ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 10(44), DOI: 10.17485/ijst/2017/v10i44/120575, November 2017 ISSN (Online) : 0974-5645

A Survey on Different Levels of Fusion in Multimodal Biometrics

Suneet Narula Garg[1]*, Renu Vig[1] and Savita Gupta[2]

[1]Department of Electronics and Communication Engineering, University Institute of Engineering and Technology, Panjab University, Gharuan – 140413,s; suneetgarg1979@gmail.com, enuvig@hotma il.com
[2]Department of Computer Science and Engineering, University Institute of Engineering and Technology, Panjab University, Gharuan – 140413, Punjab; savita2k8@yahoo.com

Abstract

Objectives: In this paper, we have compiled a survey which is based on the comparison of various fusion techniques which are most commonly used in a multimodal biometric system. **Methods/Statistical Analysis:** The Multimodal Biometric systems are providing identification and human security over last few decades. We have also discussed various techniques used in different level of fusion with the objective of improving performance and robustness at each level of fusion. **Findings:** The extensive study shows that almost perfect accuracy rates can be achieved by multimodal fusion based protection processes. A comparison has also been made depending upon fusion levels, acceptance rates and accuracy levels. It is concluded from the fact that a combination of two identities when fused together, can reach very high accuracy levels. **Applications**: The survey given in this paper will help researchers in understanding levels of fusion in multimodal biometrics.

Keywords: Accuracy, Fusion Level, Fusion Techniques, Multimodal Biometric System

1. Introduction

Biometrics is used in the field of computer security. The behavioral and physical characteristics of an individual are measured and analyzed statistically in the biometric technology[1]. This technology is majorly used for access control or identification of people who are kept under surveillance. The primary objective of authentication using biometric system is based on the fact that every human being is distinctive and everyone can be identified by her or his unique behavioral or physical traits. Biometric modalities or identifiers can be categorized into two types:

i. Physiological traits: The physical characteristics, composition or shape of the body. These include fingerprints, palm print, face, hand, retina, DNA, iris scan or ear features. Every human being on this planet is proven to have distinct fingerprints and DNA. The iris of each human being is also considered to be unique[2]. These individual physical features can identify and verify any person using a biometric authentication system.

ii. Behavioural traits*:* Certain identifiers are based on the behavioral patterns of an individual, most of these are observed over time like typing rhythm (keystrokes), gait or voice and handwriting. The behavioural patterns when used alone are not secure enough so they are used in combination with the physical identifiers for enhanced security[3]. Rather than using a single modality, using an additional behavioural trait is safer like using fingerprint and voice together[4]. All biometric security systems use similar basic components for operation[5]. A *sensor* is used for identification of the required modality, computer to read, later store the information and *software* to analyze characteristics, translating them into code or graph and finally performing the deciding comparison. Any biometric system will use three simple steps in their regular working process: Enrolment, Storage and Comparison[6].

**Author for correspondence*

When a system is installed for its first use, the initial step is ***Enrolment*** where the system requires every concerned person to input an identification number or name along with the required modality input. The modality (for example fingerprint) is required to be scanned and input into the system via a scanner or any other relevant input device for raw data.

The process is explained using Figure 1, which depicts that the image of fingerprint trait as the *biometric sample* is taken and stored in *image archive*. Each new identity created goes into the ***template Storage*** along with the corresponding fingerprints. Contrary to popular belief the complete recording or image is not stored as is into the database. Instead the system converts it into a code or graph so that the system can understand or read it easily later.

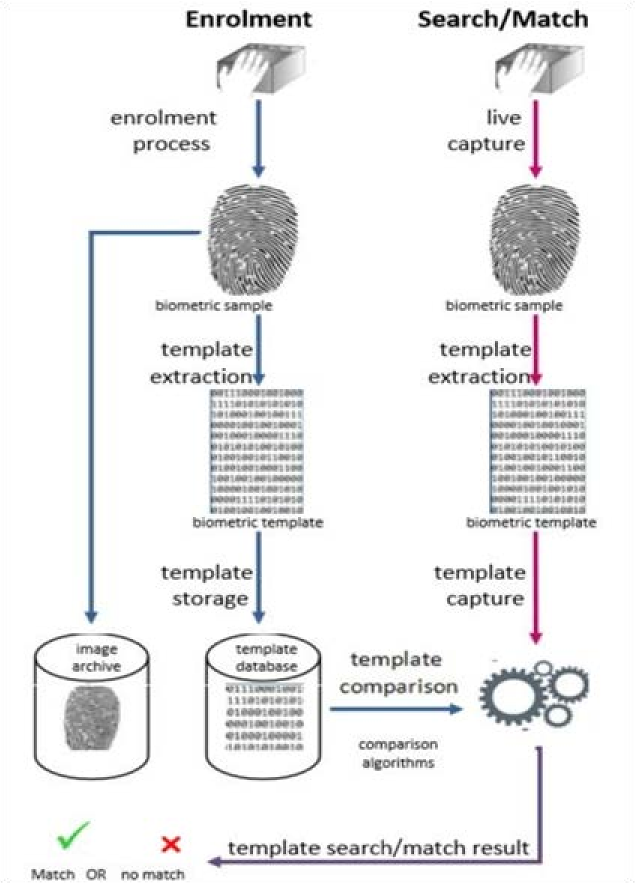

Figure 1. General biometric process.

