# A HYBRID ABC-PSO BASED MULTI-POLYNOMIAL FUZZY VAULT FOR MULTIMODAL BIOMETRIC CRYPTOSYSTEM

**[1] Gandhimathi Amirthalingam, [2] Midun Thangavel**

[1] Department of Computer Science, King Khalid University, Kingdom of Saudi Arabia
[2]Bacelor of Computer Science and Engineerin, Dr. Mahalingam College of Engineering and Technology, India

**ABSTRACT: Fuzzy vault with multiple polynomials can be able to keep away from the promising degradation of template security, which is utilized in the proposed work. According to modalities, Ear biometric has become an admired biometric modality that facilitates enhanced biometric performance because of the distinctiveness, permanence and unchanged by aging. Energy feature is extracted from the ear images with the aid of Local Principal Independent Components (LPIC). X and Y co-ordinate chaff matrix can be created with the aid of boundary matrix from the extracted features. A Hybrid ABC-PSO algorithm is utilized for calculating the optimal locations to make novel chaff matrix, in which, PSO is processed within the scout bee component that leads to fast convergence and limited search space controlled based optimization of locations. The proposed system is implemented with Yale face and IIT ear databases and its performance is 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 performance of suggested method shows the promising growth in the face and ear biometric recognition and template security.**

**Keywords: Local Principle Independent Components, Artificial Bee Colony Algorithm, Multiple polynomials, Hybrid ABC-PSO, Fuzzy vault**

## I. INTRODUCTION

Crypto biometric systems are substantiation methods which blend the concepts of cryptography and biometrics. Fuzzy vault is a deep-rooted crypto biometric scheme which is endowed with the quality of protecting the biometric templates [14]. It functions as a device ensuring added level of safety. The multimodal system of ear and face biometrics made an inspiration to develop a biometric system with more securable one [16] [17]. The main reason for this development is that both the traits are in close physical proximity to each other and when acquiring data of the ear and the face is frequently encountered as well [18]. The quality-based adaptive multimodal achieves a striking robustness to various types of unimodal corruption/occlusion [20].

In fuzzy vault scheme, the secret key S is locked by G, where G is an unordered set from the biometric sample. A polynomial P is constructed by encoding the secret S. This polynomial is evaluated by all the elements of the unordered set G. A vault V is constructed by the union of unordered set G and chaff point set C which is not in G. V = G U C, the union of the chaff point set hides the genuine point set from the attacker. Hiding the genuine point set secures the secret data S and user biometric template T.

The haunting hassles in chaff points created are successfully tackled by introducing a novel chaff point creation technique, which employs an optimizing algorithm for the selection of the new chaff feature points is 'Hybrid ABC-PSO Algorithm'. Recently, Artificial Bee Colony (ABC) algorithm [7] has become one of the most modern swarm-based algorithms for solving optimization problems [3] [10]. In a real bee colony, there are some tasks performed by specialized individuals. These specialized bees try to maximize the nectar amount stored in the hive by performing efficient division of labor and self-organization. The minimal model of swarm-intelligent forage selection in a honey bee colony, that ABC algorithm adopts, consists of three kinds of bees: employed bees, onlooker bees, and scout bees. The main reason is that the performance of the ABC algorithm is competitive with those of other population-based optimization algorithms because of its few control parameters, simplicity, and ease of implementation. Though fuzzy vault is able to effectively secure the templates of the modalities, the recognition accuracy of the resultant system with single polynomial is significantly lower compared to the accuracy on the original template. One reason for this is the inability of the fuzzy vault to effectively utilize salient information in modalities [1]. In Fuzzy vault technique, a polynomial of degree n is created from the key and thereafter it is estimated by means of the components of biometrics. These authentic points encode the data of both the key and the biometrics, and function as guidance data. In the validation phase, if we are able to arrive at the n+1 true point, the polynomial can be rebuilt and the secret key can be reclaimed accurately [13]. The single polynomial fuzzy vault structure affords ample leeway to the hackers to locate the key with ease and assault the mechanism. Further, the biometric template is not a safe device. Since biometric data cannot be easily replaced or changed once stolen, it is important that biometric templates used in biometric applications should be constructed and stored in a secure way so that the adversaries would not be able to forge biometric data easily even when the templates are compromised.

Taking due consideration of the related issues and the repercussions existing in the task of affording template safety, the task of launching the Fuzzy vault methods with multiple polynomials has taken which can function smoothly, without in any way compromising the efficient execution of the system [15]. With an eye on offering a excellent and securable biometric mechanism, multi polynomial structure based fuzzy vault technique is launched in this investigation. Consequently by means of the hybridization of ABC-PSO algorithms, chaff feature points get optimized and create novel chaff points with excellently safeguarded fuzzy vault fusion with multiple polynomials.

## II. LITERAURE REVIEW

Certain modern works rooted on fuzzy vault with multiple polynomial constructions and the employment of modalities face and ear are furnished hereunder.

Nandakumar and Anil K. Jain [11] have proposed a scheme for securing multiple templates of a user as a single entity. They have made a single multibiometric template from the individual templates and secured it using the fuzzy vault framework. They have demonstrated that a multibiometric vault provides better recognition performance and higher security compared to a unibiometric vault.

Daesung Moon et al. [6] have deftly utilized an adaptive degree of the polynomial with due weight for the number of minutiae mined from every client. They have made use of numerous polynomials to steer clear of the potential deprivation of the safety of an easy solution by means of a low-degree polynomial.

Yi C. Feng et al. [21] have proposed a hybrid approach which takes advantage of both the biometric cryptosystem approach and the transform-based approach. A three-step hybrid algorithm was designed and developed based on random projection, discriminability-preserving (DP) transform, and fuzzy commitment scheme. Their proposed algorithm has not only provided good security, but also enhanced the performance through the DP transform.

D. Yamen et al. [8] explore the feature fusion strategy to combine the profile face and ear for age and gender classification. The profile face and ear images are trained with the two separate CNN models; the two traits are concatenated to form a multi modal feature vector.

Cancellable fingerprint fuzzy vault based on chaotic sequence was proposed by DachengXu and Xiaotao Wang [5]. Their proposed method has changed the original template into transformed template by using transformation function. Then, the transformed template was used to construct the vault. In the vault unlocking phase, the transformed input template was generated when the same transformation was applied to the input template.

Abhishek Nagar *et al.* [2] have proposed a feature-level fusion framework to simultaneously protect multiple templates of a user as a single secure sketch. Their main contributions have included:1) practical implementation of the proposed feature-level fusion framework using two well-known biometric cryptosystems, namely, *fuzzy vault* and *fuzzy commitment*, and 2) detailed analysis of the trade-off between matching accuracy and security in the proposed multibiometric cryptosystems based on two different databases (one *real* and one *virtual* multimodal database), each containing the three most popular biometric modalities, namely, fingerprint, iris, and face.

Brendan F. Klareet al. [4] has offered the influence of demographics on the performance of face recognition algorithms. Dynamic face matcher selection procedure should lead to improved face recognition accuracy in many intelligence and law enforcement face recognition scenarios. Finally, they have also shown that an alternative to dynamic face matcher selection was to train face recognition algorithms on datasets that are evenly distributed across demographics, as this approach offers consistently high accuracy across all cohorts.

A two-stage geometric approach that is both scale and rotation invariant was implemented by LathaLakshmanan [12] for extracting the unique features present in the surface of an ear image. Her proposed method has worked on partial ear images and demonstrated the presence of more unique features in the middle part of the ear (as seen by the increase in recognition accuracy) and the method also helped in reducing the computation time.

Thi Hanh Nguyen *et al.* [19] have triumphantly put forward a novel chaff point creation method for the fuzzy vault in bio-crypto systems which have proved to be substantially time-conscious for the creation of more than 200 chaff points. Sophisticated research has proved 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.

## III. PROPOSED METHOD FOR MULTIMODAL BIOMETRIC CRYPTOSYSTEM

New chaff point's based Fuzzy vault is the proposed work, which is worked out with a Hybrid ABC-PSO algorithm and multiple polynomial constructions. More securable multi biometric system is formed by the proposed work with the aid of face and ear modalities. The proposed work in fig. 1 comprises of five phases such as,

(1) Feature Extraction
(2) New chaff points Generation
(3) Encoding with Fuzzy vault
(4) Decoding with Fuzzy vault
(5) Authentication

### A. *Fearture Extraction Phase*

The input RGB face and ear images are converted into grayscale image. The filtering operations of Median filter are applied on the grayscale face and ear images. Median Filter removes the blurred edges and to decrease the noises by substituting the current point in the input image by the median of the brightness in its neighborhood. The reasons for applying median filter are:

- Median filter can able to reduce the noises such as salt and pepper (impulse noises). In these noisy pixels, the information related to the original values is not presented.
- Median filter is better to preserve at sharp edges and which helps to remove the outliers.

