Multimodal Biometric System:- Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level

Grace Wangari Mwaura, Prof. Waweru Mwangi, Dr. Calvins Otieno

Abstract:- Biometrics has developed to be one of the most relevant technologies used in Information Technology (IT) security. Unimodal biometric systems have a variety of problems which decreases the performance and accuracy of these system. One way to overcome the limitations of the unimodal biometric systems is through fusion to form a multimodal biometric system. Generally, biometric fusion is defined as the use of multiple types of biometric data or ways of processing the data to improve the performance of biometric systems. This paper proposes to develop a model for fusion of the face and fingerprint biometric at the match score fusion level. The face and fingerprint unimodal in the proposed model are built using scale invariant feature transform (SIFT) algorithm and the hamming distance to measure the distance between key points. To evaluate the performance of the multimodal system the FAR and FRR of the multimodal are compared along those of the individual unimodal systems. It has been established that the multimodal has a higher accuracy of 92.5% compared to the face unimodal system at 90% while the fingerprint unimodal system is at 82.5%.

Keywords:- False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Accept Rate (GAR), Receiver Operating Characteristics (ROC), Equal Error Rate (EER), multimodal, Unimodal, K Nearest Neighbor (KNN), scale invariant feature transform (SIFT), support vector machine (SVM)

1. Introduction

Biometrics has developed to be one of the most relevant technologies used in Information Technology (IT) security. It consists of the automatic recognition of individuals by analysing intrinsic human being characteristics which cannot be easily forgotten, lost, exchange or stolen, as it may happen with passwords or cards. [1] This property has made biometric recognition to be considered the most suitable solution for applications which entail security authentication such as access control, banking and border control. [1] There are other technologies that allow the automatic recognition of individuals such as ID tokens or passwords, but these technologies entail either that users must have with them a token or that users must memorize a password respectively. Biometrics only requires an intrinsic characteristic of the user. [2] There exist a wide number of biometric modalities as well as their possible combinations. Each of them is implemented with the appropriate biometric capture devices and algorithms to acquire and process the corresponding biometric characteristics. For example face recognition and fingerprint verification; speech and signature; fingerprint and finger geometry. [3] Multimodal biometric systems fuses different biometric data for verification. [4] This system takes the advantages each modality since each presents independent evidence to make the final decision hence decreasing the false acceptance rate (FAR) and false rejection rate (FRR). [5]

2. Related works

Over the recent years a large amount of experimentation in multi-biometrics has been done. The key to successful multi-biometric systems is in development of an effective fusion scheme, which is necessary to combine information presented by the multiple domain experts. [6]

2.1. Fusion in multimodal biometrics

Biometric evidence in a multibiometrics system can be fused at several different levels. The fusion can be divided into the following main categories:- Prior to matching fusion, fusion occurs before matching of biometrics is done. This includes the following fusion levels:- sensor level fusion and feature level fusion. After matching fusion, fusion is done after the fusion of biometric data. This includes the following fusion levels:- match score level fusion, rank level fusion and decision level fusion. [7]

2.1.1. Sensor level fusion

Fusion at the Sensor level involves combining the raw data from various biometric sensors and this fusion is recommended for multi-sample and multi-sensor systems. All the modalities must be compatible raw data and must be known in advance or estimated accurately. [7] New data for feature extraction is generated from the integration of the raw data acquired from the sensors. For example, in face biometrics, 3-D texture data and 2-D depth data that is obtained by two different sensors may be fused to produce a 3-D texture image of the face to be subjected to feature extraction. Fig. 1. Below shows the sensor level fusion. [8]

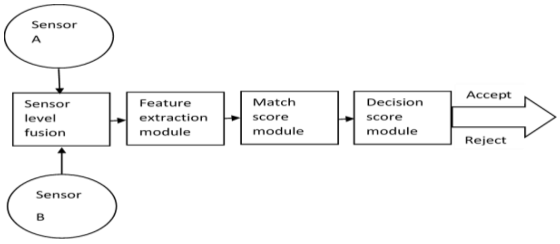


Fig. 1. *Sensor level fusion*

- *Grace Mwaura is currently pursuing masters degree program in information technology in Jomo Kenyatta university of agriculture and technology, Kenya. Email: gracemwaura90@gmail.com*
- *Prof. Waweru Mwangi is a lecturer in the computing department of Jomo Kenyatta university of Agriculture and technology. Email: waweru_mwangi@icsit.jkuat.ac.ke*
- *Dr. Calvins Otieno is a lecturer in the Information Technology department of Jomo Kenyatta University of agriculture and technology. Email: otienocalvins22@gmail.com*

2.1.2. Feature level fusion

This refers to the fusion of feature vectors obtained from a number of feature sources. Examples of feature sources are: (a) feature vectors of a single biometric trait obtained from different sensors; (b) Feature vectors from a single biometric obtained from different entities, like fingerprint feature vectors from left and right hand; and (c) Feature vectors generated from multiple biometric traits. Fig. 2. Below shows the feature level fusion. [9]

