Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FUZZY VAULT FUSION BASED MULTIMODAL BIOMETRIC HUMAN RECOGNITION SYSTEM WITH FINGERPRINT AND EAR

[1]R.VINOTHKANNA, [2]Dr.AMITABH WAHI

[1]Associate Professor, Department of Electronics and Communication Engineering,
Annapoorana Engineering College, Periyaseeragapaadi, Salem (Dt) – 636308, Tamilnadu, India,
[2]Professor, Dept. of Information Technology,
BannariAmman Institute of Technology, Sathyamangalam
E-mail: vinothkannaphd@gmail.com

ABSTRACT

Human Recognition is one of the admired tasks over the world for recognizing a person using biometrics by determining physical or behavioral characteristics of that person. In our existing work, we have already worked out a multimodal biometric recognition system with fingerprint, palm print and hand vein. For getting more accurate recognition of our biometric system, in this work, we use ear as one of the modalities with the fingerprint. In order to improve the clear visible of input image databases, pre-processing of images is initially done. After the pre-processing of these images only, the features from the fingerprint and ear modalities are extracted clearly for the further processes. In the fingerprint images, the minutiae features are extracted directly and from the ear, the shape features are extracted using Active Appearance Model (AAM). Then, a grouped feature vector point is gained using chaff points and these two extracted feature points. After acquiring the grouped feature vector points, the secret key points are attached with the grouped feature vector points to formulate the fuzzy vault. Finally, test person's grouped vector is matched up to the fuzzy vault data base to the accurate recognition of the correct person. Our proposed work is effectively evaluated in Matlab with the evaluation metrics FAR, FFR, GAR and Accuracy by changing the secret key size at every time. The results of our proposed work facilitate very better values for the recognition of persons with the fingerprint and ear modalities. Moreover, our existing work is also compared with our proposed work for proving that our proposed work is good. In addition to this, other existing work papers are also taken for our comparison work, which clearly proves that our proposed work outperforms other techniques by providing very much better recognition accuracy.

Keywords:- *Recognition, Multimodal biometric system, Minutiae Extraction, Bifurcation, Ridges, Active Appearance Model, Chaff points, Fuzzy Vault.*

1. INTRODUCTION

Automatic recognition of an individual is referred by using assured physiological or behavioral traits associated with the person, which is termed as Biometrics [2]. Biometric systems are one of the kinds of a system of pattern recognition and which collects required biometric information from a person by extracting features and then those features are matched up to the database template. Based on the perspective of the application, biometric system can be worked either of the two modes – Verification and Identification modes [1]. In Verification mode, every person asserts an identity and according to this identity, the biometric system make a decision (accept or reject) whether the person is recognized or not. In Identification mode, there is no identity assert from the person and the biometric system make a decision who the person is (sometimes, there may be strange person) [4]. Biometric systems take advantage of iris, retina, face, hand vein, facial thermograms, fingerprints, hand geometry, signature or voiceprint to verify a person's uniqueness. A uni-biometric trait that utilized in User authentication systems often have to challenge with noisy sensor information, constrained degrees of freedom, non-universality of the biometric modality and intolerable fault rates. Such these troubles are the obstacles for the progression of the individual matcher's operational significance. More number of proofs of a single person can able to solve these issues that are utilized in Multi-biometric systems. By the usage of these multi-biometric systems, the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

operational significance with the recognition of a person is accomplished [2]. Multimodal biometric systems offers better accuracy result by reducing error rates and improve the recognition process results than the uni-modal biometric systems. Thus the overall security in the multimodal biometric system is improved [10].

In the field of biometrics recognition, Ear recognition is drawing more and more consideration. Since, the ear of human beings has special characteristics such as stability and uniqueness, several researches are implementing based on ear modality [9]. The ear does not undergo from changes in facial expression and is rigidly set in the middle of the side of the head so that the immediate background is knowable [8]. As a result to non-contact biometric recognition, ear recognition has turn out to be an efficient and appealing strategy [4]. With this ear modality, fingerprint is also added as another trait for the biometric recognition. In order to combine these modalities, the process of fusion is utilized. The majority destructive attacks on a multi-biometric system are in opposition to the biometric templates. Biometric traits are also known as templates that specifies a powerful and stable "association" between a user and his/her identity [13]. Biometric templates are susceptible to various attacks because of their inbuilt character [14]. Biometric templates should not be stored in plaintext structure and fool-proof methods are needed to firmly store the templates such that both the safety of the application and the users' privacy are not compromised by rival attacks [13]. When a user's biometric is compromised, his/her identity is missed. In contradiction of password, biometric is not cancellable. Therefore, endow with security to the stored biometric template is vital one. Crypto biometric systems are authentication systems that bring together the initiative of cryptography and biometrics. Fuzzy vault is a proven crypto biometric construct which is used to secure the biometric templates [14]. This is used in our work for the effective security purpose.

Biometric systems are widely applicable in most of our day-to-day life. Ultra security authentication with better accuracy is offered by Multimodal Biometric system of multiple biometric modalities. Over traditional electronic access control techniques such as RFID tags, electronic keypads and some mechanical locks, Multimodal Biometric [5] products offer superior security. They make certain that the certified user is present in order for access to take place. The user's approved card or password pin can never be stolen or lost to gain access by employing a mixture of dissimilar biometric recognition technologies [3]. There is a hope that the applications of fingerprint biometric such as ATM, Online money transactions, border control will be raising, because of the solid-state sensors availability [3]. Hence, the biometric system has wide range of applications and works effectively for the identification of a user. The left over parts of the paper are arranged as follows: A short analysis of some of the literature works in the multimodal biometric system is offered in Section 2. The purpose of this research is accessible in Section 3. Section 4 explains the short notes for the suggested methodology and the frame work for the suggested methodology. The experimental effects and presentation study conversations are presented in Section 5. At last, the conclusion is summed up in Section 6.

2. RELATED WORKS

Lots of recent research works based on the biometric traits fingerprint and ear are given below in detail. The problems in these works motivate us to do this research.