After the initial enrolment process is done, the fingerprint and related names of the people authorized to enter through that system are stored in *template database*. Now, when ever an enlisted person comes for the live capture match or ***Comparison process*** then that person is either accepted or rejected. The comparison process can be explained using Figure 1, here a person enters the biometric sample via fingerprint scanner for live capture. The extracted template is sent for comparison with the template stored in the database. These can be compared using various image-based or comparison-based algorithms[7].

1.1 Multimodal Biometric System

In a biometric system using single identity there are many drawbacks like *Acceptability*, *Performance* and *Circumvention*. The data sensor might encounter performance issues like insufficient light or outside noise. The system might not accept faulty images or mix images which are not distinct enough. Certain physical traits like face recognition might not have enough uniqueness, so the computer system can accept two similar faces of different people as one[8]. Some people with bad intentions might try to circumvent a simple biometric security for bad ulterior motives. To avoid all sorts of problems in the traditional authentication system a new system using multiple recognition traits was required[9]. To overcome the limited freedom degree in the uni-modal system, a cheap more reliable solution using fusion techniques was developed known as ***Multimodal Biometric System***.

The multimodal modal system uses two or more traits together. It could be a combination of physical and behavioural traits or multiple physical modalities together. This reduces the risk of any spoofing and makes it tricky for an intruder to copy, steal or fake multiple identities.

1.2 Performance Parameters

The parameters to define the effectiveness of any biometric security system can be stated as False Acceptance Rate (FAR) and False Rejection Rate (FRR). The recognition performance of any good multi-modal biometric system will depend on these parameters.

1) False Acceptance Rate: During the authentication process of a biometric system if a non-authorized used is accepted as an authorized user, it is called false acceptance. A low false acceptance rate ensures a secure system.

2) False Rejection Rate: If a valid user, who is already enrolled into the system, is rejected by the system during live capture, it is false rejection. The rate at which genuine users are rejected by a biometric system is referred to as false rejection rate, for good system performance this rate needs to be kept very low.

3) Equal Error Rate: EER is FAR: FRR ratio, it is the value when FAR is equal to FRR. For keeping the value of EER a logical threshold needs to be selected, this is crucial to keep the system running with good performance[10].

4) Genuine Acceptance Rate: How many times a genuine user is accepted is measured by the GAR rate, it needs to be very low in a good system[11].

Some other parameters which might affect the final accuracy of a system are *Failure to Enrol Rate* (FER) and *Failure to Capture Rate* (FCR).

1.3 Fusion Level Types

In[12] a classification of information level fusion of any biometric system based on two major types: *Pre Classification Fusion and Post Classification Fusion* (explained in Figure 2). The Pre Classification type of fusion consists of combination of the biometric raw data prior to any application of some matching algorithm or classifier. On the other hand, Post- Classification category of fusion refers to the combination of information after all classifier decisions are obtained.

In a multimodal system, there are two broad categories of fusion. As explained above, these categories can also be explained with different names. First are techniques which are applied to *fusion-before-matching* and second is *fusion- after-matching*[13]. When fusion process is done before matching the live template with the template stored in database, it is fusion before matching. The data-sensor and feature-extraction levels are under this category.

1.3.1 Pre-classification fusion

When the biometric information is integrated before matching the templates, it is called pre-classification or fusion-before-matching[14]. It has the following two fusion levels:

1) Data-Sensor Level: For data sensor level fusion, there has to be multiple instances of the required identities. For example, if three biometric sample are taken from a fingerprint scanner, these three are combined together to form one result. The instances might be taken from one input source or from three different sources. Now, the fused result will be compared with the live fingerprint scan. It is important that the data to be fused should be of the same type, like two images from two different cameras which will be fused need to be of the same resolution. Data sensor is also called *image-level fusion* or *data-level fusion.*

2) Feature-Extraction Level: Information is extracted using feature extractors from the sensors and then depending on the type of modality it is further stored into vectors. To form a base for the next step in the process a joint feature vector is created by combining all the individual feature vectors. The feature sets are obtained by applying biometric algorithms, to get a single feature set from many sets reduction, normalization and transformation is applied. To map the feature set into a common domain location and scale of feature set is modified, this can be done by using techniques like Min-Max or Median normalization. For reducing the dimensions of a feature set, transformation techniques like Forward Sequential Selection, PCA or Sequential Backward Selection are used[15]. Fusion at feature level refers to the combination of diverse feature vectors which can be calculated by either employment of multiple algorithms for feature extraction or utilization of multiple sensors on same data collected by sensors[16]. A single feature vector resultant could be calculated as an average of weights of all the feature vectors individually in case feature vectors used are homogeneous i.e. multiple impressions of finger print of one user's finger.

