Adaptive Management of Multimodal Biometrics Fusion Using Ant Colony Optimization

Amioy Kumar, Ajay Kumar
Corresponding author email: csajaykr@comp.polyu.edu.hk; Ph: 852-27667254

Abstract: This paper presents a new approach for the adaptive management of multimodal biometrics to meet a wide range of application dependent adaptive security requirements. In this work, ant colony optimization (ACO) is employed for the selection of key parameters like decision threshold and fusion rule, to ensure the optimal performance in meeting varying security requirements during the deployment of multimodal biometrics systems. *Particle swarm optimization (PSO) has been widely utilized for the optimal selection of these parameters in the earlier attempts in the literature [3]-[4]. However, in PSO these parameters are computed in continuous domain while they are assumed to be better represented as discrete variables [4]. This paper therefore proposes the use of ACO, in which discrete biometric verification parameters are computed to ensure the optimal performance from the multimodal biometrics system.* The proposed ACO based framework is also extended to the pattern classification approach where fuzzy binary decision tree (FBDT) is utilized for two-class biometrics verification. The experimental results are presented on true multimodal systems from various publicly available databases; IITD databases of palmprint and iris, XM2VTS database of from speech and faces, and the NIST BSSR1 databases of faces and fingerprint images. Our experimental results presented in this paper suggest that (i) ACO based approach is capable of operating on significantly small error rates in comparison to the widely employed PSO for automated selection of biometrics fusion rules/parameters, (ii) the score-level fusion yields better performance with lower error rate in comparison to the decision level fusion, and finally (iii) the FBDT based classification approach delivers considerably superior performance for the adaptive biometrics verification.

Index Terms: Adaptive biometric verification, ACO, PSO, FBDT, Score-level fusion.

I. INTRODUCTION

Automated biometrics systems are increasingly replacing conventional methods of human identification especially those based on the use of passwords or the smart cards. The biometrics systems can not only ensure higher level of security for online and commercial applications but also offer higher user convenience during the personal authentication for restricted or secured access [1]. The security offered by these biometrics systems can be further enhanced by simultaneously incorporating multiple biometric modalities during the user authentication. Such multimodal biometrics systems can also enhance integrity of biometrics systems as it's extremely difficult for an impostor to simultaneously authenticate using multiple fraudulent biometrics samples. A general multibiometrics system [2] can operate on different modes of fusion like fusing multiple traits, multiple samples, multiple classifiers, and multiple features for the improvement of the performance. However, the effectiveness of a multimodal system is largely depends on the selection of the *fusion parameters*, like weights for the individual biometric matchers, decision thresholds or the score-level fusion rules, which can ensure desirable or the optimal performance under varying security requirements [3]. Inappropriate selection of any of these parameters can degrade the performance or actually reduce the advantages from respective multimodal system**.**

A. Which Module of the System can be Adaptive?

A biometric verification requires 1:1 match as its intended to verify the claimed user identity by matching the presented biometric pattern with the enrolled biometric patterns. Such verification problem can be formulated as follows: let Q be a feature vector extracted from the query biometric image and E be the enrolled biometric feature vector stored for the claimed identity C. The task is to determine if the pair (C, Q) belongs to class G which is to accept (genuine) the user or class I which is to reject (imposter) the user. Let $S(E, Q)$ denote the distance matching

score computed by matching E and Q and T denotes the decision threshold determined at learning stage [1]. Then the verification is defined as:

$$(C,Q) \in \begin{cases} G, \ if \ \mathrm{S}(Q,E) \le T \\ I, \ Otherwise \end{cases} \tag{1}$$

It can be observed from above equation that one of the important parameters of the accurate biometric verification is the decision threshold T. *Prior work in the literature has presented promising attempts on such adaptive multimodal systems [3]-[4] with decision-level fusion in [3] and score-level fusion in [4]. However, as also argued in [4], dynamic score-level fusion is expected to offer superior accuracy as compared to the decision-level fusion approach. Therefore we have also preferred to focus our investigation on the score level fusion in this work.* Let Q_1, Q_2, …, Q_b be the b number of query biometric features extracted from the input user. Let E_1, E_2, …, E_b be the biometric features of the claimed identity c from the enrolled users. Let $S_1(E_1,Q_1)$, $S_2(E_2,Q_2)$, …, and $S_b(E_b,Q_b)$ be the matching score computed from b biometric matchers by comparing the query biometric features with the enrolled biometric features [1] [2]. In the score-level fusion, the matching scores are combined using a score-level fusion rule to generate the final match score S as in the following equation:

$$S(E,Q) = w_1 \times S_1(C_1,Q_1) + w_2 \times S_2(C_2,Q_2) + \ldots\ldots w_b \times S_b(C_b,Q_b) \tag{2}$$

Here, w_1, w_2, …, w_b are the weights corresponding to the b biometric matchers and S_1, S_2, …. S_b are respective score-level fusion rules employed to compute the consolidated match score.

It can be observed from Equations (1) and (2) that a typical multimodal system requires the verification parameters such as: the weights to the biometric matchers, a fusion rule for the integration of matching scores, and the decision threshold T for the final accept and reject decision. The selection of these verification parameters depends upon the expected security requirements which can be expressed in terms of the two error rates: False Acceptance Rate

(FAR) and False Rejection Rate (FRR) [1]-[2]. The FAR represents the rate at which imposters are accepted as the genuine users while FRR represents the rate at which the genuine users are rejected or considered as the imposters by the system. Both of these error rates are complementary to each other and in the real life scenario it is not possible to achieve very low values simultaneously for both of them [1]-[2]. Whenever the decision threshold is adjusted to achieve a lower value of one of the error rates; the other increases correspondingly. The choice of acceptable error rates is essentially application dependent. For example, the high security applications like access to secured buildings or to the bank accounts require the lowest possible FAR (close to zero) but a permissible value of FRR to prevent false authentication (imposter) whereas the low security applications (like public transport or classroom access) can be managed with somewhat high FAR but FRR must be stringent, *i.e.* as low as possible.

The homeland security department has made a detailed description of such a multi-level security requirement concerning the forensic, civilian and high security applications within their color-coded terrorism threats. However, most of the multimodal systems detailed in the literature [5]-[7], [8]-[9] offer the fixed security with a fixed number of verification parameters for the desired level of accuracy. Therefore, a multimodal system should be designed by considering the conflicting requirements of the varying levels of security [10]. Since different level of security may be expected from the same multimodal system, the necessity is to develop an adaptive multimodal system which can adaptively tune the fusion parameters according to the security requirement. This paper therefore investigates an adaptive multimodal biometric system using evolutionary computational technique (ACO) to select the fusion rules/parameters for varying security levels. The advantage of the evolutionary computations lies in their flexibility, easy-to-follow, and their robustness in responding to changing circumstances. Furthermore, majority of the evolutionary techniques provide a global solution which may not be the case with the

optimization techniques which often generates the local optima. Evolutionary techniques can be applied to those real world problems for which the heuristic algorithms can lead to unsatisfactory results. Therefore the use of the evolutionary techniques is gaining immense popularity, particularly for the real life problems. This paper proposes ACO for selecting the fusion parameters in a system to meet varying security levels.

The rest of the paper is organized as follows: The prior works on the adaptive management of multimodal biometrics with our proposed work are summarized in Section *II*. The framework for the adaptive multimodal fusion is discussed in Section *III,* where the ACO algorithm is also presented. The results of application the proposed multimodal fusion find place in Section I*V*. Finally, the discussion and conclusions are given in Section *VI*.