Presently 3D ear recognition [7] carries out fine in illumination deviation or poses variation; it requires expensive computation and particular tools. The majority of the latest works of Zeng *et al. [*6] ear recognition are spotlighted on 2D images since using 2D images is more reliable with operation in surveillance or other planar image scenarios.

Hurley *et al.* [9] suggested a unique force field transformation technique that treated the image as a range of mutually drawing particles that perform as the source of a Gaussian force field. The force field changes the ear images were taken and the force fields were after that altered to convergence fields. To execute multiplicative template matching on ternary threshold convergence maps, Fourier based cross-correlation methods were employed subsequently.

The gray-level ear images classically obtain anatomy of external human ear. Iannarelli [8] has physically tried to categorize the human ear photographs into four categories, i.e., triangle, round, oval and rectangular, largely on the basis of closed contour resulting from shape of the helix ring and lobule of the ear [5]. The presently used 3D imaging technologies in the literature occupy 3D digitizer which can be bulky and in addition fairly costly.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Yan [11] combined ear and face at score-level using sum and interval fusion rules. On a database containing four ear and face images from each of the 174 subjects using earlier two images as galleries and the latter two images as probes, they obtained rank-one recognition rates of 93.1%, 97.7% and 100% for the ear, the face and the fusion respectively. Theoharis *et al.* [7] extracted geometry images from 3D face and ear modalities and fitted annotated ear and face models using the iterative closest point (ICP) and a simulated annealing (SA) algorithm based registration process.

3. MOTIVATION FOR OUR RESEARCH

Human authentication is one of the popular tasks that are used over the world for identifying a person using biometrics by measuring his/her physical or behavioral characteristics. The physical and behavioral characteristics that utilized for authentication are fingerprints, handprints, palm prints, hand veins, palm veins, face, eyes, ears, gait, voice, signature etc., Normally Biometric systems can be categorized as Uni-modal Biometric Systems and Multimodal Biometric Systems, based on whether single or multiple biometrics is applied for person validation correspondingly. Uni-modal Biometric systems have to challenge with a mixture of problems such as: noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable fault rates. By presenting multiple proofs of the same distinctiveness, Multi-biometric systems try to find alleviate some of these disadvantages. The goal of multi-biometrics is the improvement in quality of authentication over an individual method by synthesizing the multiple features. In our work, the fingerprint and ear modalities are fused together to make the multimodal biometric system. The reason to select ear as one of the modalities in our work is that it has more advantages over all other modalities by comprising rich features with it. Even the age of a person get changes, the structure of the ears does not change, since it has stable structure. The shape of the ear also does not get change, when the facial expressions changed.

4. PROPOSED WORK FOR FINGERPRINT AND EAR MULTIMODAL BIOMETRIC RECOGNITION SYSTEM

In our proposed work, the biometric recognition system uses fingerprint and ear modalities for the recognition purposes. Fingerprint and ear are the input images to be processed to recognize a person. The phases in our proposed work are given below.

Phase I: Pre-processing
Phase II: Feature Extraction
Phase III: Grouped Feature Vector Creation
Phase IV: Fusion and Recognition

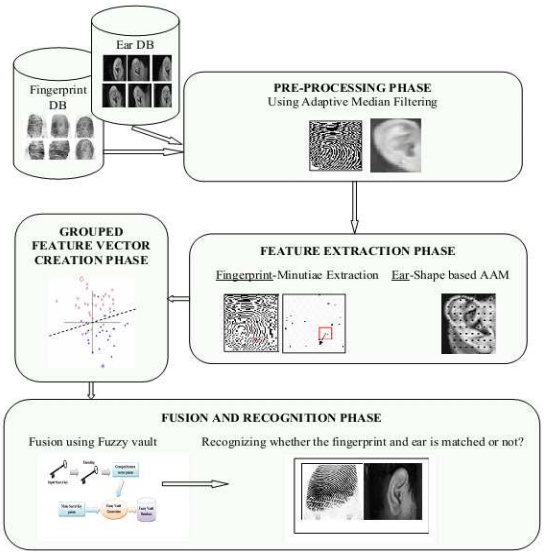

Fig.1: Proposed Block Diagram With Its Different Stages

In order to enhance the input image databases, pre-processing of images is initially made. Then only the features from the fingerprint and ear modalities are extracted effectively. In fingerprint images, the minutiae features are extracted directly and the ear features are extracted using shape based Active Appearance Model (AAM). Then using chaff points and these two extracted feature points, a grouped feature vector point is obtained. After getting the grouped feature vector points, the secret key points are added with the grouped feature vector points to make the fuzzy vault. Finally, test person's grouped vector is compared with the fuzzy vault data base to recognize correct person. The block diagram for our proposed work is given in fig. 1.

4.1. Phase I: - Pre-Processing

The input fingerprint and ear images are first changed into grey level format. Then the grey level fingerprint and ear images are preprocessed using Adaptive median filter to remove salt and pepper noise. The input image may contain noises which damage the good pixels in the image. In order to obtain good accuracy, the noise must be removed from the input image. In our proposed work, adaptive median filter is used to remove the salt and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

pepper noise. This adaptive median filter works based on the local statistics characters. It detects the impulse by calculating the difference between the standard deviation of the pixels within the filter window and the concerned current pixel.

Let the fingerprint and ear databases consists of many fingerprint and ear images and let $x_{i,j}$ be one of the grey level images x at location (i, j) taken from the database. $sd_{\min}$, $sd_{\max}$ are the lower and upper bounds of x respectively.

i.e., $sd_{\min} \le x_{i,j} \le sd_{\max} \forall (i, j) \in a$, where, $a \equiv \{1,2,...m\} \times \{1,2,...n\}$

The grey level of image x at pixel location (i, j) is given by probability

$$y_{i,j} = \begin{cases} sd_{\min}, & with\ probabilit\ y\ p \\ sd_{\max}, & with\ probabilit\ y\ q \\ x_{i,j}, & 1-p-q \end{cases} \quad (1)$$

The noise level is defined as $r = p + q$ and $sd_{i,j}^{w} = \{(k,l): |k-i| \le w \text{ and } |j-l| \le w$. Here $sd_{i,j}^{w}$ is window of size $w \times w$ centered at (i, j). $w_{\max} \times w_{\max}$ be the maximum window size.

