International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 2703 - 2720

Multi Biometric Authentication using Score Level Fusion and Non-Invertible Template Formation Technique

P. Gayathiri[1], Dr. M. Punithavalli[2]
[1]Research Scholar, [2]Professor
Department of Computer Applications
Bharathiar University, Coimbatore - 641046

Abstract

Single Level Fusion – Score Level or Feature Level is the one in which the Multimodal Biometric Recognition generally can subsists. Feature Extraction, Fusion Formation and Template are the fundamental steps of the Multimodal Biometric Recognition. The matching performance and the accuracy of fusion cannot be increased by bringing single level of fusion technique because of the variation in the matchers. As the fusion process is carried out, the secured template formation is another task in the present system. The hackers should not recognize the stored template as they can easily change the features of the original data. To overcome this, Non-Invertibility Template Formation is carried out in the multimodal biometric recognition. The proposed technique consists of new fusion technique and secured template formation technique such as Matched Performance-Based (MPB) fusion technique and Non-Invertibility Template formation technique. In order to increase accuracy, both the two levels Feature Level and Score Level are utilized in fusion process of the Matched Performance-Based (MPB). The score obtained through the Feature – Level Fusion is utilized to carry out the performance increment with the modality rate. In this article, the frequently used biometric traits-Fingerprint and Iris based multibiometric system which utilizes the Feature Level and Score Level is proposed. A novel normalization technique called the Overlap Extrema-Variation-Based Anchored Minmax (OEVBAMM) is also proposed to bring about the fusion. The feature set with unknown relationship is gained from Iris and Fingerprint and are neither compatible nor homogenous. Non-invertible transform is utilized to secure the fused pixel information at feature level. The fused image's textural information belongs to Fingerprint and Iris is employed to build a unique feature vector. Unlike the passwords and tokens, the compromised biometric templates are neither be revoked nor be reissued. Hence the principal focus of our work lie on Biometric Template Security. The possibility of getting variation in the acquired biometric traits of a user makes ensuring security very challengeable in maintaining the recognition performance. The proposed work includes the biometric fusion with the Non-Invertible Transform for template security purpose.

Keywords**:** *Biometric Template Protection, Feature Level Fusion, Score Level Fusion, Texture and Feature Level Fusion, Non-Invertible Transform.*

1. Introduction

Authentication is the important factor for the secureness of the restricted resources and the systems it can be done by giving authentication to individual person. Unimodal and multimodal are the two main type in the biometrics system. A unimodal biometric system includes the single biometric features for identification of the person whereas the Multimodal Biometric system includes the multiple biometric features for the identification of the person. Multimodal biometric system consists of various processing unit such as sensor level, feature extraction level, matching level and decision level. The sensor level includes two more sensor devices where the several biometric information of the same

person is collected. Fusion enhance the accuracy of the identification process which is the main processing unit in the multimodal Biometric system. The multimodal biometric system is organized on the following five levels: sensor level [2], [3], rank level [4], decision level [5], feature level [6], or score level [7].

A. Sensor-Level Fusion

In Sensor-Level Fusion the fusion takes place from the multiple sensor image information. The fusion technique is carried out by passing the fused image information into feature abstraction module and it is followed by the method known as matching and ranking module and finally result analyzed from the decision module for the identification of the person. A more process is required to fuse multiple sensor factor.

B. Rank -Level Fusion

In the rank-fusion level, the fusion of multiple ranking modules causes the prevailing of ranks among the modules and the identification of a person involves the usage of this fused rank. Due to verification problem of the person and the accuracy issues rank level fusion us used in less applications.

C. Decision-Level Fusion

In Decision Level Fusion, to analyze the identification of the person we must fuse various decision established from multiple decision module together. Decision-level fusion is not implemented in many applications due to the realization accuracy is less in the multimodal biometric system. For an instance, the quality assessment module is enlarged from the feature extractor analyze the scanned biometric quality for the upcoming implementation of the recognition system. The recognition process which includes enrollment and matching phase. The enrollment phase consists of unique feature of a user information retrieved from data base is maintained as Template (X_T). Since, various record of different persons is carried by template database, the security maintenance will be difficult one. Various matcher module is used for the recognition of various multimodal biometric features. With the represented similarity the inputs (X_T) and outputs (X_Q) with match score (S), the biometric feature sets are represented. T is the biometric sample obtained from the enrollment process, Q is the query biometric sample obtained in the recognition process, X_T and X_Q are the template and query feature sets, and S represents the match score. The final processing unit in the decision module gives the identity of the individual person as the response of the query sets. The following Fig.1 is the illustration of Decision-Level Fusion.

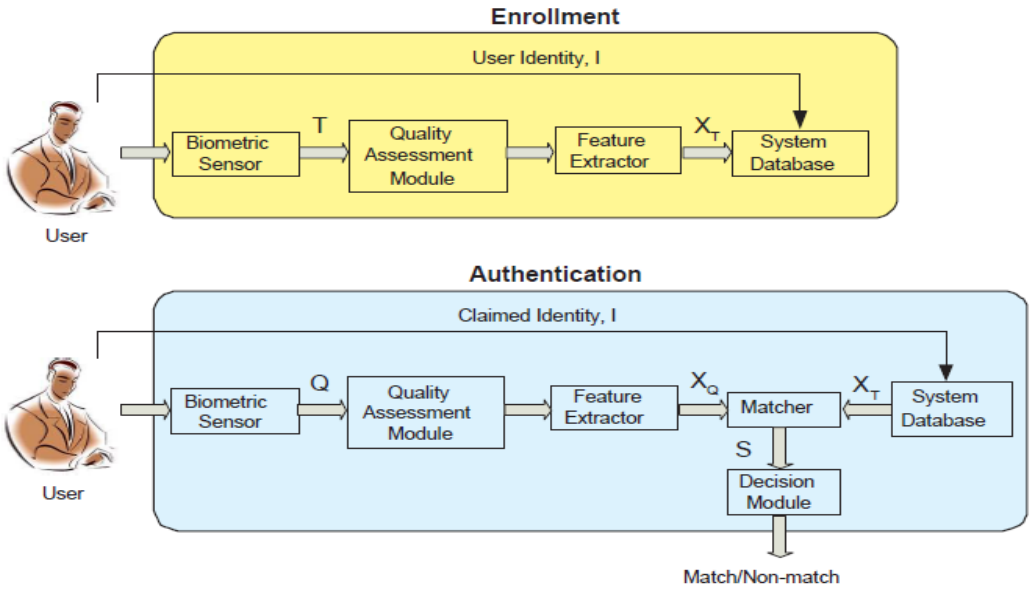


Fig. 1 Enrollment and Recognition Stages in a Biometric System

D. Feature-Level Fusion

In feature-level fusion, feature sets are established using the multiple feature extraction modules. These features are sent towards the matching and ranking modules which gives the result towards the decision modules for identifying a person. The various multimodal recognition uses feature-level fusion process as it gives the high recognition rate as well as the higher information about the matching scores or the matcher decision. Feature level fusion changes are done using the transformation of features [10], shapes of features [11], or encoded features [5], [6]. As there was a certain rule in the existing feature level fusion methods that they need to analyze the ranking level information from the extracted feature set, The analyze of ranking level transformation from the extracted feature set is must Transformation features from the given fusion and the various iteration rate to enhance the recognition technique. The traditional feature level increases the accuracy of the recognition which has not considered the performance of the matchers.