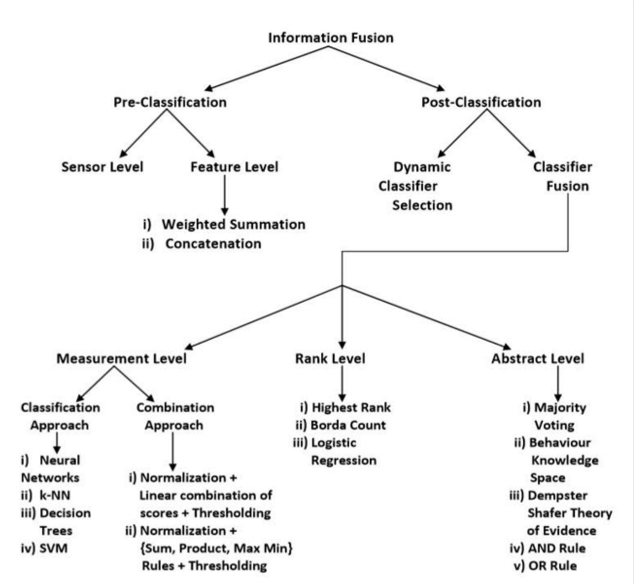

Figure 2. Fusion levels.

On the other hand, if feature vectors used are not homogeneous then concatenation can be done to obtain the final resultant feature vector. Non-homogeneous feature vectors are obtained when different techniques for one feature extraction are used, or when feature vectors from different modalities like hand geometry and face are being used. The concatenation process cannot be conducted if the feature sets used are not compatible with each other, like combining Eigen face coefficient with finger print minutiae is not possible.

It is believed that any biometric system that integrates biometric information at early stages of processing will yield more effective results as compared to a system that performs integration at later stages. It is obvious that the features will contain more rich information regarding the raw input biometric information than the output decision or matching score of a matcher/ classifier, combination at the feature level will usually provide better identification results than any other level of biometric integration process[17].

However, combination at feature level is very difficult to accomplish in practice for the reason of the following causes:

(i) The association among the feature elements of diverse biometric systems might not be identified. In such cases where relationships are already acknowledged in advance, to discard such features proper care should be taken as such features are correlated highly. This will require feature selection algorithm application before the classification process.

(ii) Concatenation of any feature vectors might produce a single feature vector which has an extremely large dimensionality that leads to the "curse of dimensionality" situation. Although, it is a very general issue faced in many pattern recognition methods, this problem is harsher in a biometric application because of cost, effort and time involved in the collection of large amount of good biometric data.

(iii) Many commercial biometric authentication systems might not provide proper usage rights to one or all feature vectors that they are using in their security products. Because of this, only some researchers have been able to study the integration at feature levels and many of them mostly prefer the post classification schemes of fusion[18].

1.3.2 Post-classification Fusion

The methods of information integration after the matcher/ classification stage are categorized into four different types, namely: Dynamic selection classifier, match-score level fusion, fusion at decision level and rank level fusion.

1) *Dynamic Classifier Selection:* This scheme will choose the result of a classifier that has the highest probability of giving a correct decision for any particular input pattern. This approach is also called 'the winner-takes- it-all approach' meanwhile the device performing such a selection is called an associative switch.
2) *Matching-Score Level:* To initiate this process an equivalent matching score is required which can be obtained by matching the features scanned. The final recognition match score result is obtained by combining all the individual matchers[19]. The scalar result can be reached by using methods like similarity score, distance score, linear or non linear weighing. The results from each matcher belonging to an individual modality are combined at this stage to become one.
3) *Decision Level:* Now each sub-system has autonomously completed the feature extraction process, matching score level and final recognition. This is *abstract-level fusion* where Boolean function strategies are used. The names of some commonly used methods are Majority Voting, Weighted Majority Voting, AND, OR, Bayesian Decision Fusion etc. After a decision is reached by all the individual *Classifiers* then only a final decision can be reached[20].
4) *Rank Level:* For fusion that is done at rank level[21], the final result of every biometric matcher that is a possible matches sub-set arranged in decreasing confidence order. Ho et al. describes three techniques for combination of ranks that belong to all different matchers. Every possible match-score will be assigned minimum (highest) rank that is computed by varying matchers in the highest rank technique. A firm ranking order is reached by breaking ties randomly and the final result is decided depending upon the combination of ranks. For calculation of combined ranks, the individual matchers have a sum of rank that is used by the Borda count technique.

To determine the weight logistic regression method is used and to calculate the sum weight of individual ranks logistic regression technique is used which is actually a generalization of Borda count technique.

1.4 Methods for Multimodal Fusion

There are certain techniques for multimodal fusion as given in Figure 3 that can be categorized into three types:

Rule-based techniques, classification based techniques and estimation-based techniques[22].

This classification of methods depends on the basic structure of these techniques and essentially it means the categorization of problem areas, like an issue of parameter estimation can be solved using estimation based techniques. On the other hand, the problems based on obtaining a result depending on a certain observation is solved using rule based or classification based technique. However, if varying types of modalities are observed, then before a classification decision or estimation is made, a fusion of all observation scores is required. All techniques are explained below:

(1) Rule-based fusion techniques:

The fusion techniques that are rule-based will include an array of some basic rules that combine multimodal information. Some statistical rule based techniques are used in this case such as product and sum based fusion (linear weighted), MIN, MAX, majority voting, OR, AND. All these rules are custom-defined and their construction is specifically based on application perspective. The rule based technique will generally perform well if the temporal alignment amongst different modalities has good quality.