The feature sets such as shape, texture and energy are extracted from the images followed by the pre-processing of face and ear images.

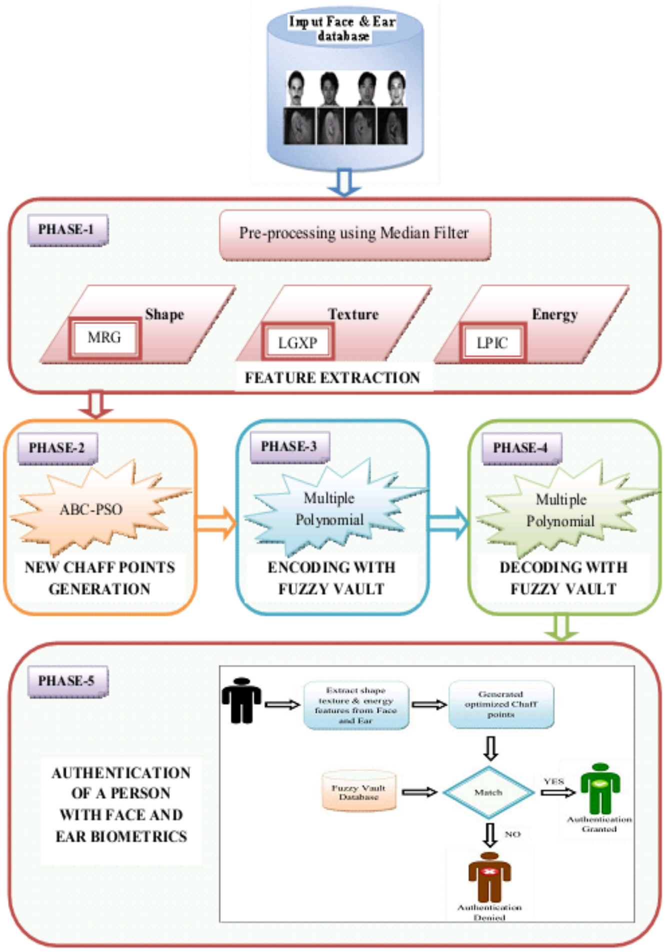

Input Face & Ear database
PHASE-1
Pre-processing using Median Filter
Shape
MRG
Texture
LGXP
Energy
LPIC
FEATURE EXTRACTION
PHASE-2
ABC-PSO
NEW CHAFF POINTS GENERATION
PHASE-3
Multiple Polynomial
ENCODING WITH FUZZY VAULT
PHASE-4
Multiple Polynomial
DECODING WITH FUZZY VAULT
PHASE-5
AUTHENTICATION OF A PERSON WITH FACE AND EAR BIOMETRICS
Extract shape texture & energy features from Face and Ear
Generated optimized Chaff points
Fuzzy Vault Database
Match
YES
NO
Authentication Granted
Authentication Denied

Fig. 1. Proposed diagram with its phases

*a) 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. The 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.

*b) Texture Feature Extraction using Local Gabor XOR Pattern (LGXP) method:* The texture features are removed from the preprocessed face and ear images, by means of Local Gabor XOR Pattern technique. In LGXP, images are segregated into 3 x 3 blocks in accordance with the dimension. Stages are initially quantized into diverse domains, and then LXP operator is applied on the quantized stages of the central pixel and each of its neighbors including the consequential binary labels are concatenated together as the restricted model of the central pixel. While applying LXP operator on the quantized stages, the original image pixel value is contrasted with it and if the values are identical, then it is substituted by 1; otherwise, it is substituted by 0. Then binary is converted into decimal value and the original mid pixel value is substituted with the new estimated value. Now the decimal values for each pixel in the blocks are obtained and then the histogram for each pixel value is found. Thus, the texture feature values are extracted from each pre-processed face and ear images.

*c) Energy Feature Extraction for ear using LPIC method:* Local Principle Independent Component (LPIC) is utilized for the extraction of the energy features from pre-processed ear images. The information values, which effectively handle the unconstrained environment, are dealt by LPIC.

Ear images are initially divided into small blocks for the energy feature set extraction. The local features obtained from more number of windows of an image provide less noise, resolution, illumination and more robust to occlusion. The information to be extracted from the ear is energy, which is represented as,

$$E = \sum_{i,j=1}^{L} P(i,j)^2 \qquad (1)$$

The energy value in eqn. (1) is obtained for each block and it is represented as, $E_1, E_2, \ldots E_L$, where $L$ indicates the number of blocks in a image, i and j represents the image block position. Then the average value of the information is computed from,

$$E^* = \frac{1}{L}\sum_{i=1}^{L}(E_i) \quad (2)$$

The difference is then calculated by using eqn. (2), which is denoted as follows.

$$D = \{E_i - E^*\} \quad (3)$$

Then from the above eqn. (3), the covariance matrix of the information sets are found as,

$$CM = D^T D \quad (4)$$

From eqn. (4) of covariance matrix, the Eigen values are computed and Eigen vectors are attained from their respective Eigen values. The Eigen vectors are represented as $EV_k$, where, $k = 1,2,\ldots m$ and $m$ indicates the number of Eigen vectors. According to the Eigen vectors and difference of information set, the “Eigen ear space” can be generated using the projection,

$$P_k = D.EV_k, \quad k = 1,2,\ldots.,m \quad (5)$$

Finally the resultant reduced dimensionality feature vector points are obtained with the aid of Eigen ear space as follows,

$$R_i = P_k^T.D \quad (6)$$

Thus, the pre-processed ear images are subjected to LPIC process for extracting the energy features.

### B. *New Chaff Points Generation Phase*

The features of shape, texture and energy are taken from the face and ear modalities to recognize a person, respectively. Each of these modalities has a number of feature vector points. The feature vector points in face and ear are represented as $f_l$ and $e_l$, respectively. It is not enough to a fuzzy vault of a person with these extracted feature points of face and ear only. Chaff points $C_l$, are also needed to fusion the multi biometrics. Chaff points are the extra added random points with the feature points that improve the security of the fuzzy vault that is to be created. An innovative chaff point’s generation method is utilized for the selection of chaff points.

**Hybrid ABC-PSO Based Optimization for the Generation of New Chaff Points**

In order to deal with the issues such as slow convergence in PSO, a Hybrid ABC-PSO algorithm is utilized for calculating the optimal locations to make novel chaff matrix. In Hybrid ABC-PSO, the processes of PSO are processed within the scout bee component, which leads to fast convergence and limited search space controlled based optimization of locations. The feature vector points obtained from the face and ear feature extraction process is converted into its corresponding locations. The best of locations are selected from these locations for the further process. The optimization algorithm of Hybrid ABC-PSO is employed for the selection of best locations.

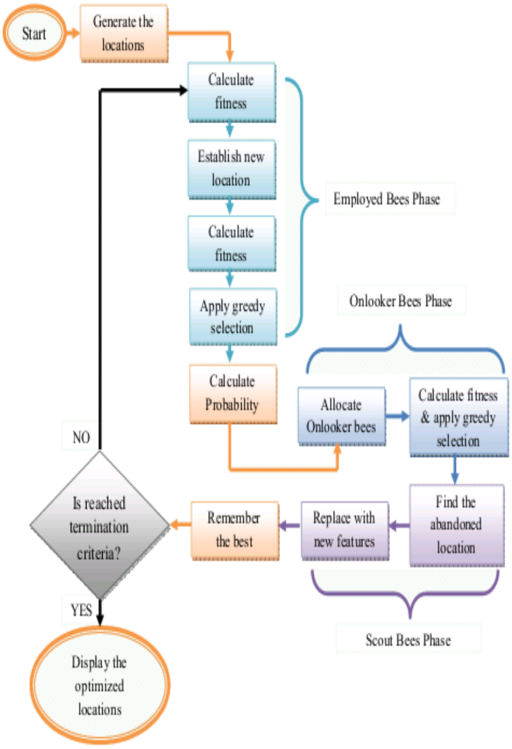


Fig. 2. Flowchart for ABC algorithm

***ABC Algorithm: -***

ABC algorithm is a swarm based meta-heuristic algorithm which was enthused by the sharp foraging behavior of the honey bees. It consists of three components namely, employed bees, onlooker bees and scout bees. The employed bees are coupled with the food sources in the region of the hive and they transfer the data to the onlookers about the nectar quality of the food sources they are exploiting. Onlooker bees are looking the dance of the employed bees inside the hive to pick one food source to exploit according to the data provided by the employed bees. The employed bees whose food source is abandoned become Scout and seeking new food source arbitrarily. The number of food sources denotes the location of feature vector points of probable solutions of optimization problem and the nectar amount of a food source denotes the quality of the solution. The working procedure of ABC algorithm is shown in fig. 2.

