Fusion Based Multimodel Biometric Authentication System using Ear and Fingerprint

Thorepadi Kannappan Thivakaran[1*]   Sathya Veera Venkata Naga Chanukya Padira[2]
Ayyanar Sanjeevi Kumar[2]   Sureddy Sivar Reddy[3]

[1]*Sri Ramaswamy Memorial Institute of Science & Technology, Ramapuram, Chennai, India*
[2]*Meenakshi Academy of Higher Education and Research University, Chennai, India*
[3]*Loyola Institute of Technology and Management, Dullipalla, Guntur, India*
* Corresponding author's Email: tktsrm4@gmail.com

Abstract: Biometrics is the art of distinguishing or analysing the identity of a person in view of physiological or behavioural attributes. Biometric recognizable strategies have turned out to be more productive, natural and simple for human identification compared to conventional techniques. Biometric validation frameworks basically design recognition frameworks, the physiological qualities like finger impression, face, and hand geometry, DNA and iris acknowledgment. The primary aim of the method is to build up a biometric validation framework by utilizing the ear and fingerprint images to distinguish a genuine user. In pre-processing step, all images are enhanced by thinning and binarization method for extracting the features. Then, a feature extraction system incorporates Minutiae and Singular point procedure for fingerprint images. Ear features are extracted by utilizing Speed Up Robust Features (SURF) and Binary Robust Invariant Scalable Keypoints (BRISK) systems. The features are fused by concatenating the fingerprint and ear features to obtain accurate information. Finally, matching is completed by registration and similarity score process and after that by utilizing the threshold esteems, the users are distinguished as genuine or an imposter. The experimental results demonstrated that the proposed multi-model biometric accomplished 95.66% precision with the error rate of 0.0434.

Keywords: Multi-model biometric, Fingerprint, Ear, Feature level fusion, Minutiae and singular point technique, Pre-processing.

1. Introduction

Reliable authentication of people has turned out to be more significant in the course of the most recent couple of years. The verification applications extend from border control to online banking system or smart phone unlocking [1]. Identification is the basis of each access control framework, specifically, there are three distinct strategies for verifying possessions. The first method uses the cards, keys and badges of a person. The second technique incorporates knowledge like client id, secret password, Personal Identification Number (PIN). The last technique is Biometrics like fingerprint, face, ear [2]. Rather than first and second techniques, biometric verification techniques straightforwardly

check the identifiable individual [3]. Physiological biometrics utilize algorithms and different strategies to characterize the personality in terms of information gathered from direct estimation of the human body [4]. A unique mark and fingerprint, hand geometry, palm prints, Iris and retina, facial geometry are generally precedents of physiological biometrics. Behavioural biometrics are characterized by dissecting a particular activity of a man, which contains a voice ID, signature elements, keystroke elements and movement acknowledgment [5]. Generally, a biometric identification process can be partitioned in two general classes' specifically dynamic and passive biometrics. Dynamic biometrics requires the subject to participate effectively in both enrolling into the framework and also in the identification process. Precedents

incorporate all technologies like Fingerprint, Hand geometry, Retina examining innovations and Signature acknowledgment advances for identification [6], [7]. Passive biometrics do not require a client's participation and it can be successful without a human knowledge, that they have been investigated [8]. Precedents of biometric technique incorporate Voice acknowledgment advances, Iris acknowledgment innovations and Facial acknowledgment.

The most widely recognized modalities utilized in biometrics are face, iris and fingerprint impression. However, these modalities experience the drawbacks such as, the face can be influenced by age, health conditions and external appearances, the iris is an intrusive modality, and the finger impression can be influenced by some drug, burns or ink on fingers. The human ear acknowledgment is a new biometric innovation because that the human ear has the capability of being a novel element of an individual [9]. The ear has numerous characteristics that improves the features than other biometric features, namely face and unique finger impression. [10]. Unlike the face, the ear is a moderately stable structure that does not change much with the age and external appearances. The shape of the ear does not change because of emotions as the face does, and the ear is generally consistent over a human's life [11]. The ear's smaller size and uniform colour shading are desirable qualities for design acknowledgment. The uniform dissemination of shading implies that all data is rationed while changing over the original picture into dim scales. However, ears may be impeded by ear ornaments and hair, which makes ear Biometry as a challenging issue [12], [13]. Numerous methodologies and a few researches have been proposed to extricate unique features from the human ear to distinguish individuals rely upon this feature. In this work, the proposed method implemented a design of ear and fingerprints biometric with the feature level combination technique. This method includes three major steps such as pre-processing, feature extraction and matching process. Novelty: The pre-processing step includes enhancing the original images of ear and fingerprint for extracting the information by using binariazation and thinning method. By using pre-processing, the minutiae are correctly extracted from the fused images. After, pre-processing the feature extraction method extracts the features from the enhanced images by using Minutiae, Singular Point, BRISK and SURF techniques. These feature extraction methods are used to speed up the proposed method. The matching process is carried

out by registration using affine transform and similarity score identification technique. The proposed method attempts to combine the data at the feature level prior to matching, because of two fundamental reasons. The amount of data accessible to the framework drastically diminishes once matcher (of a biometric framework) is invoked. The list of features contains richer data about the raw biometric information than the match score or a final choice. The proposed technique accomplished better execution over the unimodel biometric framework. The outcomes are presented in the Result sections. Compared to the existing multimodels, the proposed method achieved 95.96% accuracy with low error rates of 0.11% false acceptance rate.

The rest of the paper is organized as follows, section 2 discusses the related work, section 3 describes the proposed approach and its phases, section 4 presents the experimental results, and finally conclusion and future work are provided in section 5.

2. Literature review

There are many existing biometric systems that provide identification of individuals. Related works on multi-model biometric in the existing systems [14–18] are reviewed and discussed for identifying individuals.