$sd_{\min}$, $sd_{\max}$ are calculated as follow:

$$sum(i, j) = \sum_{m=i-k}^{i+k} \sum_{n=i-k}^{j+k} sd_{m,n} \quad (2)$$

$$W(i, j) = (2l+1)^2 \quad (3)$$

Local mean value $\mu 1(i, j)$ is of the moving window is calculated as

$$\mu 1(i, j) = \frac{sum(i, j)}{W(i, j)} \quad (4)$$

Local standard deviation $\sigma 1(i, j)$ is calculated as

$$\sigma 1(i, j) = \sqrt{\frac{\left(\sum_{m=i-k}^{i+k} \sum_{n=i-k}^{i+k} (sd_{i,j} - \mu 1(i, j)) \right)}{W(i, j)}} \quad (5)$$

Then using these local mean, standard deviation and also a user defined multiplier (um) upper and lower bounds are calculated.

Lower bound $(sd_{\min})$ is calculated as

$$sd_{\min} = \mu 1(i, j) - um \times \sigma 1(i, j) \quad (6)$$

And Lower bound $(sd_{\max})$ is calculated as

$$sd_{\max} = \mu 1(i, j) + um \times \sigma 1(i, j) \quad (7)$$

4.1.1 Process of Adaptive median filter

The working procedure of Adaptive median filtering is described below,

1. Initialize the window size w = 3.
2. Calculate maximum $\left(sd_{i,j}^{\min,\ w} \right)$, minimum $\left(sd_{i,j}^{\max,\ w} \right)$ and median $\left(sd_{i,j}^{med,w} \right)$ of the pixel values in $sd_{i,j}^{w}$.
3. If $sd_{i,j}^{\min,\ w} < sd_{i,j}^{med,w} < sd_{i,j}^{\max,\ w}$, then go to step 5. Otherwise increment the window size w by 2.
4. If $w \le w_{\max}$ go to 2. Otherwise replace $y_{i,j}$ by $sd_{i,j}^{med,w_{\max}}$.
5. If $sd_{i,j}^{\min,\ w} < y_{i,j} < sd_{i,j}^{\max,\ w}$, then $y_{i,j}$ is not a noise candidate otherwise replace $y_{i,j}$ by $sd_{i,j}^{med,w}$.

In the above adaptive median filter algorithm, the noise candidates are only replaced by the median $sd_{i,j}^{med,w}$, while remaining are unaltered. Using the above adaptive median filter algorithm the salt and pepper noise is removed from the given input fingerprint and ear images and the preprocessed fingerprint and eye images are then subjected to feature extraction process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2. Phase II: - Feature Extraction

The preprocessed fingerprint and ear images are given as the input to this feature extraction phase. The feature extractions for the fingerprint and ear images are done separately on the preprocessed images.

4.2.1. Features extracted from fingerprint

Minutiae features are extracted from the pre-processed fingerprint images. Ridges and Bifurcations are the minutiae features to be extracted from the fingerprints. In order to extract these minutiae features accurately, we need to do the thinning process on the pre-processed fingerprint images before extracting the features. The following sections explain these processes in detail.

4.2.1.1. Fingerprint thinning process

Thinning process decreases the thickness of every pattern lines into a single pixel width. A morphological thinning function is initially used which can be used easily for our work with the help of the functions used in MATLAB platform. And then the thinning operation is performed to remove the redundant pixels of pattern lines until all lines are into a single pixel width. The location of the centre black pixel is found at every continuation of the curve. The redundant pixels in every small 3x3 window of image are marked for every scan. More number of scans is occurred and then finally all those pixels that are marked down in these scans are eliminated. Now the resultant images after applying thinning algorithm are in single pixel width with no discontinuities. Every ridge is thinned to its centre pixel. Thinning process also eliminates the noise from the images. Thinned images are also called as skeletonized images, since the process is also called as skeletonization.

4.2.1.2. Fingerprint minutiae extraction

Finding minutia points on the thinned images are the next important step for the minutiae extraction. Based on the number of neighboring pixels, the minutia points are marked by locating the ridge end points and bifurcation points on the thinned images. For the minutiae extraction process, Crossing Number of each pixel is considered. Crossing Number (CN) for a pixel P is denoted as per the Rutovitz's definition, which is given below in eqn. (8).

$$CN(P) = \frac{1}{2}\sum_{i=1}^{8}\left|P_i - P_{i+1}\right| \quad (8)$$

In the above eqn. (), P_i indicates the binary pixel value in the neighborhood of P, in which the value of P_i is 0 or 1 and $P_1 = P_9$. According to the Rutovitz's definition, the pixel locations are specified as given in the following table I.

Table I: Pixel Locations As Per Rutovitz's Definition

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

If the Crossing Number at a pixel P that obtained using the eqn. (8) is equal to 1 means, it indicates that the skeleton of the image is a ridge end. And also, if an obtained Crossing Number at a pixel P is equal to 3 means, it denotes that the image is a bifurcation. This is the better condition for finding the minutia points. Thus the ridge and bifurcation minutiae features are extracted from the fingerprint images.

4.2.2. Features extracted from ear using AAM

After the extraction of the fingerprint features, we extract the features from the ear images. In our work, ear features are extracted using Active Appearance Model (AAM). Mostly, AAM is used for face images only. But, in our work, we can use this for extracting the ear features based on the shape.