II. PRIOR WORK AND MOTIVATION

The multimodal fusion approach has received a great deal of attention in the recent years and as a consequence different fusion strategies have been evolved [5-7], [8]-[9]. However, most of these techniques operate with the fixed decision threshold and do not provide a systematic way to vary the level of security. The study of the adaptive management with varying security levels in which the fusion parameters are selected using some evolutionary techniques is relatively new and of particular interest to the present work.

A. Related Prior Work

Kittler *et al*. [5] are probably among the first to explore the significance of multimodal biometrics fusion by employing several fixed fusion rules. Frischholz *et al*. [6] present their multimodal system, referred to as BioID, by using different decision strategies which offer multiple levels of security. However, their system can't vary the levels of security and requires an administrator for manually selecting the fusion parameters for the desired level of accuracy. Likelihood of the matching match scores is used in [7] for the dynamic selection of biometric

matchers. Their work on multimodal system is very interesting and it provides high accuracy. But, their experimental results show the performance of only two cases out of the four cases considered. Another very promising work on combining the verification decisions in a multi-vendor environment is by Beattie *et al*. [11]. By employing the decision level fusion rule, they have resolved the building access problem by providing the access based on the different zones. In another interesting study, a dynamic management scheme for the selection of fusion rules is proposed by Vatsa *et al*. [12]. They have designed a sequential fusion technique using the likelihood ratio test statistics in combination with the support vector machine (SVM) to compute the errors in the classification system. Their approach has been quite successful in dynamically unifying the classifiers and the fusion schemes to optimize both verification accuracy and computational cost. In a very recent attempt, adaptive representations of random patches are utilized by Mery and Bowyer [21] for the recognition of facial attributes. They build an adaptive dictionary of random patches extracted from representative face images of each class. This dictionary is further used for classification of test patches using sparse representation and classification methodology.

The use of evolutionary computation in biometrics verification has also been investigated in literature. Rabab *et al*. proposed a novel feature selection algorithm based on PSO for face recognition [14]. Konrad *et al*. utilized genetic algorithm for computing JPEG quantization tables for compressing iris polar images in iris recognition [15]. Their system has shown to outperform JPEG's standard quantization matrix. Reference [16] described a genetic type II feature extraction (referred as Genetic & Evolutionary Feature Extraction) approach for optimizing the feature sets returned by local binary pattern features for the periocular biometric identification. Kanan and Faez [17] utilize ACO to propose an improved feature selection method for the face

recognition applications. Nemati and Basiri [18] investigated dimensionality optimization by selecting relevant features using ACO for test-independent speaker verification.

An adaptive multimodal biometric management system using the decision level multi-sensor fusion is proposed in [3]. Their framework was probably the first effort to successfully demonstrate the selection of optimal decision parameters to meet the desired level of accuracy. Authors have considered all the possible combinations of binary decision rules on the participating sensors to adaptively select the optimal one using PSO. Their algorithm achieves a tradeoff between the two error rates by varying the cost of errors and selecting the appropriate fusion rules to combine the biometric modalities in the multi biometric system. However, their experimental evaluation is largely based on the simulated data. Further, this approach gives rise to a large number of fusion rules, 2^{2^N} for N sensors and the computation complexity gets unwieldy with the increase in the number of sensors, *i.e.* for three sensors, 256 fusion rules. The above approach in [4] is yet another advancement of adaptive fusion techniques to meet dynamic security requirements and is probably the first work that successfully demonstrates the feasibility of such deployments using real biometric data. Specifically, this work offers score-level combination by adaptive (or automated) selection from four rules, *i.e.* sum, product (linear), exponential-sum, and Tanh (non-linear) which are shown to be adequate for the desired accuracy in a typical multimodal system. Here, the fusion parameters are found using PSO. The performance using these rules demonstrated to be better than that reported in [3]. Authors performed a variety of experiments to reveal that the score-level fusion is more consistent and stable than the decision level fusion.

B. Key Motivation

The prior work on the adaptive multimodal fusion either uses decision level fusion [3] or the score fusion [4]. The superiority of score level fusion over the decision level fusion in reducing

the overall error rates (FAR/FRR) in the multimodal system has been demonstrated in [4]. The work in this paper is motivated from the following insights:

1. Both the approaches in [3]-[4] use PSO for the selection of fusion parameters. The PSO algorithm has its own limitations like ending up in the local minimum that often leads to the premature convergence [19]. In addition, as argued in [4], there exist optimization problems where particles are better represented by the discrete variables. PSO is defined for the continuous domain and the use of Sigmoid function for the binary PSO in [3]-[4] is a discrete variant of PSO which approximate the information on the velocity and the position updates. *Here, the use of a discrete domain evolutionary technique is certainly advantageous in place of discrete variants of PSO for the approximation of the continuous domain representation which undoubtedly causes a loss of information. Hence, there is strong motivation or desire to investigate discrete evolutionary technique in the adaptive multimodal approach provided in [3] and [4]*.
2. Biometrics verification can also be implemented using pattern classification approaches and existing work in the literature has shown interesting attempts for the biometrics verification using pattern classification approaches [20]-[27]. Information fusion using DT and involving fingerprint, hand geometry, and face biometrics is explored in [20]. The significant feature selection and fusion of palmprint and hand shape biometrics employed DT in [21] where Naïve Bayes, *k-NN* (k-nearest neighbor), SVM, FNN (feed forward neural network), and DT are compared. Another interesting effort on multi-biometrics is presented on [22] which compares *k-NN,* DT, and logistic regression during the fusion of face and voice modalities. A fuzzy binary decision tree based approach is presented in [23]-[25] for biometric verification. An ensemble of decision tree based classifiers is presented in [26]-[27] for statistical classification. It is shown that, an

ensemble of decision results in higher accuracy over support vector machine [27]. *However, most of the available works [20]-[25] do not provide any mechanism to adapt varying security applications and they operate on the fixed classification strategies.*

C. Our Work

The contributions from this paper are listed below:

1. The main contribution of this paper is to investigate ACO for the optimal selection of the verification parameters required for the adaptive multimodal biometrics fusion. ACO is well defined for the discrete domain requirements, the probabilistic approach of ACO is easy to implement, and is least likely to suffer from the problem of the local minimum as compared to PSO. The movement of an ant depends on the amount of pheromone deposited on the path and the higher concentration of pheromone on a path drives the ants to seek that path [28]. However, the ACO algorithm does not provide the status of a path in terms of its local or global positions as PSO. Hence there is a need to introduce the update mechanisms, so that the local and global solutions can be identified together and the resulting ACO will have the provisions of local and global updates. In this work the idea of global and local updates is borrowed from PSO and utilized for updating the probabilities for selecting each path. The probabilities of each path are constrained to lie between the lower and the upper values.
2. Another important contribution of this paper is the *implementation of the ACO-framework based adaptive biometric verification using predictive model of pattern classification approach in the fuzzy domain.* As detailed in *Section II-B*, the predictive model in [20]-[22] may not be able to learn different decision threshold as per variations in security level requirements. These models can only train to learn the fixed parameters to achieve fixed security requirement. *In this work, we propose ACO-framework for*

adaptive biometric verification using fuzzy binary decision tree (FBDT) which can adapt to various security applications by computing the verification parameters using ACO (detailed in Section *III-C*). The implementation of FBDT is the same as in [25]-[27].