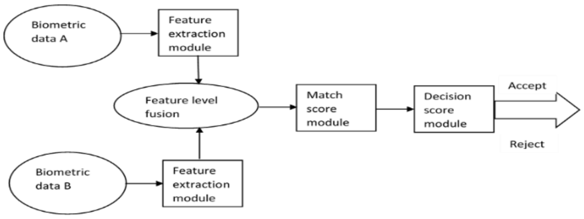


Fig. 1. *Feature level fusion*

Previous research on feature level fusion

Rattaini et al proposed to develop a multimodal system for face and fingerprint at the feature extraction level. The proposed approach was anchored on fusion of two traits by extracting independent features point sets from the two modalities and making the point sets compatible for concatenation. [9] To handle the problem of curse of dimensionality the features point sets were properly reduced in dimension. Different feature reduction techniques were implemented, prior and after the feature point set and the results duly recorded. The fused feature point set were matched using the point pattern matching or the Delaunay triangulation. [9] Face recognition in the proposed model was based on the scale invariant feature transform (SIFT). The proposed system considered spatial orientation and key point descriptors information of each extracted SIFT points. Thus the input to this system was face image while the output was a set of extracted SIFT features $S = (S_1, S_2, \ldots \ldots \ldots \ldots . S_M)$ where each feature point$S_1 = (x, y, \theta, k)$, consists of the (x, y) special location. The local orientation θ and k is the key descriptor of size 1* 128. [9] Fingerprint verification on this model was based on the minutiae matching technique where the fingerprint image was normalized, pre-processed using Gabor filters binarised and thinned, then subjected to minutiae extraction. [9] Other models based on the feature level fusion included Zhou and B. Bhanu who proposed feature fusion of face and gait. [10]

2.1.3. Matching score level fusion

This fusion involves the combination of similarity scores provided by the individual matching module of the biometric systems to produce the final combined match score. This method is also known as measurement level fusion or confidence level fusion. The combined matched score output generated by biometrics matchers provide all the required information about the input biometrics. Matching score fusion is classified by the two different approaches based on how the match score is processed. These are:- classifying the feature vector and combining the feature vector. Normalization is also needed because of the dissimilar match score generated by the various modalities. Fig. 3. Below shows the match score level fusion [7]

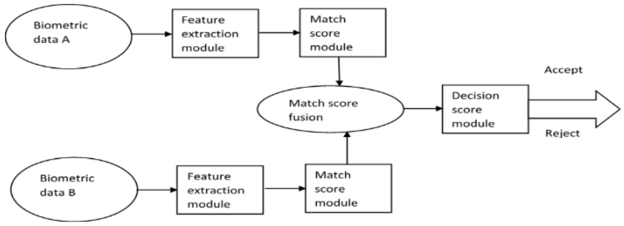


Fig. 2. *Match score level fusion*

Previous research on matching score level fusion

Hassan et al proposed a system to overcome the limitations of unimodal biometric system. The biometric modalities were processed sequentially until an acceptable match was obtained. The matching module for both modalities utilized support vector machine (SVM) classifier to generate the match scores. [11] The feature extraction for fingerprint images used the existing minutiae extraction algorithm. The matched score generated by each biometric source was directly combined into a total score by the sum- rule. The performance was then compared with the user specific weight fusion techniques. [11] The fusion scheme used to combine the score of each subsystem were the sum-rule and the trait specific weights. [11]

$$Ms = w_1 * m_{fc} + w_2 * m_{fp} \qquad (1)$$

Where $w_1 and\ w_2$ are the weights assigned to the two biometric traits m_{fc} and m_{fp} respectively. The value assigned to this research was 0.5, the final matching score were then compared to a threshold to recognize the person as genuine or imposter. [11]

2.1.4. Rank level fusion

This type of fusion is used in identification systems and entails combining numerous ranks associated with any identity and determining a new rank that would be used in determining the final decision. The aim of rank-level fusion is to combine the rank output by each individual biometric matcher in order to derive the final rank. Ross et al. defines three methods to combine the ranks assigned by different matchers. This includes (i) highest rank method (ii) the Borda count method, (iii) and the logistic regression method. [10]

Previous research on Rank level fusion

Monwar and Gorrilaava proposed to develop a multibiometric system to fuse the ear, face and signature biometric unimodal at the rank level fusion. The proposed multimodal biometric system had a number of unique features which included Fisher's linear discriminant methods for the individual unimodal (ear, face, and signature) and the utilization of the principal component analysis). [7]

2.1.5. Decision level fusion

In this level of fusion the information fusion occurs after each unimodal biometric system makes an independent individual decision about the identity of the user. [7] This is known as the simplest form of fusion since only the final output of the individual modalities is fused to form the multimodal biometric. Different methods are proposed for the decision level fusion for example, Majority voting, AND' and 'OR' rules. [7] After each unimodal has produced its outputs label that is, accept or reject in a verification system, a single final class label can be attained by using techniques such as majority voting. Fig. 4. Below shows the decision level fusion. [12]

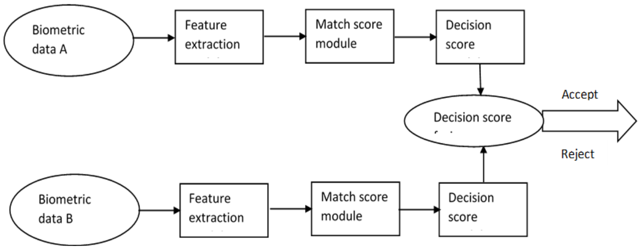


Fig. 3. *Decision level fusion*

Previous research on decision level fusion

Lin Hong and Anil Jain proposed a system for integrating face and fingerprint verification unimodal systems for personal identification. The proposed multimodal system integrated two different biometric systems (the face and fingerprint) and also incorporated a decision module to improve the identification performance. [13] The proposed system used the eigenface approach for face recognition and was composed of two stages: [13]

i The training stage:- stage in which a set of training face images were collected and used to train the model.

ii The operation stage:- stage in which each test images is projected into the M-dimensional eigenface for recognition.