4.2.2.1. Structure – AAM

AAM is made by the mixture of shape model and texture model, which is a numerical model of form. The features that are extracted contain both the information of shape and texture. The deviations in the shape are taken by lining up the landmark points and after that Principal Components Analysis (PCA) is executed on those points. The Eigen values are employed for altering the shape by varying the elements of shape model parameters. To attain a shape free patch, we can do the texture modeling by twisting the images into the mean shape for a specified means ear shape. Texture modeling is moreover related to the shape modeling. It is acquired by means of PCA. By uniting shape model parameter and grey-level model parameter, appearance model parameter can be prepared. PCA is used on united parameter

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

vector and next the appearance parameter that manages both shape and texture of the model is computed. By varying the appearance parameter, it is feasible to attain changes in both shape and texture.

4.2.2.2. Ear shape model construction

A 2-Dimensional shape model 'SM' with' p ' points are employed for this erection. Lot of texture and shape information has offered in the points, which are consigned in areas of the ear. The shape model has number of instances ' s '. Each of these instances is symbolized as a vector, which encloses '2p' elements, that is the x, y co-ordinates of each of the ' p ' points.

$$s = (x_1, y_1, x_2, ..., x_p, y_p)^T \quad (9)$$

To line up all the training shapes in the pre-processing step, Generalized Orthogonal Procrustes Analysis is employed. With the assist of this algorithm, all elements that are caused by translation, rotation, scaling is removed from the data set. This is in addition useful to make additional shapes by mirroring the training shapes parallel. This expresses to a novel training data set d of $D^{'} = 2D$ training instances. On the basis of training data set, work out the mean shape s_0 as the mean of all the training examples, $D^{'}$.

For finding the foremost components of all shapes in the training data set, Principle Component Analysis (PCA) is constructive. Select m components containing of m biggest Eigen values as the shape components s_i, where i takes the values from 1 to m. Therefore, the rebuilding of shapes of the training data set and the generation of novel shapes are feasible. The generation of novel shapes is not part of the data set which are of the basic shape s_0 and a linear combination of the components s_i.

$$s = \frac{1}{D^{'}} \sum_{i=1}^{D^{'}} d_i^{'} + \sum_{i=1}^{m} v_i s_i \quad (10)$$

where, the value of shape, $s_0 = \frac{1}{D^{'}} \sum_{i=1}^{D^{'}} d_i^{'}$.

The rebuilding of the shapes has the deviation in quality according to the number of applied components, m. We will require containing a different set of images for the training if we desire to make novel shapes that are not there in the training data set. The major components s_i, points out global deviations of the ear in accordance with the training data set, that alter shape and appear to make bigger as we age. Ears droop as soft tissue such as skin, fat, and muscle loosens up and structural support alters (bone recedes with time, so there's less foundation to hold the skin and cartilage up). Besides, loss of flexibility and collagen in the skin causes drooping. Fig. 2 demonstrates how an ear image pointed with landmarks.

Fig. 2: Overview Of Shape Based Active Appearance Model –An Ear Image With Landmark Points

4.2.2.3. Ear Appearance model Construction

In Active Appearance Models, Appearance model is as well one of the parts. Change of the high dimensional input images into a linear subspace of Eigen values are applied by the Appearance model. The output of this directs to extreme diminution of the dimension of the parameter space. We need to eradicate the noise in the image by filtering all input images in this $I(x)$ with a Gaussian Filter. For piecewise affine conversion $W(x, p)$, the input image is changed into the basic shape s_0 to $I(W(x, p))$. Use the histogram equalization on this normalized image for the decrease of lighting influences next. A PCA is used on the input images to normalize the input images in this way. Choose the k components that having the Eigen values as the appearance components $A_1(x)$ to $A_k(x)$. The mean of all stabilized input images is fabricated the mean appearance components $A_0(x)$.

$$A_0(x) = \frac{1}{D^{'}} \sum_{i=1}^{D^{'}} I(W(x, p)) \quad (11)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The generation of an image $A(x)$ with the basic shape s_0 is feasible depending on the appearance components $A_i(x)$. The subsequent equation explains this.

$$A(x) = A_0(x) + \sum_{i=1}^{m} \lambda_i A_i(x) \quad (12)$$

4.2.2.4. AAM Instances

Model instance is prepared by the combination of both shape models with the appearance model. The model instance $M(W(x, p))$ points out the joined appearance model and its shape. The appearance parameters $\lambda=(\lambda_1 \ldots \lambda_m)$ and the shape parameters $v=(v_1 \ldots v_n)$ are required because of this reason. It is uncomplicated to work out the image $A(x)$ in the form of the basic shape s_0 with the exploit of equation (12). By the practice of warp $W(x, p)$, the image $A(x)$ can be changed into the shape s. As a result the shape features from the ear images are extracted successfully by means of Active Appearance model.

4.3. Phase III: - Grouped Feature Vector Creation

To recognize a person, we need to group all the features taken from a person's modality. In this work, we want to group the feature vectors that are obtained from every feature of the modalities. The features extracted from fingerprint and ear are denoted as f and e, respectively. Each of these modalities has the number of feature points. The total number of feature points in fingerprint and ear are represented as f_n and e_n, respectively. The total number of feature points from the modalities used in our paper is represented as follows.

$$fe_n = f_n + e_n \quad (13)$$

It is not only enough to create the grouped feature vector point of a person with these extracted feature points of fingerprint and ear features only. We also need chaff points, c to create the grouped feature vector point. Chaff points are the extra added random points with the feature points that improve the security of the grouped feature vector that to be created. The number of chaff points used for creating the grouped feature vector is represented as c_n. The grouped feature vector is created by sum the total number of extracted feature points from fingerprint, ear and chaff points. Therefore, the total number of points to be extract from a person is specified as follows,

$$G_n = fe_n + c_n \quad (14)$$

Thus, the grouped feature vector G for a person p is represented as,

$$G_p = \{f_p, e_p, c_p\} \quad (15)$$

Hence, we can get the grouped feature vectors by adding the fingerprint, ear feature modalities and chaff points.