Z. Huang, Y. Liu, C. Li, M. Yang, and L. Chen, [14] presented a face and ear based multimodal biometric framework by utilizing Sparse Representation (SR), which coordinated the face and ear at the feature level, and effectively modify the combination rule based on the reliability contrast between the modalities. The strategy initially built up a novel index called Sparse Coding Error Ratio (SCER) to detect the dependability distinction among face and ear query samples. In multimodal characterization stage, SR-based classification strategies were utilized, i.e., Multimodal Sparse Representation based Classification with feature Weighting (MSRCW) and Multimodal Robust Sparse Coding with feature Weighting (MRSCW). The experimental results showed that both MSRCW and MRSCW performed fundamentally superior to existing unimodal acknowledgment using either face or ear alone, and in addition to the known multimodal strategies. The assessment of MSRCW-MRSCW proceed only on small scale multimodal databases.

K. Annapurani, M. A. K. Sadiq, and C. Malathy, [15] used a remarkable strategy to extricate the tragus feature of the ear. The technique built an improved edge identification strategy for

anticipating the ear feature tragus which is nearly impediments free. In order to build up a proficient ear authentication framework, the feature level combination was connected. The validation rate of the framework with the features of tragus, shape of the ear and the fused format was ascertained by utilizing the Hamming distance system and Euclidean distance strategy. The experiment results demonstrated that the exactness of the technique in fused features was superior to the individual features of tragus and the ear shape. The strategy taken only a few samples with impediments for testing purposes, in addition, the security of the framework during catching, transmission of ear images was not considered in this framework.

R.N. Balaka, and P.B.M. Surendra, [16] developed a Multimodal Biometric Authenticated framework that used more than one biometric quality for acknowledgment. The present framework deal with two biometric qualities such as face and finger for acknowledgment and then extracted features by utilizing Histogram Oriented Gradients system (HOG). The Probability Density Function (PDF) values were obtained from the HOG features by utilizing Gaussian mixer technique. At last, the combination the PDF esteems by utilizing score level combination. The work was useful for reducing the size of the database, usage of transmission capacity, recognizable proof of characteristics and authentication in bank framework, crime examination and so on. The technique considered only two traits, but testing the validation of the framework required a number of traits.

A. Prakash, [17] introduced a Continuous Authentication (CA) framework for verifying the client consistently once a person was signed in. The strategy passively checked the framework without intruding on the clients work progress. In this paper, score level fusion was completed by using genetic particle swarm optimization technique and utilized classifiers as Naive Bayes for acknowledgment process. The test results demonstrated that the system had accomplished better execution performance esteems for consistent confirmation process. By continuously verifying the framework, the CA technique consumed additional time and more CPU assets.

K. S. Bayram, and B. Bolat, [18] a protected multi biometric framework was created where three different biometric modalities ear, face, and thermal face were considered. For every methodology, three feature extraction techniques were utilized and four different classifiers (multilayer perceptron, decision tree, Support Vector Machines (SVM), and

probabilistic neural system) were trained by utilizing two combination strategies (i.e. matching score level and feature level combination). According to the results, the individual biometrics using ear images gave a better result than other biometric images for identifying the person. In feature level combination, SVM gave better outcomes in FAR/FRR esteems with matching score level, while other classifiers achieved less performance in FAR/FRR. However, the differences between the combination techniques were very small, hence, finding the distinction was not a simple procedure to choose best classifiers.

To overcome the above issues of the existing methods, the proposed method implemented the multi-model biometric such as ear and fingerprint images for the identification process. The proposed method uses hybrid feature extraction techniques to extract the features for verification process.

3. Proposed method

The human ear is a perfect source of information for passive individual distinguishing proof. Ear is considered as a good candidate solution, because their pictures are easy to take and structure of ear does not change drastically after some time. Ear fulfils the biometric trademark such as distinctiveness, collectability, universality and permanence.
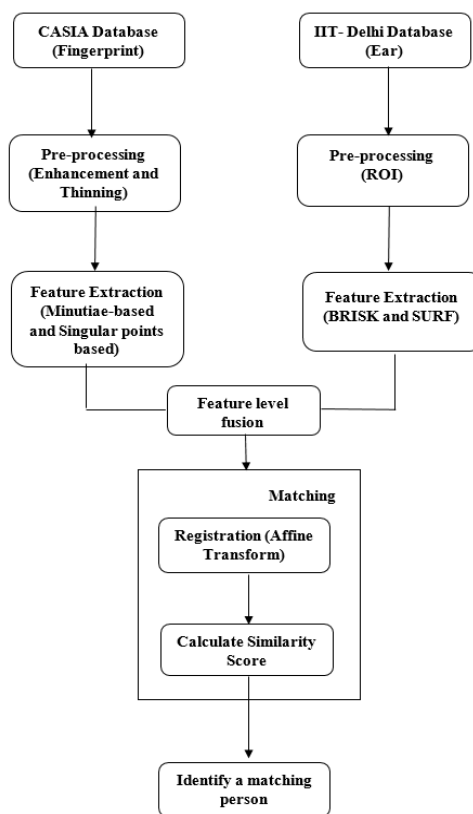

Figure.1 Structure of proposed method

Like other biometric framework, the proposed framework consists of three stages: pre-processing, feature extraction and matching. Biometric frameworks vary in the way in which these three stages are proficient. Fig. 1 shows the outline of the proposed methodology by considering all these three phases. First, in pre-processing stage, enhancement, Binarization, thinning and Region of Interest (ROI) techniques are used for enhancing the input fingerprint and ear images. Second, the proposed method uses different feature extraction methods for extracting the features from the enhanced ear and fingerprint images. Before matching process, the features of both fingerprint and ear images are fused by the feature level fusion process. Finally, the matching phases include the registration method using Affine Transform then calculate the similarity score for matching the particular person. Details about each stage are given in the following subsections.