While for the fingerprint recognition the proposed system used the minutiae extraction followed by the miniature matching method. [13] The match/ not match decision for the proposed system was determined by the following criterion:-

$$ID(II) = \begin{cases} l_k, \ if \begin{cases} H_k(\Delta X_k, Y_k) < FAR \ and \\ H_k(\Delta X_k, Y_k) = min\{H_1(\Delta X_1, Y_1),, \dots, H_n(\Delta X_n, Y_n)\} \end{cases} \\ imposter \ otherwise \end{cases} \quad (2)$$

Where $\Delta X_i = \Delta X_{i+1} - X_I$,

Since $H_i(\Delta, Y)$, define the probability that an imposter is accepted at rank i with consecutive relative DFFS,Δ fingerprint matching score, Y, the above decision criterion satisfies the FAR specification. [13]

2.1.6. Other approaches to fusion

In July 2012 Dr Shubhangi D C et al proposed the Face and Fingerprint recognition algorithm by combining ridge based matching for the fingerprint unimodal and Eigen for Face unimodal. This by recognition of the face first followed by the fingerprint recognition. The fingerprint recognition was based on the core and minutiae detection of the fingerprint data. The Eigen faces were used to classify the face image which was then followed by the training of Neural Network to perform pattern recognition and identification. [14]

2.1.7. Summary on fusion levels

For fusion to achieve higher performance than unimodal systems, the choice of appropriate fusion level is important. Biometric systems (matchers) that fuse data at earlier levels tend to be have a higher performance than those that do the fusion at a later levels. Sensor-level fusion deals with one of the major problems of the unimodal systems (noisy sensor data) but all other problems associated with unimodal biometric systems still remain. Fusion at the feature level achieves a high performance but is very hard to achieve due dimensionality problem and the unknown relationship between the feature spaces of the different biometric systems. Performance of the fusion system at the decision level is low since only a small amount of information is available at this level. The match score level has been studied extensively in literature, fusion produces acceptable performance rates though normalization is sometimes required for the scores data from different unimodal. Normalization is computationally very expensive, and an ill-chosen normalization technique results in a very low recognition performance rate. Fusion at the rank level has not been studied extensively in literature though it is possible to achieve high performance.

2.2. SIFT algorithm

The Principal component analysis (PCA) and 2D principal component analysis (2D PCA) are some of the algorithms used for extracting face and fingerprint information. These algorithms are sensitive to light, expression and pose, et cetera. To overcome these problems, Scale Invariant Feature Transform (SIFT) was introduced to be used for feature extraction. SIFT method has the advantages of rotation invariance, scale invariance has strong robustness for occlusion problem and noise and affine invariance. [15] SIFT is an algorithm in machine vision used to extract specific features of an images for applications such as matching various views of an object and identifying objects. During the feature extraction the images is pre-processed to obtain better performance by reducing the noise. The image is then subjected to the scale space extrema detection by use of cascade filtering approach to identify the locations of the candidate key points which are invariant to scale changes of the image. Key point localization is then performed on the image to remove all the unrealistic key points that is those with low contrast or is poorly localized along an edge. The image is then finally assigned a consistent orientation based on local image properties in order to achieve an image that is invariant to image rotation. The next stage involves the image description where a key point descriptor is first done followed by the object recognition. The key point descriptor is computed for the local image region which is highly distinctive for each key point. Object recognition uses the K Nearest Neighbour (KNN) to produce confidence levels by key point matching. [16] SIFT mainly includes four steps which are scale-space extrema detection, removal of unreliable key points, orientation assignment and matching. [15] Scale space detection of extreme value in space scale: In SIFT, scale transformation is done by Gaussian convolute on and the descriptor, L(x, y, σ) of input image (I(x, y)) in the difference scale can be expressed by the equation (3)

$$L(x,y,\sigma) \quad = \big(G(x,y,\sigma)\big) * I(x,y) \qquad (2)$$

Where σ is scale factor and Gaussian convolution kernel $\big(G(x,y,\sigma)\big)$ is given as

$$\big(G(x,y,\sigma)\big) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (4)$$

After the convolution, the calculated image is a Gaussian image. L(x, y, σ). The image I(x, y) zoom with σ, and the smoothness of the image would change with the change of σ, and then a series of scale image could be obtained. [15] According to those scale images, the extreme point (key-points (interest points)) will be detected while the filtering out key-points: The location of key-point is considered to filter out the key-points which are sensitive to noise or have no edge effect. So for that Taylor quadratic expansion, DoG (x, y, and σ) can delete the extreme points which have lower contrast, and the value of Hessian vector and the ratio of determinant can reduce the edge effect.

$$D(x,y,\sigma) = \big(G(x,y,k\sigma) - G(x,y,\sigma)\big) * I(x,y = L(x,y,k\sigma) - L(x,y,\sigma) \qquad (3)$$

Orientation is assigned to each key point by adding a histogram of gradient orientation θ(x, y) weighted by the gradient magnitudes m(x, y) from the key point's neighbourhood.

$$m(x,y) = \sqrt{(L(x+I,y) - L(x-1))^2 + (L(x,y+I) - L(x,y-I))^2} \ (6)$$
$$\sigma(x,y) = tan^{-1}((L(x,y+1) - \frac{L(x,y-1)}{L(x+I,y)-L(x-1,y)}) \qquad (7)$$

Where L is a Gaussian smooth image with a closet scale to that of a key point. [15]

2.3. (KNN) classifier

K-nearest neighbour algorithm (k-NN) is a type of instance based learning algorithm whereby, the function is only estimated locally while all computations are done during classification. K-NN classifies data entity based on the closest training data in the feature space. In this algorithm an entity classification is based on majority vote of its neighbours, and the test entity (t) is assigned to the class which is most common among its k nearest neighbours (k refers to a small positive integer). [15] Although there is no need for training in this algorithm, the neighbours may be regarded as training entities and are chosen from a set of entities for which their classification is known. When k is 1 the test entity is assigned to the class of its nearest neighbour. [15] Feature vectors and class of the training samples are stored in the training stage of the algorithm while in the classification stage, k is decided by the user. A test vector is classified by assigning it the label which is most common among the k training data neighbours. Hamming distance is mostly used for text classification. [15] In high-dimensional spaces, standard k-d tree search often performs poorly, however, Best Bin First (BBF) which is a variant of this search efficiently finds nearest neighbours in limited search time. This type of search has wider application in shape indexing, vision-related et cetera. [15]

3. METHODOLOGY

3.1. Fingerprint recognition

A fingerprint is composed of numerous furrows and ridges which are parallel. However, in fingerprint recognition, fingerprints are not distinguished by their furrows and ridges but are distinguished by minutia.