4.4. Phase IV: - Fusion And Recognition

In order to develop the template security, the secret key concept that generate fuzzy vault is combined to the grouped feature vector. Initially, the input secret key is encoded to make its secret key points that created based on the number of digits in the secret key. After the creation of the secret key points, the fuzzy vault is generated by fusing the secret key points with the grouped feature vector points.

4.4.1. Process of creating the secret key points and fusion

Consider that the input digit is I_d and the key digit is K_d, then the x and y co-ordinates are described as follows,

$$X - axis = K_d \times (I_d + K_d) \quad (16)$$

$$Y - axis = K_d \quad (17)$$

The representation of the secret key points for any input digit I_d is as $[K_d \times (I_d + K_d),\ K_d]$. The size of the input secret key is considered as s and now the secret key is specified as,

$$S_{dp} = S_{d1}, S_{d2}, \ldots\ldots, S_{ds} \quad (18)$$

And here, d denotes the d^{th} digit; p denotes the p^{th} person. The representation of the secret key points for each of the secret key digit is specified as,

$$P_{dp} = \{(S_{d1}, I_{d1}), (S_{d2}, I_{d2}), \ldots, (S_{ds}, I_{ds})\} \quad (19)$$

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In eqn. (19), I_{dp} denotes the secret key digit and is represented as $K_d \times (I_{dp} + K_d)$. The fuzzy vault is generated by combining the secret key points obtained from the above eqn. (19) with the grouped feature vector points obtained from the eqn. (15), which is specified as follows,

$$FV_d = \{f_d, e_d, c_d, S_{d1}, S_{d2}, ..., S_{ds}\}, \quad 0 < d < total\ no.of\ persons \tag{20}$$

Thus, fuzzy vault for every person is stored in the database and the total number of points obtained in the fuzzy vault is represented as,

$$P_n = f_n + e_n + c_n + s \tag{21}$$

By fusing the grouped feature vector points and the secret key points, we can create the fuzzy fault in this manner. The process of generating fuzzy vault is given in the following fig. 3.

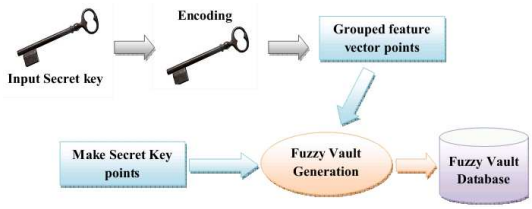

Fig. 3: Process Of Generating Fuzzy Vault

4.4.2. Recognition of a person

Recognition is a phase, in which a person is tested with his/her fingerprint and ear modalities. In our work, the fingerprint and ear modalities are subjected to pre-processing and then the features are extracted from these modalities to produce grouped feature vector points. This grouped feature vector points of a test person is compared with the database of fuzzy vault and then check whether the grouped feature vector is matched with the fuzzy vault or not. If it is matched, then the authentication is granted by generating the secret key to confirm. Otherwise, the authentication is denied. The recognition process is illustrated in the following fig. 4.

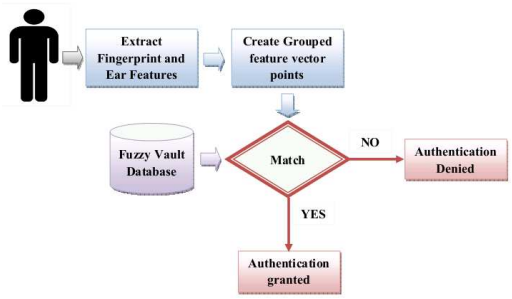

Fig. 4: Process Of Recognition Of A Person

Compare the input grouped feature vector points $G_t = \{f_t, e_t, c_t\}$, to the fuzzy vault of the database. The authentication of the test person is granted, when all the points in G_t are matched with the fuzzy vault of the database. Otherwise the authentication is failed. Once all the points in the combined feature vector of a test person matches with the fuzzy vault, then certain points in the fuzzy vault will be still left alone. These points are then used as a secret key points and the x co-ordinate of these points are taken as the secret key of the person. For example, if $P_{dp} = \{(S_{d1}, I_{d1}), (S_{d2}, I_{d2}), ..., (S_{ds}, I_{ds})\}$ be the points, then $\{I_{d1}, I_{d2}, ..., I_{ds}\}$ be the secret key. Thus, the security of a person's fingerprint and ear templates is improved using fuzzy vault.

5. RESULTS AND DISCUSSIONS

In this section, the results of proposed multimodal biometric approach for the recognition of finger print and ear modalities using Fuzzy Vault are discussed. Our proposed methodology is implemented in MATLAB platform.

5.1. Dataset Description

For each finger print and ear images, CASIA database and IIT Delhi Ear Database are used in our paper, respectively. The detailed description of each dataset images is given below.

Finger print

CASIA Fingerprint Image Database Version 5.0 or CASIA-FingerprintV5 comprises 20,000 fingerprint images of 500 subjects. The fingerprint images of CASIA-FingerprintV5 were incarcerated by means of URU4000 fingerprint sensor in one session. The volunteers of CASIA-FingerprintV5 consist of graduate students, workers, waiters, etc. Each volunteer offered 40 fingerprint images of his eight fingers (left and right thumb/second/third/fourth finger), i.e. 5 images per finger. To produce considerable intra-class variations, the volunteers were asked to revolve their fingers with different levels of pressure. All fingerprint images are 8 bit gray-level BMP files and the image declaration is 328 x 356. The subsequent fig. 5 shows the model database images for the fingerprints.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

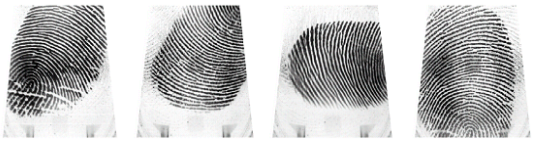

Fig. 5: Sample Fingerprint Images From CASIA-Fingerprint V5 Database

Ear

IIT Delhi Ear Database version 1.0 chiefly contains the ear images gathered from the students and staff at IIT Delhi, India. Using an easy imaging setup, this database has been obtained in IIT Delhi campus during Oct 2006 - Jun 2007. All the images are obtained from a distance (touchless) by means of simple imaging setup and the imaging is executed in the indoor surroundings. The presently obtainable database is attained from the 121 dissimilar subjects and each subject has at least three ear images. The entire subjects in the database are in the age group 14-58 years. The database of 471 images has been consecutively numbered for each user with an integer identification/number. The resolution of these images is 272 x 204 pixels and all these images are accessible in jpeg format. This database moreover offers the automatically normalized and cropped ear images of size 50 x 180 pixels besides to the original images. Lately, a larger version of ear database (automatically cropped and normalized) from 212 users with 754 ear images is moreover incorporated and made obtainable on request. Fig. 6 demonstrates the model ear database images.