***PSO Algorithm:-***

Particle Swarm Optimization is a population-based optimization algorithm designed after the simulation of social character of birds in a group [9]. In the process of PSO, the potential solution named as particles fly through the problem space by following the present optimum particles. The locations of all the feature vector points are taken as the particles *i* in the search space $R^n$. 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).

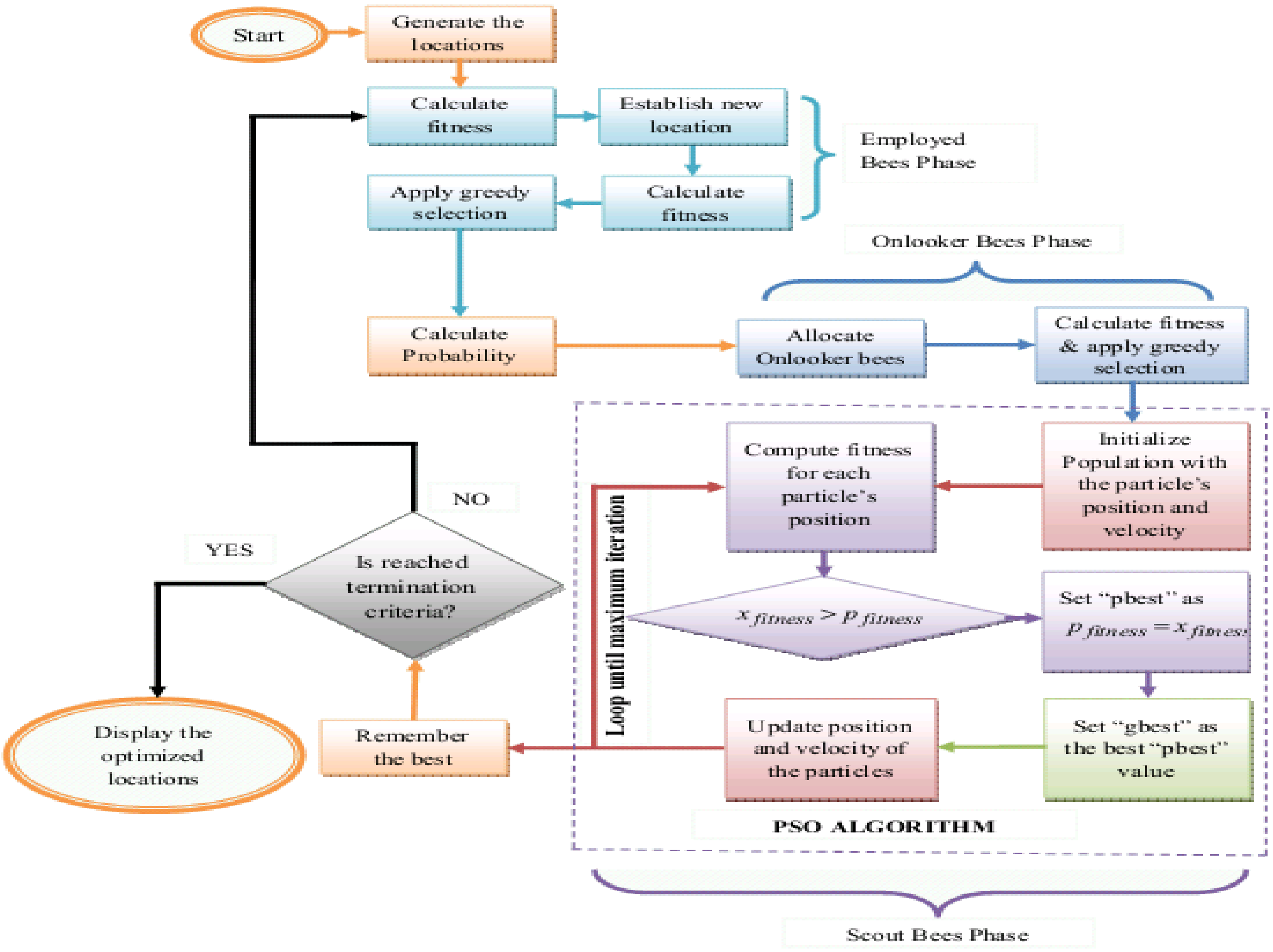

Start
Generate the locations
Calculate fitness
Establish new location
Employed Bees Phase
Apply greedy selection
Calculate fitness
Onlooker Bees Phase
Calculate Probability
Allocate Onlooker bees
Calculate fitness & apply greedy selection
Initialize Population with the particle's position and velocity
Compute fitness for each particle's position
Loop until maximum iteration
NO
YES
Is reached termination criteria?
$x_{fitness} > P_{fitness}$
Set "pbest" as
$P_{fitness} = x_{fitnes}$
Set "gbest" as the best "pbest" value
Update position and velocity of the particles
Remember the best
Display the optimized locations
PSO ALGORITHM
Scout Bees Phase

Fig. 3. Process of Hybrid ABC-PSO for the chaff points optimization

Each particle maintains the record of its coordinates in the problem space which are related with the fitness of the particle. This value is referred to as $pbes$. The value of fitness is stored in $pbes$ value. The $pbes$ value of a particle $i$ is the best position that the particle has seen so far. If $fitnes$ specifies the fitness function means, then the $pbes$ value of the particle $i$ is updates as follows.

$$pbest = \begin{cases} p_i = x_i & \\ p_{fitness} = x_{fitness} & if\, x_{fitness} > p_{fitness} \end{cases} \tag{7}$$

If a particle considers all the population as its topological neighbors the best value is called global best which is also referred to as $gbes$. The particle swarm optimization concept consists of steps for changing the velocity towards the $pbes$ and the $gbes$ locations. Acceleration is weighted by a random term, with random numbers which was generated for acceleration towards the $pbes$ and $gbes$ locations. PSO is initialized by a group of random particles. It also searches for optima by updating generations. In each Iteration, the values are updated using the two values such as $pbes$ and $gbes$.

***Hybrid ABC- PSO Algorithm steps:-***

**Step 1:- Initial Phase**

First the populations of the food sources $f_i, (i=1,2,...R)$ are generated arbitrarily. $R$ denotes the size of the population. The food sources contains the locations ($R_i$) generated for each feature vector point. This generation process is called as initialization process. To evaluate the best food source, the fitness value of the generated food sources is calculated using eqn. (8).

$$fitnessF = \min(\min(featurevectorpoints)) \quad (8)$$

After the calculation of fitness value, the iteration is set to 1. After that, the phase of employed bee is carried out.

**Step 2:- Employed Bee Phase**

In the employed bee phase, new population parameters are generated using the below equation,

$$V_{i,j} = f_{i,j} + \phi_{ij}\left(f_{i,j} - f_{k,j}\right) \quad (9)$$

Where, $k$ and $j$ is a random selected index, $\phi$ is randomly produced number in the range [-1, 1] and $V_{i,j}$ is the new value of the $j^{th}$ position. Then the fitness value is computed for every new generated population parameters of food sources. The best population parameter is selected from the computed fitness value of the population i.e. the population parameter, which has the highest fitness value by applying greedy selection process. The probability of the selected parameter is computed using the eqn. (10).

$$P_j = \frac{F_j}{\sum_{j=1}^{d} F_j} \quad (10)$$

where, $P_j$ is the probability of the $j^{th}$ parameter.

**Step 3:- Onlooker Bee Phase**

Number of onlooker bees is estimated after computing the probability of the selected parameter. Following, generate new solutions $V_{i,j}$ for the onlooker bees from the solutions $f_{i,j}$ based on the probability value $P_j$. Then the fitness function is calculated for the new solution. Subsequently apply the greedy selection process in order to select the best parameter.