Fingerprint recognition method used in this research

This research used the SIFT algorithm which is used for extending characteristic feature points of fingerprint beyond minutiae points. The fingerprint image is converted into a collection of local feature vectors which are invariant to rotation, scaling in addition to translation. These features were extracted to perform matching in a scale space extrema through a staged filtering methodology, and were robust to variations in noise, occlusion, illumination, and small changes in viewpoint. The features were also distinct allowing for accurate object recognition with low probability of mismatch. For this research the best way to match each key point was to identify its nearest neighbour in the key point's database which is the key point with minimum hamming distance from the invariant descriptor vector. To search the nearest neighbour of the key points in a high dimensional spaces the BBF algorithm was adopted. The BBF algorithm is based on the k-d tree search algorithm. K-d tree makes indexing higher dimensional spaces possible so that bins in feature space are searched in ascending order from the query point hence, returns the closest neighbour for a large fraction of queries and a very close neighbour.

3.2. Face recognition

The distinctiveness of a face can be determined by the overall, shape, structure and proportions of the face that is, the sides of the mouth, upper outlines of the eye sockets, distance between the eyes, nose, mouth, and jaw edges, the area surrounding the cheekbones and the location of the nose and eyes .

Face recognition method used in this research

This research used the SIFT algorithm. The face image is converted into a collection of local feature vectors which are invariant to rotation, scaling in addition to translation. These features were extracted to perform matching in a scale space extrema through a staged filtering methodology, and were robust to variations in noise, occlusion, illumination, and small changes in viewpoint. The features were also distinct allowing for accurate object recognition with low probability of mismatch. For this research the best way to match each key point was to identify its nearest neighbour in the key point's database which is the key point with minimum hamming distance from the invariant descriptor vector. To search the nearest neighbour of the key points in a high dimensional spaces the BBF algorithm was adopted. The BBF algorithm is based on the k-d tree search algorithm. K-d tree makes indexing higher dimensional spaces possible so that bins in feature space are searched in ascending order from the query point hence, returns the closest neighbour for a large fraction of queries and a very close neighbour.

3.3. Face and fingerprint multibiometric

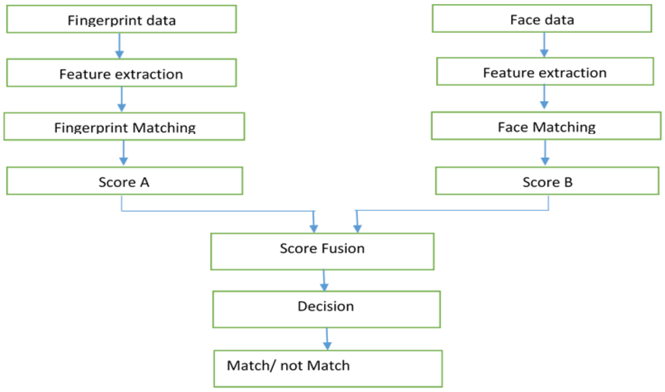


Fig. 1 *proposed fusion model*

Fig. 5.shows the sensor level fusion. The fingerprint recognition is responsible for matching the input fingerprint against the fingerprint template stored in the database to obtain fingerprint matching scores. Face recognition is responsible for matching the input fingerprint against the template stored in the database. Score level fusion integrates matching scores (score A and score B) to make a score S used to make the final decision. The simple weighted fusion is the suggested a score fusion strategy in this research and the fusion score S will be computed as follows:-

$$S = w_1 s_a + w_2 s_b \qquad (8)$$

Where:- $s_a$and s_b are fingerprint and face matching score, $w_1 and\, w_2$ Are fingerprint and face weights For this research the weight will be over the range of [0, 1] such that the constant

$$w_1 + w_2 = 1\text{, is satisfied.} \qquad (9)$$

Since both the face and fingerprint unimodal used SIFT detection and measurements were done by the use of Euclidean distance no normalization was required before the scores were fused

3.3.1. Input to the model

The experimental data was composed of 40 subjects. This was composed of 40 subjects with 10 distinct face images and 8 distinct fingerprint images. A total of 720 positive images and 80 negative images are to be used. Out of this, 360 positive face images and 280 positive fingerprint images are used to build the model while the remaining 80 positive images and 80 negative images are to be used for testing the model.

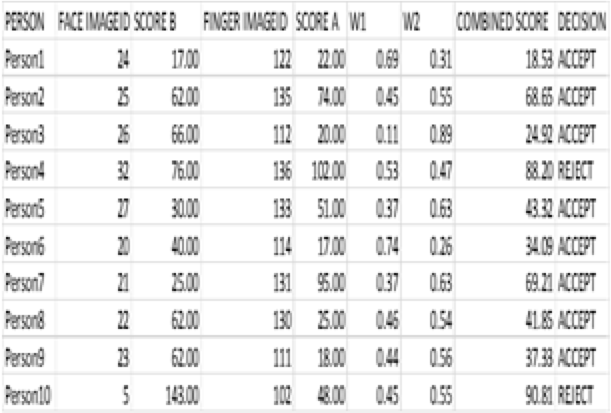
3.3.2. Output of the model

Given that this research is dealing with an identification problem in biometrics. The identification problem in this research may be stated as follows be:- Given an input feature vector, $X_{Q,}$ to determine the identity$I_k k \in \{1,2,\dots.N, N+1\}$. Here $I_1, I_2, \dots. I_N$ are the identities stored in the database and I_{N+1} indicates the not match where no suitable identity can be determined for the user.

