Journal of King Saud University – Computer and Information Sciences (2016) **28**, 381–394

King Saud University

**Journal of King Saud University – Computer and Information Sciences**

www.ksu.edu.sa
www.sciencedirect.com

# New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization

**Gandhimathi Amirthalingam** [a,*], **G. Radhamani** [b]

[a] *Department of Computer Science, Bharathiar University, India*
[b] *Department of Computer Science, Dr. G.R.Damodaran College of Science, India*

Received 31 January 2014; revised 1 October 2014; accepted 9 December 2014
Available online 31 October 2015

**KEYWORDS**

Modified Region Growing method;
Local Gabor XOR Pattern;
Chaff points;
Particle swarm optimization algorithm;
Fuzzy vault

**Abstract** An effective fusion method for combining information from single modality system requires Multimodal biometric crypto system. Fuzzy vault has been widely used for providing security, but the disadvantage is that the biometric data are easily visible and chaff points generated randomly can be easily found, so that there is a chance for the data to be hacked by the attackers. In order to improve the security by hiding the secret key within the biometric data, a new chaff point based fuzzy vault is proposed. For the generation of the secret key in the fuzzy vault, grouped feature vectors are generated by combining the extracted shape and texture feature vectors with the new chaff point feature vectors. With the help of the locations of the extracted feature vector points, $x$ and $y$ co-ordinate chaff matrixes are generated. New chaff points can be made, by picking best locations from the feature vectors. The optimal locations are found out by using particle swarm optimization (PSO) algorithm. In PSO, extracted feature locations are considered particles and from these locations, best location for generating the chaff feature point is selected based on the fitness value. The experimentation of the proposed work is done on Yale face and IIT Delhi ear databases and its performance are evaluated using the measures such as Jaccard coefficient (JC), Genuine Acceptance Rate (GAR), False Matching Rate (FMR), Dice Coefficient (DC) and False Non Matching Rate (FNMR). The results of the implementation give better recognition of person by facilitating 90% recognition result.


* Corresponding author.
E-mail address: gandhimathi0177@gmail.com (G. Amirthalingam).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

## 1. Introduction

Biometric has recently emerged as the unique function which executes an amazing task of precise identification of individual by their bodily or behavioral traits (Vandommele, 2010). Authentication is the task of substantiating or validating

http://dx.doi.org/10.1016/j.jksuci.2014.12.011

something or someone as genuine (Bhattacharyya et al., 2009). A biometric authentication mechanisms permit is validated persons by comparing a query furnished by the applicant to its biometric reference. In accordance with the outcome of this analysis, the claim is acknowledged and the system confirms that he/she owns the identity or not (Giot et al., 2012). Face (Leng et al., 2010) and ear are the modalities used in the proposed work for client identification. Facial recognition technology (FRT) has asserted itself as an eye-catching remedy to take care of several modern requirements for recognition and the authentication of identity claims. It combines the guarantees of parallel biometric mechanisms, which tend to attach an identity to independent characteristic traits of the body, and the supplementary recognizable functionality of visual supervision mechanisms (Introna and Nissenbaum, 2010). The characterizing key generation approaches regard the possibility of creating multiple keys from the same biometrics without using any external data, and the stability of the resulting cryptographic key (Rua et al., 2012). Nevertheless, it is unfortunate that no significant endeavors have been formed to explore the possibility of employing human ear for individual recognition in spite of its remarkable role in forensic science. The ear is a fairly attractive biometric candidate fundamentally because of its (i) rich and steady configuration that is conserved since birth and is reasonably distinctive in individuals, (ii) being consistent with the modifications in appearance and facial expression, and (iii) comparatively invulnerable from anxiety, privacy, and hygiene issues with various other biometric candidates. It is pertinent to note that the human ear has emerged as a catalyst for various investigations in view of its individuality and distinctiveness (Kumar and Wu, 2012).

Biometric cryptosystems and cancelable biometrics are both practical and promising schemes to enhance the security and privacy of biometric systems (Leng and Zhang, 2011). In the event of a person's biometric getting compromised, his distinctiveness will be lost. Unlike passwords, biometric cannot be revoked. Hence, furnishing safety to the saved biometric template is extremely critical. The multi-biometric cryptosystems concurrently defend the two different templates of a user using a single secure sketch (Nagar et al., 2012). Crypto biometric systems are validation techniques which combine the concepts of cryptography and biometrics. Quantization Index Modulation (QIM) has to bind biometric characteristics with binary keys (Bui et al., 2010), providing an increased flexibility in managing the templates' intraclass variability. Fuzzy vault is a well-established crypto biometric construct, which is credited to the quality of safeguarding the biometric templates (Meenakshi and Padmavathi, 2009). Moreover, due to the difficulties in managing the intraclass variability of biometric data, the recognition performances of such schemes are typically significantly lower than those of their unprotected counterparts (Sutcu et al., 2009). Usually, for the fuzzy vault creation, joint feature vector is primarily created with the assistance of characteristic features (Sowkarthika and Radha, 2012). To create this collective feature vector, supplementary feature point named 'chaff points' is required. A non-organized group of points $R = X \cup C$ furnishes joint feature vector points, where $X$ the unique feature point of the modalities and the points in $C$ are called chaff points that are arbitrarily chosen from the characteristic feature points (Chang et al., 2006). This chaff point creation module is employed to create arbitrary noise points to conceal the biometric features that are gathered from the clients' biometric template. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations (Hao et al., 2006). The blend of genuine and chaff points is called the secure fuzzy vault template which safeguards the biometric data as well as the crypto key. For a concurrent accomplishment of the bio-cryptosystem, which is a vital necessity for modern data safety mechanisms, the current technique of chaff generation is grossly insufficient (Khalil-Hani and Bakhteri, 2010). The relevant hassles in chaff point created are successfully tackled by giving shape to a new chaff point generation method, which employs an optimizing algorithm for the choice of the new chaff feature points.

The name of the optimization algorithm used in the proposed investigation is the unique PSO (Egrioglu and Ozdemir, 2014) algorithm. It is a heuristic comprehensive optimization technique introduced by Doctor Kennedy and Eberhart in 1995 (Meenakshi and Padmavathi, 2009). The algorithm imitates the social characters shown by swarms of animals. In the PSO algorithm, a point in the search space, which is a possible solution, is called a particle. The group of particles in a specific iteration is called 'swarm' (Onwunalu and Durlofsky, 2010). In the case of particle swam optimization algorithm, solution swam is linked to the bird swarm, the travel of birds from one location to another is parallel to the growth of the solution swarm and excellent data correspond to the most idealist remedy, and the food resource is akin to the most desirable solution during the entire track (Bai, 2010).

Thus, by means of similar algorithm, chaff feature points get optimized and developed new chaff points with highly protected fuzzy vault fusion. The rest of the paper is organized as follows: a brief review of some of the literature works in the multimodal biometric recognition is presented in Section 2. Section 3 explains the brief notes for the proposed methodology. The experimental results and performance analysis discussions are provided in Section 4. Finally, the conclusion is summed up in Section 5.

## 2. Literature review

A critical problem in the design of a cryptographic system is the vexed issue of key administration. A high-tech remedy to this hassle is to make use of bio-cryptosystems, wherein cryptography is blended with biometrics. In this remedy, the client biometrics are employed to safeguard the cryptographic key. A well-liked method to the blueprint of parallel bio-cryptosystems is the relevance of a fuzzy vault scheme. This self-styled vault is a safe treasure house in which the key is concealed within the biometric data jumbled with illogical chaff points. The utmost crucial function in the fuzzy vault scheme is a creation of the chaff points. A concise assessment of a parallel technique with face and ear biometrics is furnished below:

Multimodal biometric recognition of face and ear traits is analyzed initially. The habitual exclusion of local 3D features (L3DF) from ear and face biometrics and their arrangement at the feature and score levels for healthy recognition has been skillfully offered by Islam et al. (2013). The bouquet rightly reaches them for their relentless effort to introduce feature level fusion of 3D features extracted from ear and frontal face

data. Scores from L3DF based matching were additionally amalgamated with iterative closest point algorithm based matching by means of a weighted sum rule. Moreover, they have come out with flying colors by achieving recognition and verification (at 0.001 FAR) rates of 99.0% and 99.4%, respectively, with neutral and 96.8% and 97.1% with non-neutral facial expressions on the outstanding public databases of 3D ear and face.