3. Thirdly, this paper presents following noteworthy comparative analysis relevant to the adaptive biometric verification literature:
    a. In order to judge its reliability in the selection of the verification parameters, a comparison is made between the proposed ACO framework for adaptive multimodal biometrics verification and the PSO based approach in [4].
    b. A comparison is presented between ACO based adaptive biometric frameworks using decision threshold (as discussed in the first point above) and predictive classification model using FBDT (discussed in the second point above).
    c. A comparison is also presented between ACO based adaptive decision-level fusion scheme (as proposed in [3] using PSO) and ACO based adaptive score-level fusion (presented in this work).
4. Finally, in this paper, we provide rigorous experimentation on various publicly available multimodal biometric databases. The experiments are carried out on two different sets of multimodal databases: multimodal database of the matching scores computed from palmprint [29] and iris [30] from IITD databases, matching scores of fingerprint and face images from true multimodal database made publicly available from NIST BSSR1 [31], and also the publicly available XM2VTS databases [32].

The block diagram of the proposed ACO based multimodal biometric verification system is shown in Fig. 1. The inputs to the ACO are: the security level (See Section II-*A*), matching scores from the individual biometric modalities, and the fusion rules (Section II-*A*). The output is the verification parameters of the multimodal system: weights for the biometric matchers, one

score-level fusion rule for integration of the matching scores, decision threshold for final accept/reject decision.

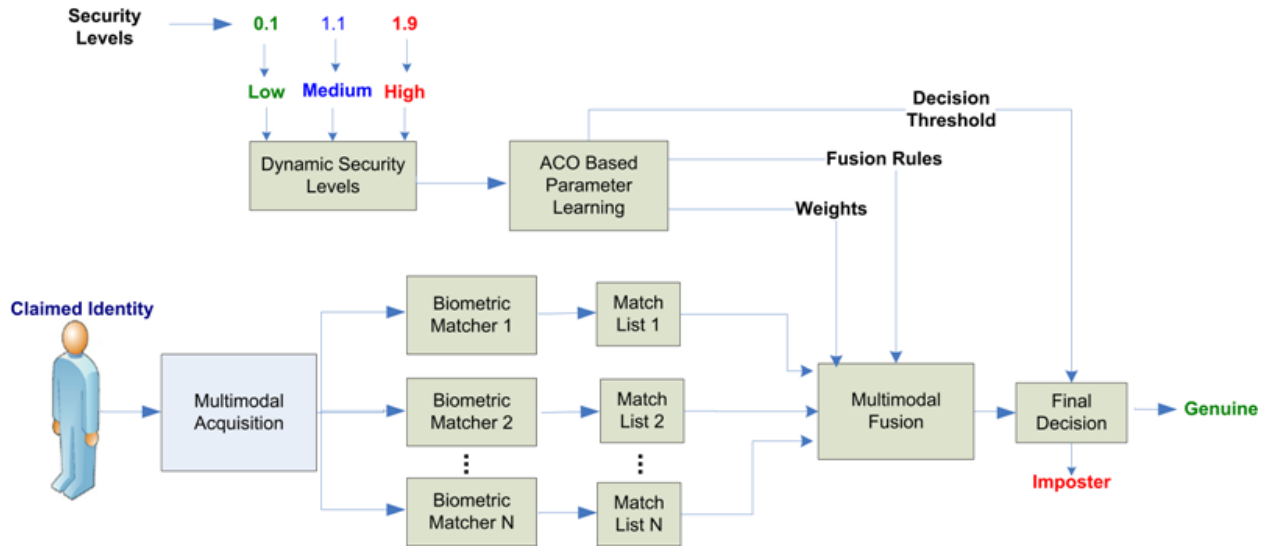


Fig. 1: Adaptive multimodal biometrics verification system capable of automatically operating at different security levels to ensure adaptive security level requirements.

III. THE ADAPTIVE MULTIMODAL BIOMETRIC VERIFICATION

As detailed in Section I-*A*, the performance and reliability of any multimodal biometric verification system can be well enumerated in terms of its two error rates, *i.e.*, FAR and FRR. In addition to FAR and FRR, Equal Error Rate (EER) is another performance measure for a typical multibiometrics system [1]. However, as discussed in Section I-*A*, the varying requirements of a security system necessitate the choice of FAR and FRR as per the application while the ERR is the operating point where FAR is equal to FRR. Hence, an adaptive multimodal biometrics verification system can be judged based on FAR and FRR as the performance indices

A. Representation of Security Levels

One way of creating different security levels is to assign different costs to these error rates (FAR/FRR) and study the effect of the verification parameters on each security level. If high security is required, the cost of FAR can be chosen higher than that of FRR. Since, in this case an

imposter acceptance must be avoided as much as possible. However, in the case of low security requirement, it is thoughtful to choose the cost of FRR to be higher in comparison to FAR. Since, in this case the convenience to the genuine rejection is the prime motive than the possibility of accepting unknown users. Therefore, different security levels in a multimodal system can be enumerated with the help of the cost of false acceptance (CFA) and cost of false rejection (CFR). Both of these costs lie in the [0, 2] range and we can choose the step size of 0.1 to denote intermediate security requirements which can lead to 20 discrete points representing the different security levels [3]-[4]. These security levels can therefore represent operational security bands which can be expected from a multimodal biometrics system during their real deployment. Hence, the optimal verification parameters need to be selected for each of them by minimizing the overall error associated with the multimodal biometrics verification system. Considering the costs (CFA/CFR) as the weights for the FAR and FRR, the overall error can be computed as follows:

$$G = CFA \times FAR\,(T) + CFR \times FRR\,(T) \tag{3}$$

$$CFA + CFR = 2 \tag{4}$$

where T represents the decision threshold employed to compute corresponding FAR and FRR. Here the optimal verification parameters for the system are to be selected, for each of the expected security levels, to minimize the overall error (G) associated with the multimodal biometrics system.

B. Representation of Population in ACO

The role of ACO is to choose an optimal solution from a population of probable solutions (verification parameters). Each component solution of the population can be represented in the *D-dimensional* space as $X_{md} = (x_{m1}, x_{m2} \ldots x_{md})$, where the first subscript m represents the component number, and d is the dimension which is different for each fusion strategy. In this

work we have implemented three approaches for the multimodal biometrics verification using ACO: (1) the score-level fusion approach as in [4], (2) decision-level fusion as in [3], and finally (3) FBDT based pattern classification approach as for finger knuckle verification [25].