E. Score-Level Fusion

In Score-Level Fusion, the fusion process is used by the scores which are published from the various matching unit. The fused score obtained is sent through the ranking and matching set which gives the results of the person identification process. Score Level Fusion technique has importance in the multimodal recognition process because of the matcher's usage. Score-Level Fusion techniques has been developed as the matchers are easy technique for fusing. Various fusion technique based on the arithmetic operations such as addition, subtraction, maximum, minimum, or median [13]. The scores are used for the weighted analyzes which is used for the improvement in the recognition of multimodal biometric system. The existing score level fusion technique doesn't take in account of individual matchers from the multiple scores. After the normalization process the fusion process is followed. To improve the overall recognition rate accuracy, the normalization is an important factor for the multimodal biometric recognition system. Normalization arises due to the different numerical factors with different statistical conditions in the Score Level Fusion. Since multiple scores may be on different numerical scales, or may not be

homogeneous, or may have different statistical distributions. Fusion process is the important factor in the multimodal biometric system which ends out with the normalization process.

F. Normalization Techniques

In order to increase the recognition rate [3][4][5], the Multimodal biometric system employs different kinds of normalization techniques. By considering the information from the matching scores, the normalization techniques such as Min-Max (MM) Median and Median Absolute Deviation (MAD), Decimal Scaling (DS), Z-Score (ZS) [10], and Improved Anchored Min-Max (IAMM) [3], have been developed. The proposed work completes the necessary security needs from the all known hacking and threats. The secureness in the template level is the difficult task as it has the various difficulties in the design and analysis of template formation. The designing procedure was the time consuming one. As there was a various template protection scheme has developed the biometric cryptosystem [2, 8, 3, 4, 5], is not used for the feature transformation process. The proposed work follows the secured template formation technique which is the next level of normalization process. Thus, the secured template formation technique is noted as the non-invertibility transformation.

G. Non-Invertible Transformation

The secureness of the feature transformation is classified into two main factors they are i) non-invertibility, and ii) diversity. Non-invertibility is used to secure the original biometric information which is not easy to recover by the hackers or any other unwanted persons. The level of difficulty in forecasting one secure template by considering another secure template which is obtained from the same biometric, can be indicated by the diversity. Both the techniques may or may not have the password protection. The effectiveness of matching process which is investigated using the Receiver Operating Characteristic (ROC) curve indicates the level of performance. In this proposed work, the non-invertibility measurement depends upon the fingerprint minutiae-based feature transformation techniques and the iris feature transformation technique for the assessment of the individual person both the technique has the special key. The implemented task consists of the measurement between the number of tries in recovering particular part of the biometric template by providing the transformed template. To obtain the Coverage-Effort (CE) curve the different (coverage-effort)-tuples are plotted.

The computation of a CE curve consists of three main steps:

1. Pre-Processed Image Computation: For the purpose of causing the given transformed minutiae from the transformation of all the pre-processed image minutiae, information is gathered from the pre-processed image that are transformed into minutiae.

2. Minutiae Likelihood Computation: The relative probability function is used to estimate the Kernel density in the preprocessed image.

3. Non-Invertibility Measure Computation: Arrangements in the pre-processed image may leads to the likelihoods computation which is the examination of an adversary checks of the image in certain portions. The major process is explained in the Table.1.

TABLE 1
EVALUATION TECHNIQUES USED FOR FEATURE TRANSFORMATION OF A FINGERPRINT TEMPLATE.

Non-invertibility	Number of adjoining minutiae that alter at the end of transformation [3]
Non-invertibility	Count of various templates capable of producing the given transformed template with unknown key ([3]) and The count of impostor biometric templates which are agreed by a matching mechanism as the corresponding to the given transformed template. ([6])

2. Review of Related Works

There are various fusion methods which is reviewed by various researchers. These fusion methods are categories into various levels based on their fusion performance. They can be rank level, feature level, decision level, score level and sensor or initial level. The individual matchers performance is analyzed using the decision level. Prabhakar, S. and Jain, A. K [4] concluded that the technique of fusion consists of mainly three algorithms namely (Hough, string and dynamic based) and one texture-based algorithm classifier (matched filter) for multimodal biometric recognition. In rare cases the rank level is used in the fusion techniques of multimodal biometrics, which requires the matching score. Bhatnagar, J., Kumar, A., Saggar, N., used board count method for the final level result in the combined rank [5] because of the combination of various matchers. The improvement in the performance is affected by the fusion technique is affected because of several rules for the fusion technique at the score level. L. Hong and A. K. Jain [6] suggested the fusion of two biometrics such as face and fingerprint of the individual person at the score level with the improvement in the accuracy. Thus, the accuracy of the technique mainly increased by the normalization factor.

The vein based biometric authentication with the combination of geometric features of the palm prints in the feature and match score level was implemented by Kumar et al. [7]. The reviewed result shows that the match score level fusion perform with more accuracy than the feature level fusion. Fierrez-Aguilar et al [8] calculated the fusion technique with the fusion of global and local feature sets using the max and sum rule. The iris features and multimodal biometric of face were fused together using the matched score level which is explained by Y. Wang, T. Tan, and A. K. Jain [9]. The first process includes the feature extraction of two biometrics and the second process includes the calculation of un-weighted, weighted sum with the usage of Fisher's Discriminant Analysis Technique and Neural Network with Radial Basis Function (RBFNN). Ke-Han represented that the fingerprint enhancement process is carried our using the median filtering technique which would remove the noise from the enhancement process. By increasing the noise -density it increases the Signal to Noise Ratio (SNR) value may increase [14]. Pavithra. R and K.V. Suresh included that fingerprint identification using the Convolutional Neural Network (CNN) which is trained and tested using the secured template techniques. The mentioned work is executed using the python platform which is used to produce constant accuracy rate

[15]. A. Ross, A. K. Jain, and J. Reisman [2] work consists of the features of fingerprint from the minutiae and ridges with the hybrid matching technique in the fingerprint recognition and authentication system.

Javier and Sébastien reveals the multimodal biometric authentication using the various biometrics such as Iris, Face and Fingerprint. This work includes the quality assessment of the recognition process with the improvement in the accuracy rate [16]. Pattabhi and Ajay concluded the Iris recognition system with the algorithm of Markov Random Fields (MRF) model. This model will include the cross-domain identification in the recognition system [17]. Lozej et al, deals with the Iris recognition using various database such as CASIA Thousand and SBVPI datasets. This dataset consists of various Iris images of different people [18].