And the authors, Huang et al. (2013) have handsomely developed a vigorous face and ear based multimodal biometric system by Sparse Representation (SR), which has integrated the face and ear at feature level, and is able to efficiently rectify the fusion rule based on reliability divergence among the modalities. SR-based categorization techniques were employed in multimodal categorization stage, i.e., Sparse Representation based Classification (SRC) and Robust Sparse Coding (RSC). In the long run, they have collected a group of SR-based multimodal detection methods, together with Multimodal SRC with feature Weighting (MSRCW) and Multimodal RSC with feature Weighting (MRSCW).

Then, another multimodal biometric system based on various traits is also disputed here. The performance of sum rule-dependent score level synthesis and support vector machines (SVM)-based score level synthesis has been magnificently investigated by He et al. (2010). The three significant biometric features taken into consideration in their investigation were fingerprint, face, and finger vein. Their test outcomes had advocated the fact that by blending the three modalities fingerprint, face, and finger vein in a multimodal biometric system took the authentication technique to the summit of accuracy. The sum rule-based synthesis was able to achieve a mean GAR of 0.996 at a FAR of $10^{-5}$ and fusion based on SVM classifier had gone further beyond in terms of precision, a mean GAR of 0.999 and a mean FAR of $3 * 10^{-7}$.

The state-of-art works for the generation of chaff points are examined for the proposed work. Nguyen et al. (2013a,b) have proposed and worked a new fast chaff point generation algorithm which was less time consuming for generating extra points to progress the performance and security of fingerprint fuzzy vault system. Their experimental results have specified that their proposed algorithm gains faster than existing algorithms and still assures general security necessitate.

The safety of the fuzzy vault is dependent on the infeasibility of the polynomial reconstruction issue. The vault execution can be refined by supplementing further noise (chaff) points to the vault. The current techniques for creating chaff points involve protracted time interval for creating 200 plus chaff points. For this, Nguyen et al. (2013a,b) have triumphantly put forward a novel chaff point creation method for the fuzzy vault in bio-crypto systems which have been time-conscious for generating 200 plus points. Intricacy investigation has indicated that their algorithm shines significantly with a lesser intricacy of O ($n^2$), vis-à-vis the intricacy of O ($n^3$) of the conventional algorithm. They have, through their test outcomes, testified that the ambitious algorithm achieved 14.84 and 41.86 times quicker than Clancy's and Khalil-Hani's algorithms in producing 240 chaff points. To create identical number of valid chaff points, their well-thought-out technique required lesser candidate points than that of the modern techniques. Moreover, their epoch-making algorithm was able to produce 11% additional chaff points in relation to the Khalil-Hani's algorithm.

The concept of fuzzy vault is also studied based on the two authors of various works. A new system called cancelable fingerprint fuzzy vault based on chaotic sequence was proposed by Xu and Wang (2010). Their proposed system has modified the original template into transformed template by means of transformation function. After that, the transformed template was used to create the vault. In the vault unlocking stage, the transformed input template was produced when the same transformation was applied to the input template. Experimental results have shown that their technique can guard the original template from crossing-matching by various transformed fingerprint templates in several applications. Consequently, the higher level of security of the vault and secret data was attained.

And also, Wu and Yuan (2010) have proposed a face based fuzzy vault system for online authentication. At the client side, the client's identity, the transformed template and key made from client's password were always facilitated to the server. At the registration phase, fuzzy vault encoding was executed by means of both key and transformed template. Along with that, the fuzzy vault was encrypted using digital signature. At the authentication phase, the equivalent fuzzy vault will be verified by the identity maintained by client, if it has been changed, the authentication will be denied. Or else, the key was picked up from the transformed template using fuzzy vault decoding, in which the nearby distance was calculated for point matching. If the recovered key was similar as that offered by client, the authentication will be successful. Otherwise it will be denied. The contribution of their work comprises: the transformed template instead of face template was used, which will allow the system to give diversity and revocability. The nearby distance based matching algorithm has accepted the much intra-class difference. The digital signature could be used to ensure if the fuzzy vault has been changed. The experimental results have shown that their proposed scheme attains better results.

Both the concept of fuzzy vault and chaff point generation are included in the work of authors, Khalil-Hani and Bakhteri (2010). The authors have majestically carried out investigations illustrating the fact that their component is the utmost compute-dynamic segment of the entire technique; they have brought to light a novel chaff creation algorithm for the fuzzy vault in a bio-cryptosystem. Their innovative algorithm, which is founded on a circle packing mathematical algorithm, was computationally less vigorous than current approaches. Test outcomes amply vouchsafe the fact that the ambitious algorithm is able to function almost 100 times swifter than conventional techniques for 200 plus number of chaff points, making it appropriate for a concurrent entrenched system execution.

## 3. Proposed method for multimodal biometric cryptosystem

Fuzzy vault is mainly used for providing security to the multimodal biometric cryptosystems. The chaff points which are formed arbitrarily from the biometric features can be identified by the hackers with ease. With a view to fine-tune the safety by hiding the secret key within the biometric data, optimized new chaff points with PSO based Fuzzy Vault are introduced. These newly created chaff points are very advantageous as they are not obsessed with high computation intricacy; instead they are very much swifter than the modern method. The four significant stages of proposed work, which are illustrated diagrammatically in Fig. 1 are as follows:

(1) Pre-processing
(2) Feature extraction
(3) Generation of grouped feature vectors
(4) Fusion and recognition.

The input face and ear images are treated with pre-processing for the elimination of noises and blur from images and then the shape and texture features of ear and face are mined from the pre-processed images. For the fusion procedure, fuzzy vault is employed by new chaff point's creation method. For the creation of secret key in fusion procedure, grouped feature vectors are generated by fusing the extracted shape and texture feature vectors with the new chaff point feature vectors. The $x$ and $y$ co-ordinate chaff matrixes with the assistance of the locations from the extracted feature vector points are generated. New chaff points are produced by choosing the best positions of the feature vector points. The optimal positions are located by means of PSO algorithm. At last, the validation is performed for each and every face and ear image.

### 3.1. Pre-processing phase

In the initial phase, the images must be pre-processed. With the intention of removing the unwanted portions of the image such as noise, blur, reflections, the pre-processing is performed.

Initially, the face and ear images are converted into a gray scale image because the input images are in the RGB format. Then, the filtering operations are applied on the grayscale face and ear images. One of the non-linear smoothing methods used is Median filter. The idea of Median filter is to eliminate the blurring of edges and to reduce the noises by substituting the current point in the input image by the median of the brightness in its vicinity. The center value is called 'median'. The neighboring pattern is called 'window' that slides entry by entry over the whole image. The process of substitution is represented as follows,

$$I(m,n) = \text{Median}\,[x(m-k, n-l) \in w] \tag{1}$$

In Eq. (1), $w$ represents the window around the pixels $m$, $n$. Hence the given input images of the face and ear are efficiently pre-processed and the obtained preprocessed images are represented as $I_f$ and $I_e$. Then, this image is separately cropped out to get only the region of interest part followed by changing the image size.