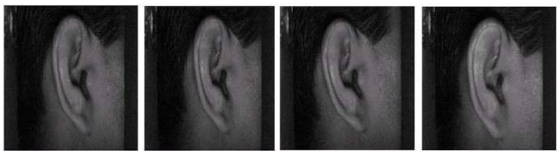

Fig. 6: Sample Ear Images From IIT Delhi Ear Database Version 1.0

5.2. Experimental Results

The fingerprint and ear images are taken from the databases details in Section 5.1. These are initially gets pre-processed using Adaptive median filter for getting noise and blur removed images. The pre-processing process is given in detail in the Section 4.1. Both the fingerprint and ear images get pre-processed in the same manner and the pre-processed images are given below in fig. 7 for both the images.

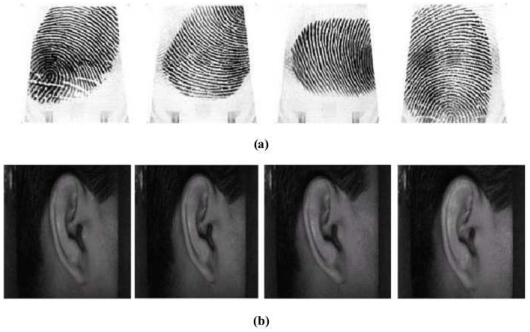

Fig. 7: Pre-Processed Images: (A) Fingerprint (B) Ear

After obtaining pre-processed images, features from both the fingerprint and ear images are extracted using separate method. From the pre-processed fingerprint image, initially the thinned image is obtained for extracting the features minutiae. From the thinned fingerprint image the bifurcations and ridges as the minutiae points are extracted. The fingerprint feature extraction process is explained in Section 4.2.1 and the feature extracted image is shown in the following fig. 8.

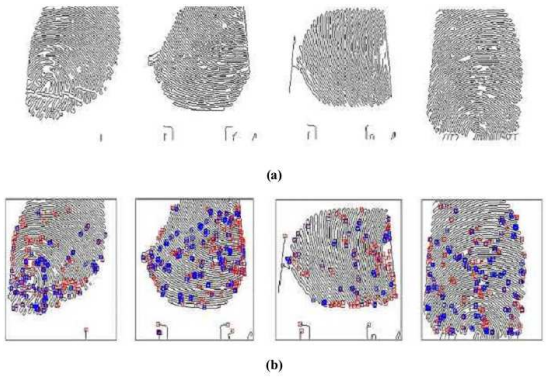

Fig. 8: Feature Extracted Images Of Fingerprint: (A) Thinned Image (B) Minutiae Extracted Image

The pre-processed ear images are also subjected to the process of feature extraction using Active Appearance Model. The shape features are extracted from the pre-processed ear images. Totally 12 points are considered for our work from the ear image. The ear feature extraction process is explained Section 4.2.2 and the shape feature pointed images are shown in the following fig. 9.

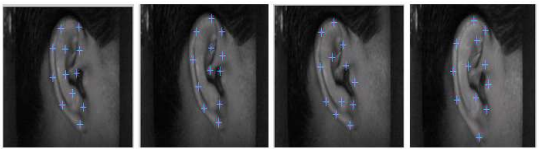

Fig. 9: Shape Feature Points Extracted From Ear Images

After extracting the features from fingerprint and ear images, the grouped vector points are generated

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(Section 4.3) and then the fusion using fuzzy vault followed by recognition process is carried out (Section 4.4). Hence, the images from the databases are authenticated for each person.

5.3. Performance Evaluation Results

In order to evaluate our proposed multimodal biometric authentication system based on fingerprint and ear images, some of the evaluation metrics are utilized. The evaluation metrics used for our work are False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GAR) and Accuracy.

False Acceptance Rate (FAR):-

It is the measure of the likelihood that the biometric security system accepts the images that are incorrectly matched with the stored database images.

$$FAR = \frac{Number\ of\ incorrect\ \ persons\ accepted}{Total\ number\ of\ \ persons\ in\ the\ database} \quad (22)$$

False Rejection Rate (FRR):-

It is the measure of the likelihood that the biometric security system rejects the images that are correctly matched with the stored database images.

$$FRR = \frac{Number\ of\ correct\ \ persons\ \ rejected}{Total\ number\ of\ \ persons\ in\ the\ database} \quad (23)$$

Genuine Acceptance Rate (GAR):-

It is the probability of truly matching images that are matched by the biometric security system and total number of images in the database. The value of GAR is calculated from the False Rejection Rate in eqn. (23) and it is given in below eqn. (24),

$$GAR = 1 - FRR \quad (24)$$

Accuracy:-

Overall Accuracy of our biometric security system is described as from the value of FAR and FRR,

$$Accuracy = 100 - \left(\frac{FAR\ /\ FRR}{2} \right) \quad (25)$$

The results for our proposed multimodal biometric system based on fingerprint and ear modalities with different secret key sizes are given below in the table II.