3.1 Dataset

In this study, two different biometric measurements such as ear and fingerprint are considered to design a secure biometric system. The databases for both measurements are described below.

3.1.1. Description of the IIT Delhi ear database:

The IIT Delhi Ear Database predominantly comprises of the hand pictures gathered from the students and staff at IIT Delhi, India. This database obtains basic ear images from Oct 2006-Jun2007 for authentication. The database is acquired from a group of people in the range of 14 and 58 years. The resolution of these images is 272x204 pixels.

3.1.2. Description of CASIA database

CASIA Image Database (CASIA-fingerprint) has been used in this method for verifying the authenticated person and these database contains images of iris, palm, finger since 2002. In this work, the method collected a sample of 10 person's ears and fingerprint images. Each sample image contains 5 different images to perform the pre-processing step.

3.2 Pre-Processing

Image enhancement is an initial step in image processing. Pre-processing enables to get higher quality images for the purpose of improving the recognition rate. In this work, the images (ear and
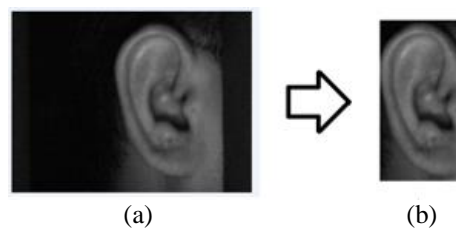

<center>(a)   (b)</center>

Figure.2 Pre-processing of ear images: (a) input image of ear and (b) enhanced image of ear

fingerprint) are re-sized into the 60×60 dimension, then the ROI, thinning, binaryzation are applied in order to improve the image quality.

3.2.1. Pre-Processing for Ear

A rough ROI is used to reduce the unnecessary burden of the proposed method, by placing around the candidate areas to remove the unwanted information. During training, the ROI was found using the marked positions themselves. During computerized land marking, the ROI is discovered by using the general protest discovery system [19]. After the ROI is discovered, a histogram standardization is performed, in which the brightness values inside the ROI is extended to cover the majority of the dynamic range. The histogram stretch parameters are modified to pass out at most 2% of the pixels in the ROI, and to white-out at most 1% of the pixels. Fig. 2 describes the pre-processing of ear images as shown in Fig.2.

3.2.2. Pre-processing for fingerprint

The first step in fingerprint matching is to effectively extract the features from the input finger impression images, which is a difficult task. The execution of a minutiae extraction technique heavily depends on the nature of the input images of fingerprints. The quality of the input images is robust with the help of enhancement algorithm, which is used for improving the performance of extraction algorithm and also improves the clarity of edge structure. Unique fingerprint enhancement can be processed on either gray-level images or binary ridge images. In the binary ridge image, the esteem 1 is assigned to all ridge pixels, whereas the esteem 0 is dedicated to all the non-ridge pixels. In a grey level unique finger impression picture, edges and wrinkles in a local neighbourhood form a sinusoidal-shaped plane wave which has a well characterized orientation and frequency.

The primary step of the unique finger impression enhancement algorithm incorporates:
1. **Standardization:** The primary aim of standardization is to decrease the varieties in

grey level qualities along the edges and wrinkles, which encourages the resulting processing steps.

2. **Orientation estimation:** The orientation picture is assessed from the standardized input finger impression picture. This image describes an inherent property of the unique finger impression pictures and characterizes invariant directions for edges and wrinkles in a local neighbourhood.

3. **Local frequency estimation:** The frequency picture is computed from the standardized input finger impression picture and the evaluated orientation picture.

4. **Filtration:** A bank of Gabor channel is tuned to local edge orientation and edge frequency is applied to the edge and-wrinkle pixels in the standardized input finger impression picture to obtain an improved fingerprint image.

In this proposed work, the enhanced images are further thinned by Binarization and thinning process. Fig. 3 explains the process of pre-processing of fingerprint images. The process of converting grey level images into binary images is called as Binarization. This enhances the differentiation between the edges and valleys in a finger impression picture, and encourages the extraction of minutiae. The binarization procedure includes analysing the grey level estimation of every pixel in the enhanced picture, and, if the esteem is more prominent than the threshold limit, at that point the pixel esteem is set to a binary esteem one; else, it is set to zero [23]. Once the threshold value is calculated, the binary picture normally experiences a morphological thinning task, where edge structures are decreased to 1-pixel thickness, referred as the skeleton, in order to help minutiae identification.

3.3 Feature extraction

In this section, feature extraction of ear and fingerprint are obtained. Ear feature extraction identifies many feature points including the standard features of the ear. Minutiae and Singular points based analysis are used to identify the fingerprint features.

3.3.1. Feature extraction for ear

In proposed methodology, by employing hybrid feature selection the global and local features are extracted from the enhanced ear image. It is done by applying features like Speed Up Robust Features (SURF) and Binary Robust Invariant Scalable Keypoints (BRISK). The SURF is used for processing the several transformations in images to extract the local features that are faster, robust and most significant in integral images.

Likewise, the global features are isolated by utilizing BRISK, which is executed with a component of orientation compensation in order to decide the orientation of keypoint and pivot. The following feature descriptors are explained below.