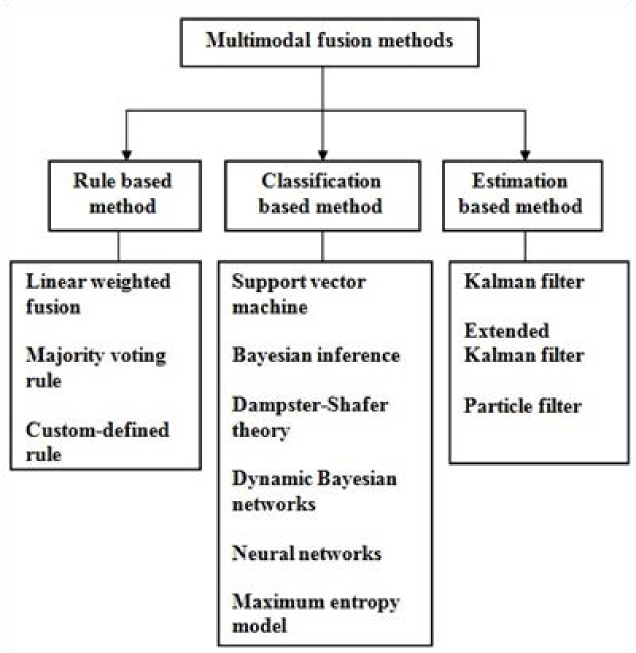

Figure 3. Types of fusion methods.

(2) Classification-based fusion techniques:

These types of techniques include a wide array of classification methods which have been utilized for classification of the multi modal observations into one of the classes that are pre-defined. The techniques in this group are maximum entropy models, neural networks, dynamic Bayesian network, Dempster–Shafer theory, Bayesian inference and Support vector machine[23].

These techniques can be noticeably further divided into two methods namely, discriminative and generative models from the perspective of machine learning. For instance, Dynamic Bayesian network and Bayesian inference are both generative representations, whereas neural networks and supportive vector machine both are discriminative representations.

(3) Estimation-based fusion techniques:

This estimation based category[24] will include particle filter fusion techniques, extended Kalman filter techniques and the Kalman filter method. All these mentioned techniques are mostly used for better estimation of the state of any moving entity based on multi modal information. For instance, the job of tracking an object requires the fusion of multiple modalities like video and audio for estimation of final object position.

4. Research related to Multibiometrics

The making of this survey paper has an extensive background study on the existing techniques proposed by various researchers. A secure and efficient multimodal biometric system is expected to have low False Acceptance and False Rejection Rates. In a multi biometric modal[25] two or more traits belonging to an individual are used, such usage ensures a more secure system. The two modalities used are combined together in the form of a code or graph to be stored into the database. Whenever required, it is retrieved from there for matching with live scan. The input is saved in the form of graph or code so that it becomes easy to understand by the software. The input saved is a single file or single component. This file is the final result obtained after the whole biometric security process. The modalities are processed one-by-one through each level starting from sensor, feature and then match score. This combining of modalities is actually the fusion process; there are many techniques available for the fusion of modality templates at each of this stage. The image level fusion is done here at the first stage, where all the raw data as images are fused together using different security methods[26].

For fusion at the stage of feature extraction, the images are converted into vectors and the vectors are combined together here to form one. In match score level the fusion results are in scalar form. Decision level fusion is also possible. This research is based on many proposed systems or surveys which consist of various fusion levels implemented at different levels. Much research has been done on various possible combinations of biometric traits. Combining two physical traits, one physical and one behavioural or both behavioural traits, the possibilities are endless.

In[27] uses the combination of Iris and Fingerprint which uses feature level fusion. There could be image inconsistencies in the snap shot of iris, so to avoid this situation the eyelashes and eyelids are removed from the image and then it is further processed. Delta and core points are extracted using a unified viewpoint for determination of Gabor function. Gabor filter is used for vector feature extraction from fingerprint and iris and then they are combined. The final match score is generated by HD (Hamming Distance), this system is tested on 50 people. The calculation speed is better which leads to less execution time and the accuracy is very good, nearly 90%. The FAR and FRR is also very low as depicted in Table 1. The fingerprint database is core delta detection based using singularity for detection. The iris recognition and detection is done using the centre circular region. Ideally the speed of the proposed system should have been *5 times quicker than other systems*. However, such a system required a large computational cost. So a within budget system was tested which was *2 to 3 times faster* as compared to its counter parts.

In[28], in this there is multi instance iris recognition and fusion at decision level as well. Outside disturbances can cause problems in proper working of a multimodal system; to overcome this, a system is proposed which is robust to occlusion and noise. The proposed SMBR technique (Sparcity based Multi Biometric Recognition) gives an accuracy of 98.6 with error and 98.7 without considering any error. That is in ideal conditions.

Another proposed system[29] using palm print and iris fusion at feature level has a very high accuracy of 99.2%. The proposed security system has a fusion technique which is wavelet based and Gabor texture is extracted from pre-processed images. Since, all the feature vectors attained are different in size but there might be correlation among equivalent images. Therefore, the stored templates are matched with the vectors by KNN classification. This system has a rejection rate of only 1.6%, working on match level. This system gives an almost perfect accuracy with 125 users in database. It would be interesting to observe the results of this system using original newly created biometric database.