3. Proposed Multibiometric System with Template Security

The proposed system mainly consists of, Iris Feature Extraction Module, Fusion Module, Fingerprint Feature Extraction Module and Matching Module. Fingerprint Feature Extraction Module consists of Fingerprint Acquisition, Enhancement and Resizing of Fingerprint Image. In Iris module first in the eye image the iris region is segmented and before using template security it is normalized. The Template Security deals with the secureness of the extracted features Of Iris and Fingerprint. The Non-Invertible transforms, namely, polar and functional (with a mixture of Gaussian as the transformation function) defined in [5]. As the polar transformation includes the central region of the iris image which was tessellated into 6 sectors of equal angular width and 30-pixel wide concentric shells. The condition of the transformation is not altering the shell while shifting only the sector number of the minutiae. The Fig.2 shows the block diagram of the proposed work.

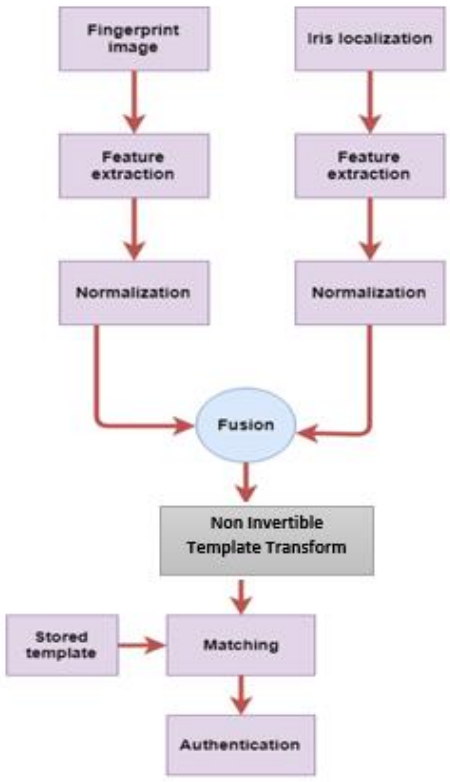


Fig. 2 Block Diagram of the Proposed Work

A. Minutiae Feature Extraction for Fingerprint

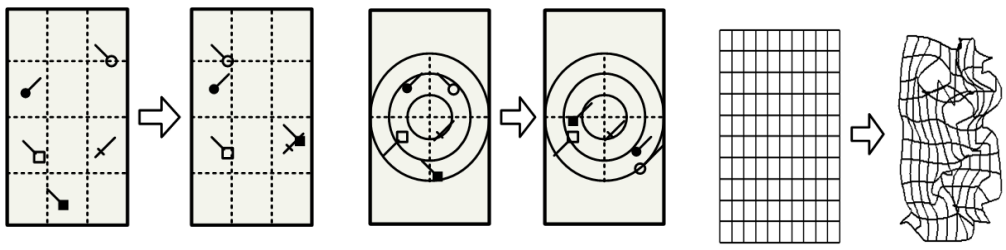
Each Fingerprint image is differentiated by the Minutiae. Minutiae is a small point on the finger which consists of friction ridges end or bifurcate. Fig 3 shows minutiae overlaid of two Fingerprints from the same finger. The important factor to be noted is that the intra-class variation in the fingerprint representations; multiple acquisitions of the same finger which tends to be variation in the different minutiae position and orientation (x, y).

(a) **(b)**

Fig. 3. Two Fingerprint Images from the Same Finger with Extracted Minutiae

Thus, the algorithm for the matching of two different fingerprint in the encrypted format is discussed below. The procedure starts with the Minutiae-Based Fingerprint Template extraction which is represented as T consists of a collection of minutiae. As the two different sets of a same fingerprint is considered which is represented as $T = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), ..., (x_n, y_n, \theta_n)\}$.

The transformation function considered here takes T to another set of n minutiae i.e. $(T) = \{(x_{01}, y_{01}, \theta_{01}), (x_{02}, y_{02}, \theta_{02}), ..., (x_{0n}, y_{0n}, \theta_{0n})\}$. To obtain the difficulty in T given θ (T) it should be estimated by a measure of non-invertibility. A number of minutiae-based feature transformation techniques have been introduced (see [3,6,7]) in which according to a user specific key the configuration of each minutia is changed to obtain the Transformed Template. Ratha et al. [3] proposed three different (a), (b), and (c) show the Cartesian, Polar, And Gaussian Mixture-Based Transformations [3] kinds of transformations i.e. Cartesian, Polar, And Functional as illustrated in Fig 4.



(a) **(b)** **(c)**

Fig 4 Feature Transformation. (a), (b), and (c) show the Cartesian, Polar, and Gaussian Mixture-Based Transformations [3].

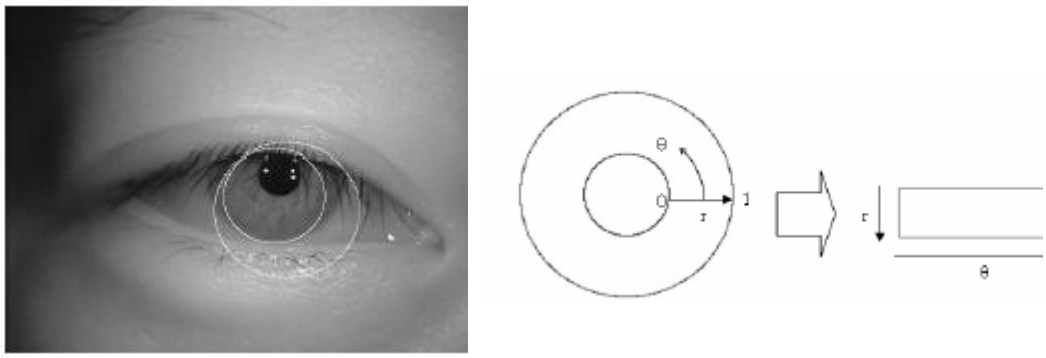
The Non-Invertibility Transforms may lead to the change of the feature point from many to one single point with the knowledge of specific key towards the adversary. The

transformation techniques which includes the Cartesian mode will tessellates the original image into the two rectangular surface which can again transformed towards the single rectangle. In the Polar transformation mode, around a center point the image plane is converted into sections of annular regions. But the transformation of the minutiae is bring about by a function which is evaluated while a minutiae configuration.

B. Iris Feature Extraction

The gathered information about iris from eye region is getting as fraction of the image. The main stages in the Iris Feature Extraction Module are Normalization, Iris Localization, and Discrete Wavelet Transform. The Localization methods includes pupil and the calculation of the boundary of iris and removal of eyelids and eyelashes. Where A (x, y) is the eye image, r is the radius of the search, G Ss (r) is a Gaussian smoothing function and s is the contour of the circle given by r, x, y. In order to find the circular path having maximum alteration in pixel values, the differential operator altering the radius and centre x and y positions of the circular contour.