**Step 4:- Scout Bee Phase**

Determine the Abandoned parameters for the scout bees. If any abandoned parameter is present, then replace that with the new parameters discovered by scouts using the followings procedure of PSO algorithm and evaluate the fitness value.

**Step 4(a):** 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 with the locations that are randomly generated in the population.

**Step 4(b):** Compute the fitness function for each particle $i$ in $d$ variables as in eqn. (8).

**Step 4(c):** Make comparison between the particle's fitness value, $x_{fitnes}$ and particle's $pbes$ fitness value, $p_{fitnes}$. If the current fitness value of particle is better than the particle's $pbes$ fitness value, then set the $pbes$ value into current position in the $d$ th dimension.

**Step 4(d):** Check out all of the particle's $pbes$ fitness value, $p_{fitnes}$ with value of $gbes$. If the current value, $pbes$ is better than the $gbes$ value means, then set the $gbes$ value into current particle's array index and value.

**Step 4(e):** Update the velocity and position of the particles given as in equations (11) and (12).

$$v_{id} = \omega \times v_{id} + \varphi_1 \times r_1 \times (pbest_{id} - x_{id}) \times pbest_{id} + \varphi_2 \times r_2 \times (gbest_{id} - x_{id}) \quad (11)$$

$$x_{id} = x_{id} + v_{id} \quad (12)$$

where, $i$ - Particle.

$\omega$ - Inertia weight.

$\varphi_1$ - Learning rates governing the particle towards to 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 4(f):** Repeat step 2, until a better fitness or maximum number of iterations are met.

The best parameters achieved so far are memorized. Then the iteration is incremented and the process is continued until the stopping criterion is reached. Finally, the optimized locations are discovered from the Hybrid ABC-PSO algorithms. The process involved in the Hybrid ABC-PSO for the chaff points optimization is illustrated in fig. 3.

After the selection of the optimized locations, the selected locations are converted into its corresponding feature vector points for utilizing as the new chaff points. The chaff points are represented as $C_l, i = 1,2,\ldots,n$ and the number of chaff points is $n$. Thus, the feature points obtained are:

(a) Extracted Face feature vector points $(f_l, l = 1,2,\ldots,n)$

(b) Extracted Ear feature vector points $(e_l, l = 1,2,\ldots,n)$

(c) New chaff points $(C_l, l = 1,2,\ldots,n)$

The New chaff points contain both face chaff points $(C_f)$ and ear chaff points $(C_e)$. These obtained feature sets are then utilized for the Fuzzy vault generation process.

*C. Fuzzy Vault Encoding Phase*

Fuzzy vault can be also attacked by hackers because of the poor polynomial reconstruction crisis, which is the drawback for the single polynomial that leads to in-securable biometric system. The usage of fuzzy vault with multiple polynomials is the best solution for providing higher security for the templates, which is also employed in the proposed work.

The fuzzy vault for the query image is encoded using multiple polynomials. The face features $(f_l)$ and ear features $(e_l)$ are extracted from the images and with the use of chaff points of face $(C_f)$ and ear $(C_e)$, the encoding phase is done.

The secret key $SK$ is randomly selected, which is represented as,

$$SK = \{S_0 \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4 \,||\, S_5 \,||\, S_6 \,||\, S_7\} \quad (13)$$

Then the secret key is split into two sub secret keys $SK_1, SK_2$ and the representation of these two sub secret keys is given below.

$$SK_1 = \{S_0 \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4\} \quad (14)$$

$$SK_2 = \{S_3 \,||\, S_4 \,||\, S_5 \,||\, S_6 \,||\, S_7\} \quad (15)$$

Then, these sub secret keys are subjected to Cyclic Redundancy Check 3-bit error code.

$$SK_1 = \{S_0 \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4\} \,||\, \{CRC3-bit\} \quad (16)$$

$$SK_2 = \{S_3 \,||\, S_4 \,||\, S_5 \,||\, S_6 \,||\, S_7\} \,||\, \{CRC3-bit\} \quad (17)$$

The corresponding polynomial for the CRC 3-bit is

$$p = x^3 + x + 1 \quad (18)$$

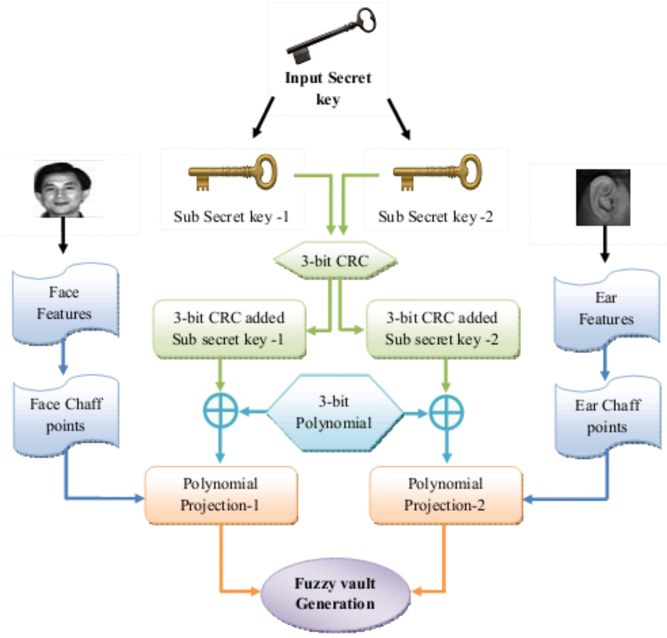


Fig. 4. Fuzzy vault encoding phase with multiple polynomials

Then the CRC applied sub secret keys are XOR-ed with the polynomial in eqn. (18) for getting the polynomial projections $p_1'$ and $p_2'$ and where, the degree of polynomial is 3.

$$p_1' = SK_1' \oplus p \qquad (19)$$

$$p_2' = SK_2' \oplus p \qquad (20)$$

After constructing the polynomial, the chaff points of face features $(C_f)$ and the chaff points of ear features $(C_e)$ are projected on to the polynomial projections $p_1'$ and $p_2'$. Thus the grouping of these polynomial projections and the new chaff points make fuzzy vault $FV$.

$$FV = \{C_f + C_e + p_1' + p_2'\} \qquad (21)$$

By the secret key points of multiple polynomials, the fuzzy fault is created in the above manner. The process of generating fuzzy vault in encoding phase is shown in the fig. 4.

*D. Fuzzy Vault Decoding Phase*

The query face and ear features $(Qf_l)$ and $(Qf_e)$ are compared in decoding phase with the Fuzzy vault features $(f_l)$ and $(f_e)$. The fuzzy vault $(FV)$ of $(f_l)$ and $(f_e)$ are re-constructed to get the original secret key via polynomial reconstruction. The decoding process of fuzzy vault with multiple polynomials is given in fig. 5.

Fuzzy vault of encoding comprises of four parts as in eqn. (21), which are: (a) Chaff points of face $(C_f)$ (b) Chaff points of ear $(C_e)$ (c) Face polynomial projection $(p_1')$ and (d) Ear polynomial projection $(p_2')$. The final two parts (c) and (d) are the required parts to find the secret key. Both the ear and face polynomial projections are XOR with the 3 bit polynomial to obtain $(SK_1')$ and $(SK_2')$. The 3-bit polynomial is same as in eqn. (18).

$$p_1' \oplus p = SK_1' \qquad (22)$$

$$p_2' \oplus p = SK_2' \qquad (23)$$

Both the resultant $(SK_1')$ and $(SK_2')$ concatenates with sub secret keys and CRC 3-bit. Here, the decoding of CRC 3-bit is formed. The sub secret keys are chosen from the first part of $(SK_1')$ and $(SK_2')$.

