufia University,
Egypt.

M. Zorkany
Electronic and Communication Engineering,
National Telecommunication Institute
Egypt.

***Abstract*—Multi-biometrics is an exciting and interesting research topic. It is used to recognizing individuals for security purposes; to increase security levels. The recent research trends toward next biometrics generation in real-time applications. Also, integration of biometrics solves some of unimodal system limitations. However, design and evaluation of such systems raises many issues and trade-offs. A state of the art survey of multi-biometrics benefits, limitations, integration strategies, and fusion levels are discussed in this paper. Finally, upon reviewing multi-biometrics approaches and techniques; some open points are suggested to be considered as a future research point of interest.**

Keywords—Biometrics; Multimodal biometric systems; fusion levels; recognition methods; authentication

I. INTRODUCTION

Authentication (identifying an individual using security system) of users is an essential but, difficult accurate and secured practical authentication technology. Traditional techniques for user authentication could be categorized as [1, 2]: (1) Token based techniques (i.e. key cards and smart cards) and (2) Knowledge-based techniques include text-based and picture-based passwords (often mix of username and password).

Due to vulnerabilities in above methods (It could be easily transgressed or lost or forgotten); Traditional techniques are considered to be not reliable or secure, and are not presently sufficient in some security application zones [3, 4]. The primary advantage of biometrics over these methods is that it cannot be misplaced, forgotten or stolen. Also, it is very difficult to spoof biometric traits . Due to greater accuracy and higher robustness of biometric recognition [1, 5]; Biometric solutions become popular and preferred methods to analyze human characteristics for security - authentication and identification - purposes[6]. It could not be duplicated or counterfeited and misused.

Practically, the use of biometrics information is the most secure method [7]. Consequently, it is now needed in many fields such as surveillance systems, security systems, physical buildings [8]. Other applications of biometrics systems include [9, 10]: access control (access to computer networks), forensic investigations, verification and authentication, e-commerce, online banking, border control, parenthood determination, medical records management, welfare disbursement and security monitoring. Biometrics applications increased dramatically in functionality in many more fields.

In the most general definition, "Biometric technologies" is defined as an automated methods of verifying and/or recognizing the identity of a living individual based on two categories : (1) *Physiological biometrics* include (Facial, hand and hand vein infrared thermogram, Odor, Ear, Hand and finger geometry, Fingerprint, Face, Retina, Iris, Palm print, Voice, and DNA) [10], and (2) *Behavioral biometrics* like (Gait, Keystroke, Signature) which measure the human actions [8]. Also, human electrocardiogram (ECG) signal is considered one of Biometric features used in individual recognition and authentication[11].

Depending on the application context, biometric systems may operate in two modes: verification mode and identification mode [5]. Through *verification mode*, the system verifies the identity by comparing the enrolled biometric trait by a stored biometric template in the system (1:1). This mode is used for positive recognition, and it aims to prevent the multiple individuals from using the same identity. In the *identification mode*, the enrolled sample is then compared with existing templates in a – central – database (1: M) . A database search is crucial and needed. The identification mode is critical in negative recognition applications, which aims to prevent a single user from using multiple identities [12]. Negative identification is also known as screening [8]. Obviously, verification is less computationally expensive and more robust compared with identification. On the other hand, the latter is more convenient and less obtrusive [13].

Multi-biometric systems distinguished over traditional uni-biometric systems as it [14] addresses the issue of non-universality and noisy data. Multi-biometric systems can facilitate the indexing of large-scale biometric databases. Also, it becomes not easy for an impostor to spoof all the biometric traits of an authorized enrolled person. Generally, It is much

more vital to fraudulent technologies because it is more difficult to forge multiple biometric characteristics. Multi-biometric recognition systems also have benefits in the continuous monitoring of an individual in situations or tracking him when a single trait is not sufficient in use. These systems continue to operate even if part of biometric sources become unavailable of a failed (i.e. sensor malfunction, software malfunction, or deliberate user manipulation); it may view as a fault tolerant system. For these benefits, multimodal expected to provide higher accuracy rate.

The rest of this paper is organized sequentially as follow: Section II will overview the biometrics characteristics followed by section III to discuss the unimodal biometrics' drawbacks. Next, Section IV will discuss the multi-biometrics advantages and limitations, categories, and integration scenarios. After that, section V is to discuss biometrics quality performance and metrics. different fusion levels before and after matching, depended on theses metrics, will be discussed in section VI. Benefits and drawbacks for each approach will be declared with evidence of previous research. Moreover, section VII will show the design issues and trade-offs related to any multi-biometric recognition system. Finally, Section VIII suggests some open points for further investigation and research.

II. BIOMETRICS OVERVIEW

A biometric system to be practical and reliable should meet the specified requirements/characteristics [15] [4]: *Universality (availability)*, each person should have the characteristic. Availability is measured by the "failure to enroll" rate. *Distinctiveness:* It declares that any two persons should sufficiently have different characteristic. It is measured by the False Match Rate (FMR), also known as "Type (II) error". *Permanence (robustness)*, the characteristic should be stable (with respect to the matching features) over a period of time. Which means the stability over age. Robustness is measured by the False Non-Match Rate (FNMR), also known as "Type (I) error" . *Collectability (accessible)*, the characteristic can be measured quantitatively, and easy to image using electronic sensors. Accessibility can be quantified by the "throughput rate" of the system. *Performance:* It means to achieve recognition accuracy, speed, and the resources required to the application. *Acceptability*, The particular user population and the public, in general, should have no (strong) objections to the measuring/collection of the biometric characteristic. Acceptability is measured by polling the device users . *Resistance to Circumvention*, tests and proofs how the system resists fraudulent methods easily.

Consequently, a brief comparison of the most known biometric techniques based on above factors are shown in table (I) [12, 16], to differentiate between the biometrics modalities as a unimodal trait.

Which biometric characteristic is best? Each biometric feature has its own strengths and weaknesses and the choice typically depends on the application. Accordingly, each one could be used in authentication and/or identification applications [17]. Predicting the "false acceptance" and "false rejection" rates, system throughput, user acceptance, and cost savings for operational systems from test data, is a surprisingly difficult task.

Consequently, it is impossible to state that a single biometric characteristic is "best" for all applications, populations, technologies and administration policies.