### 3.2. Feature extraction phase

Shape and texture features are extracted from both the pre-processed face and ear images. Shape features are extracted using the Modified Region Growing method and texture

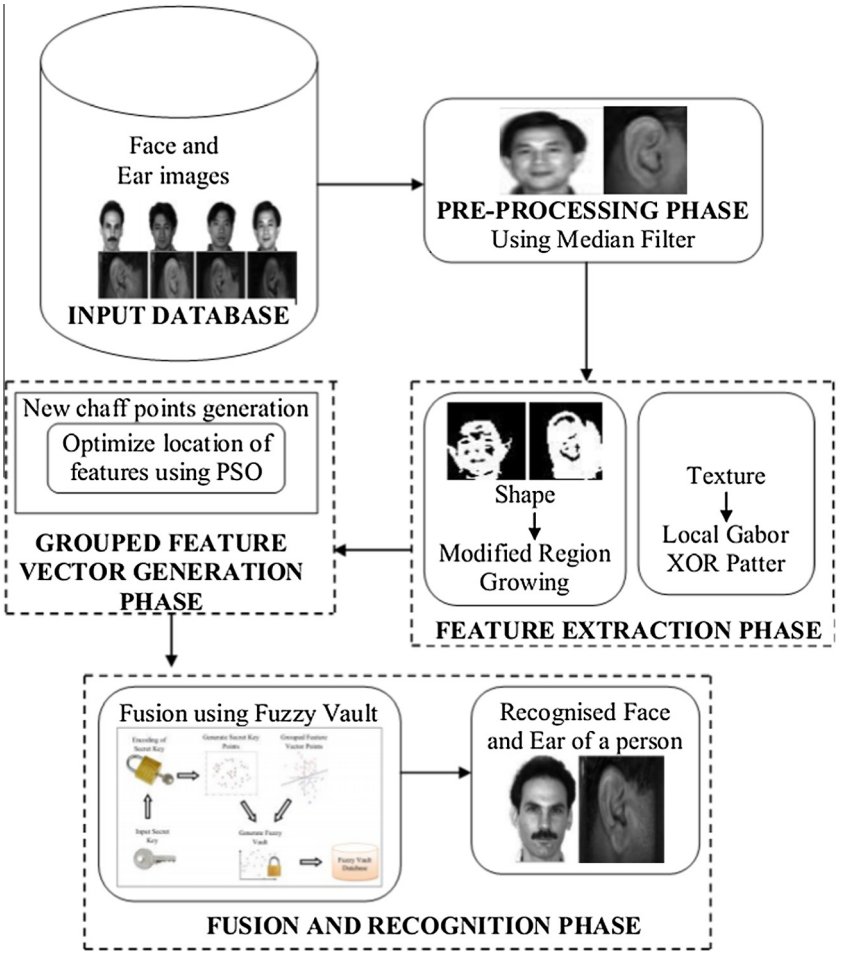


**Figure 1** Proposed diagram with its phases.

features are extracted with the help of Local Gabor XOR Pattern method. The process of feature extraction phase is given below.

#### 3.2.1. Shape feature extraction using Modified Region Growing (MRG) method

The pre-processed images of the face and ear $I_f$ and $I_e$ are given as the input to the segmentation process. Region growing method is a popular technique for image segmentation which involves seed point selection. In the segmentation process, the neighboring pixels are compared with the initial seed points to check whether, based on certain conditions, the neighboring pixels can be added to the region or not. Seed point selection is an important task in the segmentation. But, this normal region growing method selects the seed points by setting the intensity threshold, which has drawbacks of noise or variation in intensity that leads to over-segmentation or holes. Moreover, the shadings of real images may not be differentiated by this method. To overcome these difficulties, the region growing method is modified by considering the intensity and orientation thresholds from the pre-processed images to use those features in the selection of seed points. Thus, the shape features are extracted from the pre-processed ear images ($I_e$). Using the Modified Region Growing process, the shape features from the pre-processed face and ear images are extracted, effectively.

#### 3.2.2. Texture feature extraction using Local Gabor XOR Pattern (LGXP) method

From the preprocessed face and ear images, the texture features are removed by means of the Local Gabor XOR Pattern technique. Thus, the texture feature values are extracted from each face and ear image.

### 3.3. Grouped feature vector generation phase

To recognize a person, all the features taken from the face and ear modalities are needed to be grouped. The features extracted from the face and ear are denoted as $f$ and $e$, respectively. Each of these modalities has a number of feature points. The total number of feature points in the face and ear are represented as $f_n$ and $e_n$, respectively. The total number of feature points from the modalities used in the proposed work is represented as follows:

$$fe_n = f_n + e_n \tag{2}$$

It is not enough to create the grouped feature vector point of a person with these extracted feature points of the face and ear only. Chaff points, $c$ are also needed 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 is to be created. A new chaff point's generation method is used for the selection of chaff points.

#### 3.3.1. New chaff point's generation method with PSO based optimization

To generate the chaff points, one novel chaff point's generation method by optimizing the location of feature vector points using PSO is used. Initially, all the feature vector points for every shape and texture features of the face and ear are taken to generate the chaff points. All these feature vector points for ear and face are initially converted into their corresponding location. The locations of all the feature vector points are considered in the proposed work. From these feature points, the best locations are chosen by optimizing the locations using the PSO algorithm. The reasons to use PSO algorithm for the optimization are:

- PSO is easy to implement
- PSO needs few parameters to adjust
- In PSO, only gbest offers the information to others. It only seems for the best solution.

#### 3.3.2. Optimizing the locations of feature vector points using PSO

The algorithm of PSO is initialized with a set of arbitrary particles and then looks out for optima by revising generations. Each of the particles moved through the search space having its location adapted according to its distance from its own personal best location and the distance from the best particle of the swarm. The performance of each particle, i.e. how near the particles are from the universal optimum, is determined by means of a fitness function that is dependent on the optimization dilemma (Mohsen et al., 2010).

The locations of all the feature vector points are adopted as the particles in the search space. In a $n$ – dimensional search space $R^n$, each particle $i$, flies. Every particle $i$ individually contains the following three vectors.

$x_i$-vector: It represents the current position of the $i$th particle in the search space.
$p_i$-vector: It indicates the location of the best solution found so far by the $i$th particle in the search space.
$v_i$-vector: It indicates the direction in which the particle $i$ will travel (the current velocity).

According to PSO, there are two different types of versions "individual best" and "global best" that are used.

**"Individual best":** It is the individual best selection algorithm by comparing each individual position of the particle to its own best position *pbest*, only. The information about the other particles is not used in this *pbest*.

**"Global best":** It is the global best selection algorithm, which gets the global knowledge by making the movement of the particles including the position of the best particle from the entire swarm. Moreover, every particle uses its experience with previous events in terms of its own best solution. This kind of algorithm is used in the proposed work for the selection of the best particle (best location of feature vector points).

The individual best position of a particle is denoted as, *pbest*. The particles in the search space contain its coordinates that are related to the fitness as the best solution. The value of fitness *pbest* is stored in it. The *pbest* value of a particle $i$ is the best position that the particle has seen so far. If *fitness* specifies the fitness function means, then the *pbest* value of the particle $i$ is updated as follows:

$$pbest = \begin{cases} p_i = x_i \\ p_{fitness} = x_{fitness} \end{cases} \quad if\ x_{fitness} > p_{fitness} \tag{3}$$

Here, the fitness value is calculated as follows,

$$fitness = \min(\min(feature\ vector\ points)) \tag{4}$$

All the feature vector points for every shape and texture features of the face and ear are considered as their respective locations. These locations of every shape and texture features are processed as particle in the proposed work by the aid of PSO. In order to choose the best location of features, the fitness is evaluated in each stage of PSO. The location of feature vector points which have minimum value is examined from every face and ear features. Consequently, minimum set of these examined locations are chosen as the final vector points for finding fitness value.

Another location obtained by any of the particle in the population is the *gbest* value, which is the global version of the particle swarm optimizer and is the overall best value. The global best position of the whole swarm is denoted as, *gbest*:

$$gbest = best\,(pbest) \tag{5}$$

Whenever the particle changes its location from one place to another, the velocity of the particles must be updated. The velocity of a particle is computed by using weights, the position of the current pixel and the position of global pixel. The result of the velocity computation is utilized for the next iteration to find the *gbest* particle. Fig. 2 illustrates the diagram of PSO Algorithm stages.