$$SK_1 = \{SK_1'\} \,||\, \{CRC3-bit\} \qquad (24)$$

$$SK_2 = \{SK_2'\} \,||\, \{CRC3-bit\} \qquad (25)$$

These two face and ear sub secret keys are:

$$SK_1 = \{S_0 \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4\} \quad (26)$$

$$SK_2 = \{S_3 \,||\, S_4 \,||\, S_5 \,||\, S_6 \,||\, S_7\} \quad (27)$$

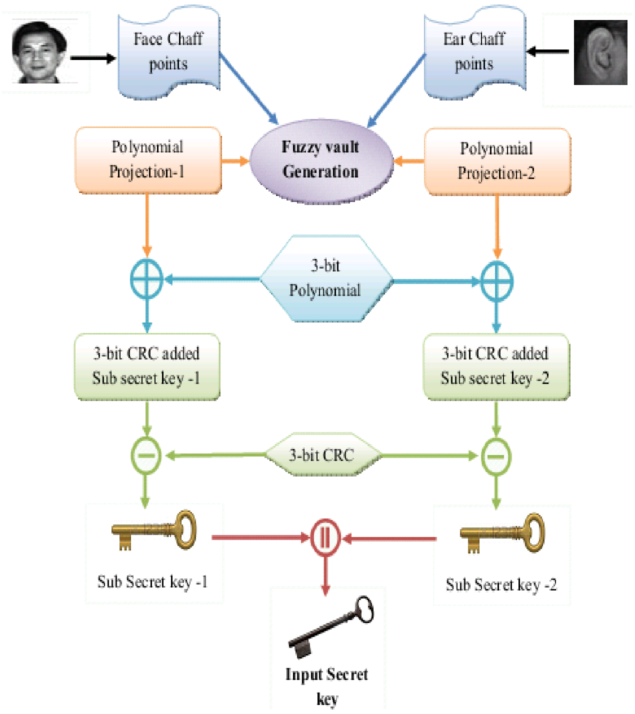


Fig. 5. Fuzzy vault decoding phase with multiple polynomials

Finally, these two face and ear sub secret keys $(SK_1)$ and $(SK_2)$ are concatenated and the original secret key is obtained as in the Fuzzy Vault encoding process.

$$\{SK_1\} \,||\, \{SK_2\} = SK \quad (28)$$

$$\{S_0 \,||\, S_1 \,||\, S_2 \,||\, S_3 \,||\, S_4 \,||\, S_5 \,||\, S_6 \,||\, S_7\} = SK \quad (29)$$

Thus, the fuzzy vault is generated with multiple polynomials, which provides high securable biometric system with multimodalities.

### E. *Authentication Phase*

A person is tested with the aid of his/her face and ear traits in order to recognize whether the particular person is correct or not. The pre-processing of face and ear modalities followed by feature extraction make a way to generate chaff points. The chaff points are optimized using Hybrid ABC-PSO algorithm and then these new optimized chaff points are helped to recognize a person. These obtained new chaff points of a test person are compared with the fuzzy vault database and then verified to find whether the chaff points are coordinated with the fuzzy vault or not. If it is coordinated, then the authentication is approved by producing the secret key to validate. Otherwise, the authentication is rejected.

Let the feature chaff points of input person be $C_i, i = 1,2,...,n$, which is compared to fuzzy vault in the database, $FV_i \; for 0 < i < N$. $C_i$ contains both face and ear feature chaff points. If all the feature chaff points 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 chaff points matches with the fuzzy vault from the database, then certain points in the fuzzy vault will be 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. The generation of the person is a second confirmation of the person and improves the template security.

## IV. Results and Discussion

The proposed new chaff point based multiple polynomial multi biometric cryptosystem with face and ear has processed effectively and the results with the performance evaluation can be evaluated MATLAB 7.12 using various images.

### A. *Description of Datasets*

Face and ear images are taken from the Yale face Database and IIT Delhi Ear Database for evaluating the proposed work, respectively.

*a) Yale Face Database:* Totally, 165 grayscale images of 15 persons are included with the GIF format of size 6.4 MB. The collected face images of persons are of from students, engineers, workers etc. The sample Yale face database images are shown in fig. 6.A.

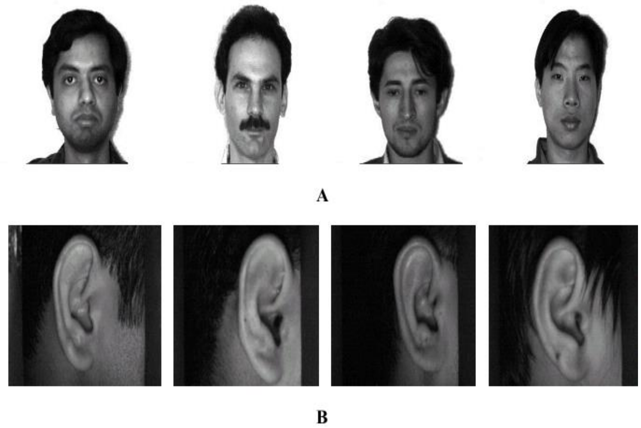


Fig. 6. Sample input images: A) Yale Face Database B) IIT Delhi Ear Database

*b) IIT Delhi Ear Database:* IIT Delhi Ear database contains the collected ear images from the students and staff of IIT Delhi, India, during Oct 2006 – Jun 2007. All these ear images are acquired from a distance (touch less) by means of an easy imaging setup and the imaging is performed in the indoor atmosphere. The database available at present is gathered from the 121 diverse subjects, each of them possessing at least three ear images. All the subjects in the database are aged between 14years 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 x 204 pixels and all these images are obtainable in jpeg format. In addition to the original images, the database also furnishes the mechanically adapted and cropped ear images of size 50 x 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.B shows the sample input ear images from IIT Delhi Ear database.

### *B. Experimental Results*

Feature Extraction is carried out using the proposed system. The first step of this phase is pre-processing, which is performed using a non-linear Median filter. Before the images are subjected to Median filter, all the face and ear images are cropped out. Thus, the input images get pre-processed and the noises and blurs acquired in these images are removed clearly. The result of the pre-processed images of Feature Extraction phase is given in fig. 7.

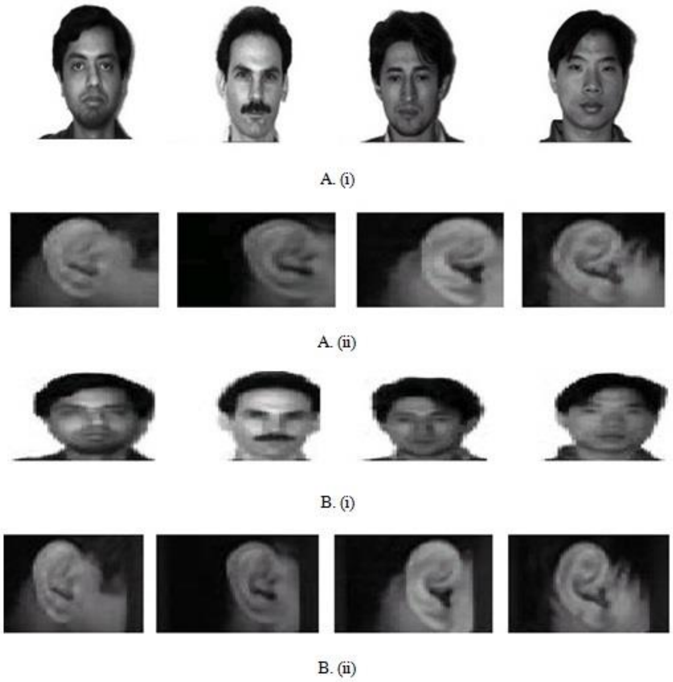


Fig. 7. Pre-processed images of Feature Extraction phase: 1. Face images 2. Ear images - (a) Cropped out images (b) Median filter applied images

The second step in the feature extraction phase is the extraction of shape features from both the face and ear images. The second step is processed with the aid of Modified Region Growing method. The experimental results of the extraction of shape features from both the face and ear are given in fig. 8.

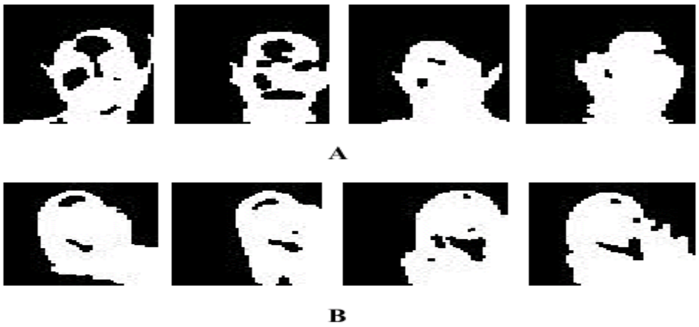


Fig. 8. Shape feature extraction: A) Face Images B) Ear images

Next step of Feature Extraction phase is the texture feature extraction of face and ear images. The texture feature is extracted using Local Gabor XOR Pattern. The output of texture feature extraction is not the images; but it gives feature values of texture results. The resultant texture feature values are tabulated in table 1 for each face and ear images. 4 of face and ear images are given as the sample input and these 8 of the images have 10 texture feature values on each.