3.3.1.1. Speed up robust features

The following section summarizes the SURF algorithm, which is a robust local feature descriptor that is widely used in computer vision applications. This algorithm has three major steps, those are, Integral Image Generation (IIG), Interest Point Description (IPD) and Interest Point Localization (IPL). In SURF, the detection of key points depends on the scale space theory. In order to determine the SURF features in an image I, this algorithm employs fast Hessian detector. Here, the Hessian Matrix (HM) is identified correspondingly to every pixel position of the image I and it is mathematically given by Eq. (1),

$$H(X, \sigma) = \begin{pmatrix} C_{xx}(X, \sigma) & C_{xy}(X, \sigma) \\ C_{yx}(X, \sigma) & C_{yy}(X, \sigma) \end{pmatrix} \qquad (1)$$

Where, X is represented as the point of the image, σ is mentioned as scale,

Normally, $C_{xx}(X, \sigma)$ is denoted as the convolution of Gaussian second order derivative of image at the corresponding point with co-ordinates (x, y). The Gaussian second order derivative is represented as in Eq. (2),

$$\frac{\partial^2}{\partial x^2} g(\sigma), g(\sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} \qquad (2)$$

Likewise, the second order Gaussian derivative for $C_{yy}(X, \sigma)$ and $C_{xy}(X, \sigma)$ are respectively given as follows in Eq. (3),

$$\frac{\partial^2}{\partial y^2} g(\sigma) \text{ and } \frac{\partial^2}{\partial x \partial y} g(\sigma) \qquad (3)$$

In SURF, a straightforward box channel is used as the estimation of convolution Gaussian second order derivative in smooth picture, it makes the activity with less computational complexity. Here, the box filters are computed in constant time by utilizing integral images and this integral images are employed to achieve convolution of box filters B_{xx}, B_{yy} and B_{xy}. The approximate determinant of

the HM is employed to identify the key-point, which is mentioned as follows in Eq. (4),

$$Det[H(X,\sigma)] = B_{xx}B_{yy} - (0.912\ B_{xy})^2 \qquad (4)$$

Where, 0.912 is utilized to stable the HM determinant.

3.3.1.2. Binary robust invariant scalable keypoints

BRISK is used as a surface descriptor, which achieves a noteworthy nature of matching, with constrained computation time and producing a significant key-points from a picture. Here, it utilizes a symmetric sampling pattern over example purpose of smooth pixels in feature descriptor. The intensity of the image is represented as i_x and then employ Gaussian smoothing with standard deviation σ_x, which is equivalent to the distance between the circle and points.

The key-point k in an image is patterned according to its scaling and position, the sampling-point pairs are denoted as (i_x, i_y). Respectively, the intensity of smoothed values of points is denoted as $S(i_x, \sigma_x)$ and $S(i_y, \sigma_y)$, helps to determine the local gradients. Mathematically, the local gradients $G(i_x, i_y)$ are represented as follows in Eq. (5),

$$G(i_x, i_y) = (i_y - i_x).\frac{S(i_y,\sigma_y) - S(i_x,\sigma_x)}{\|i_y - i_x\|^2} \qquad (5)$$

Assuming, the set A of sampling point pairs in Eq. (6),

$$A = \{(i_x, i_y) \in \Re^2 \times \Re^2 | x < N \wedge y < x \wedge$$
$$x, y \in N\} \qquad (6)$$

Where, N is mentioned as the number of sampling point pairs,

Divide the pixel sets into two sub-sets, namely short separation pairs and long distance sets and it is mentioned as d_1 and d_2 respectively. The following Eq. (7) represent the distance pairing of sub-sets,

$$d_1 = \{(i_x, i_y) \in A | \|i_y - i_x\| < \delta_{max}\} \subseteq A$$
$$d_1 = \{(i_x, i_y) \in A | \|i_y - i_x\| < \delta_{min}\} \subseteq A \qquad (7)$$

Analysis, the local gradient in long distance pairs and not necessary in the global gradient information. The threshold distance is set as $\delta_{max} = 9.75t$ and $\delta_{min} = 9.75t$ (t is the scale of k). Hence, the point pairs are iterated through L, to identify the complete pattern direction of key points k, which is given by Eq. (8),

$$G = \begin{pmatrix} G_x \\ G_y \end{pmatrix} = \frac{1}{L}.\sum_{(i_x, i_y) \in L} G(i_x, i_y) \qquad (8)$$

Sampling pattern rotation of orientation is mentioned as $\propto = arctan2(G_y, G_x)$ of the key-point. The binary descriptor b_k is generated by utilizing short distance paring and each bit in b_k is calculated from a pair in F. Hence, the descriptor is $512bits$ long and it is gathered by performing short distance intensity at every binary feature vectors v, it is mentioned as follows in Eq. (9),

$$v = \begin{pmatrix} 1, S(i_y^\alpha, \sigma_y) > S(i_x^\alpha, \sigma_x) \\ 0, otherwise \end{pmatrix} \forall (i_x^\alpha, i_y^\alpha) \in F \qquad (9)$$

The registration relies upon affine geometrical transform, the accompanying feature combination (SURF and BRISK) gives a superior affine geometrical change. BRISK and SURF are adaptable for quicker execution by diminishing the quantity of sampling-points in the pattern to some detriment of matching quality-which may be reasonable in a specific application. Besides, scale and rotation invariance can be precluded inconsequentially, expanding the speed and the matching quality in applications where they are not required.
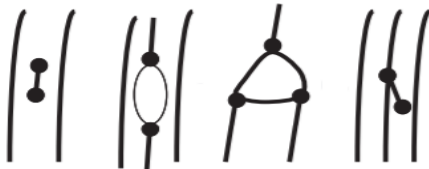
3.3.2. Feature extraction of fingerprint

The enhanced images of fingerprint features are extracted in this section. In this fingerprint feature extraction, Minutiae based feature extraction and singular point based feature extraction methods are applied to feature level fusion process.

3.3.2.1. Minutiae feature extraction

The commonly employed strategy for minutiae extraction is the Crossing Number (CN) concept. This strategy includes the utilization of the skeleton picture where the edge stream design is eight-connected. The minutiae are separated by checking the nearby neighbourhood of each edge pixel in the picture utilizing a 3×3 window. The CN esteem is then registered, which is characterized as a half the sum of the difference between sets of nearby pixels in the eight-neighbourhood. Utilizing the properties of the CN which appear in Table 1, the edge pixel can be classified as edge ending, bifurcation or non-minutiae point.