TABLE I. COMPARISON OF BIOMETRIC CHARACTERISTICS [12, 16]

Biometric Characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial Thermogram	H	H	L	H	M	H	L
Hand Vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand Geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palm Print	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

[a.] (H: High, M: Medium, and L: Low)

III. UNIMODAL BIOMETRICS LIMITATIONS

Any single modal biometric has limitations. For example, iris recognition suffers from some problems like camera distance, eyelids and eyelashes occlusion, lenses, and reflections [18-20]. Face changes overages and unstable, and twins may have similar face features. Also, fake faces from mobiles as example, and masks used to attack the system . Fingerprint may have some cuts, burns, and small injuries temporary or permanent . Moreover, fake fingers made from gelatin and/or silicon have ability to attack the fingerprint-based recognition system . Cold leads to voice problems and a tape recordings may be used to hack the system [13]. The fingerprint of DNA needs several hours to be obtained. Besides, DNA includes sensitive information related to genetic of individuals and the test is quite expensive to perform . Hand geometry is not distinctive enough to be applied to a large population. Thus, it is not suitable for purpose of identification [16]. Gait is sensitive to body weight and not stable; it is not used for large population and not reliable enough . Signature is not universal and changes with time. Offline ones are forgery while, Online signature cannot applied for documents verification (i.e. Government documents and bank cheques) . None of above traits alone can ensure perfect recognition performance. Nevertheless, the biometric system (either an 'identification' system or a 'verification' system) can also be attacked by the outsider or unauthorized person at various points [21]. Combining multiple modalities is a good idea to decrease these conditions.

The unimodal biometric rely on the evident single source of information for authentication (e.g., single fingerprint, face) . Single modal biometric traits may not achieve the desired performance requirements; as they have plenty of error rates [5,

15]. These systems have to contend with a variety of problems such as:

- *Noise in sensed data;* defective or improperly maintained sensors (i.e. accumulation of dirt on a fingerprint sensor) could produce deformed and noisy data. For instance, a cold has effects on the voice, wearing glasses alters iris recognition performance, variations in light or illumination in face sensed …etc.
- Distinctiveness (Intra-class variations and Inter-class similarities); Biometric trait is expected to be varied significantly across two persons. Intra-class variations occur when a user interacts with the sensor incorrectly (e.g., incorrect facial pose). Also, characteristics of the individuals are formed with the large inter-class similarity (overlap) in the feature sets of multiple users.
- Non-universality; means the non-ability of the biometric to acquire meaningful biometric data from a group of users due to the poor quality and consistency of the acquired biometric data as a result to error or a fault in the sensor. For example, many of population (about 4%) may have scars or cuts in fingerprints. As a result, a fingerprint biometric system, may extract incorrect minutiae features from them. Also, user-sensor interaction is adjustment incorrectly. Of course, this may give undesired matching result.
- Spoof attacks; a fake traits or biometrics of the authorized user are enrolled and saved in the template database; an imposter person may attempt to spoof these sensed data when the traits are used. As in [22], artificial fingers/fingerprint can be used to spoof the verification system. This type of attack is common when using behavioral characteristics.

On behave of above problems, unimodal biometric systems suffer other drawbacks like: insufficient population coverage, lack of individuality, lack of invariant representation, and susceptibility to circumvention [7].

These problems lead to higher False Reject Rate (FRR) and False Accept Rate (FAR) [4, 10, 23] as will be shown later in quality metrics, in section 5.

IV. Multi-Biometrics as a Solution

Biometric fusion has a history of more than 30 years . More than one biometric combined to investigate high performance multi-biometric recognition system. Multi-biometrics has addressed some issues related to unimodal this make it has some benefits over unimodal biometrics such as recognition accuracy, privacy, and biometric data enrollment.

Recognition accuracy: Its accuracy is better as compared to the unimodal biometric system [24]. The multi-biometric system is expected to be more accuracy and reliability due to the multiple, biometric traits independency, and difficult to forge all of them [5, 10]. As the combination of each of the biometric identifiers offers some additional evidence about the authenticity of an identity claim, one can have more confidence in the result. For example, two persons may have the similar signature patterns, in which case, the signature verification system will produce large FAR for that system. Addition of face recognition system with the signature verification system may solve the problem and reduce the FAR [9]. Experiments have shown that the accuracy of multimodality can reach near 100% in identification.

Privacy: Multimodal biometric systems increase resistance to certain type of vulnerabilities. It prevents from stolen the templates of biometric system as at the time it stores the two characteristics of biometric system in the database [25]. For example, it would be more challenge for attacker to spoof many different biometric identifiers[9]. Further, when two or more modalities are used for authentication, it leads to become not easy to spoof the biometric system.

Biometric data enrollment: Multimodal biometric systems can address the problem of non-universality. In case of unavailability or poor quality of a particular biometric data, other biometric identifier of the multimodal biometric system can be used to capture data. For example, a face biometric identifier can be used in a multimodal system (involves fingerprint of general labors with lots of scars in the hand) [9]. It makes better system operation [24]. Multi-biometric system also addresses the problem of noisy data effectively (i.e. illness affecting voice, scar affecting fingerprint). They allow indexing or filtering of large biometric databases, and are robust to noise. Thus, it provides universal coverage and improves matching accuracy [10, 15, 26].

A. Multimodal Categories

Multi-biometric systems have two basic categories: synchronous and asynchronous. In synchronous, two or more biometrics combined within a single authorization process. On the other hand, asynchronous system uses two biometric technologies in sequence (one after the other) [27]. Multimodal biometric systems can operate in three different modes [5]:

- *Serial Mode (cascade mode)* – each modality is examined before the next modality is investigated. The overall recognition duration can be decreased, as the total number of possible identities - before using the next modality - could be reduced
- *Parallel Mode* – sensed/captured data from multiple modalities are used in concurrent way to perform recognition. Then the results are combined to make final decision.
- *Hierarchical Mode* – individual classifiers are combined in a hierarchy -tree like- structure. This mode is preferred when a large number of classifiers are expected.

B. Multi-Biometrics Integration Scenarios

Recognition systems using multiple biometric traits are designed to operate in one of the integration scenarios as below:

1) Multi-sensor systems

The information of the same biometric obtained from different sensors are combined for all. For example, complementary information corresponding to fingerprints can be acquired using different types of sensors (like optical and

capacitive sensors). Information obtained are then integrated using sensor level fusion technique[15].

2) Multi-modal systems

More than one biometric trait is used for user identification. For example, the information obtained using face and voice features or other can be integrated to establish the identity of the user[27]. This can be more costly; because it requires multiple sensors with each sensor sensing different biometric characteristics. But, the improvement in performance is substantial.

3) Multi-instance systems

Multiple instances of a single biometric trait are captured. For example, images of the left and right irises can be used for iris recognition. Also, fingerprints from two or more fingers of a person may be combined or one image each of the same person may be combined. If a single senor is used to acquire these images in a sequential manner, the system can be made really cost effective, as it does not require multiple sensors. Moreover, it does not incorporate additional feature extraction and matching modules [17].

4) Multi-sample systems

Multiple samples of a same biometric trait are used for the enrollment and recognition. For example, along with the frontal face, the left and right profiles are also captured. Multiple impression of the same finger, and multiple samples of a voice can be combined. Multiple samples may overcome poor performance. But, it requires multiple copies of sensors, or the user may wait a longer period of time to be sensed or a combination of both[15].