Final step in feature extraction phase is the energy feature extraction using Local Principle Independent Component method. Each of 4 face image and 4 ear images gives 176 energy values, respectively. The sample output of 10 energy values for each images are shown in the following table 2.

New chaff points generation is the second phase of the proposed work using the Hybrid ABC-PSO algorithm. By this method, the additional random features of face and ear can be added with the whole features as one of the features. For both face and ear images, totally 50 chaff points are chosen, respectively. The results of chaff points are given in the table 3 with its 50 chaff points.

TABLE I. TEXTURE FEATURE EXTRACTION RESULTS OF BOTH FACE AND EAR IMAGES

| **Face Texture Feature Values** | | | | **Ear Texture Feature Values** | | | |
|---|---|---|---|---|---|---|---|
| Face-1 | Face-2 | Face-3 | Face-4 | Ear-1 | Ear-2 | Ear-3 | Ear-4 |
| 58 | 48 | 48 | 48 | 33 | 26 | 32 | 32 |
| 25 | 19 | 22 | 22 | 16 | 9 | 10 | 24 |
| 10 | 4 | 8 | 8 | 6 | 0 | 6 | 8 |
| 3 | 2 | 4 | 4 | 2 | 1 | 0 | 0 |
| 19 | 19 | 20 | 20 | 19 | 10 | 7 | 20 |
| 7 | 6 | 10 | 10 | 7 | 10 | 9 | 11 |
| 6 | 5 | 1 | 1 | 3 | 1 | 2 | 5 |
| 5 | 3 | 9 | 9 | 2 | 1 | 5 | 6 |
| 13 | 14 | 19 | 19 | 15 | 9 | 9 | 7 |
| 184 | 210 | 189 | 189 | 227 | 263 | 250 | 217 |

TABLE II. SAMPLE ENERGY FEATURE EXTRACTION RESULTS OF BOTH FACE AND EAR IMAGES

| **Face Energy Feature Values** | | | | **Ear Energy Feature Values** | | | |
|---|---|---|---|---|---|---|---|
| Face-1 | Face-2 | Face-3 | Face-4 | Ear-1 | Ear-2 | Ear-3 | Ear-4 |
| -1.36E-07 | 3.73E-09 | 2.17E-07 | -1.89E-07 | 5.59E-09 | 1.97E-08 | 1.66E-08 | -2.00E-07 |
| 3.91E-08 | -7.68E-09 | 1.00E-08 | 2.61E-08 | -9.78E-09 | 3.56E-08 | -8.15E-10 | -1.58E-08 |
| 1.57E-09 | 4.66E-10 | 1.85E-08 | -3.23E-08 | 1.69E-08 | 1.34E-08 | 1.68E-08 | 4.44E-08 |
| -3.60E-08 | -5.01E-09 | 2.52E-09 | -9.16E-09 | -1.30E-08 | 4.80E-10 | -1.12E-08 | 1.36E-08 |
| 1.60E-08 | 4.11E-08 | 1.62E-09 | -1.81E-09 | -2.64E-08 | 6.78E-10 | -1.28E-08 | -1.15E-09 |
| -3.98E-09 | 3.73E-09 | -6.18E-09 | 1.64E-08 | -7.80E-10 | 3.46E-09 | 8.32E-09 | 1.76E-08 |
| -2.20E-08 | -5.53E-09 | 3.00E-09 | -1.64E-08 | -4.24E-09 | -2.82E-09 | -1.16E-09 | -2.86E-09 |
| -7.20E-09 | -5.82E-10 | -7.04E-09 | -3.79E-08 | -1.49E-08 | -2.91E-11 | 1.25E-08 | 6.86E-09 |
| 8.33E-09 | -8.85E-09 | -3.28E-08 | 1.82E-08 | 2.33E-09 | 1.07E-09 | 2.42E-09 | 6.91E-10 |
| 1.09E-08 | 7.45E-09 | 1.13E-08 | 7.93E-09 | 4.61E-09 | 1.69E-09 | -6.52E-09 | 9.75E-09 |

TABLE III. NEW CHAFF POINTS OF BOTH FACE AND EAR IMAGE

| **FACE CHAFF POINTS** | | **EAR CHAFF POINTS** | |
|---|---|---|---|
| 5.07E-09 | 220839451.6 | -3.48E-08 | -5.54E-08 |
| -6.86E-09 | 1.36E-08 | 23 | -9.80E-10 |
| 220839451.6 | 1.16E-10 | 1.75E-08 | 1.70E-08 |
| 1.46E-11 | -2.68E-09 | -6.29E-09 | 3.62E-09 |
| -1.48E-08 | -1.23E-09 | -3.08E-10 | 1.80E-09 |
| -2.22E-09 | -1.24E-08 | 2.76E-08 | -1.97E-08 |
| 3.27E-09 | 220839451.6 | -4.67E-09 | -5.13E-09 |
| 220839451.6 | -2.33E-09 | -1.06E-08 | 7.32E-10 |
| -7.86E-09 | -1.92E-09 | -5.13E-09 | 1.04E-08 |

| | | | |
|---|---|---|---|
| -1.62E-08 | 220839451.6 | -3.08E-10 | 24 |
| 4.23E-09 | 2.82E-09 | 8 | 4.64E-10 |
| -1.59E-08 | -3.08E-08 | 6.44E-09 | 2.94E-09 |
| -6.13E-09 | 220839451.6 | 3.47E-09 | 2.11E-09 |
| -1.41E-08 | -7.00E-09 | -6.15E-08 | 9.03E-09 |
| 220839451.6 | 166 | 4.25E-09 | 5.82E-09 |
| -9.39E-09 | -1.17E-08 | -1.63E-08 | 1.66E-09 |
| 220839451.6 | -3.31E-09 | 11 | 1.18E-08 |
| -2.71E-09 | 220839451.6 | -6.47E-08 | -9.46E-09 |
| -7.24E-09 | -2.73E-09 | 9.24E-09 | -4.97E-09 |
| 220839451.6 | -1.40E-08 | -6.10E-09 | 1.59E-09 |
| 220839451.6 | 220839451.6 | 1.19E-08 | 7.48E-10 |
| -4.19E-10 | -2.72E-10 | 1.49E-09 | 2.35E-08 |
| -1.03E-08 | -2.26E-09 | 1.99E-09 | 28 |
| 1.72E-09 | 4.49E-09 | -5.51E-09 | 52 |
| 6.22E-10 | -5.33E-10 | 1.38E-08 | -1.58E-08 |

TABLE IV. EVALUATION METRICS WITH FORMULA

| Evaluation metrics | Formula |
|---|---|
| FMR | $FMR = \frac{Number of non-authorized inputs which are falsely recogniz}{Total number of inputs}$ |
| FNMR | $FNMR = \frac{Number of authorized inputs which are falsely not recogniz}{Total number of inputs}$ |
| GAR | $GAR = 1 - FNM$ |
| DC | $DC = \frac{2\|A \cap B\|}{\|A\| + \|B\|}$ |
| JC | $JC = \frac{\|A \cap B\|}{\|A \cup B\|}$ |
| In both DC and JC, A refers the target set of accurate recognized images and B refers the set of accurate recognized images obtained by the proposed work. | |

### C. *Evaluation metrics*

The Evaluation metrics are used for evaluating the proposed new chaff point based multiple polynomial of multimodal biometric authentication system based on face and ear images. False Matching Rate (FMR), False Non-Matching Rate (FRR), Genuine Acceptance Rate (GAR), Dice Co-efficient (DC) and Jaccard Co-efficient (JC) are the five metrics are utilized in the proposed system for analyzing the performance and it is shown in the table 4.

### D. *Performance Analysis of the proposed work*

The performance for the proposed multimodal biometric system based on face and ear modalities with different secret key sizes are attained, which are evaluated using above evaluation metrics. The results can be taken by applying noise and not by applying noise to the face and ear images with various secret key sizes. The secret key sizes are varied as 1, 2, 3 & 4.