The main operations involved in the process is the smoothing of edges in the image to reduce the error rate in the localization technique. The final result implements the center coordinates and radius of iris and pupil. The outer layer which is the eyelids and eyelashes are eliminated using the Circular Hough Transform Technique. When the segmentation of Iris is undergone successfully from the image of an eye, the next step is proceeded with the transformation. The transformation is done to fix the Iris region into a fixed dimension which would reduce the localization error. After the segmentation process normalization is carried out which is the main process for the multimodal recognition. The normalization technique which is used here is the Daugman's rubber sheet model [10] which consists of constant dimensions model. The midpoint of the iris is also known as the reference point which moves towards the radial vector. The features from the iris region is selected using the radial line from the reference point and its vertical dimensional point and illustrated in Fig. 5.



(a) Segmentation of Iris **(b) Feature Extraction from the Iris**

Fig 5. Segmentation and Feature Extraction from Iris Images

In the iris image the collection of radial lines is defined as the Angular resolution (O) and it is in horizontal dimension. If the pupil in the iris is tends to be non-circular, the remapping formula [11] is done to collect the rescaled points based on the angle within the circle. As the Iris Normalization is done, it undergoes towards the Fingerprint normalization which finally results in the fusion of features of both biometrics.

C. Normalization Techniques

As there was a various normalization technique in the biometric recognition process, none of the technique includes the genuine and imposter score sets. The improvement in the multimodal biometric system will depends upon the Normalization Technique. As the proposed Normalization Technique consists of various information which is used to interrogate the multimodal biometric system using the SL fusion and the proposed fusion scheme. Hampel influence function, Performance Anchored Min-Max (PAN-MM) [8] and Anchored Min-Max (AMM) [2] or Improved Anchored Min-Max (IAMM) [3] normalization methods, respectively are not essential for our proposed normalization technique. Unlike the Mean – To – Overlap Extrema – Based Anchored Min-Max (MOEBAMM) our proposed normalization technique does not need the information of neighboring scores of the overlap region between the genuine and impostor scores. A block diagram of the proposed normalization technique is shown in Fig.6.

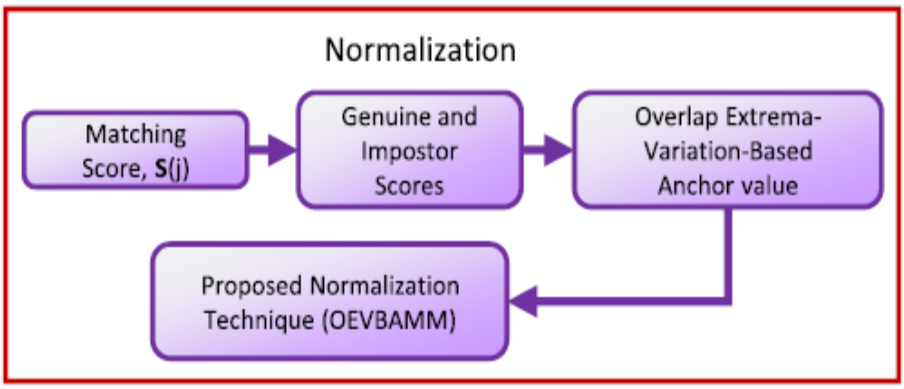


Fig.6 Block Diagram of the Proposed Normalization Technique

From the normalization techniques, the Features of both Iris and Fingerprint is obtained which will under goes the fusion process which is the major processing unit of the Multimodal biometric system.

4. Proposed Matchers Performance Based Fusion Scheme

In this following section, the detailed explanation of the proposed fusion technique which is Matcher Performance Based Fusion (MPBF) is derived. The features obtained from the fingerprint and the iris is taken as *(x, y)* which has the modality rate of *k*. The modality *k* depends upon the number of biometrics used in the recognition system. A block diagram of the proposed fusion scheme is shown in Fig. 7 using two biometric sources. Let the biometric and feature images for the modality k (k=1,2) which is denoted as *X(k)*, and *F(k)*, respectively. Let the feature value at the position (x, y) of *F(k)* be denoted by $f_{xy}(k)$, $h_{xyi}(k)$ being the encoded form of $f_{yx}(k)$, and *i* is the bit position. *F(k)*, $f_{xy}(k)$, $h_{xyi}(k)$ are obtained using feature extraction technique [6].

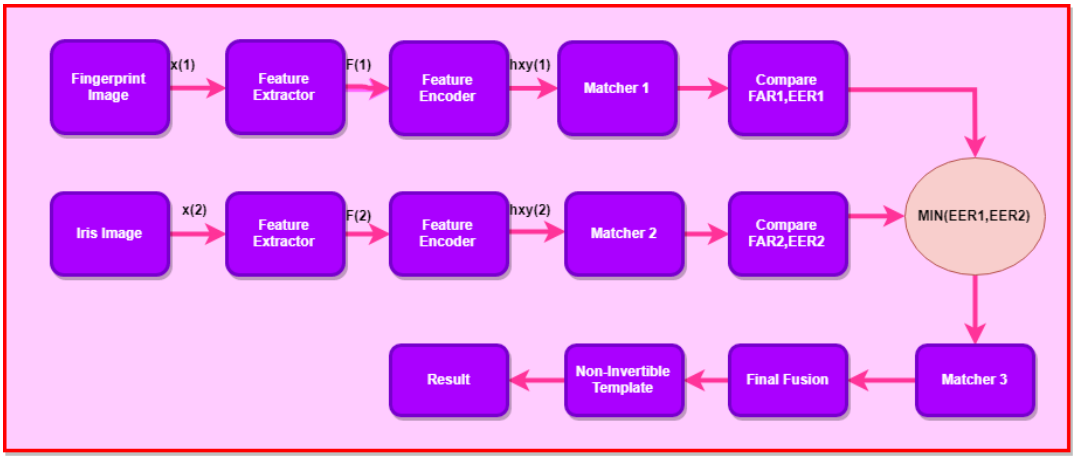


Fig.7 Proposed Matcher Scheme for the Multibiometric Recognition

Next, the matching process are obtained using the Non-Invertible Template Transforms Matching condition. The matching, genuine and impostor score sets denoted by *S(k), G(k) and I (k),* respectively. The proposed MPBF fusion technique consists of two steps, and is described in brief explanation.