5) Multi-algorithm systems

Multiple different approaches to feature extraction and matching algorithms are applied to a single biometric trait. Final decision obtained if any of the matching fusion technique can be applied on the results obtained using different matching algorithms. These systems are more economical as no extra device is required to capture the data. But, these are more complex because of application of different algorithms[15].

6) Hybrid systems

It is a system which integrates more than one of the above mentioned multi-biometric systems. For example, two face recognition algorithms can be combined with two fingerprint recognition algorithms. Such a system will be multi-modal and multi-algorithmic system. Moreover, if multiple sensors are used to obtain these images, then it will be multi-sensory, and if multiple instance of the finger is used, it will be multi-instance system also.

Both of hybrid systems and multi-modal systems can be desired by using multiple modalities. However, the rest can be achieved with the only help of even single modality [23]. The different types of multi-biometric are shown in figure (1).

C. Limitation of Multi-biometrics System

Some lacks are still found such as noise in the biometrics like scratches in the fingerprint and lens mark in iris, this will lead to increase the (FRR). Moreover, the accuracy of the multi-biometric enrollment and multi-biometric identification need to be improved. In multi-biometrics, failure of one biometrics will make the whole system to fail [28]. In addition, multimodal biometric systems, may be more expensive and complicated due to the requirement of additional hardware and matching algorithms, and there is a greater demand for computational poser and storage [9]. Recent research has revealed that multi-biometric systems can increase the security level as a means to enhance network security to people who are encouraged to use biometric systems in this field. However, it need more efforts and research to face some types of attacks such as: spoof attack, replay attack, substitution attack, Trojan horse attack, transmission attack, template database attack, and decision attack [17]. Next section will list the performance metrics that distinguish between the multi-biometrics techniques.

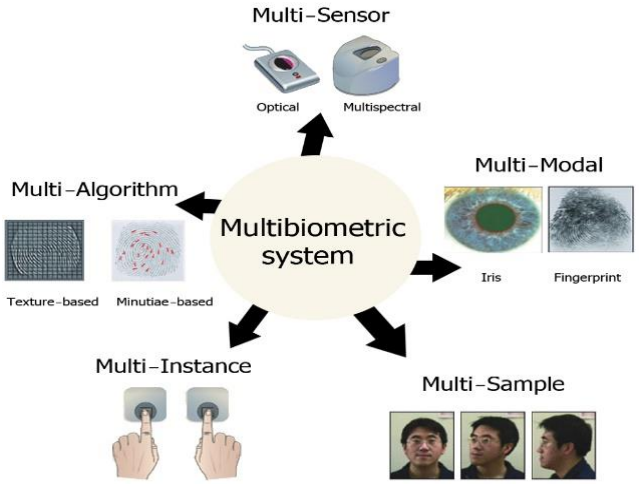

Fig. 1. The different types of multi-biometric system. [15]

V. Quality Performance and Metrics

Various quality performance metrics measure the performance of any biometric authentication techniques. It helps comparing systems and motivating the progress [13]. The most common performance metrics of biometric systems are described below [12] :

False Accept Rate (FAR) or (False Match Rate (FMR)): Mistaking the biometric measurements from two different persons to appear as if they are from the same person due to large inter-user similarity. It measures the percent of invalid matches. The FAR is defined as in (1) [1, 29, 30]:

$$FAR\% = \frac{T_{Faccept}}{T_{Fsubmit}} \times 100 \quad (1)$$

Where, $T_{Faccept}$ is total number of forgeries accepted and $T_{Fsubmit}$ is total number of forgeries submitted to the system test. In a good authentication system this rate must be low.

False Reject Rate (FRR) or (False Non-Match Rate (FNMR)): Mistaking two biometric measurements from the same person to appear that they are from two different persons due to large intra-class variations. It measures the percent of valid inputs being rejected. The FRR is defined as in (2) [24]:

$$FRR\% = \frac{T_{Greject}}{T_{Gsubmit}} \times 100 \quad (2)$$

Where $T_{Greject}$ is the total number of genuine test pattern rejected, and $T_{Gsubmit}$ is total number of genuine test submitted to the system. This must be low to achieve good Performance. The average of the FRR and FAR is called the Average Error Rate (AER)[29].Genuine Acceptance Rate (GAR) sometimes used, which is the percentage of the likelihood that a genuine individual is recognized as a match [8]. GAR of a valid user can be obtained by equation (3) [31].

$$GAR\% = 1 - FRR\% \quad (3)$$

Equal Error Rate (EER): For a simple empirical measure, it is used to summarize the performance of a biometric system that is defined at the point where False Reject Rate (FRR) and False Accept Rate (FAR) are equal . System with the lower EER, is the more accurate and precise [1, 9, 30]. The EER is also called the type (III) error [29].

Failure to Capture (FTC): denotes the percentage of times the biometric device fails to automatically capture a biometric characteristic when presented correctly. This usually happens when system deals with a signal of insufficient quality [24].

Failure to Enroll Rate (FER or FTE): denotes the percentage of times users cannot enroll in the recognition system[32]. Data input is considered invalid due to poor quality.

Template Capacity: It is the maximum number of sets of data which can be input in to the system [24].

Usually, the above performance metrics are expressed using different graphs such as Receiver Operating Characteristic (ROC), Score Histogram (SH), and Cumulative Match Characteristic (CMC) [9]. *Receiver Operating Characteristic (ROC) curve*: There is a trade-off between FAR and FRR in every biometric system. In fact, both of them are functions of the system threshold (t); if it is declined to make the system achieves higher tolerance to input variations and noise, then FAR increases. On the other hand, if it is raised to make the system more secure, then FRR increases accordingly . The ROC plot is obtained by graphing the values of FAR against FRR, at various operating points (thresholds) on a linear or logarithmic or semi-logarithmic curve. Detection Error Trade off (DET) is a common variation, which is obtained via normal deviate scales on both axes [24]. This graph is more linear that illuminates the differences for higher performances. *Cumulative Match Characteristic (CMC) curve*: is used in biometric identification to summarize the identification rate at different rank values [8]. *Score Histogram (SH)*: plots the frequency of the scores for matches and non-matches over the match score range. These metrics are needed to differentiate between each level fusion and method considered for the multi-biometrics as a solution. Categorization of different levels of fusion will be discussed in next section.

VI. Levels of Fusion in Multimodal Biometrics

Multimodal biometric fusion combines the distinguished aspect from different biometric features to support the advantages and reduce the drawbacks of the individual aspects [5]. The fundamental issue of information fusion is to determine the type of information that should be fused and the selection of method for fusion . The goal of fusion is to devise an appropriate function that can optimally combines the information rendered by the biometric subsystems [8].