Table 1. Properties of CN

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

(a)Spur   (b) Hole   (c) Triangle   (d) Spike

Figure.4 Examples of typical false minutiae structures: (a) spur, (b) hole, (c) triangle, and (d) spike

Table 2. Pixel in anti-clockwise direction

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

False minutiae might be acquainted into the picture due to some variables such as noisy pictures, and picture antiquities made by the diminishing procedure. Henceforth, after the minutiae are extricated, it is important to utilize a post processing stage to approve the minutiae. Fig. 4 is taken from [20] describes a few precedents of false minutiae structures, which incorporate the spur, hole, triangle and spike structures. It tends to be seen that the spur structure creates false edge endings, whereas both the hole and triangle structures produce false bifurcations. The spike structure makes a false bifurcation and a false edge finishing point.

The algorithm is able to cancel out false minutiae based on configuration of the edge pixels associated with the minutiae point. In this research, the CN method for a pixel P is slightly modified with a view to speed up its operation. The CN for an edge pixel P is given by the Eq. (10)

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| , P_9 = P_1 \qquad (10)$$

Where P_i is the pixel value in the neighborhood of P. For a pixel P, its eight neighbouring pixels are scanned in an anti-clockwise direction as Table 2.

After the CN for an edge pixel has been figured, the pixels are classified according to the property of its CN esteem.

Minutiae based unique fingerprint matching calculation is frequently intended for solving the issues of correspondence and similarity calculation. Minutiae based representation is storage productive

and a master declaration about speculate identity based on mated particulars allowable in courts of law. Later, the proposed technique enhances the minutiae matching to utilize neighbourhood minutiae structures to rapidly locate an admissible arrangement between two fingerprints and after that solidify the nearby matching outcomes at a global level.

3.3.2.2. Singular-point feature extraction

Singular point is a basic worldwide feature in finger impression pictures. Finger impression singular focuses like upper core, lower core and delta are characterized as where the orientation field is broken or the edge curvature are fundamental for enlistment and recognizable proof. Existing strategies require checking the picture to register an amount at every pixel or block, and henceforth they are tedious. Subsequently, in this examination, a quick algorithm for recognizing singular focuses is proposed by strolling straightforwardly to pictures instead of checking the pictures. Walking Directional Fields (WDFs) are set up from the orientation field [21]. Then, following the walking directions on WDFs, the method can quickly walk to the singular focuses. The walking algorithm is greatly quick and implemented easily with satisfactory exactness.

3.3.2.2.1. Zero-pole model

This model considers core as zero and delta as pole in the complex plane, and uses the argument of complex function $p(z)$ to approximate the orientation $o(z)$ of a point z in the fingerprint. $p(z) \ and \ o(z)$ are defined as Eq. (11).

$$p(z) = \sqrt{e^{2jo_\infty} \frac{(z-z_{c1})...(z-z_{cm})}{(z-z_{d1})...(z-z_{dn})}} \qquad (11)$$

$$o(z) = arg\big(p(z)\big) \ mod \ \pi \qquad (12)$$

Where $z_{ci} \ and \ z_{dj}$ are the ith core and j^{th} delta of fingerprint respectively, and o_∞ is a constant correction term. This direction is called walking direction, and the field of direction is defined as Walking Directional Field (WDF) of upper core, represented by WDF_{uc},

$$WDF_{uc(z)} = 2o_{uc}(z) - \frac{\pi}{2} \qquad (13)$$

Similarity, the WDF of lower case and delta can be defined in Eq. (14) and Eq. (15)

$$WDF_{lc}(z) = 2o_{lc}(z) + \frac{\pi}{2} \qquad (14)$$

$$WDF_d(z) = -2o_d(z) + \frac{\pi}{2} \qquad (15)$$

3.4 Feature level fusion

Feature Level Fusion (FLF) is accepted to be more successful than alternate levels of combination because of the fact that the feature set contains richer data about the input biometric information than the coordinating score or the output decision of a classifier. Hence, combination at the feature level is required to give better acknowledgment results. In this work, FLF combines the biometric information such as ear and fingerprint. The response time of the FLF is less than the score level fusion. FLF concatenates the extracted features. The dimensionality of the fused feature vector is maximized by feature set concatenation. The steps which are performed in the FLF is given as follows:
1. Normalization of feature vector
2. Fusing the feature vector

3.4.1. Normalization of feature vector

The feature vectors which are extracted from face, iris and fingerprint are incompatible in nature due to the variation in its own range and distribution. This problem is overcome by normalizing the feature vector.

3.4.2. Fusing the feature vector

The final fused vector is achieved by concatenating the feature vector from face, iris and fingerprint. The Fused vector is shown in the following Eq. (16).

$$Fused_{vector} = [f_1, f_2, \ldots f_n i_1, i_2, \ldots i_n fp_1, fp_2, \ldots fp_n] \qquad (16)$$

Where, $f_1, f_2, \ldots f_n$, $i_1, i_2, \ldots i_n$ and $fp_1, fp_2, \ldots fp_n$ are the normalized vectors of face, iris and fingerprint respectively. These fused vectors are stored in the database and it is used for identification of individuals.

3.5 Registration using affine transform

After fusing the features of ear and fingerprint, the Affine Transform can be used to register the point correspondences together, accounting for a rigid global transformation and local non-linear transformation.