In the score level fusion, each component solution has *"n+2"* dimensions, *i.e.* $d = n+2$, where n is the number of modalities. The first n dimensions are meant for the weights (w) assigned to each modality for the generation of the fused matching scores [4], the $(n+1)^{th}$ dimension is kept for the decision threshold, and $(n+2)^{th}$ dimension represents a fusion rule. The representation of a population in ACO for score-level fusion strategy is of the form:

$$X_{md} = (w_1, w_2 \ldots w_n, T) \tag{5}$$

For the matching score m_{Score}^{j} and w_j be the corresponding weight with $j = 1$ to n; n being the number of modalities. The four score-level fusion rules considered in this work are:

$$Sum = \sum_{j=1}^{n} w_j \times m_{Score}^{j} \tag{6}$$

$$\text{Product} = \prod_{j=1}^{n} \left(m_{Score}^{j} \right)^{w_j} \tag{7}$$

$$\exp = \sum_{j=1}^{n} w_j \times \exp(m_{Score}^{j}) \tag{8}$$

$$tanh = \sum_{j=1}^{n} w_j \times \tanh(m_{Score}^{j}) \tag{9}$$

In the decision level fusion, each component has "n+1" dimensions. The first n dimensions indicate the decision thresholds (T) corresponding to each biometric matchers and the $(n+1)^{th}$ dimension is solely for the binary fusion rule □ . So the representation of a population in this strategy is denoted by:

$$X_{md} = (T_1, T_2 \ldots T_n) \tag{10}$$

The decision-level fusion rules are the same as in [3]. For the FBDT based strategy, each component has *"n+1"* dimensions, where n is the number of modalities. Therefore out of three

dimensions, the first two dimensions are meant for the weights (w) assigned to each modality, and the third dimension is used for the fusion rule. An ant is therefore initialized as:

$$X_{md} = \{w_1, w_{2....}w_n\}. \quad (11)$$

C. Ant Colony Optimization

ACO, as firstly introduced by Marco Dorigo, represents a class of optimization algorithms which is applicable to the problems seeking optimal paths [28], [33]-[34]. As acknowledged by many users of ACO, its salient features include the positive feedback, distributed computation, and greedy heuristic [28], [33]-[34]**.** The positive response ensures quick search for optimal solutions, the distributed computation withstands the premature convergence while the greedy heuristic assists in identifying the desirable solutions at the early stages of the algorithm [28] [34]. The ACO algorithm relies on pheromone based probabilities to search for the optimal paths [34]. As part of searching, the moving ants (probable solutions) deposit some pheromone which evaporates over a trail time on the chosen paths. Any ant encountering a previous trail decides to follow a path having a high concentration of pheromone suggesting thereby that many ants had already tread that path. As a result, the collective behavior that emerges over several trails is a form of a positive feedback for the selection of an optimal path [34]. *The pheromone evaporation prevents the premature convergence as no single ant can ever dictate a path; and the selected path is an indicator of the collective judgment [28]*.

The ants (fusion parameters) are initialized with the population of probable solutions and each ant chooses its optimal solution from the population by minimizing G (Eqn 3). The constituents of population are defined in Section *II A*. For each ant, G is computed and pheromone levels of all the selected paths (solutions) are updated. The pheromone level of each path is updated only after the completion of iteration. The update on pheromone level τ_m^{t+1} at $(t+1)^{th}$ iteration where m denotes the m^{th} ant is given by

$$\tau_m^{t+1} = \rho \times \tau_m^t + \frac{Q}{G}, \text{ if } m^{th} \text{ ant chosen}$$
$$= \rho \times \tau_m^t, \text{ if } m^{th} \text{ ant not chosen} \quad (12)$$

As the pheromone levels are updated, probability of the selecting the m^{th} ant can be calculated for the next iteration as:

$$P_i = \frac{\tau_i^{(t)}}{\left\{\sum_{k=1}^{m} \tau_k^{(t)}\right\}} \quad (13)$$

Here m is the number of the ants. If any of the ants (newly computed solutions) participates in the minimization of the objective function (G), the value of pheromone level increases by Q/G in (12). Consequently, the probability (Eqn. 13) of selecting such paths in the next iteration gets better than others (as the pheromone levels on these paths are negligible). One important parameter of ACO is the evaporation factor (ρ) that enters the probability computation (Eqn 12). The ACO suffers from the problem of saturation of pheromone level for small values of ρ (close to 0) getting the algorithm stuck up on a particular path (solution). On the other hand if ρ is close to 1, every path will have equal probability with no optimization being accomplished. To overcome this, ρ is set to 1 initially and subsequently decreased in the steps of 0.005. This strategy not only prevents the ants from being dragged on any non-optimal path but also allows them to navigate to an optimal path.

In ACO, after updating the pheromone levels, the new paths for the next iteration are selected from the available candidate paths. Instead of trying out all candidate paths, the ones with low probability should be discarded. This will narrow down the search space and improve the quality of paths chosen by ants. For the improvisation of ACO, the idea of global and local updates is borrowed from PSO and utilized for updating the probabilities of selecting each path. Here, the probabilities of each path are constrained to lie between the lower and the upper values,

i.e. *L* and *U* based on their local best, the global best positions and the current position, denoted by A_{lb}, A_{gb} and A_{cp} respectively. The A_{lb} is calculated using ant's own probability and A_{gb} is obtained by comparing the probabilities of the all ants. After getting the values of A_{lb}, A_{gb} and $A_{cp,}$ the values of *L* and *U* are determined from Table 1. At the first iteration, an equal amount of pheromone is assigned to all paths and the probabilities are calculated accordingly. Over several iterations, the limits are determined. In the view of the limits *L* and *U*, the probabilities are modified as:

$$p_i = \frac{\tau_i^{(t)}}{\{\sum_{k=L}^{U} \tau_k^{(t)}\}} \tag{14}$$

Table1: Limiting Conditions for the A_{cp}, A_{lb} and A_{gb}

Condition	L	U
$A_{cp} < A_{lb} < A_{gb}$	A_{cp}	1
$A_{lb} < A_{cp} < A_{gb}$	A_{lb}	1
$A_{lb} < A_{gb} < A_{cp}$	A_{lb}	A_{cp}
$A_{cp} < A_{gb} < A_{lb}$	A_{cp}	A_{lb}
$A_{gb} < A_{cp} < A_{lb}$	0.001	A_{lb}
$A_{gb} < A_{lb} < A_{cp}$	0.001	A_{cp}

D. The ACO Algorithm

This algorithm consists of the following steps:

I. Initialize the population of the ants randomly in the search space (as discussed in Section *III-B*). Ants are initialized according to the score-level, decision-level, and FBDT based adaptive biometrics verification.

II. Specify the pheromone level of each ant as the discrete array (τw_1 , τw_2 , ……, τwn) for the score level fusion but as (τT_1, τT_2, , τT_n) for the decision level fusion. In the first iteration they are fixed randomly at the same pheromone value and the probabilities are calculated using (13).

III. Update the local and global best positions of the ants as detailed in Section *III B* and evaluate the probabilities using (14).

IV. Iterate step *III* until the completion of the specified number of iterations.

IV. EXPERIMENTAL RESULTS

The earlier authentication systems in the literature exhibit diverse performance depending on the modalities employed. In the light of this observation the performance of ACO is judged on a variety of true multimodal databases, *i.e*. palmprint [29] and iris database [30] of IITD, two multimodal systems of NIST BSSR1 [31], and the XM2VTS database [32]. The methodology for performance evaluation, performance metric, and details of the parameters are summarized in the following:

I. The parameters of ACO are empirically selected. These parameters are: ρ which is chosen as 1 initially and decreased in the steps of 0.005 in each iterations of the algorithm until the global optimum is attained [28]; Q which is experimentally chosen in the range of [0.005 0.01] (it was found that Q=0.01 is acceptable); and the number of ants which was selected as 15 for the convergence of the algorithm.