In multimodal biometrics, the fusion scheme can be classified as sensor level, feature level, match score level, rank level, and decision level [4] as shown in figure (2). The process can be subdivided into two main categories: prior-to-matching fusion and after matching fusion [33]. Figure (3) [9], shows these fusion levels possibilities at each module. The hybrid one is mixing two or more from these level fusions.

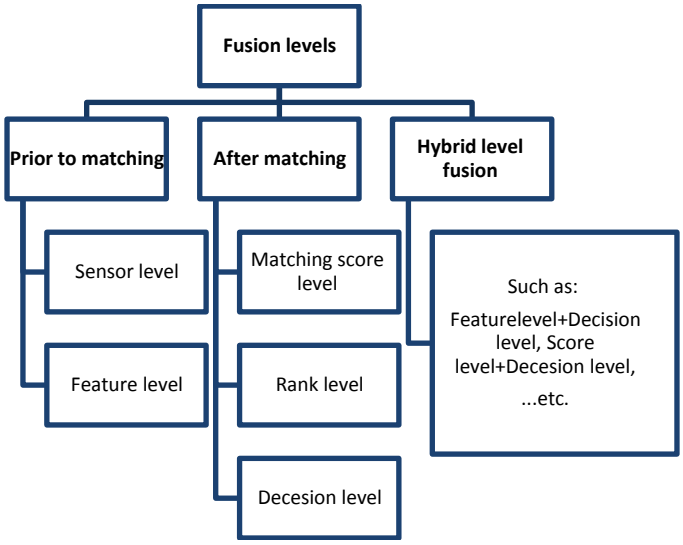

Fig. 2. Categories of different fusion levels

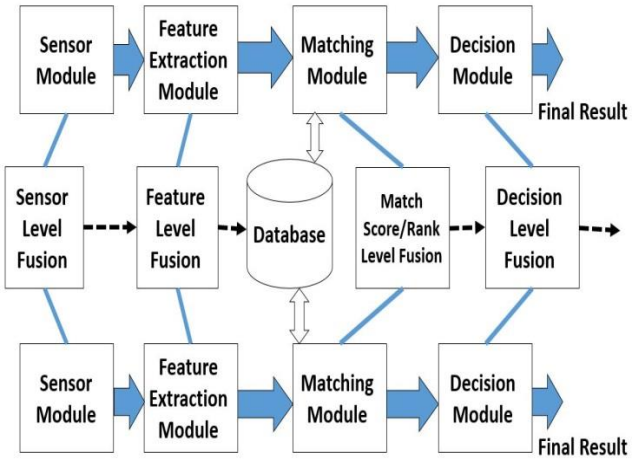

Fig. 3. Prior-to-matching and after matching fusion levels related to biometric system modules [9]

A. Prior to Matching Fusion

Fusion in this category integrates evidences before matching. This can be classified into two different categories as follows:

1) Sensor level fusion

Principles- A new biometric data generated by merging the raw data obtained from multiple sources. Then, trait can be extracted. A single sensor or different compatible sensors like

fingerprint, iris scanner, etc., represents the samples of the single biometric trait sensed [23]. This level of fusion is also known as data level fusion or image level fusion (for image based biometrics) [4].

Discussion- Sensor level fusion can benefit multi-sample systems which capture multiple snapshots of the same biometric [15]. Compared to other fusion types, it has a lot of information. It is projected to improve the recognition accuracy. Sensor fusion addresses the problem of noise in sensed data because improper maintenance of sensors [4]. However, raw images are either not available or the information available from the different sources is not compatible. For this unavailability and incompatibility of desired information, sensor level and feature level fusion are not possible in all cases [9]; Very less work has been done in this type of fusion [17]. As an example of sensor level fusion, Ratha et al. [34] described a fingerprint mosaicing scheme to integrate multiple snapshots of a fingerprint as the user rolls the finger on the surface of the sensor.

2) Feature level fusion

Principles- The correlated feature sets extracted from different biometric channels (modalities) can be fused by using specific fusion algorithm forming a composite feature set, passed to the matching module [5, 27]. This done after normalization, transformation and reduction schemes [33]. The goal of feature normalization is to modify the location (mean) and the scale (variance) of the feature value via a transform function in order to map them into a common domain. (e. g. Min-max normalization, Median normalization...etc.) . Transformation or Feature Selection is algorithm use to reduce the dimensionality of the feature set. (e. g. Sequential forward selection, Sequential backward selection, Principal Component Analysis (PCA), etc.) [15].

Discussion- Final feature vectors could be either homogeneous or heterogeneous. The feature sets are from different algorithm and modalities; so the consolidation of feature set may have some problems [5, 23]. The relationship between these features of different biometric systems may not be well known, and structurally incompatible features are common. In addition, concatenating two feature vectors might lead to the dimensionality problem [4]. Lead to these difficulties, fusion level reported in limited research work.

For example, in year 2004, Feng et al. [19] developed a feature level fusion based multimodal biometric system using face and palm print. They used Principal Component Analysis (PCA) and Independent Component Analysis (ICA) as classification algorithms. The PCA-based accuracy rate was (70.83%, 85.83%) for (face, palm print), while 95.83% after fusion. Moreover, ICA-based accuracy rate was (85%, 92.5%) for (face, palm print), while 99.17% after fusion. some previous fused modalities based on feature level fusion as in [35-41].

B. After Matching Fusion

Prior to matching fusions sometime don't involve multiple modalities. Also, the fusion of data set is more complex, and it is not good to ignore any data [23]. After matching fusion integrates evidences of after matching module. This can be classified into three different categories:

1) Matching score level fusion

Principles- Individually, Extracted feature vectors (generated separately for each modality) are compared with the templates enrolled in the database for each biometric trait in order to generate the match scores [5]. Output set of match scores are fused to create composite matching score (single scalar score) [4]. This fusion technique is also known as confidence level or measurement level fusion. Density, transformation, and classifier based score fusion are different methods to achieve this fusion level [23].

The matching scores cannot be used or combined directly; because these scores are from different modalities and based on different scaling methods. Score normalization are required, by converting the scores into common similar domain or scale. This can be carried out with different methods. Slobodan Ribaric and Ivan Fratric discovered - piecewise linear normalization - new normalization technique. Their experiments used palm print and facial features.

Discussion- Applying fusion at this level is preferred as it is easy to obtain and combine matching scores of different biometrics [10]. It provides richest set of information about the biometric data. But complexity is more [23]. A lot of work has been done using match score level fusion. It is the most investigated fusion method so far which considers the match or similarity/distance score for fusion. But, the similarity/distance scores need to be normalized before fusion (as they can be in different ranges) [9]. Choosing inappropriate normalization technique result leads to very low recognition performance rate [4].