Hence

$$X_Q \in \{ {}^{i_k}_{I_{N+1},} \quad if \max\{S(X_Q, X_{IK})\} \geq T, K = 1,2,\dots.,N \quad otherwise\ not\ match$$
(10)

Where X_I is the biometric template corresponding to identify I_K and t is predefined threshold. Hence the expected outcome will be match or not match for the given biometric data. Table 1. Gives a sample output produced by the multimodal system multimodal system.



PERSON	FACE IMAGEID	SCORE B	FINGER IMAGEID	SCORE A	W1	W2	COMBINED SCORE	DECISION
Person1	24	17.00	122	22.00	0.69	0.31	18.53	ACCEPT
Person2	25	62.00	135	74.00	0.45	0.55	68.65	ACCEPT
Person3	26	66.00	112	20.00	0.11	0.89	24.92	ACCEPT
Person4	32	76.00	136	102.00	0.53	0.47	88.20	REJECT
Person5	27	30.00	133	51.00	0.37	0.63	43.32	ACCEPT
Person6	20	40.00	114	17.00	0.74	0.26	34.09	ACCEPT
Person7	21	25.00	131	95.00	0.37	0.63	69.21	ACCEPT
Person8	22	62.00	130	25.00	0.46	0.54	41.85	ACCEPT
Person9	23	62.00	111	18.00	0.44	0.56	37.33	ACCEPT
Person10	5	143.00	102	48.00	0.45	0.55	90.81	REJECT

Table 1. *Sample output produced by the multimodal system multimodal system*

3.4. Evaluation of the multimodal biometrics

The evaluation of the proposed multimodal model was done against the face and the fingerprint unimodal models developed using SIFT algorithm. The face and fingerprint unimodal were also evaluated against each other to establish which unimodal performs better than the other. The performance evaluation is done using the FAR (false acceptance rate) and FRR (false rejection rate).

$$\text{FAR} = \frac{N_a}{N} \qquad (11)$$

$$\text{FRR} = \frac{\boldsymbol{N_r}}{\boldsymbol{N}} \qquad (12)$$

Where N_a is the number of imposters which were falsely accepted i.e. scores of imposters match are more than T. N_r is the number of genuine sample which were false rejected i.e. score of genuine match T; N is total number of match: T is the threshold.

4. Experimental Results and Discussion

4.1. Experimental data

The fingerprint database was derived from the FVC 2004 (fingerprint verification competition) and contains four different databases DB1, DB2, DB3 and DB4. Each database has eight different images and has 10 distinct subjects, hence making a total of 400 from all the databases .The data was then divided into two training data (360 images) and the testing data (40 images). [17] The fingerprint database was derived from the face 94. The data was then divided into two; one for model creation (280 images) and the second was testing data (40 images). [18] The simulation has been built using the python programming language. Table 2. Shows the Data from secondary sources.

Table 1. *Data from secondary sources*

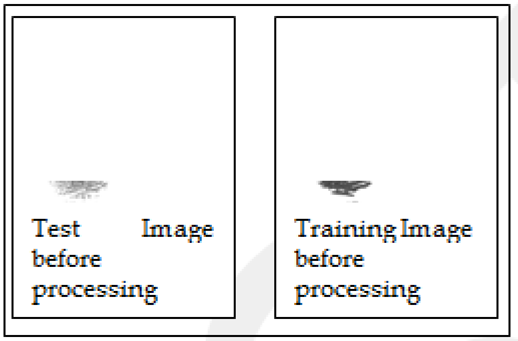
Image	Number to be used in building the model	Number to be used in testing the model
Fingerprint images	280 positive images	40 negative images 40 positive images
Face images data	360 positive images	40 negative images 40 positive images
Total images used	**640**	**160**

The unimodal databases ware combined to form a chimeric multimodal dataset. The creation of chimeric datasets for the purpose of multi-modal biometrics experimentation has become a common practice owing to a lack of publicly available genuine multi-modal data. In chimeric datasets, samples of one modality from one set of users are arbitrarily paired with samples of a second modality from a different set of users to create "virtual identities". Chimeric datasets rely on the assumption that the modalities being fused are independent of one another, though for many years this independence was not formally tested. Recently, several studies have been done to investigate the validity of the independence assumption.

4.2. Experimental Results and discussion

I. Fingerprint Recognition using SIFT

a. *Fingerprint image before being subjected to SIFT algorithm*


Test Image before processing
Training Image before processing

b. *Fingerprint image after Key point and descriptors have been identified using SIFT*

c. *Fingerprint Matching of the two images*

From the fingerprint recognition module the error rate curve and the receiver operating curves of the fingerprint were drawn as shown below in Table 3.

Table 2. *FAR and the FRR of the fingerprint at different threshold values*

Threshold	7	8	9	10	11	13	22	23	24	25	26	27	29	30	31	35	38	40	43	47	54	70	71	72	75	88
FAR	0	0	0	0	0	0	0.0125	0.0125	0.0125	0.0125	0.0125	0.0125	0.0375	0.0375	0.0375	0.0375	0.05	0.05	0.05	0.0625	0.0625	0.1125	0.1125	0.1375	0.175	0.3375
FRR	1	1	1	1	1	0.975	0.725	0.725	0.725	0.65	0.625	0.6	0.575	0.575	0.55	0.5	0.45	0.425	0.425	0.425	0.2	0.2	0.2	0.2	0.175	0.15

The graph below shows the error rate curve of the fingerprint. The point of intersection of the FAR and the FRR forms the threshold of the fingerprint unimodal as this is the point where the FAR and the FRR are most similar as shown in fig. 6.