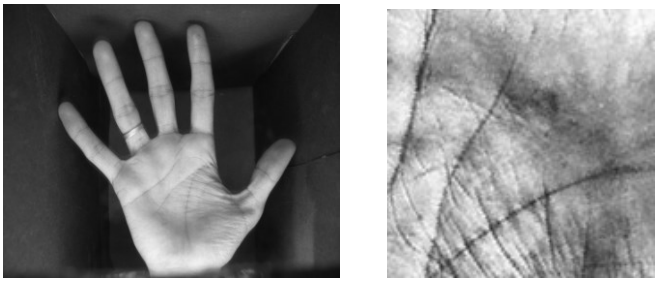
II. The performance evaluation of the proposed approach is made on various multimodal biometrics systems constructed from the publicly available databases and matching scores such as: Palmprint and iris multimodal system from IITD databases, and two multimodal systems developed from the matching scores of fingerprint and face of NIST BSSR1 [31]. The multimodal systems developed from these databases are evaluated to ensure adaptive security requirements.

III. Since the ACO based selection of the verification parameters in these algorithms can differ in each run, the ACO is executed 100 times, as in [3]-[4], for each of the CFA in

equation (3). The average and the standard deviation of the *minimum weighted error* over 100 runs are computed as the performance metric for the proposed algorithms. The average error for each CFA not only gives the generalized performance of the dynamic security algorithm but also depicts the complete tradeoffs in the error rates. The standard deviation (SD) indicates the stability of the algorithm during the 100 runs of ACO. In order to compare the performance of the four fusion rules, their frequencies of selection in the 100 runs are computed for each of the security levels. The rule which is selected most of the times can be considered as the optimal rank-level fusion rule. A detail discussion on each of the multimodal systems is as follows:

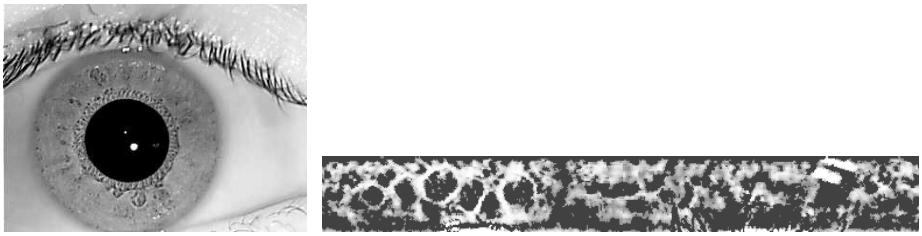
A. The Palmprint and Iris Multimodal System

The first set of experiments on the ACO based for the multimodal fusion is carried out on a bimodal database of palmprints and iris. The combination of palmprint and iris makes a potential bimodal system. In order to judge the performance of the proposed approach using ACO on a true bimodal system, the IITD database of palmprint and iris is utilized. The IITD multimodal palmprint and iris databases have 235 users each. The ROI extraction and normalization method employed are the same as in [35]. The palmprint images are of size 384×384 whereas ROIs are of size 128×128, shown in Fig. 2 (a) and 2 (b) respectively. The feature extraction method and matching using Hamming distance to compute matching scores are the same as detailed in [36]. A sample iris image of size 340 × 240 is shown in Fig. 3 (a). The image normalization, enhancement, and feature extraction employed are the same as in [37]. A normalized iris strip of size 48 × 432 is shown in Fig. 3(b). The log Gabor based feature extraction and Hamming distance based matching are the same as in [37].



(a) (b)

Fig.2: (a) Sample Image from IITD database (b) Corresponding ROI image.



(a) (b)

Fig. 3: Iris Images (a) sample image (b) Iris normalized strip.

The multimodal database of palmprint and iris is divided into two sets of users. The first set, consists of 110 users, is called as the learning set which is used to compute the verification parameters as detailed in *Section I-A* and *Section III-A*. The second set, consists of 125 users, is called as the evaluation set which used to assess the verification parameters learnt from the training set. The matching scores from 110 users are computed for the learning set {220 (110×2) genuine score and 23980 (110×109×2) impostor scores} while matching scores from independent 125 users are computed for the second set {250 (152×2) genuine scores and 31000 (125×124×2) impostor scores}.

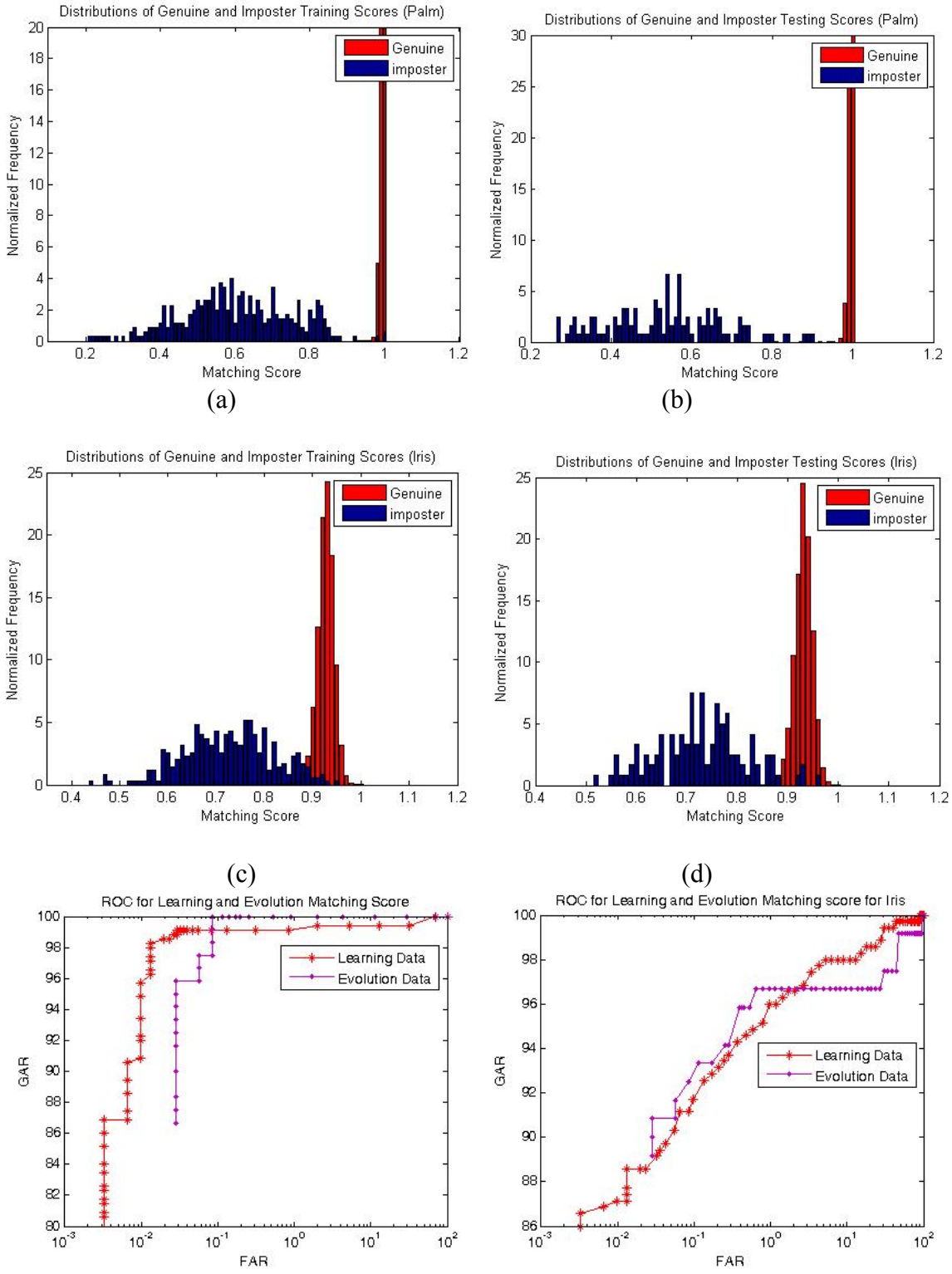
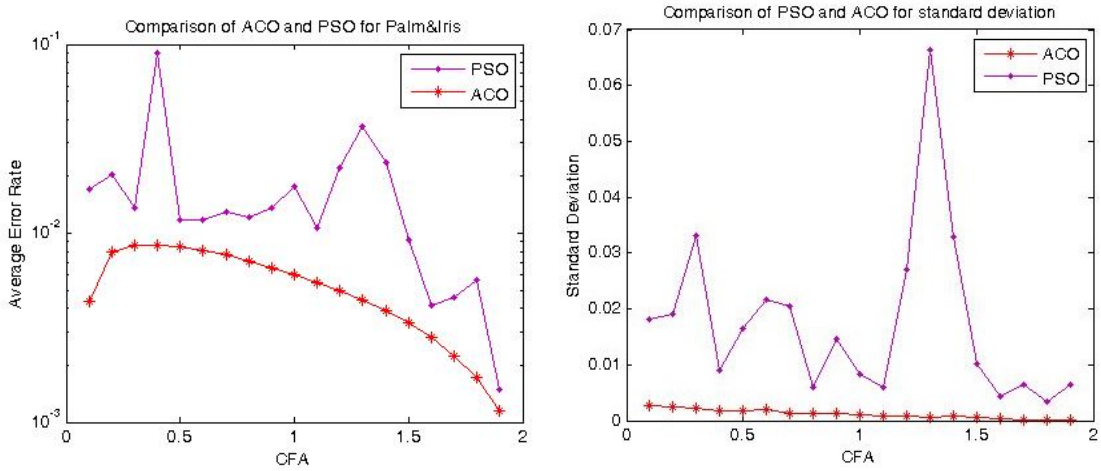