As an example, face modality and hand modality match scores together are combined in paper. Also, the match scores generated by the face, fingerprint and hand modalities of a user combined via the simple sum rule to obtain a new match score, after that it is used to make the final decision [18]. A rest of some previous work in [15, 18, 26, 33, 34, 42-57], considers matching score level fusion.

2) Rank level fusion

Principles- In this new fusion approach, each classifier associates a rank with each enrolled trait to the system (a higher rank indicating a good match). It consolidates multiple unimodal biometric matcher outputs, and determining a new rank that would help in estimating the final decision [4, 5]. Generally, the rank level fusion is adopted for the identification rather than verification. Here, the working procedures are: first, generate a rank of identities sorted with all modalities. Second, by help of any method of fusion, the ranking for each individual available for different modalities fused. Finally, the identity with the lowest score is the correct identified one [23].

Discussion- Beside it orders the identities based on those similarity/distance, it does not need any normalization procedure [9]. This method provide more accuracy comparing with just identifying best match with one modality. Unlike match score level fusion, it is easily possible to compare the ranking from different biometric modalities. As a result, it is so easy to make the decision [23].

However, this type of fusion has one weakness. In a case of multimodal biometric, which more different identities output from number of matching modules appear some identities of only one matcher, a wrong results act a risk of achieving the rank level fusion [33]. Unlike to match score level fusion, rank level fusion provides less information. It is better, because it provides a rank to different matches and also weights can be assigned to some classifiers [23].

Some of previous work listed in [4, 33, 58-60] as an examples for rank level fusion with fusion approaches used and modalities fused. In general, it remains significantly understudied.

3) Decision level fusion

Principles- The final decision - in multimodal biometric systems - is formed from obtaining individually separate decision of different biometric modalities using different techniques include behavior knowledge space, majority voting, , weighted voting, AND rule, and OR rule[5, 8]. Decision level fusion is also named abstract level fusion; because it is used when there is access to only decisions from individual [8, 23].

Majority voting approach is the mostly used for decision level fusion. The input sample with agreed in majority of matchers is given the identity. AND/OR rules are rarely used; because they combine two different matchers, so this sometimes degrade of performance of the system. AND combination improves the FAR while, OR combination improves the FRR. The main advantage of the majority voting method is that it does not require prior knowledge about the matcher, and it requires no training for final decision making too [42].

Discussion- Decision level fusion approaches are well investigated for biometric systems but are too rigid (inflexible) because of availability of limited amount information; probability of having a tie may appear [4]. And only consider single information for fusion, which has a high probability of producing wrong recognition result [5, 18]. As it have a less amount of features or scores information of different modalities; it is very easy to implement. [23]. This type is less preferred in multi-biometric system implementation.

Decision level fusion based examples include: majority voting rule and behavioral knowledge space method, weighted voting based on Dempster - Shafer theory, AND/ OR rules for deciding the decision , and that naïve Bayesian decision fusion as it works well, even if the matchers used in fusion are dependent to each other. In addition, some of other last research found in [61-64].

C. Hybrid Level Fusion

Tri-level fusion scenarios (different fusion in different levels of the system) can be investigated to make the system faster and significantly reduce the error rate. The fusion of level increased the performance. In 2007, C. Lupu et al. [65] fused fingerprint, voice and iris. Next year 2008, S. Asha et al. [7] combined fingerprint with mouse dynamics. In 2011, Parallel Feature Extraction with the help of SIFT, SIMD, and HMA techniques was used by Anukul Chandra Panda et al.[66] to fuse multiple iris. Next in 2013, Gandhimathi Amirthalingam, and Radhamani. G. [5] used fuzzy vault to implement multimodal system based on Face and ear traits. Some examples of previous work used such fusions are in [42, 67-71]. Fusion approaches, fusion levels, and performance for these papers ordered by year, are listed in table (II) below.

VII. Design and Implementation of Multi-Biometrics Recognition Trade-Offs

Generally, any biometric recognition system architecture is related to software-based techniques and hardware-based techniques. The obstacles here is to satisfy all challenges requirement such as: user friendly, fast (i.e. the system must identify individuals in real time), low cost, high performance, less intrusive, fraud prevent and high fake detection rate [72]. Briefly, design issues in multi-biometrics include [17]:

- Choosing the biometric modalities and number of traits (defining and estimation of each modality reliability is still open research issue).
- Choosing the best samples for a particular biometric.
- Fusion level and fusion methodology.
- Fusion scenario and common strategy.
- Learning weights of individual biometric for users.
- Cost versus performance and accuracy versus reliability trade-offs.
- Verification and/or identification system for application.
- Expert features selection difficulties.

In order to optimize the multi-biometric recognition benefits, the issues of system design firstly should be understood better; so the more effective design methodology and system architecture can be developed. For instance, to decide whether combining multiple biometrics or combining multiple samples of the same trait is better, to achieve economic system. In addition, privacy issues should be considered, and compromising between accuracy and coverage.

VIII. Multi-Biometrics - Discussion and Research Direction

Several research directions arise from the work proposed in this topic. There are some issues and open questions still need some efforts. We suggest the following tasks and discussion as future work that would significantly improve the security or other performance metrics of multi-biometric systems. Below is a hot point in this field still under research.

A. Multi-data Database / Real dataset

A dataset is not a research result in itself but, a well-designed one can facilitate the research. Many researchers are putting efforts in fusing multimodal biometrics. There are different approaches for biometric fusion. One approach is to use heterogeneous database (i.e. one biometric trait from one database and other trait from another database). But this approach is not reflecting the performance of multimodal users. The other approach, is to use homologous database. It means

different biometrics from the same person. Only few multimodal databases are available publicly [73]. BANCA and XM2VTS includes face and voice biometrics. BIOMET which includes face, voice, fingerprint, hand and signature. BIOSEC includes fingerprint, ace, iris and voice. SDUMLAHMT is a homologous database which includes face images from 7 angles, finger print images, gait videos, iris images. But these databases have some limitations. Homologous multi-biometrics dataset should be complete (contains all the biometrics for large population) for future research testing and multi-biometric system evaluation.

B. Soft Multi-biometrics

Using multiple biometric identifiers in a single system will increase the identification or verification times and hence, cause more inconvenience to the users and increase the overall cost of the system. Thus, soft biometric is introduced in 2004 to obtain the same recognition performance without causing any additional inconveniences to the users by incorporating it (soft biometric identifiers) to the primary multimodal systems [8]. Soft biometric identifiers include gender, ethnicity, height, weight, eye color, skin color, hair color, etc. Two key challenges need to be addressed to incorporate soft biometrics into the traditional multimodal biometric framework. The first challenge, is the automatic and reliable extraction of the soft biometric information without causing inconveniences to the users, and the second challenge, is to combine optimally this information with the primary biometric identifier to achieve the best recognition performance. Soft multi-biometrics could be implemented by using Oracle or SQL Server programming language tool that integrates the database implementation with pattern recognition and image processing techniques.