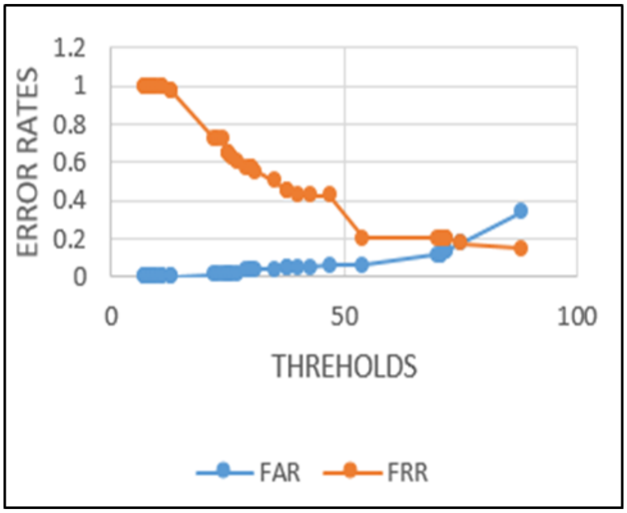


Fig. 4 *FAR and FRR curves of fingerprint*

The ROC curve in fig. 7 and the Table 4 shows the genuine acceptance rate (GAR) against the false acceptance rate (FAR) of the fingerprint unimodal. The GAR is used to measure the accuracy of a biometric system which from the model is 82.5%

Table 3*. FAR and the GAR of the fingerprint at different threshold values*

FAR	0	0.0125	0.0375	0.05	0.0625	0.1125	0.1375	0.175	0.3375
GAR	1	0.9875	0.9625	0.95	0.9375	0.8875	0.8625	0.825	0.6625

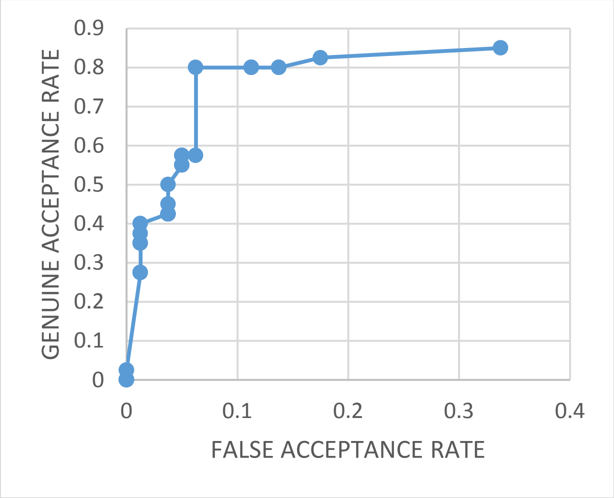
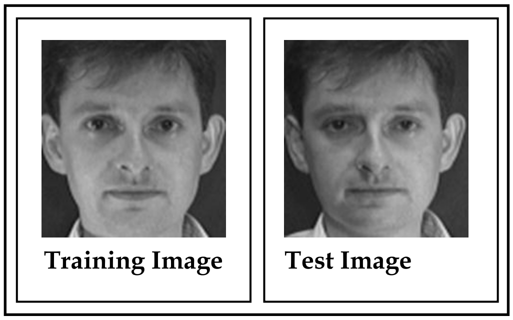


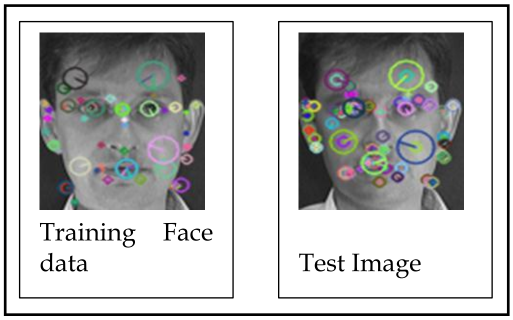
Fig. 5 *Receiver operating curve of fingerprint*

II. Face Recognition using SIFT algorithm

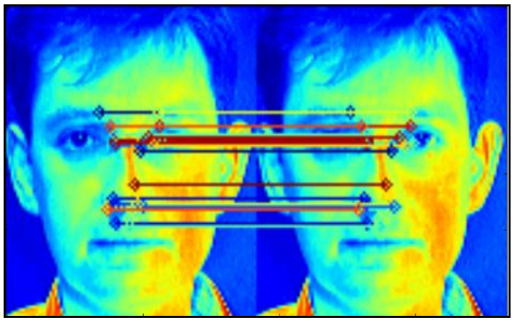
a. Face images before being subjected to SIFT algorithm



b. Face image after Key point and descriptors have been identified using SIFT



c. Face Matching of the two images



From the face recognition module the error rate curve and the receiver operating curves of the face were drawn as shown in Table 5

Table 4. *FAR and the FRR of the face at different threshold values*

Threshold	17	19	25	27	32	34	35	37	39	40	44	45	47	48	49	50	52	57	58	62	63	64	67	68	70	72	76	78	82
FAR	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.0125	0.0125	0.0125	0.0125	0.0125	0.0125	0.0125
FRR	0.975	0.95	0.825	0.825	0.775	0.775	0.775	0.75	0.75	0.7	0.65	0.65	0.65	0.6	0.6	0.575	0.55	0.5	0.475	0.375	0.35	0.35	0.25	0.25	0.25	0.225	0.2	0.2	0.125

The graph in Fig 8 shows the error rate curve of the face. The point of intersection of the FAR and the FRR forms the threshold of the face unimodal as this is the point where the FAR and the FRR are most similar.