TABLE V. PERFORMANCE OF PROPOSED MULTIMODAL BIOMETRIC SYSTEM USING FACE AND EAR WITH NOISES FOR VARIOUS SECRET KEY SIZES

| Secret Key Size | FMR (in %) | FNMR (in %) | GAR (in %) | DC (in %) | JC (in %) |
|---|---|---|---|---|---|
| 1 | 20 | 20 | 80 | 80 | 80 |
| 2 | 20 | 20 | 80 | 80 | 80 |
| 3 | 20 | 20 | 80 | 80 | 80 |
| 4 | 20 | 20 | 80 | 80 | 80 |

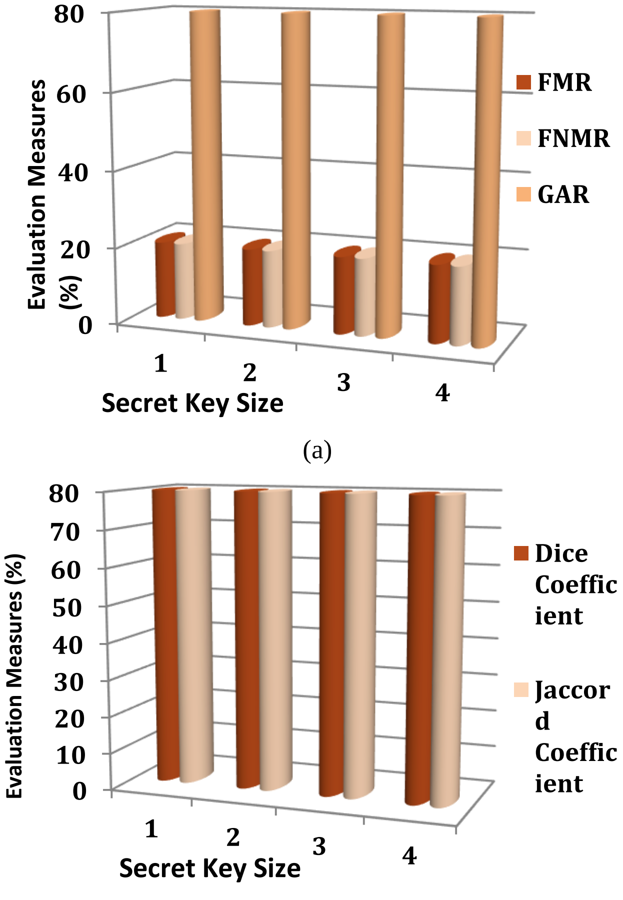
TABLE VI. PERFORMANCE OF PROPOSED MULTIMODAL BIOMETRIC SYSTEM USING FACE AND EAR MODALITIES WITHOUT NOISES FOR DIFFERENT SECRET KEY SIZES

| Secret Key Size | FMR (in %) | FNMR (in %) | GAR (in %) | DC (in %) | JC (in %) |
|---|---|---|---|---|---|
| 1 | 0 | 10 | 90 | 95 | 95 |
| 2 | 0 | 10 | 90 | 95 | 95 |
| 3 | 0 | 10 | 90 | 95 | 95 |
| 4 | 0 | 10 | 90 | 95 | 95 |

The performance analysis results of the proposed system with noises by changing the secret key size in table 5 are also shown in the graphical representation of fig. 9.

White Gaussian noises are added to face and ear images and the proposed method is applied on the noise added images to tabulate the measure values in table 5 and to plot its corresponding representation. From the performance results using the modalities face and ear with the addition of noises, it can be understood that the accuracy result of multiple polynomial based multimodal biometric system does not give up significantly high values but only average high values for the recognition of the correct person. FMR, FNMR and GAR values are evaluated with the varying secret key sizes of 1, 2, 3 and 4.

The FMR and FNMR values are low (20%) for the proposed system with White Gaussian noises for all the varying size of secret keys. Lesser values in FMR and FNMR only can boost the recognition accuracy with high GAR values, because, the incorrect recognition is nominal and correct recognition of person is considerable significantly in the proposed work. And also, the DC and JC values are at standard high values of 80%, respectively, with the addition of noises. However, the results of recognition accuracy also offer better-quality values for the proposed work with noise. The following table 6 shows the results of multiple polynomial based multimodal biometric system without any noises. The analysis output of the proposed system without noises and by changing the secret key sizes are also shown in fig. 10 as a graphical illustration.

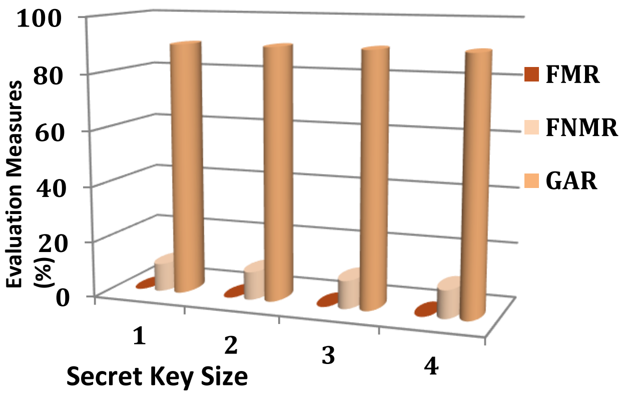


(a)

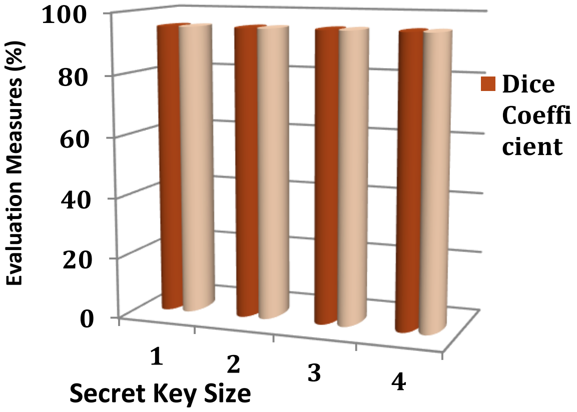
(b)

Fig. 9. Performance analysis for the proposed system using face and ear with noises for various secret key sizes- (a)FMR, FNMR and GAR (b) DC and JC

The results for the proposed systems can be evaluated without adding the White Gaussian Noises for the tabular values of table 6. The performance is analyzed only by varying the size of secret keys as 1, 2, 3 & 4. In compared with the output of table 5, the proposed system without adding noises in table 6 facilitates appreciable results for the recognition of accurate person with the modalities face and ear. It gives very good results for both FMR and FNMR metrics, which gains only 0% values FMR and 10% of FNMR for all the key sizes. But for the noise added system, FMR and FNMR attains 20% of values, which is 20% higher value for FMR and 10% higher value for FNMR. 90% of GAR values are acquired without noises, which is also 10% increased value, if the system is added with noise. But, the proposed system without noises provides very high value of DC and JC metrics, which gives 95% better recognition results. But the addition of noises gives only 80% of DC and JC values, which is 15% lower than without adding noises. Furthermore, it can be monitored that the values for FMR, FNMR, GAR, DC and JC values are identical for all the sizes of secret key, irrespective of whether the images are with noise or without. Images without the noises gives better quality results for the recognition of a correct person. Nevertheless, the results of recognition accuracy furnish extremely superior value for the proposed work without the addition of White Gaussian noises.



(a)



(b)

Fig. 10. Performance output for the proposed work using face and ear without noises for different secret key sizes – (a) FMR, FNMR and GAR (b) DC and JC

*E. Compaarison Results*

According to the selection of chaff points, the proposed system can be proved that it is highly improved work. It is compared with the existing algorithms such as

(1) Without ABC-PSO
(2) With only PSO
(3) With ABC-PSO (proposed system).

Thus, the recognition comparison results of FMR, FNMR, GAR, DC and JC without adding Gaussian noises with other works are given in the following table 7. The graph for the comparison results with other works are plotted in fig. 11 as a graphical structure.