C. Multi-Algorithms fusion methods

Such systems seek to improve the speed, reliability, and accuracy of a biometric system. A variety of fusion methods and approaches have been described in [14]. We suggest new methods and modified algorithms to build and test the multi-biometric system. In [56], a new robust linear programming method proposed theoretically to fuse multi-biometrics by combining the modalities optimally. The robustness and accuracy have to be practically measured.

Another suggestion is to adopt K-means to cluster data and other advanced clustering methods to offer the best solutions especially when data are influenced by kinds of noise. The new modified feature descriptor Scale Invariant Feature Transform (F-SIFT) algorithm, Incremental Granular Relevance Vector Machine (iGRVM), Particle Swarm Optimization (PSO), and Hidden Markov Models (HMM) have not been used practically yet as new fusion techniques. The performance of multi-unit biometric trait recognition may be improved. Also, using the classifiers in matching fusion is still under research. In the multimodal biometric literature, a lot of attention has been paid to the parallel fusion of multiple classifiers. A few of reported works dealt so far with serial architecture. It would also be of interest to study the performance of the proposed techniques with the serial fusion of multiple classifiers using F-SIFT, iGRNM, PSO, and HMM algorithms suggested.

D. Identification of Identical Twins

The identification of identical twins is a big challenge, as the unimodal system is less accuracy in this state. Twins are the most similar persons in terms of genetics. The multimodal can increase the recognition rate as the Twins cannot have the same modalities together. Face, fingerprint, and iris could be fused to identify twins. To extend the study on the similarity of biometrics of identical twins, the use of siblings' data would be a hot point in future.

E. Indexing Search (Time and Complexity Enhancement)

During identification mode, search time plays a significant role. The search space of large biometrics database can be reduced through indexing and cloud computing. Various local feature based indexing approaches are proposed using multi-dimensional trees. Though k-d tree improves searching time, but insertion into the tree is not dynamic [54]. This is not suitable as databases are continuously updated to new enrollments. Another data structure known as k-d-b tree suggested to resolve such these issues. To improve the rank of identification for R-tree indexing, a hybrid coarse-to-fine searching strategy will be proposed. Also, we suggest parallel sorting of vote counts using Hypercube Mesh Architecture (HMA) in order to retrieve the image and get the top k matches; this may achieve less in time and complexity, when indexing scores are combined with match scores. Indexing using parallel geometric hashing is faster and could find its applicability in various real-time applications. All these points, if practiced upon multi-biometrics over cloud computing topology, it may become a solution for some biometric architecture design issues. Some problems and promises of using the cloud and biometrics are discussed in [74].

F. Embedded Hybrid Recognition System

From the above survey, some points noticed as a few research used sensor level fusion; we suggest fusion between physiological and behavioral traits such (iris, fingerprint, face…etc.) with (gait, signature). Fusion between the offline and online signature acts more authentication for critical documents signing. At the same time, the multi-fusion also can be used with multi classifiers and using different fusion levels. The multi-biometric system then may be more complex. This can be resolved by using the parallelism in feature extraction and identification phases, or execution by using H/W devices like Arduino or FPGA or parallel processing elements. In most cases, multi-biometric based security systems need to operate actively in the real-time public network and authentication environment.

IX. Conclusion

Multi-biometrics topic has attracted more interest in recent research. It is used to identify individuals based on their physiological and behavioral characteristics for security purposes. Overview of biometrics showed that it is impossible to find the best single biometric suitable for all applications, populations, technologies and administration policies. Also, integration of biometric modalities can solve unimodal system limitations to achieve higher performance.

Benefits and limitations of multi-biometrics discussed as we introduced it as a solution. In this paper, a state of the art survey of integration strategies, and fusion levels prior to matching and after matching are discussed with advantages and disadvantages of each type. However, Design and evaluate the multi-biometric systems raises many issues and trends. Finally, some open points suggested to be considered as a future research and enhance applications.

TABLE II. SOME UPTODATE EXAMPLES OF PREVIOUS RESEARCH BASED DIFFERENT FUSION IN DIFFERENT LEVELS

Year	Modalities fused	Author(s)	Fusion Level	Fusion Approach	Performance in percentage
2004	Fingerprint + Face	Kalyan, et al.[67]	Score + Decision	Sum Rule and Likelihoods	58.33% improvement with correlation 0.9 And (sum rule, PSO)=(0.0324,0.0135)%
2011	Face + Palm print	Linin Shen [68]	Feature+ Decision	FPCODE	Feature level fusion : 91.52% Decision level fusion : 91.63%
2013	Face + Ear	S.M.S. Islam[69]	Feature + Score	L3DF, Iterative closet point	FAR = 0.001 % Recognition: 96.8% Verification: 97.1%
2014	Face + Fingerprint + Iris	A. Annis Fathima et al. [71]	Score + Dynamic decision	Weighted average fusion, and K-NN	Recognition Rate= 78.5484% (Iris + Face) = 85%

REFERENCES

[1] M. Manjunath and K. B. Raja, "A Novel Approach for Iris Recognition using DWT&PCA," Int. J. Advanced Networking and Applications, vol. 5, no. 1, pp. 1830-1836, 2013.

[2] S. Malhotra and D. C. Kant, "A Novel Approach for Securing Biometric Template," Internal Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 3, no. 5, pp. 397-403, 2013.

[3] A. Bhargava and R. S. Ochawar, "Biometrics in Access Control System," International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 2, pp. 269-273, 2013.

[4] N. Radha and A. Kavitha, "Rank Level Fusion Using Fingerprint and Iris Biometrics," Indian Journal of Computer Science and Engineering (IJCSE), vol. 2, no. 6, pp. 917-923, 2011.

[5] G. Amirthalingam, "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues (IJCSI), vol. 10, no. 5, pp. 234-241, 2013.

[6] S. Sharma, "An Improved Iris Recognition System Based on 2-D DCT and Hamming Distance Technique," ICRTEDC-2014, GV/ICRTEDC/08, vol. 1, no. 2, pp. 32-34, 2014.

[7] S. Asha and C. Chellappan, "Authentication of E-Learners Using Multimodal Biometric Technology," presented at the Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, Islamabad, 2008. pp. 1-6.

[8] A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics vol. 6. New York: Springer Science & Business Media, 2006.

[9] M. L. Gavrilova and M. M. Monwar, "Current Trends in Multimodal Biometric System Rank Level Fusion," in Pattern Recognition, Machine Intelligence and Biometrics, ed: Springer, 2011, pp. 657-673.

[10] R. Singhal, N. Singh, and P. Jain, "Towards An Integrated Biometric Technique," International Journal of Computer Applications, vol. 42, no. 13, pp. 20-23, 2012.