In[30] proposes a multimodal biometric system which combines iris and fingerprint modalities at feature level by using pre-processed images of these modalities. The system has good performance with an accuracy of 91%. The FRR is 5.3 percent and FAR is 10 percent. A cryptography key is generated which incorporates biometric features. The cryptographic security key generated is user specific. It is a complex process and one small glitch in the key generation method can jeopardize the whole biometric process.

In[31] presents a multi-biometric system with fusion at feature level. The proposed system uses a simple algorithm for fusion of palm prints and face modalities. The fusion process when done on feature level is always required to give more precise result in comparison to fusions at other level. This is expected because the feature set is supposed to contain rich and relevant information about the evidence captured. The GAR (Genuine Acceptance Rate) for images of palm print is about 81.48 percent whereas; the GAR which uses the images of face modality is 88.88 percent. When fused together, there is found to be substantial increase in the overall accuracy. With FRR of 1.2 percent and FAR of 0.5 percent, the accuracy is 95 percent. A thorough go-through tells that there is a limitation to this process. The data acquisition technique used is developed by amateurs who have used basic techniques. These techniques are obsolete now and not very accurate either.

In[32] combines palm print and fingerprints for fusion at feature level using image based techniques which depend up on wavelet techniques. Feature extraction is done using IG or information gain while min.max approximation is also used. The accuracy attained for this process was 98.43 percent with acceptance rate of 1.02 percent and rejection rate of 0.9 percent only. Since both modalities used are based on the hand of an individual, it can cause a problem if the person to be enrolled does not have hands. This is a rare case but a possibility which needs to be kept in mind. Another drawback could be wrinkled hands which can cause problem with proper scanning.

In[33] combines fingerprint and palm print modalities for fusion after feature extraction in a multimodal bio-

Table 1. Fusion level accuracy

Reference	FUSION	DATA SET	DATABASE Used	FRR (%)	FAR (%)	Accuracy (%)
[27]	Feature level	Iris, Fingerprint	Newly created iris and finger print database	4.30	0	90.00
[28]	Feature level	Iris, Fingerprint	WVU multimodal dataset	0.00	0.01	98.70
[29]	Feature level	Iris, Palm print	IITK Iris database, PolyU palm print database	1.60	0.00	99.20
[30]	Feature level	Iris, Fingerprint	CASIA Iris database, publically available fingerprint databases	5.30	10	91.00
[31]	Feature level	Face, Palm print	captured using Canon Power shot SX 120 IS	1.20	0.50	95.00
[32]	Feature level	Fingerprint, Palm print	FVC 2002 DB4B fingerprint dataset, Hong Kong PolyU palm print database	0.90	1.02	98.00
[33]	Score level	Fingerprint, Palm print	PolyU finger print database	1.10	0.20	87.00
[34]	Score level	Iris, Fingerprint	Iris CASIA database, fingerprint NIST	2.46	1.23	97.00
[35]	Score level	Iris, Fingerprint	UBRIS Iris database, (FVC) 2002 DB2 fingerprint database	0.50	0.30	99.50
[36]	Score level	Face, Palm print	Captured using digital camera	0.80	2.40	97.00
[37]	Score level	Face, Finger vein	Newly created low res. web cam for face and controlled environment for finger veins	0.23	0.50	95.00
[38]	Score level	Fingerprint, Finger vein	Newly created using Zhong Zheng Inc. fingerprint scanner & finger vein capture with a Wuhan University creation	0.75	1.20	95.00
[39]	Decision level	Iris, Fingerprint	Pheonix Iris database, Futronics FS88 fingerprint scanner for texture feature extraction	0.00	0.00	84.40
[40]	Decision level	Face, Palm print	Public domain face databases, MSU fingerprint database	1.80	1.00	92.00
[41]	Decision level	Iris, Fingerprint	CASIA Iris database, NIST fingerprint database	2.00	2.00	98.00
[42]	Decision level	Face, Voice	BANCA bimodal database	3.00	1.10	87.00
[43]	Decision level	Face, Ear	A newly created face, ear database using digital camera	4.00	0.00	96.00

metric authentication system. In this system Gabor filter is used for feature extraction, in this case 87% was the recognition rate. This system has FRR% of 1.1 and 0.2FAR. One possible drawback of this biometric system is that both the biometric identities used are related with hands, palm print and fingerprint. So, when a person ages wrinkles developed on hands can cause hindrance in proper scanning of the modality.

In[34] proposes a system which has a combination of fingerprint and iris modalities in which score level fusion is used. The proposed system is a two-level approach in which the modalities are matched at level-I and if they do not match then only level-II is deployed. This system has an accuracy of 97%, the FAR is 1.23 and FRR is 2.46%. When confusion matrix is used with 50 templates already existing in the database, the biometric system identifies 48 out of 50 as true positives. The other 50 in the matrix are new entries that are not earlier known to the system and it identifies 49 out of 50. The identification of these true negatives led us to believe that this system has high recognition accuracy.