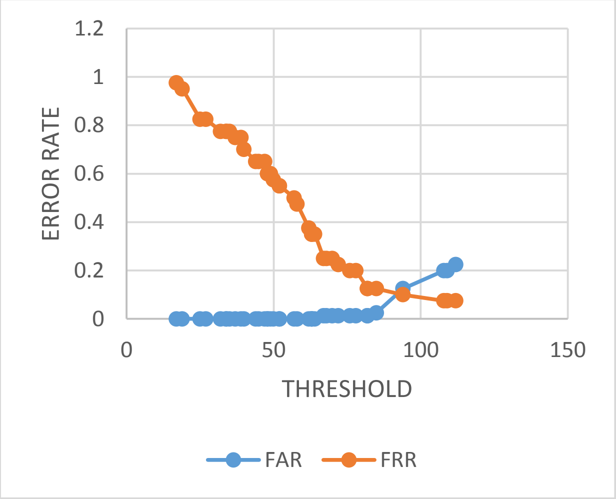


Fig. 6 *FAR and FRR curves of fingerprint*

The ROC curve in Fig 9 and Table 6 shows the genuine acceptance rate (GAR) of the face unimodal against the false acceptance rate (FAR). The GAR is used to measure the accuracy of a biometric system. The accuracy of the face unimodal in this research was 90%

Table 5. *FAR and the GAR of the face at different threshold values*

FAR	0	0	0	0	0	0	0	0	0	0	0	0	0	0.0125	0.0125	0.0125	0.0125	0.025	0.125	0.2	0.225
GAR	0.025	0.05	0.175	0.225	0.25	0.3	0.35	0.4	0.425	0.5	0.525	0.625	0.65	0.75	0.775	0.8	0.875	0.875	0.9	0.925	0.925

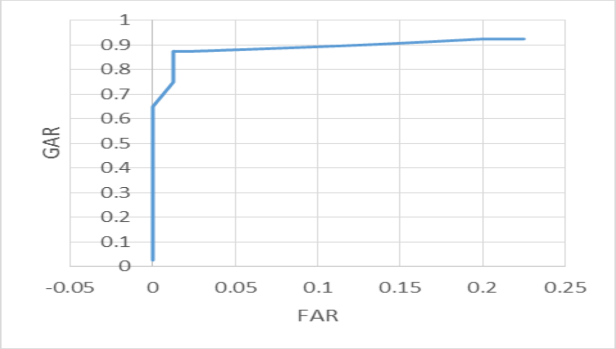


Fig. 7 *Receiver operating curve of fingerprint*

Face and fingerprint Multimodal

The FAR and FRR is used to evaluate the performance of the face unimodal, fingerprint unimodal and the proposed face and fingerprint multimodal biometric system. The graph in Fig.10 and Table 7 shows the FAR and the FRR of the proposed multimodal system, the EER is at the point of intersection of the two curves and this forms the threshold of the proposed multimodal system, and it's the point where the FAR and FRR are most similar.

Table 6. *FAR and the FRR of the multimodal at different threshold values*

Threshold	15	19	21	23	24	25	30	31	34	35	36	37	39	40	42	43	44	45	46	48	54	55	59	60	60	63	64	68	107
FAR	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.0125	0.0125	0.025	0.025	0.025	0.025	0.025	0.025	0.3125
FRR	0.5	0.475	0.475	0.4625	0.425	0.425	0.3875	0.375	0.375	0.35	0.35	0.3375	0.325	0.325	0.325	0.3125	0.3	0.3	0.275	0.275	0.2375	0.2375	0.1875	0.1875	0.1625	0.15	0.1375	0.125	0

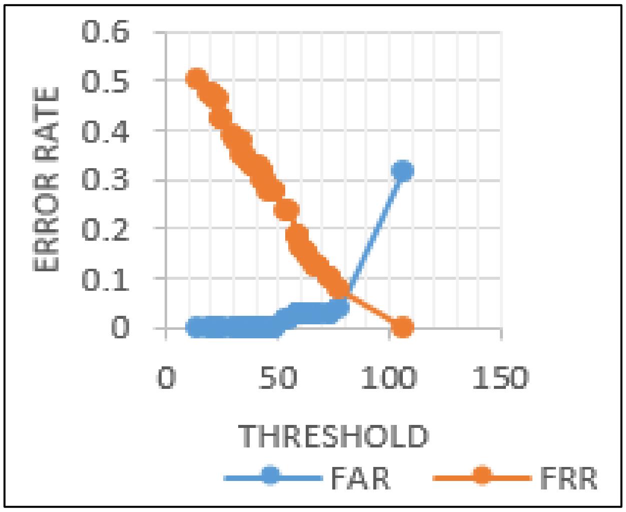


Fig. 8 *Receiver operating curve of multimodal*

The ROC curve below shows the genuine acceptance rate (GAR) of the face unimodal, fingerprint unimodal and the proposed multimodal against the false acceptance rate (FAR). The GAR is used to measure the accuracy of biometric systems. From the curves it is clear that the multimodal performs better than the face and fingerprint unimodal. It is also remarkable to note that the face unimodal performs better than the fingerprint unimodal system.

Table 7. *FAR and the GAR of the fingerprint, face and multimodal at different threshold values*

FAR of multimodal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.013	0.013	0.025	0.025	0.025	0.025	0.025	0.025	0.025	0.025	0.025	0.025	0.038	0.313
GAR of multimodal	0.5	0.525	0.525	0.538	0.575	0.613	0.625	0.65	0.65	0.663	0.675	0.675	0.688	0.688	0.7	0.7	0.725	0.725	0.725	0.763	0.763	0.813	0.813	0.838	0.85	0.85	0.863	0.875	0.875	0.9	0.9	0.925	1
FAR of face	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.013	0.013	0.013	0.013	0.013	0.013	0.025	0.125	0.2	0.2	0.225
GAR of face	0.025	0.05	0.175	0.225	0.225	0.225	0.25	0.3	0.35	0.35	0.35	0.4	0.425	0.45	0.45	0.5	0.525	0.625	0.65	0.65	0.65	0.65	0.75	0.75	0.775	0.8	0.8	0.875	0.875	0.9	0.925	0.925	0.925
FAR of fingerprint	0	0	0	0	0	0	0	0	0	0	0.013	0.013	0.013	0.013	0.013	0.013	0.038	0.038	0.038	0.038	0.038	0.038	0.05	0.05	0.05	0.063	0.063	0.113	0.113	0.138	0.138	0.175	0.338
GAR of fingerprint	0	0	0	0	0	0	0	0	0.025	0.025	0.275	0.35	0.35	0.35	0.375	0.4	0.425	0.425	0.425	0.425	0.45	0.5	0.55	0.575	0.575	0.575	0.8	0.8	0.8	0.8	0.8	0.825	0.85