SVM for Feature Matching

It mainly consists of subsequent steps:

- Taking imagery into preliminary procedure in the catalog
- Making fragmentation of database in preparation as well as verify the sets taking the input information

  Selecting the mode of training to be used

  1. Multi-class preparation mode
  2. The penalty term c

To secure the penalty term C for misclassification the Training / Preparation Check cum assessment of the performance SVM is employed. The stable value has to be chosen very carefully if the preparation data is not divisible. To make the data in all-purpose linearly noticeable, the input gap is great compared to the training set dimension while dealing with imagery. From the obtained result it can be noted that C is permanent value to a random great one and clearly not making difference

Step 1: In a multimodal biometric system, the calculation of Equal Error Rate (EER) depends upon the acceptance and rejection rates which tends to be equal. The genuine score set *G(k)* and the impostor score set *I (k)* for the modality k in order to select the matcher that provides the lowest EER in comparison with others in a multimodal biometric system using the comparator. The modality *k* which represents the number of biometrics used for the identification of the person. The region of the genuine and impostor scores can be divided into four parts. [12]

For the purpose of computing the threshold values of modality k, two parameters of the genuine and impostor scores, namely, min*(I(k)*), and max(*G(k))*, which are the

minimum value of impostor scores, and maximum value of genuine scores, respectively, are derived. The threshold value is computed for the modality k as follows,

$$Th(k)=[min(I(k)): step\_size: max(G(k))] \quad (1)$$

where

$$step\_size= \frac{max(G(k))-min(I(k))}{p} \quad (2)$$

The argument p maintains the step size for the variable *Th(k)* that is used to calculate the number of falsely rejected genuine and falsely accepted impostor. The value of p and step size are inversely proportional for Th(k). From a several number of experiments conducted, it is concluded that $p=10^3$ is the optimum value for the step size. Then we calculate the count of rejected genuine scores agreed falsely as impostor scores for $G(k)<Th(k)$,and accepted impostor scores accepted falsely as genuine scores for $I(k) \geq Th(k)$, and refer to them as Falsely Rejected Genuine (*FRG(k)*) and Falsely Accepted Impostor (*FAI(k)*) for the modality *k*, respectively, as shown in Fig. 7.

Now, False Acceptance Rate (*FAR*), False Rejection Rate (*FRR*) and EER for the modality *k* are calculated by,

$$FAR(k) = \frac{100*FRG(k)}{length(G(k))} \quad (3)$$

$$FRR(k) = \frac{100*FAI(k)}{length(I(k))} \quad (4)$$

$$EER(k) = \frac{FAR(k)+FRR(k)}{2} \quad (5)$$

The fusion at starting stage is carried out between the encoded features derived from the modalities 1 and 2. Clearly, the encoded features $h_{xyi}(k)$ for the modality k are binary and its digits 1 gives more information when compared to its digits 0. Therefore, the initial fusion can be done using the logical operators, such as XOR, AND, and OR in order to obtain the fused encoded feature. We employ the logical OR operator for fusion at starting stage because it is capable of considering the encoded featured value of '1' at the location (x,y,i) available from the modality 1 or 2.

$$h_{xyi}(1,2) = h_{xyi}(1) \oplus h_{xyi}(2) \quad (6)$$

at the position (*x*, *y*, *i*), and the sign $\oplus$ indicates the logical OR operation. Next, following the method in [30], the matching score *S (4)* is obtained from matcher 4

Step 2: The matching score *S* (4) obtained from Step 1 and the score *S* (3) from matcher 3 are fused using the Weighted-Sum (WS) fusion rule. The Fused score FS_{MPbF}, is obtained as

$$FS_{MPbF}= w(3)\, \boldsymbol{S}_N(3) + w(4)\, \boldsymbol{S}_N(4) \quad (7)$$

where $w(j)$ represents the weight attached to the score from matcher *j* and $\boldsymbol{S}_N(j)$ denotes the normalized value of $\boldsymbol{S}(j)$. In [13], The score normalization is dispensable task under WS rule for the score level (SL) fusion as there is the possibility of getting non-homogenous or of being different numerical scale or of having different statistical distribution matching scores as reported by authors in [13].

The proposed method includes the major processing unit called non-invertibility transform which leads to the protection of the original information. As the fusion has been carried out, the results of the fusion are followed by the secured template formation which is formulated by Non-invertibility transforms.

5. Non-Invertibility Measure

Template Formation is the major task in the proposed work. The main difficulty arises in the formation of secured template during the multimodal biometric recognition. Using the non-invertibility transform the secureness of the template formation is carried out. In the Non-Invertibility Transform, the transformation process is carried out using the similar adversary which could not find the real template from the transformed template. The template security structures has been classified into various classes such as Feature Transformation Approach and Biometric Cryptosystem.

The transformed template gathered as database unit is formed by substituting a transformation function (F) towards the biometric template (T) in the Feature Transform Approach. The features of the transformation technique are extracted from the fusion process. This fusion process which extends the random key (K). The query features (Q) which consists of the transformation function (F (Q, K)) is matched with the transformed template (F (T, K)). The further categorization of transformation technique is carried out on the basis of the features of the transformation function F. Although the key is known, it is difficult to invert a transformed template in the case of Non-Invertible Transformation schemes as it is generally a one way function on the template. The entire Non-Invertibility Template Transformation and Authentication process is shown in the Fig.8.

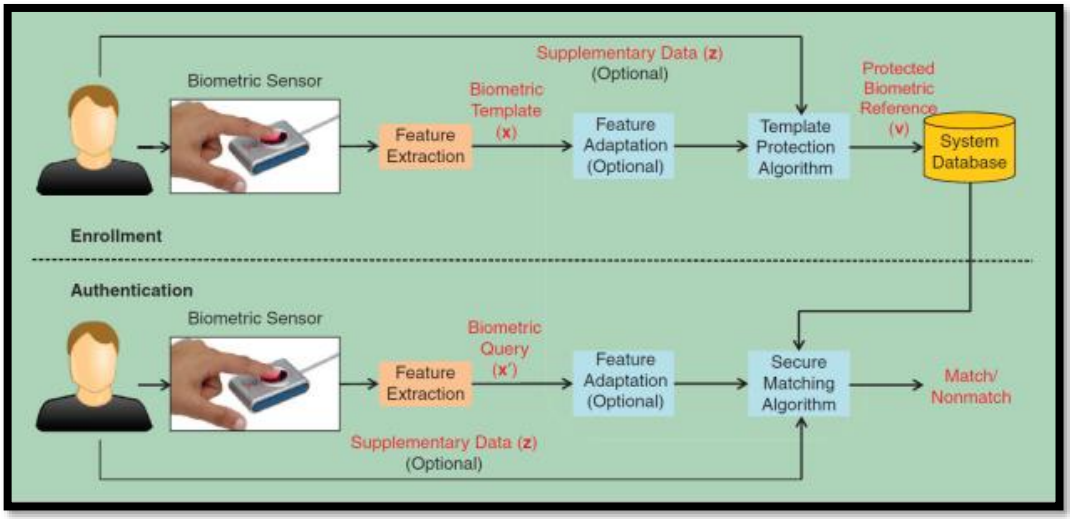


Fig.8 Non-Invertibility Template Transformation and Authentication

A. Role of Non-Invertibility Transform in Secured Template

The Functional Transformation technique depends upon the combination of Gaussian and variance techniques which results in the formation of Non-Invertibility because of its generic nature [3]. As there is a need to transform a minutia, the combination of gaussian with the variance derivatives with the position value of minutia is used. The proposed work consists of biometric template formation with the secured manner. This protection was given by the technique called Non-Invertible Transformation. Non-Invertible

Transformation also referred as one-way function which is represented as F which is easy for matching but difficult to transform towards the original feature. It is given F(x), the probability of finding x in polynomial-time is small.