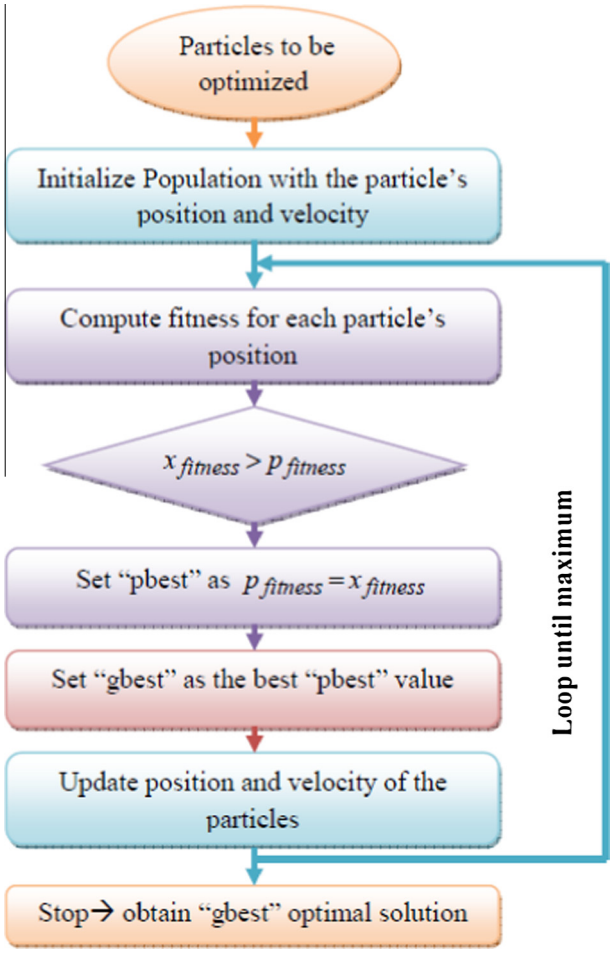


**Figure 2** Steps for PSO.

*3.3.3. PSO Algorithm steps*

Step 1: Initialize a population of $i$ particles with each particle's position $x_i$ and velocity $v_i$ on a problem space $R^n$ of dimension $n$. The locations are the particles and the locations given as the input for PSO are added to the locations that are randomly generated in the population.

Step 2: Compute the fitness function for each particle $i$ in $d$ variables as in Eq. (4).

Step 3: Make comparison between the particle's fitness value, $x_{fitness}$ and particle's *pbest* fitness value, $p_{fitness}$. If the current fitness value of particle is better than the particle's *pbest* fitness value, then set the *pbest* value into the current position in the $d$th dimension.

Step 4: Check out all of the particles' *pbest* fitness value, $p_{fitness}$ with value of *gbest*. If the current value, *pbest* is better than the *gbest* value means, then set the *gbest* value into current particle's array index and value.

Step 5: Update the velocity and position of the particles given in Eqs. (6) and (7).

$$v_{id} = \omega \times v_{id} + \varphi_1 \times r_1 \times (pbest_{id} - x_i d) \times pbest_{id} + \varphi_2 \times r_2 \times (gbest_{id} - x_{id}) \tag{6}$$

$$x_{id} = x_{id} + v_{id} \tag{7}$$

where, $i$ – Particle; $\omega$ – Inertia weight; $\varphi_1$ – Learning rates governing the particle toward its best position; $\varphi_2$ – Learning rates governing the social components; $r_1, r_2$ – Random numbers that are uniformly distributed in the range [0,1]; $d$ – $d$th dimension; $v_{id}$ must be in the range of $[v_{\max}, v_{\min}]$, $v_{\max}$ indicates the maximum velocity.

Step 6: Repeat step 2, until a better fitness or maximum number of iterations are met.

The selection of locations for the chaff point feature vector is therefore optimized with the help of the PSO method. After the locations are optimized, the chaff points within these optimized locations of feature vector points are chosen. The processes continue from step (1) to (6) for the generation of new chaff points. Then, the obtained best locations are converted into its corresponding feature vector points and which are utilized as the new chaff points in the proposed work.

The number of chaff points used for creating the grouped feature vector is represented as $c_n$. The grouped feature vector is created by adding the total number of extracted feature points from face, ear and chaff points. Therefore, the total number of points to be extracted from a person is specified as follows,

$$G_n = fe_n + c_n \tag{8}$$

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

$$G_p = \{f_p, e_p, c_p\} \tag{9}$$

Hence, the grouped feature vectors are obtained by adding the face, ear feature modalities and the new chaff points. These grouped feature vectors are then involved in the fusion process.

### 3.4. Fusion and recognition phase

In the process of fusion, fuzzy vault is generated from the grouped feature vector points and the secret key points. In order to develop the template security, the secret key concept that generates fuzzy vault is combined to the grouped feature vector. Initially, the input secret key is encoded to make its secret key points that are 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.

#### 3.4.1. Process of creating the secret key points and fusion

Generation of points for the secret key is based on the below mentioned designed mechanism which provides security to the combined ear and face templates. Suppose the input digit is $I_d$, then the $x$ and $y$ co-ordinates are designed as:

$$X\text{-axis} = K_d \times (I_d + K_d) \tag{10}$$

$$Y\text{-axis} = K_d \tag{11}$$

Hence the points can be represented as $[K_d \times (I_d + K_d)K_d]$ for the input digit $I_d$. Suppose the input key is of size $s$ and the key is represented

$$S_{dp} = S_{d1}, S_{d2}, \ldots, S_{ds} \tag{12}$$

where, $S_{dp}$ is the $d$th digit of the $p$th person secret key. The points for each of the secret key digit are formed as in the above equations so as to result in points represented as

$$P_{dp} = \{(S_{d1}, I_{d1}), (S_{d2}, I_{d2}), \ldots, (S_{ds}, I_{ds})\} \tag{13}$$

where, the secret key digit is $I_{dp}$ and $S_{dp}$ is defined as $K_d \times (I_{dp} + K_d)$. These above points from Eq. (14), are added with the combined feature vector points from Eq. (9), and the fuzzy vault is generated. The representation of the fuzzy vault is,

$$FV_d = \{f_d, e_d, c_d, S_{d1}, S_{d2}, \ldots, S_{ds}\},$$
$$0 < d < \text{total no. of persons} \tag{14}$$

Each fuzzy vault for each corresponding person is stored in the database. Thus we can obtain the total number of points in the fuzzy vault as,

$$P_n = f_n + e_n + c_n + s \tag{15}$$

The fuzzy vault is created in the above manner by fusing the grouped feature vector points and the secret key points. The process of generating fuzzy vault is given in the following Fig. 3.

#### 3.4.2. Recognition of a person

In this Recognition phase, a test person's face and ear images are given as input which is pre-processed and feature extracted to form the combined feature vector. The input feature vector is compared to the fuzzy vaults in the database and if matched, the secret key is generated to confirm with the person and authentication is provided. The recognition process is illustrated in the following Fig. 4.

Let the input person's feature vector points be represented by $G_t = \{f_t, e_t, c_t\}$, which is compared to fuzzy vault in the database. If all the points' feature vector of the test person matches into the fuzzy vault, then the person is granted authentication else the authentication is denied. Once all the points in test person feature vector match with the fuzzy vault from the database, then certain points in the fuzzy vault will still be left alone. These points are the secret key points and the $x$-coordinate of these points will give the secret key of the person. Suppose $P_{dp} = \{(S_{d1}, I_{d1}), (S_{d2}, I_{d2}), \ldots, (S_{ds}, I_{ds})\}$, then the secret key is $\{I_{d1}, I_{d2}, \ldots, I_{ds}\}$. The generation of the person is a second confirmation of the person and improves the template security.

## 4. Results and discussion

The proposed technique optimized new chaff points using PSO to generate face and ear based fuzzy vault for multi-biometric cryptosystem are evaluated and analyzed in this section. The proposed technique is implemented in MATLAB 7.12 platform.