In[35] explains that security should be the sole purpose of any multimodal biometric system. This system works on match score level fusion. With a very high accuracy of

99.5 %, low acceptance rate of 0.3 and 0.5 (FAR and FRR respectively), this is a fingerprint and iris based biometric system. The proposed system uses the FVC 2002 DB2 fingerprint database and UBRIS iris database. The system takes 5 images each of iris and fingerprint, in total theses 10 images per person will be used for user identification. These tests are performed on a set of 10 people, so the successful working of this system on a large group of population is yet to be approved.

Table.1. Fusion Level Accuracy

In[36] proposes a system combining the face image and palm prints in which fusion at score level is used. The ultimate result of this system is actually very encouraging, with an accuracy of 97%. This combination has an acceptance rate of 2.4% and rejection rate of 0.8%. This is a multimodal biometric system using face and palm prints, which achieves a very high accuracy. But, in case of any other modality combination, this technique might not attain such high accuracy results.

In[37] combines finger vein and face which utilizes fusion at score level leading to improvement in system robustness. CSLDA or Client Specific Linear Decimation Analysis is used for score level fusion of the identities. Weight fuzzy fusion is used for the combination of finger vein and face modalities. The recognition rate of the system is 95 percent with very low rejection rate of 0.23 percent and acceptance rate of 0.05 percent. The database used for this security authentication system is newly created using a low resolution web camera for capturing face images. Thirty-five CAIRO staff members gave their contribution for creating this database. The finger vein images were also taken in controlled environment. There is a big lack of good quality available database for finger veins, which ultimately led them to create a new dataset which might not be as accurate.

In[38] combines finger vein and fingerprint with fusion at score level. First the individual recognition rate is calculated which 95.3% for fingerprint and 93.72% is for finger vein. After fusion, the accuracy percentage is 98.74 with acceptance of 1.2% and rejection rate of 0.75%. The database used was created using an optical fingerprint scanner which was developed by Zhong Zheng Inc. The finger vein database was also made newly using images by a device designed by a joint lab for Intelligent Computing and Intelligent systems of Wuhan University. This proposed system uses a small database to reach the final results. A larger dataset is required to ensure to ensure proper working of the proposed biometric system.

In[39] has another feature level extraction system example with hybrid wavelet system for texture extraction. This system has an accuracy of 84.4% when FAR and FRR are ideally taken as 0%. In this proposed system different combinations of hybrid wavelets is considered, kekre wavelets give the highest CCR% with better capability of extracting texture information. Biometric fusion using multi-algorithmic method does not give accuracy as high as other techniques like multi-sensor, multi-sample or multi-instance.

Decision level fusion is used in this proposed system by[40] which uses face and palm print images for fusion. The fusion at decision level of feature extractions from fingerprints and face in this process is done in a very effective way which improves the performance by a big margin. The acceptance rate is 1 percent, rejection rate is 1.8 percent and the overall accuracy is 92 percent. This approach might not work well if a few correct face matches need to be selected from millions of templates in a database. The decision fusion used might not be as accurate for other modality combinations as with face and fingerprint here. In[41] performs a multi-modal biometric system process by the fusion of iris and fingerprints, this system uses fusion at decision level. For fusion fuzzy logic technique is utilized which results in better accuracy and performance with 2 percent FAR, 2 percent FRR and 98 % recognition rate. This rate is very high for a process that follows decision-level fusion. The iris recognition has more weight in the final outcome. A code is generated with 80% iris code weight and only 20% fingerprints.

In[42] states that a combination of speech and face can be performed with fusion at decision level. The recognition rate of the system is 87 percent with performance parameters FRR of 1.1 percent and FAR of 3.0 percent. The information used is from a uni-modal reliability estimation that is later used for fusion of modalities. This does impose the reliability but might cause problems to other.

In[43] depicts a combination of ear and face images, these images go through a module for quality check which reduces FRR. The recognition result is improved when both the modalities are fused together; it is up to 96 percent. The parameters are also improved hugely; acceptance rate is 0 percent and rejection rate is only 4 percent in this case. The proposed system uses ear as a biometric identity and it can cause a problem if the ear is covered with some cloth, cap or scarf. This can cause a big issue with passive identification, so this system needs a lot of improvement if it needs to be used for security surveillance[44].

Such work helps in promoting research in the field of multimodal biometric authentication systems. Observation of various proposed systems here leads us to believe that a biometric system using multiple modalities gives high accuracy, robustness and good overall performance[45–48].

2. Conclusion and Future Scope

Biometric systems are already being used in many huge corporate and national security based organizations. *Biometric enabled smart cards* are used by authorized people for access control and security. These smart cards have the embedded biometric information of the individual carrying them. A multimodal biometric system using multiple instances like *Iris and Fingerprint together* has the highest level of accuracy. As in the survey above various fusion techniques are discussed which can be applied at any level from the four fusion levels. In the researches discussed above majority of them use fusion at a single level, which ever level it is. So, if fusion is conducted at any two levels in one multimodal biometric system, it will lead to better performance. *Fusion at more than two levels* can also be done, or at all four levels. This might create a very complex system but with the advancement in the efficiency of computational resources attention could be paid towards this. Further research on this matter can be very fruitful and lead to more secure and accurate systems.