TABLE VII. COMPARISON RESULTS OF THE PROPOSED WORK WITH OTHER WORKS

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|

| Secret key . size<br>Evaluation Metrics | Without ABC-PSO | With only PSO | Proposed (With ABC-PSO) | Without ABC-PSO | With only PSO | Proposed (With ABC-PSO) | Without ABC-PSO | With only PSO | Proposed (With ABC-PSO) | Without ABC-PSO | With only PSO | Proposed (With ABC-PSO) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FMR (in %) | 20 | 10 | 0 | 20 | 10 | 0 | 20 | 10 | 0 | 20 | 10 | 0 |
| FNMR (in %) | 30 | 10 | 10 | 30 | 10 | 10 | 30 | 10 | 10 | 30 | 10 | 10 |
| GAR (in %) | 80 | 90 | 90 | 80 | 90 | 90 | 80 | 90 | 90 | 80 | 90 | 90 |
| DC (in %) | 75 | 90 | 95 | 75 | 90 | 95 | 75 | 90 | 95 | 75 | 90 | 95 |
| JC (in %) | 75 | 90 | 95 | 75 | 90 | 95 | 75 | 90 | 95 | 75 | 90 | 95 |

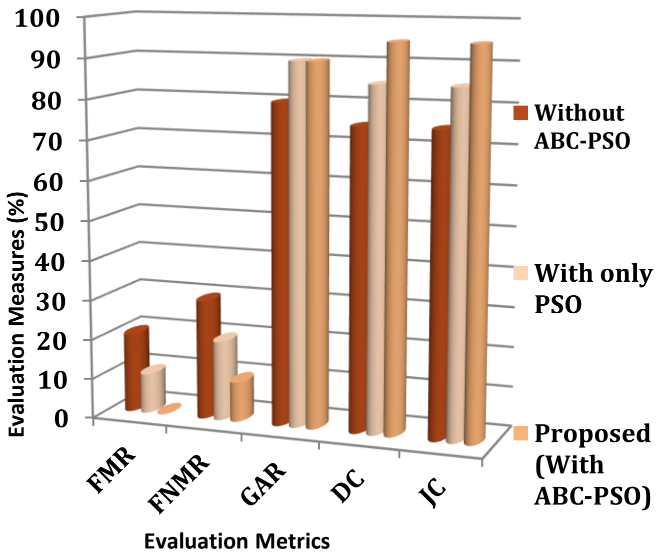


Fig. 11. Comparison graph for the recognition result between the proposed work with PSO and the proposed work without PSO without noise

The comparison results of tabular values and graphs shows that the ABC-PSO method put forwards excellent recognition accuracy with GAR of 90% value for all the secret key sizes, respectively. But, the method without ABC-PSO and with only PSO gives 80% and 90% of GAR values for all the secret key sizes, respectively. Both FMR and FNMR values for the proposed work with ABC-PSO are 0% & 10% and also for without ABC-PSO and with only PSO are 20% & 30%; and 10% & 20%, respectively. The low values in FMR and FNMR suggest for raising GAR results by providing privileged recognition accuracy results. Both DC and JC values with ABC-PSO are 95%; for without ABC-PSO and with only PSO are 75% and 85%, respectively, with every secret key size variation. Taken as a whole, the proposed system with ABC-PSO yields precise results of recognition accuracy, because the ABC-PSO offers valuable optimization results by selecting exact distances from the particular range of locations foremost to catch superior recognition rate. In addition to that, for all the comparison results of evaluation metrics are not getting changed, when the secret key size gets changed. Hence, this research shows that the multimodal face and ear biometric system facilitates very precise recognition accuracy with the use of new chaff point's generation and multiple polynomials.

## II. CONCLUSION

A Hybrid ABC-PSO algorithm was introduced in the proposed system for the generation of chaff points. This algorithm is helpful for the selection of best feature vector points from the extracted features by preferring optimal distance ranges, which increased the convergence speed and the search space location was also controlled to limited space. Multiple polynomials were combined with encoding and decoding the features using fuzzy vault, which increased the template security by providing best polynomial construction. Thus the proposed system could be very securable one and also could be recognized correct persons. White Gaussian noises to the images and also without noises were evaluated with the evaluation metrics FMR, FNMR, GAR, DC and JC. For the noise addition, GAR, DC and JC yielded 80% of values, respectively. But, without noises have achieved 90% of GAR and 95% of DC and JC values, which clearly tells that the proposed system recognize the persons in a superior manner with very low error rates. Additionally, Hybrid ABC-PSO was also compared the work without ABC-PSO and only with PSO. The comparison results of Hybrid ABC-PSO have yielded very accurate results of recognition than the other methods. This novel chaff point generation and multiple polynomial based multimodal biometric systems with Fuzzy vault avoid hacking of biometric data by an attacker. From all the results, proposed system could be able to confirm that the multimodal biometric system with ABC-PSO based new chaff points and multiple polynomials gives well improved recognition results for a person.

## References

1. Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain, “A Hybrid Biometric Cryptosystem For Securing Fingerprint Minutiae Templates, ELSEVIER Journal of Pattern Recognition Letters, Vol. 31, pp. 733-741, 2010.
2. Abhishek Nagar, Karthik Nandakumar, and Anil K.Jain, “Multibiometric Cryptosystems Based on Feature-Level Fusion”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 255-268, February 2012.
3. Banharnsakun A, Achalakul. T, and Sirinaovakul B,“The best-sofarselection in artificial bee colony algorithm,” ELSEVIER Journal of Applied Soft Computing, Vol. 11, pp. 2888–2901, 2011.
4. Brendan F. Klare, Mark J. Burge,Joshua C. Klontz,Richard W. Vorder Bruegge, and Anil K. Jain, "Face Recognition Performance: Role of Demographic Information", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, pp. 1789-1801, December 2012.
5. Dacheng Xu and Xiaotao Wang, "A Scheme for Cancelable Fingerprint Fuzzy Vault Based on Chaotic Sequence", In Proceedings of IEEE International Conference on Mechatronics and Automation, pp. 329-332, August, 2010.
6. Daesung Moon, Woo-Yong Choi, Kiyoung Moon and Yongwha Chung , "Fuzzy Fingerprint Vault using Multiple Polynomials", In Proceedings of IEE 13th International Symposium on Consumer Electronics, pp. 290-293, May 2009.
7. Dervis Karaboga and Bahriye Akay, "A comparative study of Artificial Bee Colony algorithm", Journal Of Applied Mathematics and Computation, Vol. 214, pp. 108–132, 2009.
8. D. Yaman, F. I. Eyiokur, and H. K. Ekenel, “Multimodal age and gender classification using ear and profile face images,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, June 2019.
9. Fahd M. A. Mohsen, Mohiy M. Hadhoud, and Khalid Amin, "A new Optimization-Based Image Segmentation method By Particle Swarm Optimization", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, pp. 10-18, 2010.
10. Gandhimathi A. and Radhamani G., “New Chaff Point’s Based Fuzzy Vault for Multimodal Biometric Cryptosystem using PSO”, Journal of King Saud University – Computer and Information Sciences, Vol. 28,No. 4, pp. 381-394, 2016.
11. Karthik Nandakumar and Anil K. Jain, "Multibiometric Template Security Using Fuzzy Vault", In Proceedings of IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems, pp. 1-6, 2008.
12. Latha Lakshmanan, "Efficient person authentication based on multi-level fusion of ear scores", Journal of IET Biometrics, Vol. 2, No. 3, pp. 97-106, 2013.
13. Lifang Wu, Peng Xiao, Songlong Yuan, Siyuan Jiang and Chang Wen Chen, "A Fuzzy Vault Scheme for Ordered Biometrics", Journal of Communications, Vol. 6, No. 9, pp. 682-690, December 2011.
14. Meenakshi V.S. and Padmavathi G., "Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault", World Academy of Science, Engineering and Technology, Vol. 32, pp. 312-320, 2009.
15. Sahil Gupta and Manvjeet Kaur, "Meliorating Fingerprint Fuzzy Vault using Multiple Polynomials", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 7, July 2013.
16. S.Itani, S.Kita and Y.Kajikawa, "Multimodal Personal Ear Authentication Using Acoustic Ear Feature for Smartphone Security," IEEE Transactions on Consumer Electronics, vol. 68, no.1,pp.77-84,Feb.2022, doi: 10.1109/TCE.2021.3137474.
17. Sowkarthika S. and Radha N., "Securing Iris Templates using Double Encryption Method", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 11, pp. 259-264, November 2012.
18. Steven Cadavid, Mohammad H. Mahoor and Mohamed Abdel-Mottaleb, "Multi-modal Biometric Modeling and Recognition of the Human Face and Ear", In Proceedings of IEEE International Workshop On Safety, Security & Rescue Robotics, pp. 1-6, November 2009.
19. Thi Hanh Nguyen, Yi Wang, Yajun Ha and Renfa Li, "Improved chaff point generation for vault scheme in bio-cryptosystems", Journal of IET biometrics, Vol. 2, No. 2, pp. 48-55, 2013.
20. Yichao Ma, Zengxi Huang, Xiaoming Wang, and Kai Huang, “An Overview of Multimodal Biometrics Using the Face and Ear”, Mathematical Problems in Engineering Volume 2020, pp.1-17.
21. Yi C. Feng, Pong C. Yuen, and Anil K. Jain, “A Hybrid Approach for Generating Secure and Discriminating Face Template”, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, pp. 103-117, March 2010.