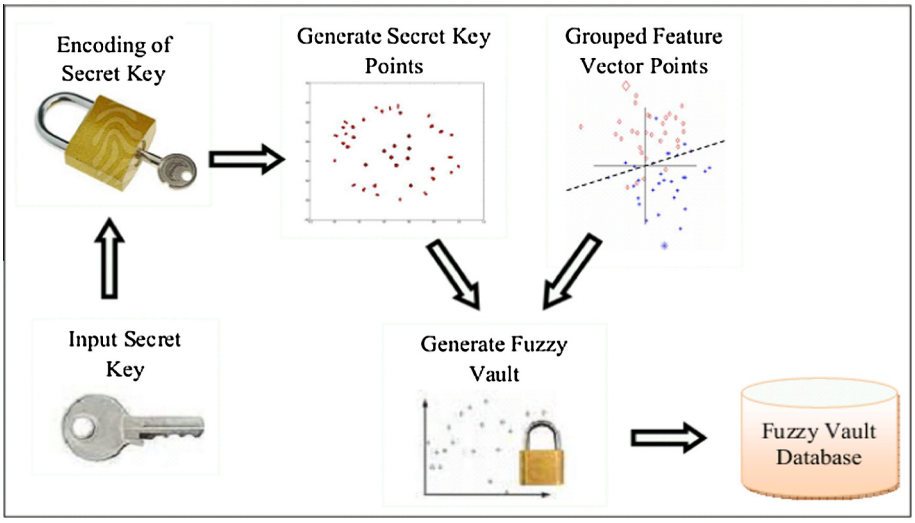


**Figure 3** Process of generating fuzzy vault.

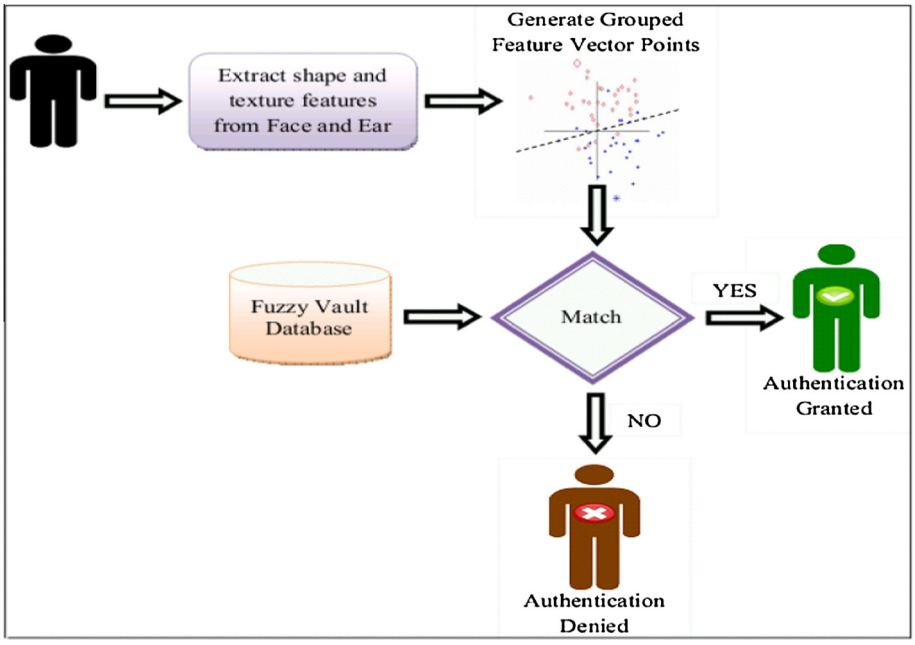


**Figure 4** Process of recognition of a person.

### *4.1. Dataset description*

For evaluating the proposed work, face and ear images are taken from the Yale face database and IIT Delhi ear database, respectively.

#### *4.1.1. Face – Yale face database*

The Yale face database with size 6.4 MB comprises 165 grayscale images in GIF format of 15 persons. The clients are healthy and hail from all walks of life such as students, engineers, workers. Fig. 5 shows the sample Yale face database images.

#### *4.1.2. Ear – IIT Delhi ear database*

IIT Delhi ear database comprises the ear images gathered from the students and staff at IIT Delhi, India. All the images are obtained from a distance (touch less) by means of an easy imaging setup and the imaging is executed in the indoor atmosphere. The database available at present is gathered from the 121 diverse subjects, each of them possessing at least three ear

**Figure 5** Sample face images from Yale face Database.

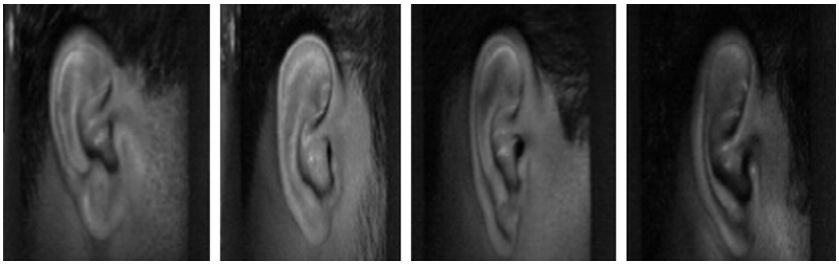

**Figure 6** Sample ear images from IIT Delhi ear database.

images. All the subjects in the database are aged between 14 years and 58 years. The database of 471 images has been serially numbered for every client with an integer recognition/number. The resolution of these images is 272 × 204 pixels. In addition to the original images, this database also furnishes the mechanically adapted and cropped ear images of size 50 × 180 pixels. Of late, a bigger version of ear database (automatically cropped and normalized) from 212 users with 754 ear images is also included and made accessible on request. Fig. 6 clearly shows the sample ear database images.

### 4.2. Experimental results

Initially, the face and ear images are converted from the RGB format into gray scale format images. Then, the filtering operations are applied on the grayscale face and ear images. For both the grayscale face and ear images, one of the non-linear smoothing methods, Median filter is exploited. The preprocessed face and ear images are shown in the following Fig. 7.

After obtaining pre-processed images, features from both the face and ear images are extracted using separate methods. Shape features and texture features are extracted from the pre-processed image. From the pre-processed face and ear images, using Modified Region Growing method shape features are extracted. The face and ear shape feature extraction process is explained in Section 3.2.1 and the shape feature extracted images are shown in the following Fig. 8.

Texture features are also extracted from the pre-processed face and ear images using the Local Gabor XOR Pattern method. Only the histogram is obtained as the results of LGXP and the pixel values are changed according to it. The process of LGXP is given in Section 3.2.2. After extracting the shape and texture features from the face and ear images, the grouped vector points are generated (Section 3.3). Grouped feature vectors are generated with the chaff points from the two extracted feature points of the face and ear. The optimization algorithm PSO has helped to create these chaff points. Totally 100 chaff points are generated, in which 50 are from face features and 50 from ear features. The optimized chaff points are given in the following Table 1.

In Table 1, some of the chaff points get similar values. The reason is that the chaff points are also the feature vector points, which have identical points. And then the fusion using fuzzy vault followed by recognition process is carried out (Section 3.4). Hence, the face and ear images from the databases are authenticated for each person.

### 4.3. Evaluation metrics

In order to evaluate the proposed multimodal biometric authentication system based on face and ear images, the evaluation metrics used are False Matching Rate (FMR), False Non-Matching Rate (FNMR), Genuine Acceptance Rate (GAR), Dice Co-efficient (DC) and Jaccard Co-efficient (JC).

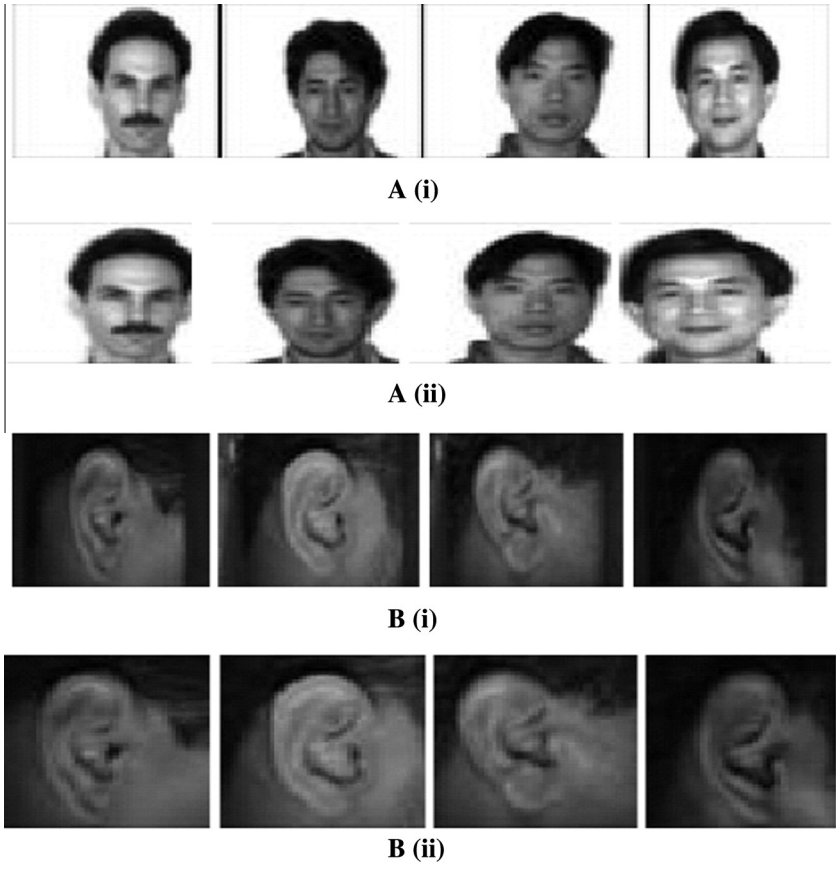


**Figure 7** Preprocessed images: (A) face images, (B) ear images – (i) Median filter applied image; (ii) crop out images.