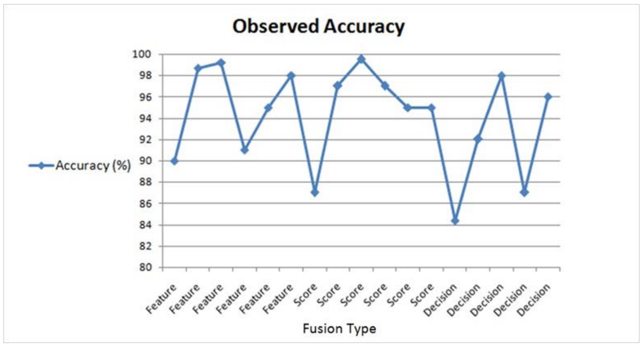

Figure 4. Observed accuracy percentage.

This is a comparison of feature, score, match and decision level fusions performed on biometric modalities. The aim of a multimodal biometric system is to improve accuracy over a uni-modal system. By some earlier work in the field of biometrics, it is observed that good dataset or existing databases need to be used, as they are the basis for all research in this field. A good quality database utilized in a multi-biometric will lead to results with better accuracy given in Figure 4.

It is observed that *feature-level fusion* is very commonly used in multimodal biometric systems. Another observation clearly shows that majority of authentication systems that use the combination of *Iris-Fingerprint* modalities result in the highest recognition percentages. The accuracy percentage range is between *85%-99% range*, which is very commendable. This depicts that it is a very secure combination.

It is explained above in detail how fusion at an earlier stage is the best for multi modal systems and this survey concretely puts forward this point. *The amount of information goes on decreasing as one proceeds from sensor level to decision level.* So, a Multi Biometric System that fuses information at an early processing stage will yield more promising results. Sensor fusion addresses the problem of noise in sensed data because of improper maintenance of sensors. More work can be done in the future to make fusion at initial levels easy by removing existing hindrances. Such improvements will lead to the development of more accurate and secure biometric systems.

3. References

1. Maheswari MAP, Ancy S, Devanesam KEP. Biometric identification system for features fusion of iris and fingerprint. Recent Research in Science and Technology. 2012; 4(6):1–4.
2. Choudhari P, Hingway SP, Sheeja S, Suresh, Wagh A. Fusion of iris and fingerprint images for multimodal biometric identification. IOSR Journal of Engineering. 2014 Aug; 4(8):1–4.
3. Marasco E, Johnson P, Sansone C, Schuckers S. Increase the security of multi biometric systems by incorporating a spoofing detection algorithm in the fusion mechanism, Springer Berlin Heidelberg, Italy; 2011. p. 309–18.
4. Barde S, Khobragade, Singh R. Authentication Progression through Multimodal Biometric System, International Journal of Engineering and Innovative Technology. 2012 Sep; 2(3):255–8.
5. Wayman JL, Jain AK, Maltoni D, Maio D. Biometric systems: Technology, design and performance evaluation. Springer-Verlag New York, Inc. Secaucus, NJ, USA; 2004.
6. He M, Horng S, Fan P, Run R, Chen R, Lai J, Khurram M, Octavius K. Performance evaluation of score level fusion in

multimodal biometric systems. Pattern Recognition. 2009 Nov:1–12.