3.5.1. Affine transform

Assume $f(x,y)$ is an image signal, an affine geometric distorted image $f^d(x,y)$ is defined by parameters $\{A, d\}$ as

$$f^d(x,y) = f(x_d, y_d) \qquad (17)$$

Where,
$$\bar{X} = \begin{pmatrix} x_d \\ y_d \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = AX + d \qquad (18)$$

By re-entering the signal with respect to the centre of mass, we can remove the translation factor d easily. Based on Singular Value Decomposition (SVD), the matrix A can be decomposed as:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} \cos(\emptyset) & \sin(\emptyset) \\ -\sin(\emptyset) & \cos(\emptyset) \end{bmatrix} \begin{bmatrix} \sqrt{\lambda_1} & 0 \\ 0 & \sqrt{\lambda_2} \end{bmatrix} \begin{bmatrix} \cos(\tau) & -\sin(\tau) \\ \sin(\tau) & \cos(\tau) \end{bmatrix} \qquad (19)$$

Where $\lambda_1 \ and \ \lambda_2$ are eigenvalues of AA^T , $\emptyset \ and \ \tau$ are angles related to the eigenvectors of AA^T . If A is nonsingular matrix, $\lambda_1 \ and \ \lambda_2$ will have positive values. From (18) and (19), it can be concluded that any affine transform can be decomposed as combination of translation, rotations, scaling or aspect ratio change. Using the affine transformation method, n iterations are applied, where each iteration has minutiae mappings reassigned and transformation re-estimated using the previous minutiae set transformed state of the test fingerprint.

3.6 Similarity score

Once the n iterations are performed, the final pairs have been established. From this, the shape similarity Euclidean distance measure can be calculated as Eq. (20).

$$D_{sc}(P,Q) = \frac{1}{n}\sum_{p\in P} \underset{q\in Q}{arg\ min} C(p, T(q)) + \frac{1}{m}\sum_{q\in Q} \underset{p\in P}{arg\ min} C(p, T(q)) \qquad (20)$$

Where $T(.)$ denotes the affine transformed representative of the contour point q. In addition, an appearance term, $D_{ac}(P,Q)$, measuring pixel intensity similarity and a bending energy term, $D_{be}(P,Q) = I_f$, can be added to the similarity score.

Afterward, the similarity measure was modified as

$$D_{sc}^* = D_{sc} + \beta D_{be} \qquad (21)$$

Although this measure does not consider the strict one-to-one mapping of minutiae, through experimentation, this strategy turned out to be great, giving worthy execution in ear and fingerprint similarity assessment. But, the outcomes of minutiae mapping from the use of the Hungarian calculation on the contextually based cost histograms produced some un-normal sets. This is because of the absence of a minutiae pair pruning system. The presence of un-regular sets could possibly skew the affine transform performed. Moreover, such pairs increment the bending vitality generously, in this way prompting invalid matching outcomes, especially for genuine matches.

3.7 Identify a matching person

The person submits his/her ear to the framework, then the process of matching the biometric images against the related template is carried out. If the subsequent score is in excess of a pre-characterized threshold, the subject is acknowledged as a genuine user. Otherwise, the subject is asked to present his fingerprint as optional biometric. The fused features of ear and fingerprints are handled and coordinated against the related template. If the score is more than the threshold, the subject is acknowledged as a genuine client and else it is stated as imposter.

4. Experimental analysis

The proposed feature-level fusion technique is executed in MATLAB stage. Here Multimodal biometrics are used, which consists of CASIA database of fingerprint and IIT Delhi database of ear images. The framework designed using i5 processor and 4GB RAM for effective identification. This examination contains ear and fingerprint database images which are considered to the authentication strategy.

4.1 Performance evaluation

The proposed method uses several parameters for validating the performance. The parameters such as sensitivity, specificity, accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR) and Genuine Accept Rate (GAR). The mathematical equations of these parameters are given in the below sections.

4.1.1. Sensitivity

Sensitivity (Se) is a basic property of the image processing. Sensitivity is also named as TP rate. Mathematically, Sensitivity equations is show in Eq. (22):

$$Se = \frac{TP}{TP+FN} \qquad (22)$$

Where, TP is True Positive, FN is False Negative.

4.1.2. Specificity

The specificity (SP) describes, how the test provides the negative characteristic of the proposed method. Specificity also called the tn rate. Mathematically, Specificity equations is shown in Eq. (23).

$$SP = \frac{TN}{TN+FP} \qquad (23)$$

Where, TN is True Negative, FP is False Positive.

4.1.3. Accuracy

By using the Specificity and Sensitivity, the Accuracy of the image is calculated. Accurately represent the quantity of the image. Mathematically, it is show in Eq. (24).

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \qquad (24)$$

4.1.4. False acceptance rate

FAR is defined as the probability of an imposter being accepted as a genuine individual. FAR is measured as the fraction of impostor score exceeding the pre-defined threshold. The given is shown in Eq. (25).

$$FAR = \frac{FP}{FP+TN} \qquad (25)$$

4.1.5. False rejection rate

FRR is defined as the probability of a genuine individual being rejected as an imposter. FRR measured as the fraction of the genuine score below the pre-defined threshold. The mathematical equation is shown in Eq. (26).

$$FRR = \frac{FP}{TP+FN} \qquad (26)$$

Table 3. Performance of sensitivity and specificity

Performance	tp	tn	fp	fn	sensitivity	specificity
Ear	1	6	1	2	85.71	33.33
Finger	1	7	1	1	87.50	50
Ear- Finger	1	8	0	1	88.9	100

Table 4. Performance of various parameters

Performance	Accuracy	Error Rate	FAR	FRR	GAR
Ear	80.21	20	14.29	27.67	72.33
Finger	85.01	15	12.50	23.27	76.73
Ear- Finger	95.66	5	11.11	19.99	80.01

4.1.6. Genuine accept rate

GAR is defined as a percentage of genuine users accepted by the system. It is given by $GAR = 100 - FRR$.

The parameters are evaluated for predicting the performance of the proposed method. Table 3 shows the performance of ear, fingerprint and proposed (ear+fingerprint) method's sensitivity and specificity values in terms of TN, TP, FP and FN. Then, Table 4 represents the performance of various metrics which are used in the proposed methodology.