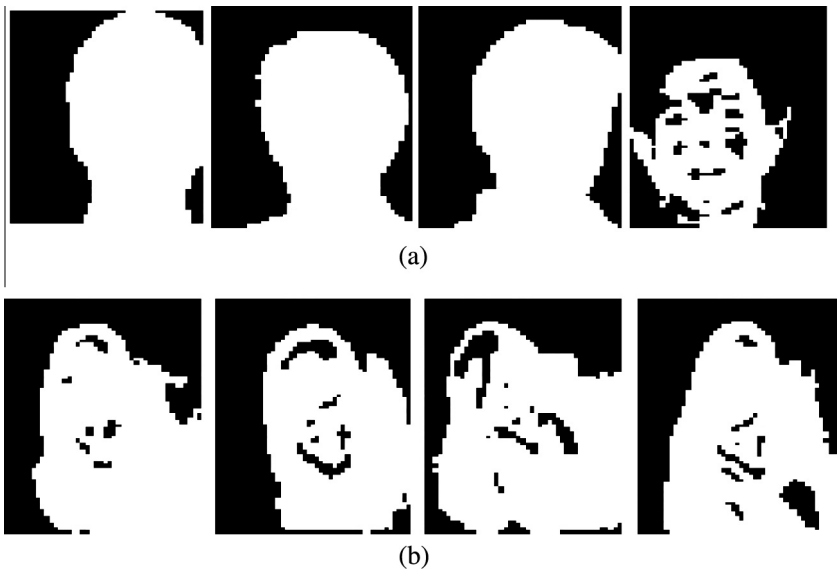


**Figure 8** Shape feature extracted images – (a) face; (b) ear.

#### 4.3.1. False Matching Rate (FMR)

The False Matching Rate is that which incorrectly recognized the non-authorized people. The FMR is specified as follows,

$$\text{FMR} = \frac{\text{Number of non-authorized inputs which are falsely recognized}}{\text{Total number of inputs}} \tag{16}$$

**Table 1** Optimized chaff points from the face and ear features.

| Optimized chaff points from face features | | Optimized chaff points from ear features | |
|---|---|---|---|
| 202 | 224 | 37 | 51 |
| 202 | 50 | 60 | 43 |
| 12 | 14 | 63 | 43 |
| 3 | 40 | 37 | 34 |
| 53 | 33 | 4 | 39 |
| 16 | 11 | 227 | 59 |
| 18 | 10 | 31 | 32 |
| 33 | 44 | 50 | 200 |
| 40 | 24 | 49 | 9 |
| 24 | 217 | 13 | 30 |
| 52 | 12 | 60 | 28 |
| 31 | 60 | 227 | 5 |
| 56 | 41 | 37 | 19 |
| 11 | 8 | 62 | 4 |
| 17 | 13 | 42 | 61 |
| 8 | 23 | 40 | 49 |
| 5 | 43 | 35 | 32 |
| 32 | 61 | 33 | 14 |
| 6 | 5 | 1 | 58 |
| 55 | 27 | 42 | 32 |
| 41 | 3 | 39 | 55 |
| 31 | 64 | 7 | 13 |
| 29 | 45 | 31 | 19 |
| 36 | 32 | 47 | 46 |
| 32 | 43 | 63 | 46 |

#### 4.3.2. False Non-Matching Rate (FNMR)

The False Non-Matching Rate is that which incorrectly did not recognize the authorized people. The FNMR is specified as follows,

$$\text{FNMR} = \frac{\text{Number of authorized inputs which are falsely not recognized}}{\text{Total number of inputs}} \tag{17}$$

Authorized and Non-Authorized persons are the two major targets and here class 1 indicates authorized persons and class 0 indicates non-authorized persons.

#### 4.3.3. 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 Non-Matching Rate in Eq. (17) and it is given in Eq. (18) below,

$$\text{GAR} = 1 - \text{FNMR} \tag{18}$$

#### 4.3.4. Dice Co-efficient (DC)

Dice Coefficient (DC) was planned to be applied to the presence or absence of recognized images, and is given by,

$$\text{DC} = \frac{2|A \cap B|}{|A| + |B|} \tag{19}$$

#### 4.3.5. Jaccard Co-efficient (JC)

The Jaccard coefficient (JC) measures similarity between two sets (target accurate recognized images and accurate recognized images obtained), and is defined as the size of the intersection divided by the size of the union of the two sets:

$$\text{JC} = \frac{|A \cap B|}{|A \cup B|} \tag{20}$$

In both the Eqs. (19) and (20), A indicates the target set of accurate recognized images and B indicates the set of accurate recognized images obtained by the proposed work.

### 4.4. Performance analysis of the proposed work

The results of the proposed multimodal biometric system based on face and ear modalities with different secret key sizes are obtained. The results can be taken by applying noise to the face and ear images with various secret key sizes, which are given below in Table 2.

The performance results of the proposed work with noises by varying the secret key sizes are also illustrated in the graphical representation in Fig. 9.

Table 2 and Fig. 9 show the results of the proposed multimodal biometric system using face and ear modalities by varying the secret key sizes 4, 6, 8, 10 with noises. For this, White Gaussian noises are added to the proposed work and the results for the noise added images are acquired. From the graphs and tabular values, it can be understood that the accuracy of the multimodal biometric result does not yield appreciably high values, but only average high values for the recognition of the correct person using the modalities face and ear with the addition of noises. For the secret key sizes 4, 6, 8 and 10, 70% of GAR values are obtained. With White Gaussian noises, the FMR and FNMR values are low (average values) for the proposed study. The value of both FMR and FNMR are 30% for all the secret key sizes. Low values in FMR and FNMR only can increase the recognition accuracy with high GAR values because, the incorrect recognition is minimal and correct recognition of person is significant in the proposed work. And, also the DC and JC values are at average high values, 70% and 73%, respectively. However, the results of recognition accuracy offer superior values for the proposed work with noise. The following Table 3 shows the results of biometric system using face and ear alone, respectively.

The size of the secret key does not change the results of the proposed work. The performance results of the proposed work without noises and by changing the secret key sizes are also illustrated in the following graphical representation in Fig. 10.

Table 3 and Fig. 10 show the results of the proposed multimodal biometric system by changing the secret key sizes 4, 6, 8, 10 using face and ear modalities without applying noises. The above graphs and tabular values are being able to prove that the accuracy of the multimodal biometric result facilitates superior value for the recognition of the correct person using the modalities of the face and ear without applying any noises to the images. The FMR and FNMR values are very low for

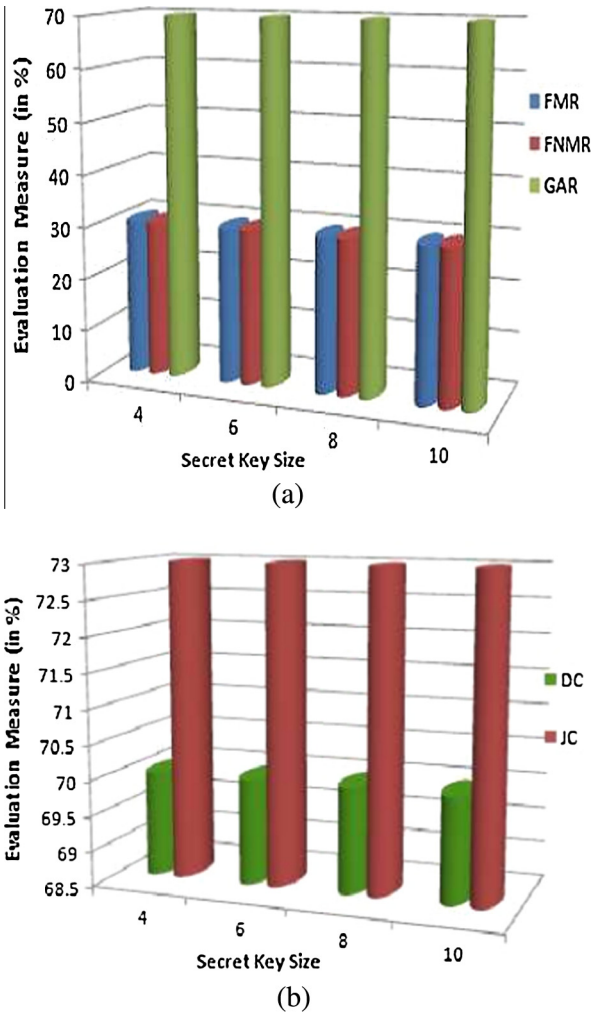


**Figure 9** Performance analysis for the proposed work using face and ear modalities with noises for various secret key sizes – (a) FMR, FNMR and GAR; (b) DC and JC.