7. AlMahafzah H, Imran M, Sheshadri HS. Multibiometric: Feature level fusion using FKP Multi Instance Biometric. International Journal of Computer Science Issues. 2012 Jul; 9(4):1–8.
8. Sharma S, Sodhi JS. Implementation of biometric techniques in social networking sites. International Journal of Security and Its Applications. 2014; 8(6):51–60.
9. Atrey PK, Hossain MA. Multimodal fusion for multimedia analysis: A Survey. Multimedia systems. 2010; 16(6):345–79.
10. Peng D, Zuo X, Wu J, Wang C, Zhang T. A Kalman Filter based information fusion method for traffic speed estimation. Power Electronics and Intelligent Transportation System (PEITS); 2009.
11. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems For Video Technology. 2004; 14(1):4–20. Crossref
12. Sanderson C, Paliwal KK. Information fusion and person verification using speech and face information. Research Paper IDIAP-RR 02-33, IDIAP; 2002.
13. Sankar SP, Dinakardas CN. Multimodal biometric authentication system based on high level feature fusion approach. European Journal of Scientific Research. 2012; 84(1):55–63.
14. Thomas T, Babu HK. A novel fake detection system for biometric modalities. International Journal of Advanced Research in Computer Science and Engineering. 2015; 5(4):439–44.
15. Soliman H, Mohamed AS, Atwan A. Feature level fusion of palm veins and signature biometrics. International Journal of Video and Image Processing and Network Security. 2012 Feb; 12(1):1–12.
16. Mahoor MH. A multimodal approach for face modelling and recognition. IEEE Transactions on Information Forensics and Security. 2008 Sep; 3(3):431–40. Crossref
17. Ben-Yacoub S, Abdeljaoued Y, Mayoraz E. Fusion of face and speech data for person identity verification. IEEE Transactions on Neural Networks. 1999; 10(5):1065–75. Crossref. PMid:18252609
18. Ross A, Jain AK. Information fusion in biometrics. Pattern Recognition Letters. 2003; 24(13):2115–25. Crossref
19. Jain A, Nandakumar K, Ross A. Score normalization in multimodal biometric systems. Pattern Recognition Society. 2005:2270–85.
20. Garje PD, Agrawal SS. Multimodal Identification System. IOSR Journal of Electronics and Communication Engineering. 2012; 2(6):1–5.
21. Ho TK, Hull JJ, Srihari SN. Decision combination in multiple classifier systems. Pattern Analysis and Machine Intelligence. 1994 Jan; 16(1):66–75. Crossref
22. Gagandeepkaur, Mittal AK. A new hybrid wavelet based approach for. International Journal of Innovative Research in Science, Engineering and Technology. 2015:19034–43.
23. Dhriti, Kaur M. K-nearest neighbor classification approach for face and fingerprint at feature level fusion. International Journal of Computer Applications. 2012; 60(14):13–17. Crossref
24. Hong L, Jain AK. Integrating faces and fingerprints for personal identification, IEEE Transactions on PAMI. 1998; 20(12):1295–307. Crossref
25. Radha N, Kavitha A. Rank level fusion using fingerprint and iris biometrics. Indian Journal of Computer Science and Engineering. 2012 Jan; 2(6):1–7.
26. Tripathi KP. A comparative study of biometric technologies with reference to human interface. International Journal of Computer Applications. 2011 Jan; 14(5):1–6. Crossref
27. Gawande U, Nair SR, Balani H, Pawar N, Kotpalliwar M. A high speed frequency based multimodal biometric system using iris and fingerprint. International Journal on Advanced Computer Engineering and Communication Technology. 2012; 1(2):1–8.
28. Shekhar S, Patel VM, Nasrabadi NM, Chellappa R. Joint Sparsity-based robust multimodal biometrics recognition. European Conference on Computer Vision; 2012. p. 365–74. Crossref
29. Gayathri R, Ramamoorthy P. Feature level fusion of palm print and iris. International Journal of Computer Science. 2012 Jul; 9(4):1–10.
30. Jagadessan K, Duraisamy. Secured cryptographic key generation from multimodal biometrics: Feature level fusion of fingerprint and iris. International Journal of Computer Science and Information Security. 2010; 7(1):296–305.
31. Bokade GU, Sapkal AM. Feature level fusion of palm and face for secure recognition. International Journal of Computer and Electrical Engineering. 2012; 4(2):1–10. Crossref
32. Krishneswari K, Arumugam S. Multimodal biometrics using feature fusion. Journal of Computer Science. 2012; 8(3):431–5. Crossref
33. Dhameliya MD, Chaudri JP. A multimodal biometric recognition system based on fusion of palm print and fingerprint. International Journal of Engineering Trends. 2013; 4(5):1–4.
34. Hamad AM, Elhadary RS, Elkhateeb AM. Multimodal biometric personal identification system based on fingerprint and iris. International Journal of Computer Science and Communication Networks. 2013; (4):226–30.
35. Lahane PU, Ganorkar SR. Fusion of iris and fingerprint biometric for security purpose. International Journal of Scientific & Engineering Research. 2012 Aug; 3(8):1–5.

36. Nageshkumar, Mahesh PK, Swami MN. An efficient multimodal biometric fusion using palm print and a face image, International Journal of Computer Science. 2009; 2(3):1–5.
37. Razzak MI, Yuosf R, Khalid M. Multimodal face and finger veins biometric authentication. Scientific Research and Essays. 2010; 5(17):2529–34.
38. Cui F, Yang G. Score level fusion of fingerprint and finger vein recognition. Journal of Computer Information's Systems. 2011; 16(1):5723–73.
39. Bharadi VA, Pandya B, Nemade M. Multimodal biometric recognition using iris and fingerprint. IEEE Transactions; 2014.
40. Hong L, Jain A, Integrating faces and fingerprints for personal identification for personal identification. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2008; 20(12):1295–307. https://doi.org/10.1109/34.735803
41. Abdolahi M, Mohamadi M, Jafari M. Multimodal biometric system fusion using fingerprint and iris with fuzzy logic. International Journal of Soft Computing and Engineering. 2013; 2(6):1–7.
42. Krzysztof, RJ, Prodanov P, Drygajlo A. Reliability- based decision fusion in multimodal biometric verification systems. EURASIP Journal on Advances in Signal Processing. 2007; 2007(1):74–74.
43. Boodoo NB, Subramanian RK. Robust multi-biometric recognition using face and ear images. International Journal of Computer Science and Information Security. 2009; 6(2):164–9.
44. Sree SS, Radha N. A Survey on fusion techniques for multimodal biometric identification. International Journal of Innovative Research in Computer and Communication Engineering. 2014; 2(12):1–5.
45. Kaur D, Kaur G. Level of fusion in multimodal biometrics: A review. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(2):1–5.
46. Shi J-Z, Gu X-F, Li J-P, Lin J, Liu L, Huang Y. A new method of iris image location research. IEEE Conference on Image Processing, Cairo, Egypt; 2009. p. 329–32.
47. Zaim A. Automatic segmentation of iris images for the purpose of identification. IEEE International Conference on Image Processing, 2005. ICIP 2005, 2005 Sep 14, Genova, Italy; 2006.
48. Peng J, Abd El-Latif AA, 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):6891–7. Crossref