In Table 3, the specificity values of ear obtained 33.33%, whereas fingerprint obtained 50% of specificity. But, while combining both ear and fingerprint, the proposed method obtains 100% specificity and also achieved higher sensitivity (88.9%) than other biometric.

The proposed method achieved 95.66% accuracy while combining the ear and fingerprint biometric images for identifying the genuine users. Figs. 5 and 6 describe the graphical representation of the performance of various parameters in the proposed method.

From the below figures, the results stated that the proposed method achieved better results than the unimodels of ear and fingerprint biometrics. The error rate of the unimodel achieved nearly 20%, but the proposed multi-biometric model reduced the error rate up to 5%. The accuracy of the proposed achieved 95.66%, whereas, the ear model achieved 80.21% and the fingerprint obtained 85.01% accuracy.

4.2 Comparative analysis

Table 5 presents the comparative analysis of existing method with the proposed multi-biometric model in terms of accuracy, FAR and FRR. A. Tahmasebi, and H. Pourghassem, [22], presented an efficient verification system by game theory based on rank-level fusion of ear images was implemented.
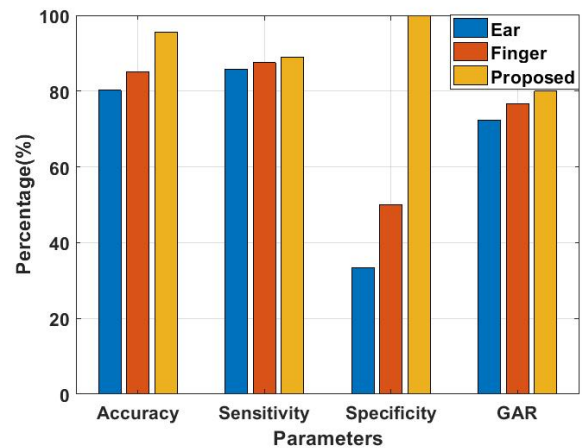
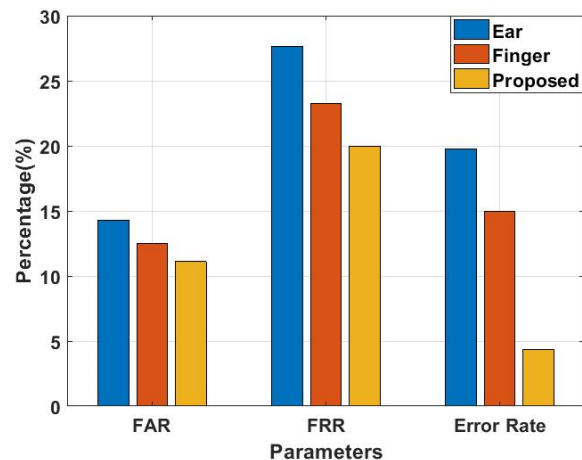Figure.5 Performance of parameters of proposed method

Figure.6 Performance of error rate of proposed method

In addition, texture information of palm print images and combination of dynamic information of online signature was proposed. In this system, Gabor channel was utilized to separate locally the surface features of the ear, palm print, and signature pictures.

A. Prakash, [17] presented a Continuous Authentication (CA) system which verified the user continuously once a person was logged in. In this paper, score level fusion was carried out using optimization that was the genetic particle swarm optimization and used classifiers as Naive Bayes

Table 5. Comparative analysis of existing methods with proposed methodology

Approaches	Bio-Metrics	FAR	FRR
A. Prakash [17]	Fingerprint + Palm + Face + Iris	0.42	0.79
A. Tahmasebi, and H. Pourghassem, [22]	Ear + Signature + Palm	0.17	0.37
V. Sireesha, and S.R.K. Reddy [24]	Iris + Fingerprint	0.11	0.11
Proposed Method	Ear	0. 14	0.27
	Fingerprint	0.12	0.23
	Ear-Fingerprint	0.11	0.19

held for the recognition process. The existing methods consumed more time and CPU resources. The existing method in [24] implemented a biometric model for iris and fingerprint images by using feature level and score level fusion. In feature fusion, the method used group search optimizer, whereas the particle swarm optimizer was used for score level fusion. The adaptive fuzzy classifier was used for classifying the fused images.

The existing work mostly focused on hand geometry, fingerprints, palm prints, ear, iris, retina, and face bio-measurements, however the existing technique faces numerous challenges because of external appearance, fingerprints and iris can't be effectively caught from a distance without a complete cooperation of the subject. There are many advantages of the biometric model by using the ear as a source of information for human identification. Ears have both reliable and robust features which are extractable from a distance. From the above results of the existing methods with the proposed multi-biometric model it is stated that the proposed method achieved better performance in terms of different error rates such as FAR and FRR. The FRR of existing method achieved nearly 0.79 for fingerprint verification, while the proposed fingerprint method achieved 0.23 FRR. With the combination of both ear and fingerprint bio-metric, the proposed method achieved 0.19 FRR. The proposed method uses the minutiae, BRISK and SURF feature extraction to speed up the process of the identification.

5. Conclusion

Compared with the unimodal biometric framework, multi biometric frameworks give an effective verification technique. In multi biometric framework, various fusion levels and scenarios are possible, but fusion at feature level is more important. Fundamentally, multimodal biometrics framework is a combination of many biometric

characteristics. This paper presents a multi-model biometric of ear and fingerprint images for the authentication process. The feature extraction process includes hybrid techniques such as Minutiae and Singular point based feature extraction for fingerprint, whereas BRISK and SURF techniques are used for ear feature extraction. Then, the feature level fusion process is carried out for more reliable information about the features. At last, the matching process is done by using registration with the help of affine transform with similarity score. In a developing requirement for security in different domains, ear biometrics appear to be a good solution, because ears are noticeable and its pictures can be easily taken, even without the knowledge of the inspected individual. The experimental results were carried on CASIA database for fingerprint and IIT-Delhi database for ear images. The results stated that the proposed method achieved 95.96% accuracy with low error rates of 0.11% FAR and 0.19% FRR, while the existing method obtained 0.17% FAR and 0.37% FRR in ear alone. In future work, the accuracy of the proposed method with more biometric images such as iris, face and palm print can be improved by using different optimization techniques.