The factors of the transformation technique are concluded by the random key (K) which is obtained from the query feature set at the time of authentication process. The main aim of this proposed technique is that the key factor or the transformed template features are known, one cannot recover the original information from the transformed template or the key. The procedure of the Non-Invertibility includes the three stages namely,

- Preprocessed-Image Identification,
- Preprocessed-Image Likelihood Evaluation
- Non-Invertibility Measure Computation.

The computing mechanism for the Non-Invertibility transformation begins with the count of tries made by an adversary to identify the original minutiae set employing a certain attach strategy. As we consider the fingerprint biometric, the different minutiae which is represented as *n* in the transformed template from the Preprocessed image. The output of the fusion which is done using the feature level and score level will leads towards the secured template formation. The proposed work shows the secured template formation with the use of non-invertibility transform in the biometrics such as iris and fingerprint. The flowchart in the Fig. 9 indicates the performance analysis of the various fusion technique with the proposed fusion structure.

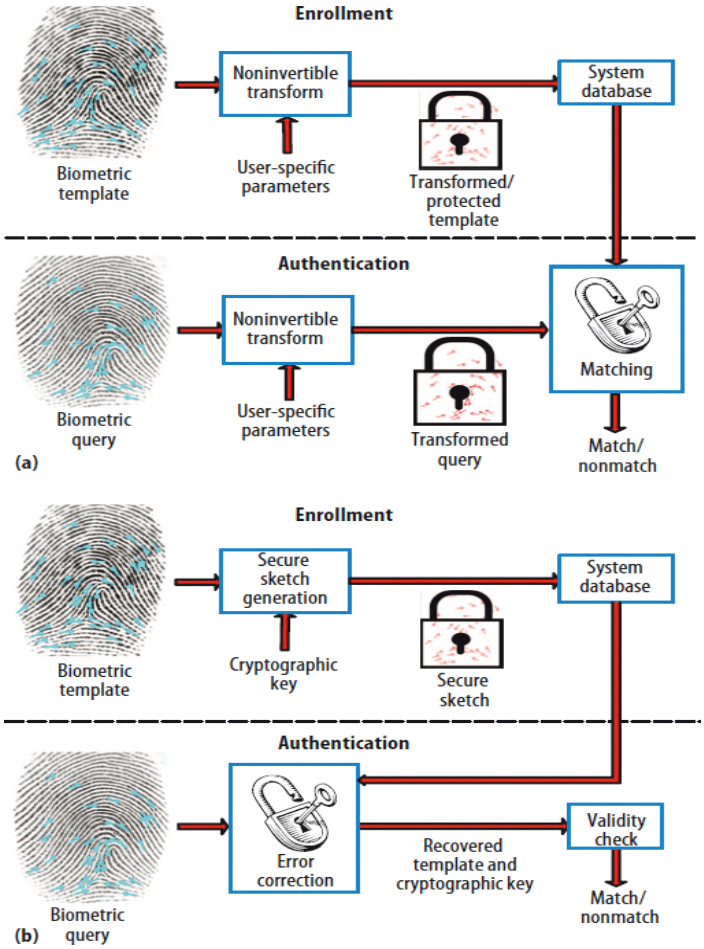


Fig 9. Shows the Template Formation and Matching using Non-Invertible Transform using Single Biometric

As the multi biometric recognition can also done using the same method in the non-invertible transform with the help of fusion process as explained above. A binary template produced by the feature extraction and it contains the iris and fingerprint representation. From the fingerprint and iris features, the multi biometric template was created by using the feature level fusion technique. The transformation of templates into row vectors and joining one at the end of the other to carry out this process of the feature level fusion. As the fusion output is obtained from the equation 8 (FS_{MPbF}), the template formation undergoes by changing the rows and column vector in the obtained binary code of fused features (iris and fingerprint). The matching of the stored template in the data base with feature derived from the query image is employed to carry out the authentication process.

The computation of each elementary permutation matrix of the fusion image involves choosing and interchanging a couple of rows of a general permutation matrix randomly. An n by n general permutation matrix is used to compute a total of n! elementary permutation matrix. The combination of elementary permutation matrices with the fusion matrices produces the non-invertible matrices. The non-invertible matrices are obtained by multiplying the fusion matrices. The non-invertible template obtained is denoted as $M_{T.}$

$$M_T = FS_{MPbF} * FS_{MPbF}\text{‘} \qquad (8)$$

where FS_{MPbF} is the fused score of the iris and fingerprint image and FS_{MPbF} ‘is the transformation of matrices of the fusion score in iris and fingerprint images. The Transformed Template (M_T), is stored in the database not the original feature vector (x,y).

6. Experimental Results

The Database images such as Fingerprint and Iris images are obtained from the two databases namely U which captures the fingerprint images using the U 4500 Fingerprint reader and the CASIA v4. The fingerprint images consist of Eight fingerprint images per individual person. The collection of 20 person images which tends to be 160 images to form the Fingerprint database. The iris database consists of Eight images of that same individual person. Thus, the same 20 persons Iris images were collected which is around 160 images in database. The implementation of the proposed work is done in the MATLAB. The principal goal of the proposed work is formation of the template and to implement it in the fusion of Iris and Fingerprint images. The implementation is done using the matching of query image features with the stored database template features. The score of the matched authentication is shown as the genuine scores and the non-matched authentication is shown as the imposter scores. By calculating the threshold value, False Accept Rate (FAR) and False Reject Rate (FRR) can be found. The False Accept Rate (FAR) is defined as the ratio of the False matching to that of threshold value. False Reject Rate (FRR) is defined as the ratio of the False Rejection to that of threshold value. The ratio between number of genuine images of the persons and total number of the persons in the database collection is used to the Genuine Acceptance Rate (GAR). Thus, the Equal Error Rate calculated is defined as EER. If the EER value is low, GAR value is high, FRR value is low, FAR value is also appeared to low then the process provides higher accuracy in the biometric system recognition. The performance evaluation of the proposed work is shown in the Table 2 with a comparative performance.

TABLE 2
PERFORMANCE ANALYSIS OF PROPOSED METHOD

MEASURE	SF	MPBF	SF-NI	MPBF-NI
EER (%)	0.54	0.47	0.31	0.30
GAR (%)	95.47	96.73	97.62	99.01
FRR (%)	0.53	0.27	0.20	0.18
FAR (%)	0.60	0.71	0.52	0.35

Table 2 provides the performance analysis based on Equal Error Rate (EER), Genuine Acceptance Rate (GAR), False Reject Rate (FRR) for SF- Single Fusion, MPBF - Matcher Performance Based Fusion, SF-NI - Single Fusion with Non-invertibility, MPBF-NI - Matcher Performance Based Fusion with Non-Invertibility.