the proposed work. The value of both FMR and FNMR are 10% for all the secret key sizes without adding any noises to the face and ear images. For the secret key sizes 4, 6, 8 and 10, the GAR values of 90% is obtained. In addition to this, without applying any noise to the images, the results of DC and JC are also high (90% values for both DC and JC) for the proposed work of changing all the secret key sizes. Moreover, it can be observed that the values for FMR, FNMR, GAR, DC and JC values are the same for all the secret key sizes, irrespective of whether the images are with noise or with-

**Table 2** Results of proposed multimodal biometric system using face and ear modalities with noises for various secret key sizes.

| Secret key size | FMR (in %) | FNMR (in %) | GAR (in %) | DC (in %) | JC (in %) |
|---|---|---|---|---|---|
| 4 | 30 | 30 | 70 | 70 | 73 |
| 6 | 30 | 30 | 70 | 70 | 73 |
| 8 | 30 | 30 | 70 | 70 | 73 |
| 10 | 30 | 30 | 70 | 70 | 73 |

**Table 3** Results of proposed multimodal biometric system using face and ear modalities without noises for various secret key sizes.

| Secret key size | FMR (%) | FNMR (%) | GAR (%) | DC (%) | JC (%) |
|---|---|---|---|---|---|
| 4 | 10 | 10 | 90 | 90 | 90 |
| 6 | 10 | 10 | 90 | 90 | 90 |
| 8 | 10 | 10 | 90 | 90 | 90 |
| 10 | 10 | 10 | 90 | 90 | 90 |

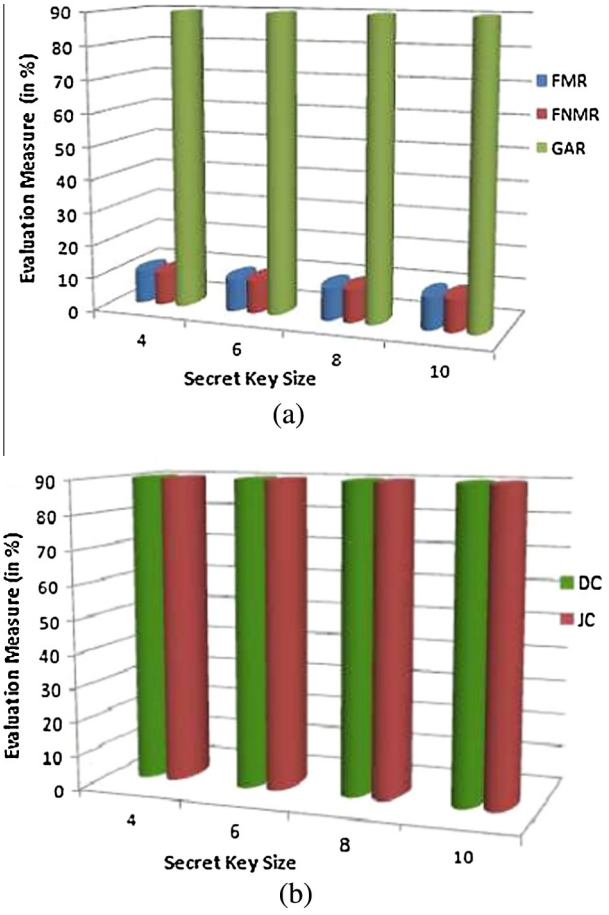


**Figure 10** Performance analysis for the proposed work using face and ear modalities without noises for various secret key sizes – (a) FMR, FNMR and GAR; (b) DC and JC.

out. And, also the recognition results of the proposed work are superior, when there is no addition of noise to the images. Nevertheless, the results of recognition accuracy furnish very much better value for the proposed work without noise.

### *4.5. Comparison results*

The comparison results evaluate the proposed work in relation with PSO and without the use of PSO. The location of the shape and texture features extracted from the face and ear images is considered by selecting the chaff points in the proposed work. From the particular range of these locations, four distances are set by optimizing the distant locations using the PSO algorithm. Thus, the recognition comparison results of FMR, FNMR, GAR, DC and JC without noise results of the proposed work with PSO and without PSO are given in Table 4. The graph of the comparison results of recognition accuracy in Table 4 is plotted in the following Fig. 11.

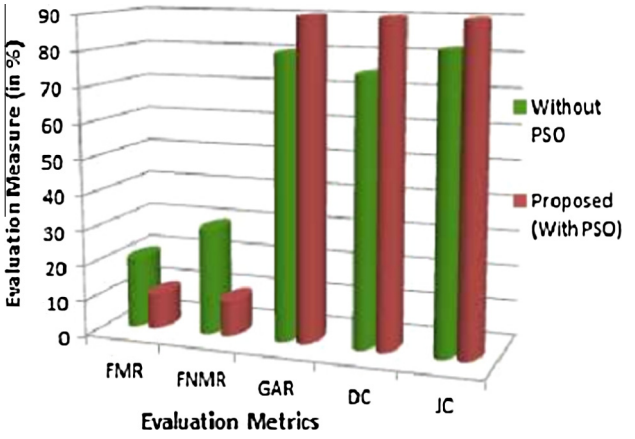


**Figure 11** Comparison graph for the recognition result between the proposed work with PSO and the proposed work without PSO without noise.

From Fig. 11 and Table 4, it is shown that the proposed work with PSO offers good recognition accuracy with GAR of 90%, value for the secret key sizes 4, 6, 8 and 10, respectively. But, the proposed work without PSO gives 80% of GAR values for all the secret key sizes 4, 6, 8 and 10. Both FMR and FNMR values for the proposed work with PSO are 10% and also for the proposed work without PSO are 20% and 30%, respectively. The low values in FMR and FNMR offer a means to increase GAR results by giving higher accurate recognition accuracy results. Both DC and JC values for the proposed work with PSO are 90% and also for the proposed work without PSO are 75% and 82%, respectively, with each secret key size change. Overall, the proposed work with PSO provides higher results of recognition accuracy and the reason behind this is that the PSO provides effective optimization results by choosing correct distances from the particular range of locations leading to get a higher recognition rate for the proposed work. Moreover, in both of the proposed work with PSO and without PSO, the evaluation metric values are not changed, when the secret key size gets changed.

**Table 4** Comparison results of the proposed work with PSO and proposed work without PSO.

| Evaluation metrics | Secret key size | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 4 | | 6 | | 8 | | 10 | |
| | Without PSO | Proposed (with PSO) | Without PSO | Proposed (with PSO) | Without PSO | Proposed (with PSO) | Without PSO | Proposed (with PSO) |
| FMR (in %) | 20 | 10 | 20 | 10 | 20 | 10 | 20 | 10 |
| FNMR (in %) | 30 | 10 | 30 | 10 | 30 | 10 | 30 | 10 |
| GAR (in %) | 80 | 90 | 80 | 90 | 80 | 90 | 80 | 90 |
| DC (in %) | 75 | 90 | 75 | 90 | 75 | 90 | 75 | 90 |
| JC (in %) | 82 | 90 | 82 | 90 | 82 | 90 | 82 | 90 |

**Table 5** Comparison between multi-modality and uni-modality using face and ear.

| Modalities | FMR (%) | FNMR (%) | GAR (%) | DC (%) | JC (%) |
|---|---|---|---|---|---|
| Proposed face and ear | 10 | 10 | 90 | 90 | 90 |
| Only face | 20 | 20 | 80 | 80 | 75 |
| Only ear | 20 | 20 | 80 | 80 | 75 |

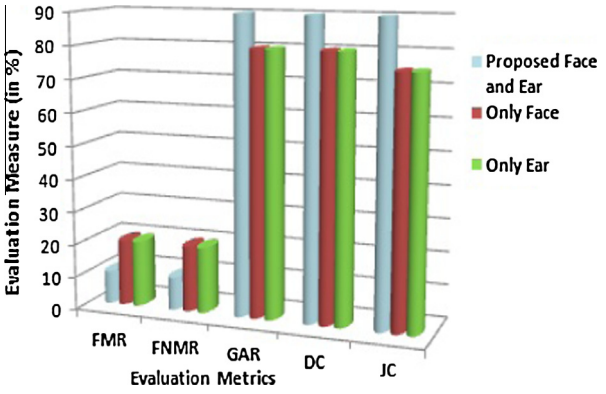


**Figure 12** Graph for comparing multi-modal and uni-modal biometric system of face and ear.

The proposed biometric system aims for the recognition of multimodal biometric system based on face and ear of human beings. There is a need to compare our proposed work, when it is worked along with either face or ear. The results of only unimodalities with the multimodality are given in Table 5 and its graph is illustrated in Fig. 12.