Fig. 4: (a) Histogram of matching score distribution: (a) learning set of palmprint (b) evaluation set of palmprint (c) learning set of iris (d) evaluation set of iris.

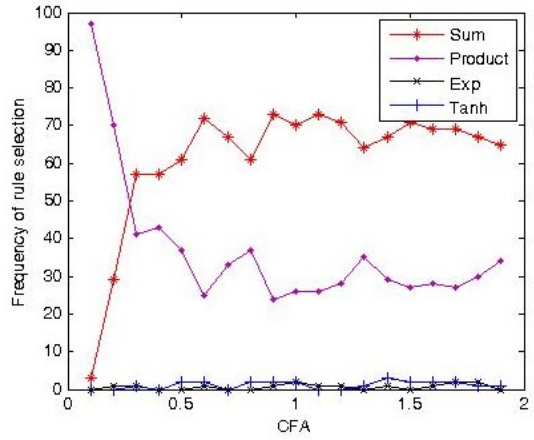
The histogram distribution of matching scores from the first set and the second set for palmprint database is shown in Fig. 4 (a) and Fig. 4 (b) respectively. It can be observed that, the learning and the evaluation sets of the matching scores from palmprint show similar distribution of matching scores. The matching scores distributions for iris from the two sets is shown in Fig. 4 (c) and Fig. 4 (d) respectively. The ROC curve for the learning and evolution datasets of palmprint and iris modalities are shown in Fig. 4 (e) and 4 (f) respectively.

The learning sets of the multimodal palmprint and iris are used to learn the verification parameters by incorporating ACO. The *average error* of the *weighted sum* (Equation (3)) over the 100 runs of ACO algorithm corresponding to each CFA is computed for this multimodal system. The ACO Vs PSO plot for the average error from the score level fusion is shown in Fig. 5 (a) while the *standard deviation* is shown in Fig. 5 (b). It can be observed that, the ACO based approach proposed in this paper outperforms PSO based approach in terms of the average error of the multimodal system. The *standard deviation* plot from Fig. 5 (b) shows that The ACO based approach is more stable than PSO while computing the verification parameters in the 100 runs of the algorithm. The plot for the frequency of rule selection from 100 runs of the algorithm corresponding to each CFA is shown in Fig. 5 (c). It can be observed that, for first two values of CFA product rule is selected with high frequency while for others sum rule is selected with high frequency.

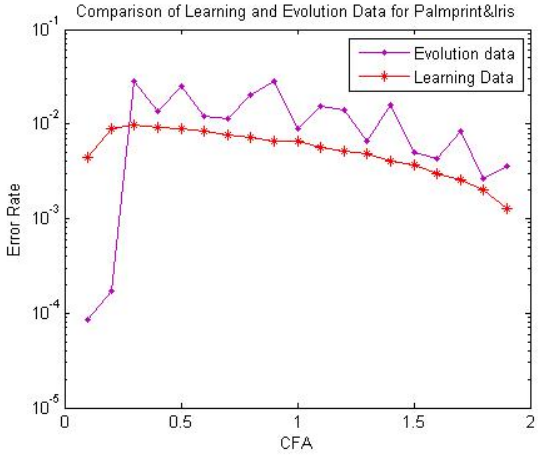


(a)

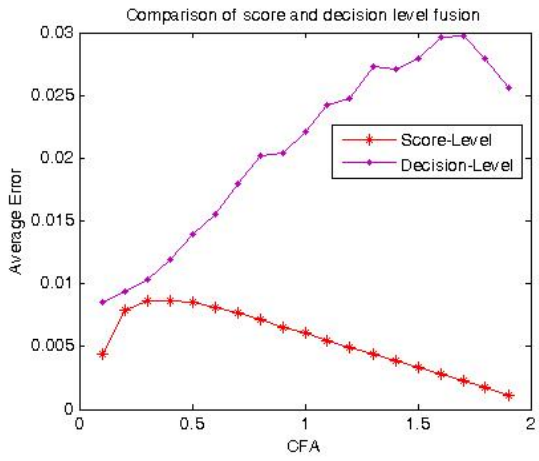
(b)



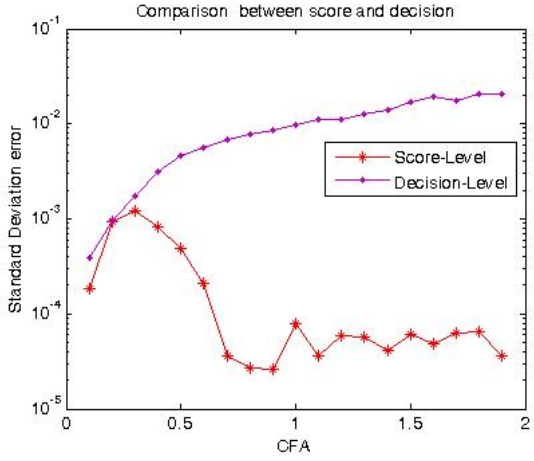
(c)



(d)



(e)



(f)

Fig.5 Results from palmprint and iris (a) Average error (b) standard deviation (c) the frequency of rule selection (d) comparison between learning and evaluation data (e) average error for score and decision level fusion (f) standard deviation error for score and decision level fusion.

The verification parameters selected with the evaluation set corresponding to each CFA are shown in Table 2. The verification parameters computed from learning set is applied on evaluation data of the multimodal system. The error rate (equation 3) computed from learning and evaluation for each CFA is shown in Fig. 5 (d). It can be observed from Fig. 5 (d) that, the evaluation set yields slightly high error rate in comparison to the learning set for higher values of CFA (>=0.3). Here it is also important to observe from the Fig. 4 (c)-(d) that learning set is operating on slightly better performance than evaluation set. However, it is also important to remark here that, the earlier approaches on adaptive multimodal verification [3]-[4] utilize all the available training data to compute verification parameters. This condition also seems judicious as biometrics verification is always required to take decision from the target/known set of the users enrolled in the database.