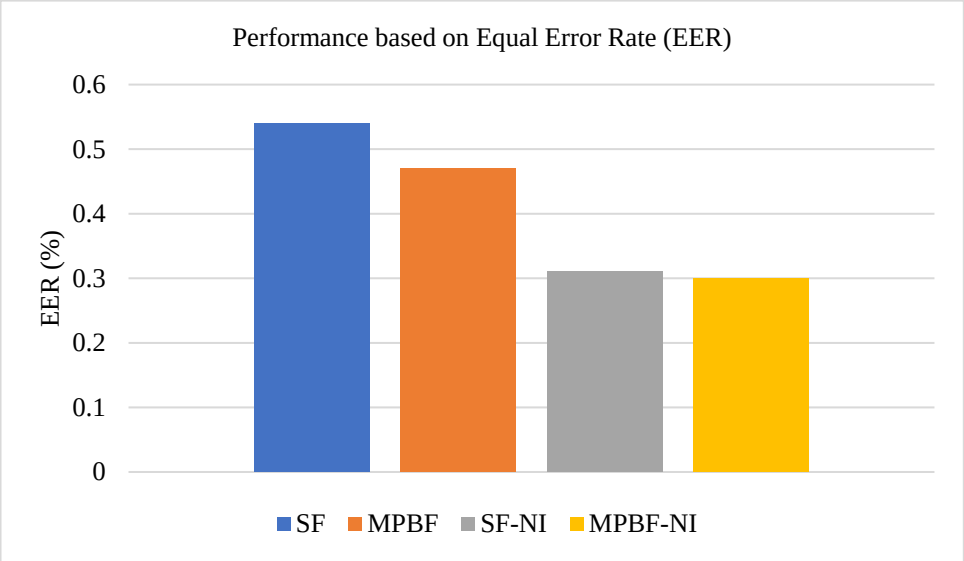


Fig.10 Performance Analysis Based on Equal Error Rate (EER) for 20 Persons

The Genuine Acceptance Rate (GAR) will be lesser in the Single Fusion technique due to the lesser number of matchers whereas the Matched Performance based technique consist of better GAR rate as compared to the Single Fusion due to the 3 matchers in the fusion technique. The proposed system Matched Performance based Fusion with Non-Invertibility consist of n number of matchers which would gives the best GAR rate as compared with the other proceedings.

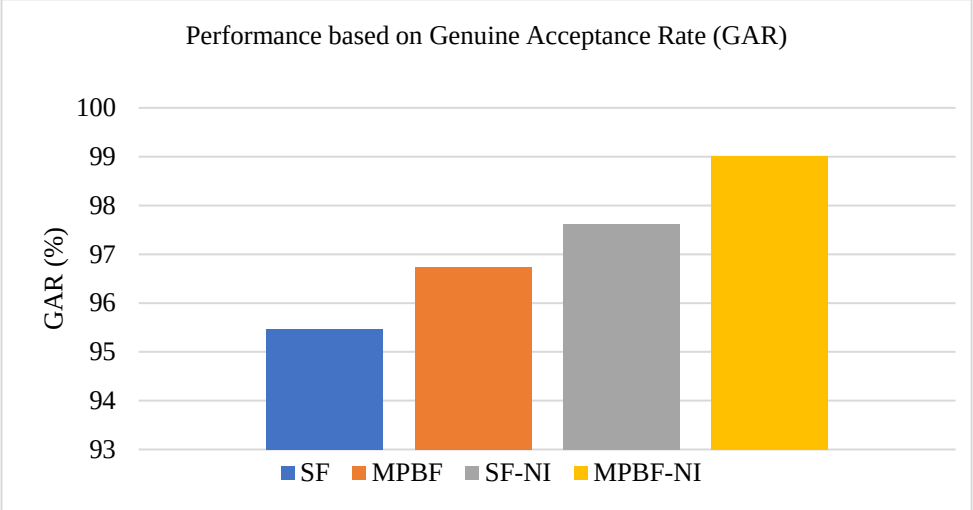


Fig.11 Performance Analysis Based on Genuine Acceptance Rate (GAR) for 20 Persons

The False Reject Rate (FRR) taken into account based on the false biometric rejected. This False Rejection Rate will be high in the Single Fusion due to the greater number of attackers with the lesser adversary techniques. As proposed algorithm have the lesser False Rejection Rate due to increase in the template security which leads to the less attackers.

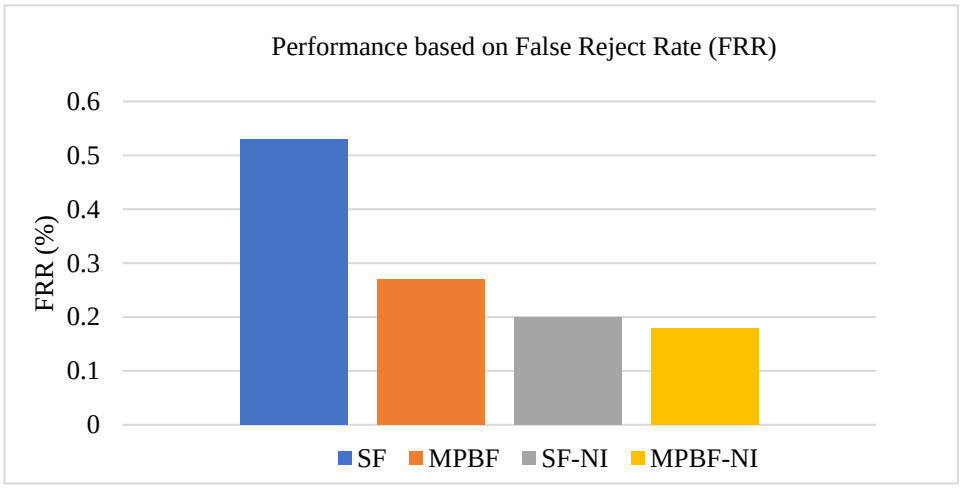


Fig.12 Performance Analysis Based on False Reject Rate (FRR) for 20 Persons

A pictorial representation which gives the connections between the parameters tends to be defined as Receiver Operating Characteristics (ROC). It is mainly used for the analyzing of the overall performance of the multi biometric system. By representing on ROC plots with their independent thresholds, the effectiveness of various biometric system is compared. The ROC characteristic of the proposed work is shown in the Fig.13.