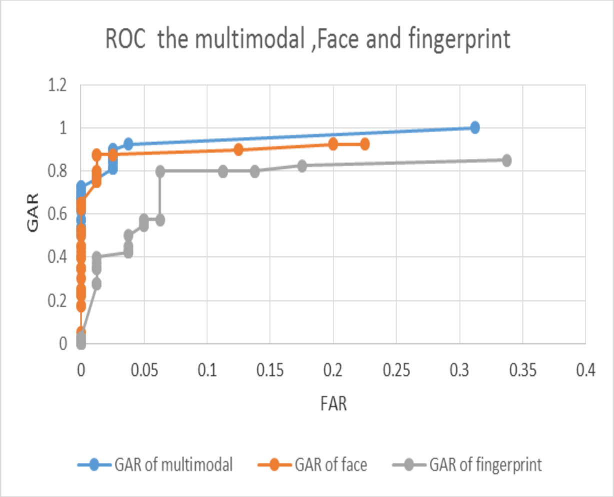


Fig. 9 *ROC of the multimodal face and fingerprint*

Unimodal biometric fingerprint recognition and the face unimodal biometric system performance is compared against the multi modal biometric system. The performance is analysed using the FAR and FRR of the models. Table 9 below shows the evaluation of the proposed multimodal systems against the respective unimodal systems.

Table 8. *Evaluation of the proposed multimodal system model*

Models	FAR	FRR	Accuracy
Face unimodal system	12.5%	10.0%	90.0%
Fingerprint unimodal system	17.5%	17.5%	82.5%
Proposed Multimodal system	3.75%	7.5%	92.5%

From Table 9. Evaluation of the proposed multimodal system; It can be seen that the multimodal system has a higher accuracy at 92.5% and also reduces the error rates (FAR and FRR) of the individual unimodal systems.

5. Conclusion

In this paper a model for fusion of the face and fingerprint multimodal system has been presented. SIFT has been used for feature extraction and image description of the face and fingerprint images. Finally, matching is done using KNN by comparing an image to images stored in the database. The Sum rule has been used to fuse the score at the match score level. The experiment result of the proposed system has also been tested against the face and the fingerprint unimodal system and it has been established that the multimodal system performs better than the unimodal system with an accuracy of 92.5%, FRR of 7.5% and FAR of 3.75%

REFERENCES

[1] Jain A . K. , Ross A., & Pankanti S., “Biometrics: A tool for information security”. IEEE Transactions on Information Forensics and Security, 2006, 125-143.

[2] K.Sasidhar, Kakulapati V. L., & Ramakrishna K., “multimodal biometric systems study to improve accuracy and performance”, International Journal of Computer Science & Engineering Survey (IJCSES) , 2010.

[3] Jain A. K., Ross A., Prabhakar S., “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology. Special Issue on Image- and Video-Based Biometrics ,2004

[4] G. Chandran and Dr. R.S. Rajesh.” Performance Analysis of Multimodal Biometric,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009, pp 290-296

[5] Ross A., and Jain A., “Information fusion in biometrics” Pattern Recognition Lett., 2003, pp. 2115-2125.

[6] Ross A., Nandakur K., and Jain A., “Handbook of multibiometrics”, springer-verlag , 2006.

[7] Ghayoumi M., “A review of multimodal biometric systems: Fusion methods and their applications” IEEE/ACIS 14th International Conference Computer and Information Science (ICIS), Las Vegas, 2015 ,pp. 131 - 136.

[8] Anil Jain and Arun Ross., “fingerprint mosaicking . Acoust speech signal process,” In Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) , Orlando, Florida, May 13 - 17, 2002 (pp. 4064-4064).

[9] Rattaini A., kisku D., and Bicego, M., “ Feature level fusion of face and fingerprint biometrics” . Institute of Electrical and Electronics Engineers (IEEE). May 25, 2007

[10] Zhou X., and Bhanu B., “Feature Fusion of Face and Gait for Human Recognition at a Distance in Video”. Journal of Computational Information Systems , 2011, 5723-5731.

[11] Hassan N., Ramli D. A., and Siandi S. A. , “Fusion of face and fingerprint for robust personal verification system”, International journal of machine learning and computing , 2014

[12] Kinnunen T., Hautamaki V., and Franti P., “fusion of spectral feature set for accurate speaker identification” . 9th conf. speech computer, peterburg Russia, 2004 , pp. 361-365.

[13] Hong L., and Jain A. “intergrating face and fingerprint for personal identification” . IEEE transactions on pattent ananlysis and machine intelligence , 1998, 1295-1307.

[14] Shubhangi D. and Manohar B., “Multi-Biometric Approaches to Face and Fingerprint Biometrics”. International Journal of Engineering Research & Technology, Vol. 1 Issue 5, 2012, 2278- 0181.

[15] Mr. Amit Kr. Gautam, M. T. (2014). Improved Face Recognition Technique using Sift. Journal of Electrical and Electronics Engineering (IOSR-JEEE), pp. 72-76.

[16] Park, U., Pankanti, S., & Jain, A. K. (2008). Fingerprint Verification Using SIFT Features. SPIE Defense and Security Symposium. Orlando, Florida,.

[17] Biometric System Lab - University of Bologna., University of Bologna. Retrieved from Biometric System Lab, 2003. Accessed August 2016 http://bias.csr.unibo.it/fvc2004/download.asp

[18] AT&T Laboratories Cambridge. (2002). AT&T Laboratories Cambridge. Retrieved from The database of faces, 2002. Accessed August 2016 http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html