[11] Y. S. a. S. Singh, "Evaluation of Electrocardiogram for Biometric Authentication," Journal of Information Security, vol. 3, no. 1, pp. 39-48, 2012.

[12] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.

[13] F. Karray, J. A. Saleh, M. N. Arab, and M. Alemzadeh, "Multi Modal Biometric Systems: A State of the Art Survey," Pattern Analysis and Machine Intelligence Laboratory, University of Waterloo, Waterloo, Canada, no. 2007.

[14] A. M. Siddiqui, R. Telgad, and P. D. Deshmukh, "Multimodal Biometric Systems: Study to Improve Accuracy and Performance," International Journal of Current Engineering and Technology, vol. 4, no. 1, pp. 165-171, 2014.

[15] H. AlMahafzah and M. Z. AlRwashdeh, "A Survey of Multibiometric Systems," International Journal of Computer Applications vol. 43, no. 15, pp. 36-43, 2012.

[16] K. Delac and M. Grgic, "A Survey of Biometric Recognition Methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, ELMAR-2004, Zadar, Croatia, 2004, pp. 184-193.

[17] M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics," International Journal of Computer Science and its Applications, vol. 1, no. pp. 157-160, 2011.

[18] A. A. Ross, A. K. Jain, and K. Nandakumar, "Information Fusion in Biometrics," in Handbook of Multibiometrics, ed, 2006, pp. 37-58.

[19] G. Feng, K. Dong, D. Hu, and D. Zhang, "When Faces are Combined With Palmprints: A novel Biometric Fusion Strategy," presented at the In proc. of 1st Int. Conf. on Biometric authentication, Hong Kong, China, 2004. pp. 701-707.

[20] R. Gad, M. Mohamed, and N. El-Fishawy, "Iris Recognition Based on Log-Gabor and Discrete Cosine Transform Coding," Journal of Computer Science and Engineering, vol. 5, no. 2, pp. 19-26, 2011.

[21] R. Bhatia, "Biometrics and Face Recognition Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 93-99, 2013.

[22] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," in Electronic Imaging 2002, Proceedings of SPIE, San Joes, USA, 2002, pp. 275-289.

[23] D. T. Meva and C. K. Kumbharana, "Comparative Study of Different fusion techniques in multimodal biometric authentication," International Journal of Computer Applications, vol. 66, no. 19, 2013.

[24] S. Kalra and A. Lamba, "A Survey on Multimodal Biometric," International journal of computer science and information technologies, vol. 5, no. 2, pp. 2148-2151, 2014.

[25] M. A. P. C. Mr. Rupesh Wagh, "Analysis of Mutlimodal Biometrics with Security Key," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). vol. 3, no. 8, pp. 1363-1365, 2013.

[26] A. Meraoumia, S. Chitroub, and A. Bouridane, "Multimodal Biometric Person Recognition System based on Iris and Palmprint Using Correlation Filter Classifier," in Proc. of the Second International Conference on Communications and Information Technology, Hammamet, Tunisia, June 26-28, 2012, pp. 782-787.

[27] M. Deriche, "Trends and Challenges in Mono and Multi biometrics," presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, Sousse, 2008. pp. 1-9.

[28] N. Geethanjali and K. Thamaraiselvi, "Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System," International Journal of Computer Applications, vol. 70, no. 14, pp. 17-23, 2013.

[29] D. Satyarthi, Y. P. S. Maravi, P. Sharma, and R. K. Gupta, "Comparative Study of Offline Signature Verification Techniques," International Journal of Advancements in Research & Technology, vol. 2, no. 2, pp. 1-6, 2013.

[30] G. Sathish, S. V. Saravanan, S. Narmadha, and S. U. Maheswari, "Multi-Algorithmic Iris Recognition," International Journal of Computer Applications, vol. 38, no. 11, pp. 13-21, 2012.

[31] K. Elumalai and M. Kannan, "Multimodal Authentication for High End Security," International Journal on Computer Science and Engineering, vol. 3, no. 2, pp. 687-692, 2011.

[32] B. Schouten and B. Jacobs, "Biometrics and Their Use in E-Passports," Image and Vision Computing, vol. 27, no. 3, pp. 305-312, 2009.

[33] M. Monwar and M. L. Gavrilova, "Multimodal Biometric System Using Rank-Level Fusion Approach," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,, vol. 39, no. 4, pp. 867-878, 2009.

[34] M. Soltane, N. Doghmane, and N. Guersi, "Face and Speech Based Multi-Modal Biometric Authentication," International Journal of Advanced Science and Technology, vol. 21, no. 6, pp. 41-56, 2010.

[35] F. Anwar, M. A. Rahman, and S. Azad, "Multibiometric Systems Based Verification Technique," European J. Scientific Research, vol. 34, no. 2, pp. 260-270, 2009.

[36] R. S. Choras, "Hybrid Iris and Retina Recognition for Biometrics," presented at the Image and Signal Processing (CISP), 2010 3rd International Congress on, Yantai,, 2010. pp. 2422-2426.

[37] Z. Huang, Y. Liu, C. Li, M. Yang, and L. Chen, "A Robust Face and Ear Based Multimodal Biometric System Using Sparse Representation," Pattern Recognition, vol. 46, no. 8, pp. 2156-2168, 2013.

[38] L. Lu and J. Peng, "Finger Multi-biometric Cryptosystem using Feature-Level Fusion," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp. 223-236, 2014.

[39] A. S. Makinde, Y. Nkansah-Gyekye, and L. S. Laizer, "Enhancing the Accuracy of Biometric Feature Extraction Fusion Using Gabor Filter and Mahalanobis Distance Algorithm," (IJCSIS) International Journal of Computer Science and Information Security, vol. 12, no. 7, pp. 1-8, 2014.

[40] P. A. KUMARI and G. J. SUMA, "A Novel Mutimodal Biometric Scheme or Personal Authentication," IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET) vol. 2, no. 2, pp. 55-66 2014.

[41] S. Kalra and A. Lamba, "Improving Performance by Combining Fingerprint and Iris in Multimodal Biometric," International Journal of Computer Science & Information Technologies, vol. 5, no. 3, pp. 4522-4525, 2014.

[42] A. Jain, K. Nandakumar, and A. Ross, "Score Normalization in Multimodal Biometric Systems," Pattern Recognition, vol. 38, no. 12, pp. 2270-2285, 2005.

[43] A. R. a. R. Govindarajanb, "Feature Level Fusion Using Hand and Face Biometrics," presented at the SPIE Conference on Biometric Technology for Human Identification II, Orlando, USA, 2005. pp. 196-204.

[44] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, "Likelihood Ratio-Based Biometric Score Fusion," IEEE Transactions on Pattern Analysis and Machine Intelligence,, vol. 30, no. 2, pp. 342-347, 2008.