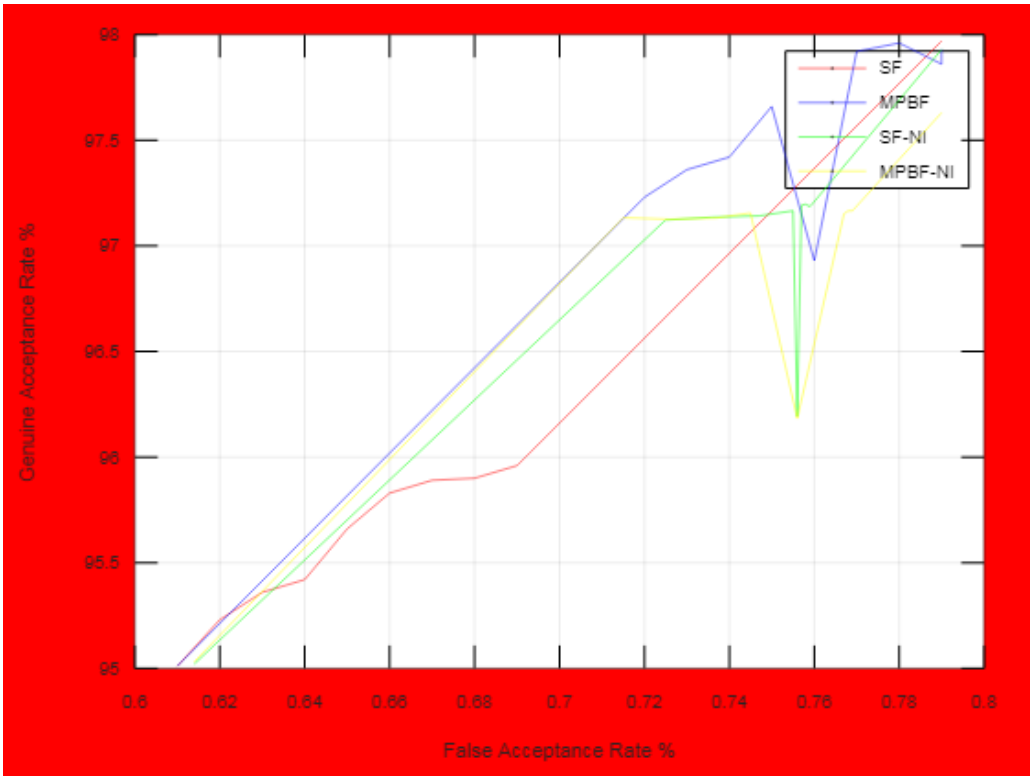


Fig.13 ROC Performance Analysis of Various Fusion Techniques

By analyzing the characteristics of ROC, it is pointed out that proposed technique has the lower False Acceptance Rate (FAR) than that of existing techniques. This is noted that the Genuine Acceptance Rate (GAR) of the Matched Performance Based Fusion with Non-Invertibility is higher than that of the Single Fusion with Non-Invertibility. By comparison with the existing methods of Single Fusion and Matched Performance Based Fusion, the implemented technique has the higher rate of genuine acceptance which tends to increase in accuracy.

7. Conclusion

The proposed work achieves the required accuracy rate as they have the various number of matcher block as well as the secureness in the Template Formation technique. According to the fusion process, the original template is protected and it forms the basis of Template Formation. The Error rate of the proposed work will be low as compared with the various algorithm due to the secured template formation which acquires the accuracy range of 99% in the authentication and recognition process.

References

[1] Ross, K. Nandakumar, and A. K. Jain, Handbook of Multi-biometrics. New York, NY, USA: Springer, 2011.
[2] Juels and M. Sudan, “A Fuzzy Vault Scheme,” in Proc. IEEE Int’l on Information Theory, Lausanne, Switzerland,2002, p. 408.
[3] Juels and M. Wattenberg, “A Fuzzy Commitment Scheme,” in Proc. 6th ACM Conference on Computer and Communications Security, Singapore, November 1999, pp. 28–36.
[4] K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security,” EURASIP Journal on Advances in Signal Processing.

[5] Kumar and S. Shekhar, ``Personal identification using multi-biometrics rank-level fusion," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 41, no. 5, pp. 743752, Sep. 2011.
[6] Andrew B.J. Teoh, Yip Wai Kuan, and Sangyoun Lee, "Cancellable biometrics and annotations on bio-hash," Pattern Recognition, vol. 41, no. 6, pp. 2034–204s4, 2008.
[7] Haynes and M. Todd, ``Enhanced damage localization for complex structures through statistical modeling and sensor fusion," Mech. System Signal Process., vols. 5455, pp. 195209, Mar. 2015.
[8] Fuster-Garcia, A. Bresó, J. Martínez-Miranda, J. Rosell-Ferrer, C. Matheson, and J. M. García-Gómez, ``Fusing actigraphy signals for outpatient monitoring," Inf. Fusion, vol. 23, pp. 6980, May 2015.
[9] Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and Revocable Fingerprint Recognition," in Proc. Computer Vision and Pattern Recognition, Minneapolis, June 2007
[10] Globally, J., Marcel, S., & Fierrez, J. (2013). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE transactions on image processing, 23(2), 710-724.
[11] S. Bhatt, R. Singh, and M. Vatsa, ``On recognizing faces in videos using clustering-based re-ranking and fusion," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 10561068, Jul. 2014
[12] Han, K., Wang, Z., & Chen, Z. (2018, November). Fingerprint Image Enhancement Method based on Adaptive Median Filter. In 2018 24th Asia-Pacific Conference on Communications (APCC) (pp. 40-44). IEEE.K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint based Fuzzy Vault: Implementation and Performance," IEEE Trans. Information Forensics and Security, vol. 2, no. 4, pp.744–757, 2007.
[13] Lozej, J., Stepec, D., Struc, V., & Peer, P. (2019). Influence of segmentation on deep iris recognition performance. Ar-Xiv preprint arXiv: 1901.10431.
[14] M. M. Monwar and M. L. Gavrilova, ``Multimodal biometric system using rank-level fusion approach," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 39, no. 4, pp. 867878, Aug. 2009.
[15] M. R. Alam, M. Bennamoun, R. Togneri, and F. Sohel, ``A condense based late fusion framework for audio-visual biometric identification," Pattern Recognition. Lett., vol. 52, pp. 6571, Jan. 2015.
[16] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancelable Fingerprint Templates," IEEE Trans. PAMI, vol. 29, no. 4, pp. 561–572, April 2007.
[17] Nalla, P. R., & Kumar, A. (2016). Toward more accurate iris recognition using cross-spectral matching. IEEE transactions on Image processing, 26(1), 208-221.
[18] P. P. Paul, M. L. Gavrilova, and R. Alhajj, ``Decision fusion for multimodal biometrics using social network analysis," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 11, pp. 15221533, Nov. 2014.
[19] Pavithra, R., & Suresh, K. V. (2019, April). Fingerprint Image Identification for Crime Detection. In 2019 International Conference on Communication and Signal Processing (ICCSP) (pp. 0797-0800). IEEE.
[20] Q. Tao and R. Veldhuis, ``Threshold-optimized decision-level fusion and its application to biometrics," Pattern Recognition., vol. 42, no. 5, pp. 823836, May2009. processing, January 2008.
[21] R. Nishii, ``A Markov random field-based approach to decision-level fusion for remote sensing image classification," IEEE Trans. Geo-science. Remote Sens., vol. 41, no. 10, pp. 23162319, Oct. 2003.
[22] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data," SIAM Journal on computing, vol. 38, no1, pp. 97–139, 2008.
[23] Y. Sutcu, H. T. Sencar, and N. Memon, "A Secure Biometric Authentication Scheme Based on Robust Hashing," in Proc. ACM Multimedia and Security Workshop, New York, August2005, pp. 111–116.