Table II: Results Of Proposed Multimodal Biometric System Using Fingerprint And Ear Modalities With Various Secret Key Sizes

Secret Key Size	FAR (in %)	FFR (in %)	GAR (in %)	Accuracy (in %)
4	0.72	0.3	0.7	98.8
6	0.72	0.3	0.7	98.8
8	0.7	0.3	0.7	98.8333
10	0.7	0.3	0.7	98.8333

The above table II shows the Results of proposed multimodal biometric system using fingerprint and ear modalities with various secret key sizes 4, 6, 8, and 10. From this, we can able to understand that accuracy of the multimodal biometric result gets high value for the recognition of the correct person using the modalities fingerprint and ear. For the secret key sizes 4, 6, 8 and 10, we can obtain the accuracy values of 98.83%, 98.61%, 98.83% and 98.61%, respectively. The FAR values are not low value in compared with the FFR value. Even the FAR values are low, it does not affect the recognition accuracy result, since our proposed method provides above 98.5% accuracy value. In our work, the value of GAR for each various secret key size is 70%. However, the results of recognition accuracy are very much better value for our proposed work. The following table III and IV shows the results of biometric system only using fingerprint and ear alone, respectively.

Table III: Results Of Biometric System Of Fingerprint Alone With Various Secret Key Sizes

Secret Key Size	FAR (in %)	FFR (in %)	GAR (in %)	Accuracy (in %)
4	0.9	0.1	0.9	95.5
6	0.9	0.1	0.9	95.5
8	0.8	0.2	0.8	98
10	0.7	0.3	0.7	98.8333

Table IV: Results Of Biometric System Of Ear Alone With Various Secret Key Sizes

Secret Key Size	FAR (in %)	FFR (in %)	GAR (in %)	Accuracy (in %)
4	0.8	0.2	0.8	98
6	0.9	0.1	0.9	95.5
8	0.7	0.3	0.7	98.8333
10	0.9	0.1	0.9	95.5

The results of these two tables II, III and IV are plotted in the following graph in fig. 10 for the comparison of the uni-modal system and multimodal biometric system.

Journal of Theoretical and Applied Information Technology
20th January 2014. Vol. 59 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

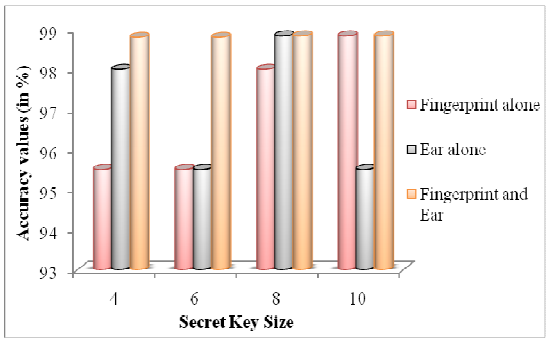

Fig. 10: Graph For Accuracy Values Of Uni-Modal Recognition System And Proposed Multimodal Recognition System

The above fig. 10 illustrates that our proposed multimodal biometric system is better than the Uni-modal system. For our convenience and proof, we also implement the results of fingerprint alone and ear alone biometric system. For each secret key size, the accuracy values get changed. The fingerprint alone system and the ear alone system facilitates 95.5% and 98% of accuracy values, which is lower than 98.8% of proposed fingerprint and ear biometric system. Likewise, for the secret key sizes 6, 8 and 10, our proposed work only gets higher accuracy value of 98.8%, 98.83% and 98.83%, respectively. The FAR and FRR values are high for the fingerprint alone and ear alone modality system, when compared with the proposed multimodal system. From the results of fig. 10, we can prove that our proposed fingerprint and ear multimodal biometric system is very better in compared with the uni-modal system recognition.

5.4. Comparison Results

Our proposed work is compared with our existing multimodal biometric system based on the fingerprint, palm print and hand vein and the existing work in ref. [12]. The recognition FAR, FRR, GAR and accuracy results of our proposed and our existing work are given in the following table. V.

Table V: Comparison Results Of Our Proposed And Our Existing Works

Secret key size / Evaluation Metrics	4		6		8		10	
	Existing	Proposed	Existing	Proposed	Existing	Proposed	Existing	Proposed
FAR (in %)	0.45	0.72	0.45	0.72	0.45	0.7	0.45	0.7
FRR (in %)	0.15	0.3	0.15	0.3	0.15	0.3	0.15	0.3
GAR (in %)	0.85	0.7	0.85	0.7	0.85	0.7	0.85	0.7
Accuracy (in %)	98.5	98.8	98.5	98.8	98.5	98.8333	98.5	98.8333

Our Proposed work is compared with our existing work and the comparison results of which is given in the above table V. Our existing work is based on the modalities fingerprint, palm print and hand vein, but our proposed work is based on the fingerprint and ear modalities. Ear is the effective trait for the accurate recognition of person. The graph for our comparison results of recognition accuracy in table V is plotted in the following fig. 11.

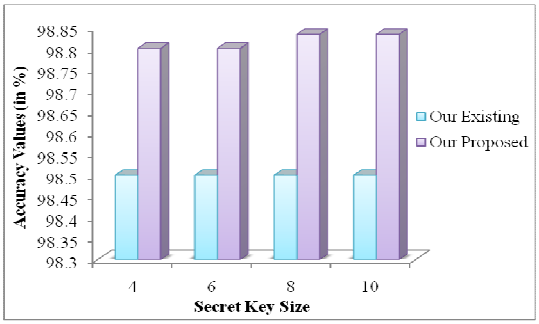

Fig. 11: Comparison Graph For The Recognition Accuracy Between Our Proposed And Our Existing Work With Various Secret Key Sizes

From fig. 11, we can find that our proposed work offers good recognition accuracy of 98.8%, 98.8%, 98.83% and 98.83% value for the secret key size 4, 6, 8 and 10, respectively. But, our existing work gave 98.5% of accuracy for all the secret key size 4, 6, 8 and 10. Even the FAR and FRR values of our existing system is better than our proposed system, the recognition accuracy is lower than our proposed one. But, in our proposed work, the higher value of FAR and FRR in our proposed system does not affect the recognition accuracy. Both the existing and proposed works has good GAR values. Moreover, in our existing work, the accuracy values not changed according to the key size changed. But, the recognition accuracy of our proposed work has changed with the changes in secret key size. From all these results, we can additionally prove that our proposed biometric system is good for the recognition of correct person in compared with our existing biometric system by the use of ear modality.