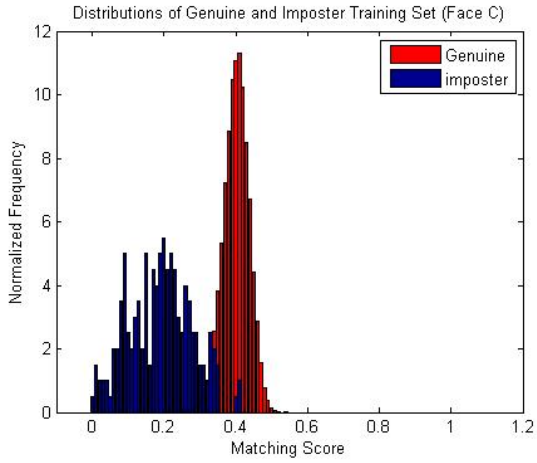
Table 2: Verification parameters computed from learning set of the palmprint and Iris

CFA	Weight1 (Palm)	Weight2 (Iris)	Average Error	Fusion Rule
0.1	0.757	0.89	0.004	Product
0.2	0.765	0.842	0.007	Product
0.3	0.284	0.869	0.0086	Sum
0.4	0.532	0.862	0.0086	Sum
0.5	0.194	0.369	0.0085	Sum
0.6	0.222	0.836	0.0081	Sum
0.7	0.891	0.603	0.0076	Sum
0.8	0.302	0.362	0.0071	Sum
0.9	0.806	0.633	0.0065	Sum
1.0	0.653	0.475	0.0060	Sum
1.1	0.756	0.599	0.0054	Sum
1.2	0.332	0.437	0.0049	Sum
1.3	0.878	0.479	0.0044	Sum
1.4	0.998	0.626	0.0038	Sum
1.5	0.875	0.529	0.0033	Sum
1.6	0.295	0.322	0.0027	Sum
1.7	0.905	0.632	0.0022	Sum
1.8	0.583	0.848	0.0017	Sum
1.9	0.545	0.665	0.0011	Sum

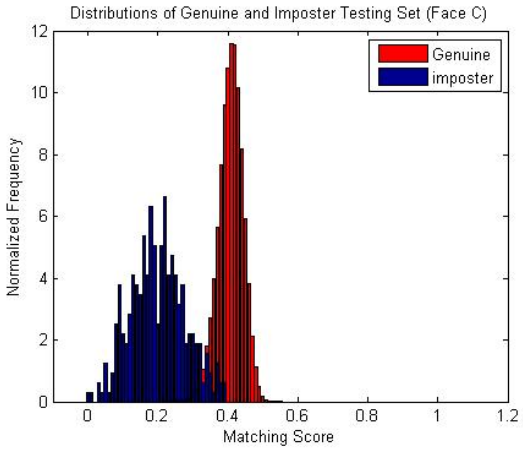
Further, if the verification parameters can be learnt from the complete set of the target users, the likelihood of accurate learning is very high. The presented results therefore are the best even in the worst possible scenario of learning and evaluation from different set of matching scores. Finally, decision-level fusion approach is implemented using ACO and compared with score-level fusion as in [4]. The average error and the standard deviation error plots of this comparison are shown in Fig. 5 (e) and 5 (f). It can be seen that in both the plots, score-level fusion approach dominates over the decision-level fusion.

B. The BSSR1 Database

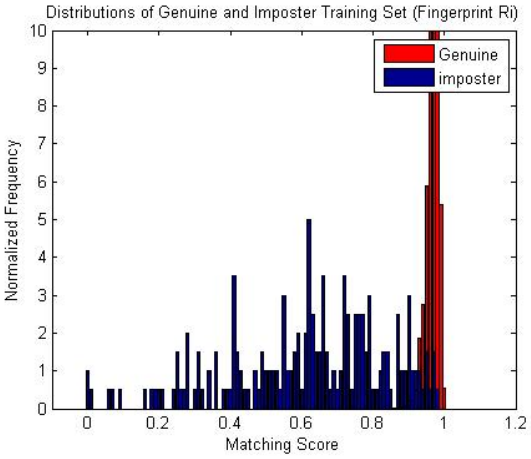
The NIST BSSR1 multimodal database contains the matching scores of fingerprint and face biometrics. The NIST BSSR1 multimodal database contains scores from 517 users. There are 517 genuine scores and 266,772 (516×517) imposter scores for each user. One fingerprint matchers (Ri) and one face matcher (C) are considered in this work. The learning set consists of 200 users, which is used to compute the verification parameters. The evaluation set consists of 317 users, which is used to assess the verification parameters learnt from the training set. The matching scores from 200 users of the learning set are computed as: {Genuine = 200 (200×1) and Imposter = 23800 (200×119)} while second set of 317 users indicates: {Genuine = 317 (317×1) and Imposter = 100172 (317×316)}. The histogram distribution of matching scores from the two sets of BSSR1 databases is shown in Fig. 6 (a) and Fig. 6 (b) for face C and in Fig. 6 (c) and Fig. 6 (d) for fingerprint Ri. The ROC curve for the learning and evolution datasets of palmprint and iris modalities are shown in Fig. 6 (e) and 6 (f) respectively. It can be observed that both the sets of the databases have the similar ROC curves.


Distributions of Genuine and Imposter Training Set (Face C)
Genuine
imposter
Normalized Frequency
Matching Score

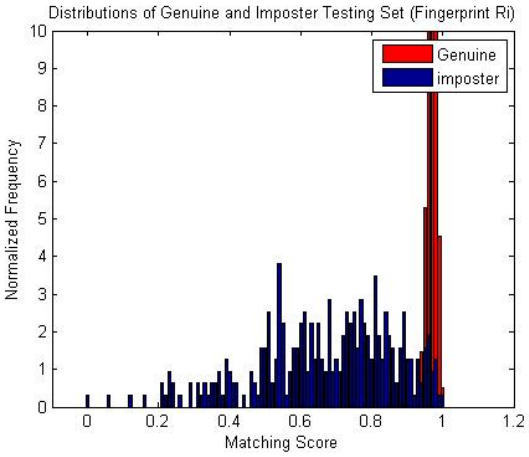
(a)


Distributions of Genuine and Imposter Testing Set (Face C)
Genuine
imposter
Normalized Frequency
Matching Score

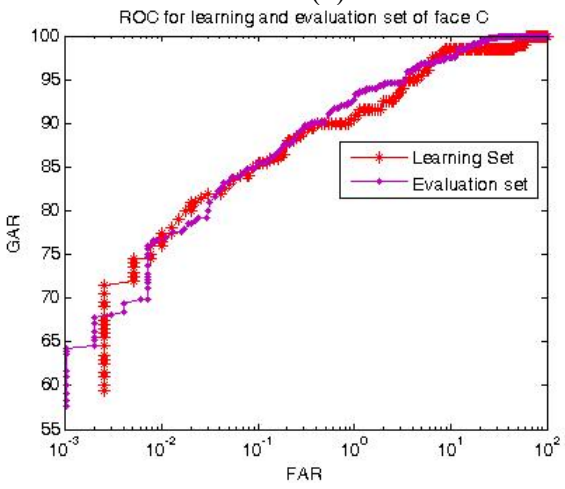
(b)