Only the face and ear modalities of the proposed work cannot improve the accuracy, which provides more error rates when recognizing target person. But, the proposed multimodality of face and ear helps to improve the accuracy by reducing the error rates. These comparison results show the proposed multimodality system to get higher recognition of persons with the aid of face and ear. From all these results, it is additionally proved that the proposed biometric system is superior for the identification of the correct person in comparison with the proposed work without PSO by the use of face and ear modalities.

## 5. Conclusion

New $x$ and $y$ co-ordinate chaff matrix points were produced from the best locations of extracting feature vector points in the proposed human recognition system. The optimization algorithm PSO helps to choose the best feature vector point location for creating high grade security at fusion process. Using the suggested method, the recognition was carried out for both the face and ear images. For the evaluation, metrics FMR, FNMR, GAR, DC and JC were measured by changing the secret key size each and every time. The recognition results of the proposed work without noise addition significantly offered better results. The multi-biometric without the employ of PSO was also compared with use of PSO for proving that the proposed work is superior, in which the method with PSO provides 10% of GAR, 15% of DC and 8% of JC value higher than the method without PSO. This comparison shows that the chaff point selection with PSO can give higher security in a multimodal biometric cryptosystem with the fuzzy vault template. This new chaff point generation method in fuzzy vault avoids hacking of biometric data by an attacker. From all the results, it could be able to prove that the multimodal biometric system with the usage of PSO based new chaff points gave better recognition results for a person.

## References

Bai, Qinghai, 2010. Analysis of particle swarm optimization algorithm. J. Comput. Inf. Sci. 3 (1), 180–184.

Bhattacharyya, Debnath, Ranjan, Rahul, Alisherov, Farkhod, Choi, Minkyu, 2009. Biometric authentication: a review. Int. J. u e-Serv., Sci. Technol. 2 (3), 13–28.

Bui, F.M., Martin, K., Lu, H., Plataniotis, K.N., Hatzinakos, D., 2010. Fuzzy key binding strategies based on quantization index modulation (QIM) for biometric encryption (BE) applications. IEEE Trans. Inf. Forensics Security 5 (1), 118–132.

Chang, Ee-Chien, Shen, Ren, Teo, Francis Weijian, 2006. Finding the original point set hidden among chaff. In: Proceedings of the ACM Symposium on Information, Computer and Communications Security, pp. 182–188.

Egrioglu, Erol, Ozdemir, Bahadir, 2014. Lagged variables selection for fuzzy time series models by using binary particle swarm optimization. AJSCA 1 (1).

Giot, Romain, Rosenberger, Christophe, Dorizzi, Bernadette, 2012. Hybrid template update system for unimodal biometric systems. In: Proceedings of the IEEE International Conference on Biometrics: Theory, Applications and Systems, pp. 1–7.

Hao, F., Anderson, R., Daugman, J., 2006. Combining crypto with biometrics effectively. IEEE Trans. Comput. 55 (9), 1081–1088.

He, Mingxing, Horng, Shi-Jinn, Fan, Pingzhi, Run, Ray-Shine, Chen, Rong-Jian, Lai, Jui-Lin, Khan, Muhammad Khurram, Sentosa, Kevin Octavius, 2010. Performance evaluation of score level fusion in multimodal biometric systems. Pattern Recogn. 43 (5), 1789–1800.

Huang, Zengxi, Liu, Yiguang, Li, Chunguang, Yang, Menglong, Chen, Liping, 2013. A robust face and ear based multimodal biometric system using sparse representation. Pattern Recogn. 46 (8), 2156–2168.

Introna, Lucas D., Nissenbaum, Helen, 2010. Facial Recognition Technology – A Survey of Policy and Implementation Issues Report of the Center for Catastrophe Preparedness & Response. New York University, pp. 1–60.

Islam, S.M.S., Davies, R., Bennamoun, M., Owens, R.A., Mian, A.S., 2013. Multibiometric human recognition using 3D ear and face features. Pattern Recogn. 46 (3), 613–627.

Khalil-Hani, Mohamed, Bakhteri, Rabia, 2010. Securing cryptographic key with fuzzy vault based on a new chaff generation method. In: In Proceedings of IEEE International Conference on High Performance Computing & Simulation, France, pp. 259–265.

Kumar, Ajay, Wu, Chenye, 2012. Automated human identification using ear imaging. Journal of Pattern Recognition 45, 956–968.

Leng, Lu, Zhang, Jiashu, 2011. Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. J. Netw. Comput. Appl. 34 (6), 1979–1989.

Leng, Lu, Zhang, Jiashu, Khan, Muhammad Khurram, Chen, Xi, Alghathbar, Khaled, 2010. Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain. Int. J. Phys. Sci. 5 (17), 2543–2554.

Meenakshi, V.S., Padmavathi, G., 2009. Security analysis of password hardened multimodal biometric fuzzy vault. World Acad. Sci. Eng. Technol. 32, 312–320.

Mohsen, Fahd M.A., Hadhoud, Mohiy M., Amin, Khalid, 2010. A new optimization-based image segmentation method by particle swarm optimization. Int. J. Adv. Comput. Sci. Appl. 7 (4), 10–18.

Nagar, Abhishek, Nandakumar, Karthik, Jain, Anil K., 2012. Multibiometric cryptosystems based on feature-level fusion. IEEE Trans. Inf. Forensics Secur. 7 (1), 255–268.

Nguyen, Thi Hanh, Wang, Yi, Nguyen, Trung Nhan, Li, Renfa, 2013. A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm. In: Proceedings of IEEE International Conference on Signal Processing, Communication and Computing, pp. 1–6.

Nguyen, Thi Hanh, Wang, Yi, Ha, Yajun, Li, Renfa, 2013b. Improved chaff point generation for vault scheme in bio-cryptosystems. J. IET Biom. 2 (2), 48–55.

Onwunalu, Jérôme E., Durlofsky, Louis J., 2010. Application of a particle swarm optimization algorithm for determining optimum well location and type. J. Comput. Geosci. 14 (1), 183–198.

Rua, E.A., Maiorana, E., Castro, J.L.A., Campisi, P., 2012. Biometric template protection using universal background models: an application to online signature. IEEE Trans. Inf. Forensics Secur. 7 (1), 269–282.

Sowkarthika, S., Radha, N., 2012. Securing iris templates using double encryption method. In: Int. J. Adv. Res. Comput. Sci. Software. Eng., 2, pp. 259–264.

Sutcu, Y., Li, Q., Memon, N., 2009. Protecting biometric templates with sketch: theory and practice. IEEE Trans. Inf. Forensics Security 2 (3), 503–512.

Vandommele, Tjark, 2010. Biometric authentication today. In: Proceedings of the Seminar on Network Security.

Wu, Lifang, Yuan, Songlong, 2010. A face based fuzzy vault scheme for secure online authentication. In: Proceedings of IEEE Second International Symposium on Data, Privacy and E-Commerce, pp. 45–49.

Xu, Dacheng, Wang, Xiaotao, 2010. A scheme for cancelable fingerprint fuzzy vault based on chaotic sequence. In: Proceedings of IEEE International Conference on Mechatronics and Automation, pp. 329–332.