In addition to this comparison, we also compare our proposed work with the existing work -

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Feature Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature", which was worked out by Dakshina Ranjan Kisku [12] using the modalities fingerprint and ear. In the following table VI, we can find the recognition accuracy of the work in ref. [12].

Table VI: Comparison Results Of Recognition Accuracy Between Our Proposed And Existing Feature Level Fusion Works

Recognition in type	Average Accuracy of the works (in %)	
	Existing feature level fusion	Proposed fuzzy vault fusion
Fingerprint	95.02	96.958
Ear	93.63	96.958
Fingerprint and Ear	98.71	98.8166

The comparison graph for the table VI is given in the fig. 12, which shows the effectiveness of our proposed work.

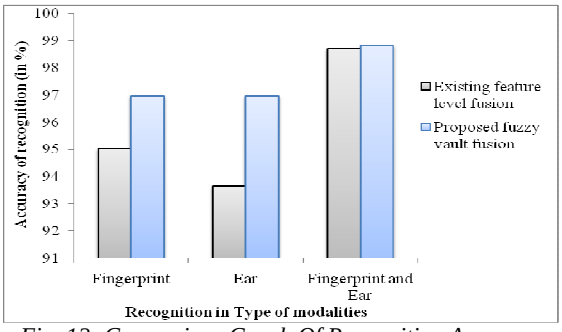

Fig. 12: Comparison Graph Of Recognition Accuracy Results Of Existing And Our Proposed Work

The comparison results in fig. 12 explain the separate work of modalities also. In the existing work in ref [12], 98.71% of recognition accuracy was achieved by the multimodal system using both the fingerprint and ear modalities. But, our proposed system using both the fingerprint and ear modalities facilitate 98.8166% of average accuracy, which outperforms the existing work with its higher accuracy value. Even the modalities were separately worked out in the existing work, the fingerprint alone and ear alone provided 95.02% and 93.63% of accuracy values, which is lower value in compared with our proposed work of accuracy values 96.958% and 96.958%, respectively. From these comparison results of existing works, we can prove well that our proposed multimodal biometric system is very good recognition of persons by using the modalities fingerprint and ear.

6. CONCLUSION

The stages in our proposed work for the effective human recognition system were (1) Pre-processing (2) Feature Extraction (3) Grouped feature vector creation (4) Fusion and Recognition. Our proposed multimodal biometric recognition system with fingerprint and ear modalities was effectively implemented in Matlab. For the evaluation of our work, the evaluation metrics FAR, FFR, GAR and Accuracy were measured by changing the secret key size at each time. The results of our proposed work facilitated better accuracy value of 98.8166% on average, for the recognition of persons with the fingerprint and ear modalities. Moreover, our existing work - multimodal biometric recognition system with fingerprint, palm print and hand vein modalities was also compared with our proposed work for proving that our proposed work is good, in which our proposed work provides 0.3166% of accuracy than our existing work. In addition to this, other existing work papers were also taken for our comparison work, which clearly proved that our proposed work outperforms other existing techniques by providing very much better recognition accuracy by exceeding 0.1066% of the recognition accuracy of existing work.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Transaction on Circuits and Systems for Video Technology, Vol. 14, pp. 4–20, Jan 2004.

[2] A. Ross and A. K. Jain, "Information fusion in biometrics," Pattern Recognition Letters, Vol. 24, pp. 2115–2125, Sep 2003.

[3] A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for a high security fingerprint verification system," Pattern Recognition Letters, Vol. 20, pp. 1371–1379, 1999.

[4] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of face and speech data for person identity verification", IEEE Transaction on Neural Networks, Vol. 10, pp. 1065–1074, 1999.

[5] Ribaric, S., and Fratric, I., "A biometric identification system based on eigen palm and Eigen finger features", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No.11, pp. 1698-1709, 2005.

[6] Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S., "Filterbank-based fingerprint matching",

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IEEE Transactions on Image Processing, pp. 846-859, 2000.

[7] Burge, M. and Burger, W., "Ear biometrics in computer vision", In Proceedings of 15th International Conference on Pattern Recognition, Spain, Vol. 2, pp. 822–826, 2000.

[8] Hurley, D., Nixon, M., Carter, J., "Force field feature extraction for ear biometrics", Computer Vision Image Understanding, Vol. 98, No.3, pp. 491–512, 2005.

[9] Yuan, L., and Zhang, F., "Ear detection based on improved Adaboost algorithm", In Proceedings of International Conference on Machine Learning and Cybernetics, Vol. 4, pp. 2414–2417, 2009.

[10] Baig, A., Bouridane, A., Kurugollu, F., and Qu, G., "Fingerprint-Iris fusion based identification system using a single hamming distance matcher", International Journal of Bio-Science and Bio-Technology, Vol. 1, No. 1, pp. 47-58, 2009.

[11] Shekhar, S., Patel, V. M., Nasrabadi, N. M., and Chellappa, R., " Joint sparsity-based robust multimodal biometrics recognition", In proceedings of Computer Vision–ECCV 2012, Springer, pp. 365-374, January 2012.

[12] Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing, "Feature Level Fusion of Biometrics Cues: Human Identification with Doddington's Caricature", Communications in Computer and Information Sciences, Vol. 58, pp. 157-164, Springer, 2009.

[13] V Evelyn Brindha and AM Natarajan, "Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault", Journal of Biometrics & Biostatistics, Vol. 3, No. 6, pp. 1-6, 2012.

[14] V. S. Meenakshi, and G. Padmavathi, "Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault", World Academy of Science, Engineering and Technology, Vol. 32, pp. 312-320, 2009.