[45] M. Nageshkumar, P. Mahesh, and M. S. Swamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image," (IJCSI) International Journal of Computer Science Issues, vol. 2, no. 4, pp. 49-53, 2009.

[46] A. Darwish, R. A. Elghafar, and A. F. Ali, "Multimodal Face and Ear Images," Journal of Computer Science, vol. 5, no. 5, p. 374, 2009.

[47] M. I. Razzak, R. Yusof, and M. Khalid, "Multimodal Face and Finger Veins Biometric Authentication," Scientific Research and Essays, vol. 5, no. 17, pp. 2529-2534, 2010.

[48] P. Dalka and A. Czyzewski, "Human-Computer Interface Based on Visual Lip Movement and Gesture Recognition," IJCSA, vol. 7, no. 3, pp. 124-139, 2010.

[49] M. Kawulok and J. Szymanek, "Precise Multi-Level Face Detector for Advanced Analysis of Facial Images," Image Processing, IET, vol. 6, no. 2, pp. 95-103, 2012.

[50] F. Alsaade, "Neuro-Fuzzy Logic Decision in a Multimodal Biometrics Fusion System," Scientific Journal of King Faisal University (Basic and Applied Sciences), vol. 11, no. 2, p. 14, 2010.

[51] F. CUI and G. Yang, "Score Level Fusion of Fingerprint and Finger Vein Recognition," Journal of Computational Information Systems, vol. 7, no. 16, pp. 5723-5731, 2011.

[52] M. Romaissaa and R. Abdellatif, "On Comparing Verification Performances of Multimodal Biometrics Fusion Techniques," International Journal of Computer Applications, vol. 33, no. 7, pp. 24-29, 2011.

[53] A. A. Paulino, "Contributions to Biometric Recognition: Matching Identical Twins and Latent Fingerprints," PhD degree of Computer Science, Michigan State University, 2013.

[54] H. Mehrotra, "On the Performance Improvement of Iris Biometric System," PhD, Departmant of Computer Science and Engineering, National Institute of technology Rourkela, Rourkela, Odisha, India, 2014.

[55] H. M. Sim, H. Asmuni, R. Hassan, and R. M. Othman, "Multimodal Biometrics: Weighted Score Level Fusion Based on Non-Ideal Iris and Face Images," Expert Systems with Applications, vol. 41, no. 11, pp. 5390-5404, 2014.

[56] D. Miao, Z. Sun, and Y. Huang, "Fusion of Multibiometrics Based on A New Robust Linear Programming," presented at the Pattern Recognition (ICPR), 2014 22nd International Conference on, Stockholm, 2014. pp. 291-296.

[57] A. Gambhir, S. Narke, S. Borhade, and G. Bokade, "Person Recognition Using Multimodal Biometrics," International Journal of Emerging Technology and Advanced Engineering (IJETAE), vol. 4, no. 4, pp. 725-728, 2014.

[58] M. Monwar and M. Gavrilova, "Secured Access Control Through Markov Chain Based Rank Level Fusion Method," presented at the in proc. of 5th Int. Conf. on Computer Vision Theory and Applications (VISAPP), Angres, France, 2010. pp. 458-463.

[59] A. Kumar and S. Shekhar, "Personal Identification Using Multibiometrics Rank-Level Fusion," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, , vol. 41, no. 5, pp. 743-752, 2011.

[60] M. MONWAR, "A Multimodal Biometric System Based on Rank Level Fusion," PhD, Department of Computer Science University of Calgary, ALBERTA 2012.

[61] S. A. S. DzatiAthiarRamli, AiniHussain, "A Multibiometric Speaker Authentication System with SVM Audio Reliability Indicator," International Journal of Computer Science & Information Technologies (IAENG), vol. 36, no. 4, pp. 313-321, 2008.

[62] S. K. Grewal, "A Composite Approach for Biometric Template Security," International Journal and Conference Service Center (IJCSC), vol. 5, no. 1, pp. 170-176, 2014.

[63] I. A. Saleh and L. M. Alzoubiady, "Decision Level Fusion of Iris and Signature Biometrics for Personal Identification using Ant Colony Optimization," International Journal of Engineering and Innovative Technology (IJEIT), vol. 3, no. 11, pp. 35-42, 2014.

[64] A. Naghate, M. Sahu, P. Bhange, S. Lonkar, P. Wankhede, and Y. Bute, "Implementation of Multibiometric System Using Iris and Thumb Recognition," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 3, pp. 932 – 940, 2014.

[65] C. Lupu and V. Lupu, "Multimodal Biometrics for Access Control in An Intelligent Car," presented at the Computational Intelligence and Intelligent Informatics, 2007. ISCIII'07. International Symposium on, Agadir, 2007. pp. 261-267.

[66] A. C. Panda, "Parallel Algorithms for Iris Biometrics," M.Sc., Department of Computer Science and Engineering, National Institute of Technology Rourkela, Odisha, India, 2011.

[67] K. Veeramachaneni, L. Osadciw, A. Ross, and N. Srinivas, "Decision-Level Fusion Strategies for Correlated Biometric Classifiers," presented at the Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, Anchorage, AK 2008. pp. 1-6.

[68] L. Shen, L. Bai, and Z. Ji, "FPCODE: An Efficient Approach for Multi-Modal Biometrics," International Journal of Pattern Recognition and Artificial Intelligence, vol. 25, no. 02, pp. 273-286, 2011.

[69] S. M. Islam, R. Davies, M. Bennamoun, R. A. Owens, and A. S. Mian, "Multibiometric Human Recognition Using 3D Ear and Face Features," Pattern Recognition, vol. 46, no. 3, pp. 613-627, 2013.

[70] W. Almayyan, "Performance Analysis of Multimodal Biometric Fusion," PhD, Faculty of Technology, De Montfort University, England, United Kingdom, 2012.

[71] A. A. Fathima, S. Vasuhi, N. N. Babu, V. Vaidehi, and T. M. Treesa, "Fusion Framework for Multimodal Biometric Person Authentication System," IAENG International Journal of Computer Science, vol. 41, no. 1, pp. 1-14, 2014.

[72] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," IEEE Transactions on Image Processing, , vol. 23, no. 2, pp. 710-724, 2014.

[73] V. SIREESHA and K. SANDHYARANI, "Multimodal Biometric System Using Iris-Fingerprint: An Overview," International Journal of Engineering Sciences Research-IJESR, vol. 02, no. Special Issue 01, pp. 1342-1349, 2013.

[74] A. A. Albahdal and T. E. Boult, "Problems and Promises of Using the Cloud and Biometrics," presented at the 11th International Conference on Information Technology: New Generations (ITNG)2014,, 2014. pp. 293-300.