References

[1] M. Gomez-Barrero, C. Rathgeb, G.Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters", *Information Fusion*, Vol.42, pp.37-50, 2018.

[2] M. M. Al Rahhal, M. L. Mekhalfi, M. Guermoui, E. Othman, B. Lei, and A. Mahmood, "A Dense Phase Descriptor for Human Ear Recognition", *IEEE Access*, Vol.6, pp.11883-1187, 2018.

[3] S. A. Bargal, A. Welles, C. R. Chan, S. Howes, S. Sclaroff, E. Ragan, and C. Gill, "Image-based Ear Biometric Smartphone App for Patient Identification in Field Settings", In: *Proc. of the 10th International Conf. on VISAPP*, Vol.3, pp.171-179, 2015.

[4] C. Cintas, M. Quinto-Sánchez, V. Acuña, C. Paschetta, S. De Azevedo, C. C. S. de Cerqueira, and S. Canizales-Quinteros, "Automatic ear detection and feature extraction using geometric morphometrics and convolutional neural networks", *IET Biometrics*, Vol.6, No.3, pp.211-223, 2016.

[5] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "A robust embedded biometric authentication

system based on fingerprint and chaotic encryption", *Expert Systems with Applications*, Vol.42, No.21, pp.8198-8211, 2015.

[6] R. Venkatesh, N. U. Maheswari, and S. Jeyanthi, "Multiple Criteria Decision Analysis Based Overlapped Latent Fingerprint Recognition System Using Fuzzy Sets", *International Journal of Fuzzy Systems*, Vol.20, No.6, pp.2016-2042, 2018.

[7] E. J. Ragan, C. Johnson, J. N. Milton, and C. J. Gill, "Ear biometrics for patient identification in global health: a cross-sectional study to test the feasibility of a simplified algorithm", *BMC Research Notes*, Vol.9, No.1, pp.484, 2016.

[8] G. Amirthalingam and G. Radhamani, "A multimodal approach for face and ear biometric system", *International Journal of Computer Science Issues*, Vol.10, No.5, pp.234, 2013.

[9] X. Li, Y. Yin, Y. Ning, G. Yang, and L. Pan, "A hybrid biometric identification framework for high security applications", *Frontiers of Computer Science*, Vol.9, No.3, pp.392-401, 2015.

[10] P. Chidananda, P. Srinivas, K. Manikantan, and S. Ramachandran, "Entropy-cum-Hough-transform-based ear detection using ellipsoid particle swarm optimization", *Machine Vision and Applications*, Vol.26, No.2-3, pp.185-203, 2015.

[11] M. Bansal and M. Hanmandlu, "A new entropy function for feature extraction with the refined scores as a classifier for the unconstrained ear verification", *Journal of Electrical Systems and Information Technology,* Vol.4, No.1, pp.135-158, 2017.

[12] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition", *IEEE Transactions on Information Forensics and Security,* Vol.11, No.9, pp.1984-1996, 2016.

[13] P. Gnanasivam and S. Muttan. "Ear and fingerprint biometrics for personal identification", In: *Proc. of IEEE International Conf. On Signal Processing, Communication, Computing and Networking Technologies*, pp.347-352, 2011.

[14] Z. Huang, Y. Liu, C. Li, M. Yang, and L. Chen, "A robust face and ear based multimodal biometric system using sparse representation", *Pattern Recognition*, Vol.46, No.8, pp.2156-2168, 2013.

[15] K. Annapurani, M. A. K. Sadiq, and C. Malathy, "Fusion of shape of the ear and tragus–a unique feature extraction method for ear authentication system", *Expert Systems with Applications,* Vol.42, No.1, pp.649-656, 2015.

[16] R. N. Balaka and P. B. M. Surendra, "A Novel Biometric Authentication System with Score Level Fusion", *Annals of Data Science,* Vol.4, No.3, pp.383-404, 2017.

[17] A. Prakash, "Continuous user authentication based score level fusion with hybrid optimization", *Cluster Computing,* pp.1-11, 2018.

[18] K. S. Bayram, and B. Bolat, "Multibiometric identification by using ear, face, and thermal face", *EURASIP Journal on Image and Video Processing,* No.1, pp.32, 2018.

[19] P. Viola and M. J. Jones, "Robust real-time face detection", *International Journal of Computer Vision*, Vol.57, No.2, pp.137-154, 2004.

[20] G. B. Iwasokun, O. C. Akinyokun, B. K. Alese, and O. Olabode, "A modified approach to crossing number and post-processing algorithms for fingerprint minutiae extraction and validation", *IMS Manthan International Journal of Computer Science and Technology, Indian,* Vol.6, No.1, pp.1-9, 2011.

[21] E. Zhu, X. Guo, and J. Yin, "Walking to singular points of fingerprints", *Pattern Recognition*, Vol.56, pp.116-128, 2016.

[22] A. Tahmasebi and H. Pourghassem, "Robust Intra-Class Distance-Based Approach for Multimodal Biometric Game Theory-Based Rank-Level Fusion of Ear, Palmprint and Signature", *Iranian Journal of Science and Technology, Transactions of Electrical Engineering,* Vol.41, No.1, pp.51-64, 2017.

[23] M. I. Naja and R. Rajesh, "Fingerprint Image Enhancement Algorithm and Performance Evaluation", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.3, No.1, pp.441-446, 2015.

[24] V. Sireesha, and S.R.K. Reddy, "Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities", *International Journal of Intelligent Engineering and Systems,* Vol.9, No.3, pp.21-35, 2016.