Distributions of Genuine and Imposter Training Set (Fingerprint Ri)
Genuine
imposter
Normalized Frequency
Matching Score

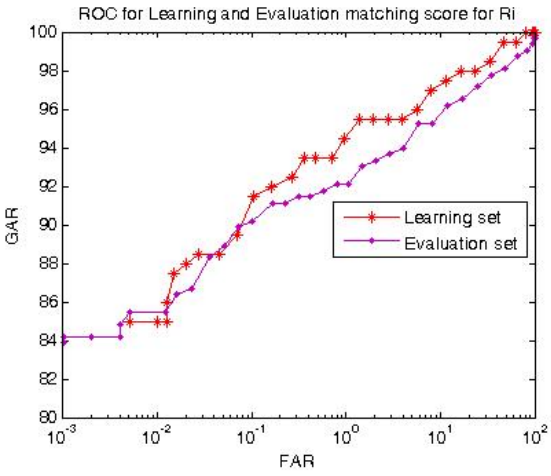
(c)


Distributions of Genuine and Imposter Testing Set (Fingerprint Ri)
Genuine
imposter
Normalized Frequency
Matching Score

(d)


ROC for learning and evaluation set of face C
Learning Set
Evaluation set
GAR
FAR

(e)


ROC for Learning and Evaluation matching score for Ri
Learning set
Evaluation set
GAR
FAR

(f)

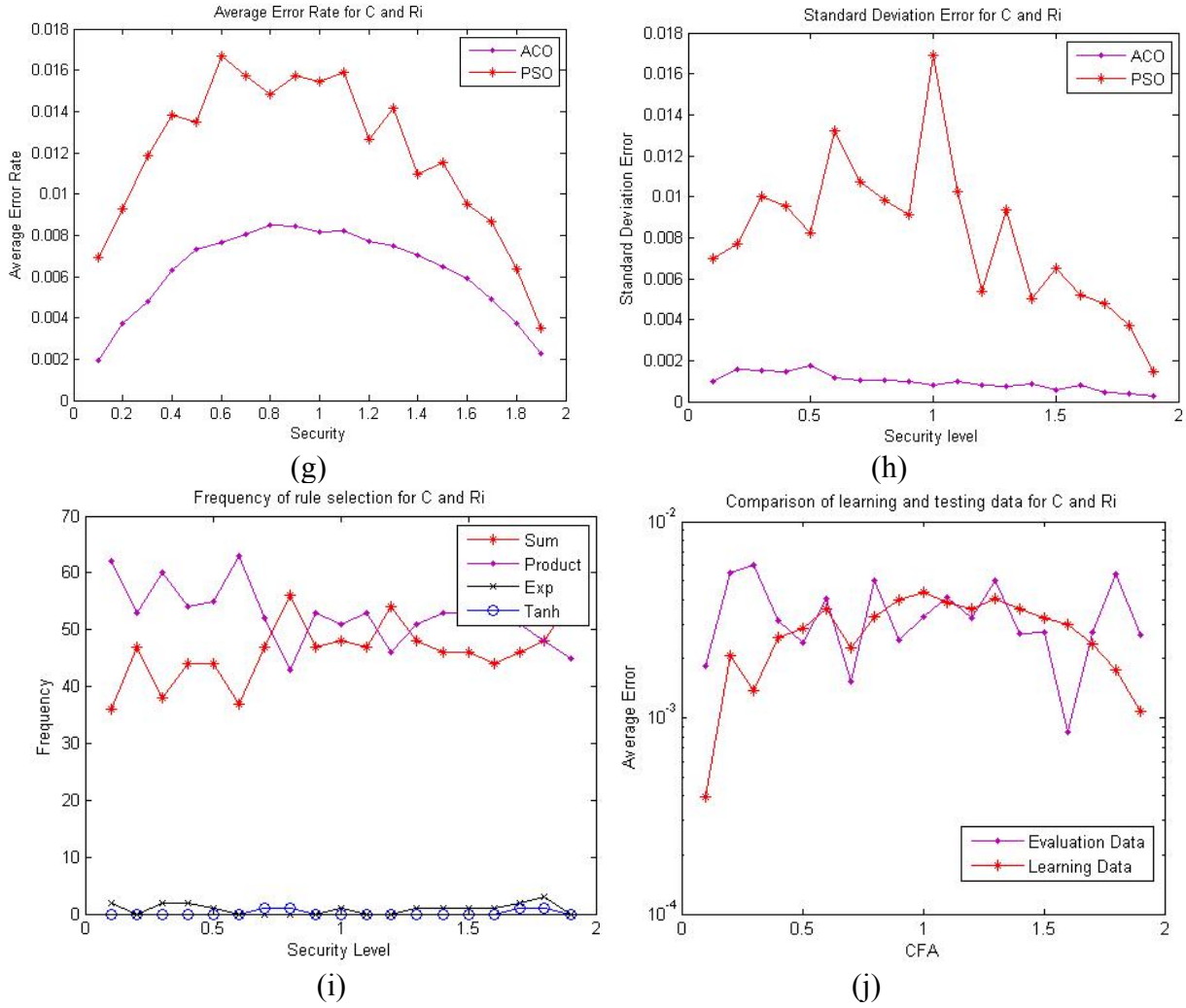


Fig.6: Histogram of matching score distribution: (a) learning set of face C (b) evaluation set of face C (c) learning set of RI (d) evaluation set of iris (e) comparison between learning and evaluation data for C (f) comparison between learning and evaluation data for Ri (g) comparison of average error for c and RI (h) standard deviation for C and Ri (i) the frequency of rule selection for C and Ri (j) comparison between learning and evaluation data for C and Ri.

The learning sets of the multimodal C and Ri are used to learn the verification parameters by incorporating ACO. The plot of ACO vs. PSO of the average error for the score-level fusion is depicted in Fig. 6 (g) and that for the standard deviation of the errors in Fig. 6 (h). It can be examined from both the plots that ACO base approach yields significantly low error rates in comparison to PSO based approach. The plot for the frequency of rule selection from 100 runs

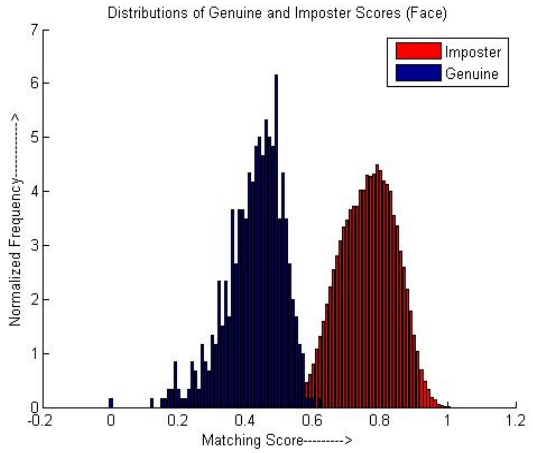
of the algorithm corresponding to each CFA is shown in Fig. 6 (i). It can be observed that, both the sum rule and the product rule are selected with similar frequencies. However, for most of the CFAs product rule is selected with slightly better (higher) frequency. The error rate (Equation 3) computed from the learning and evaluation for each CFA is shown in Fig. 6 (j). It can be observed that, both of the evaluation and learning data sets provide almost similar performance.

C. The XM2VTS Database

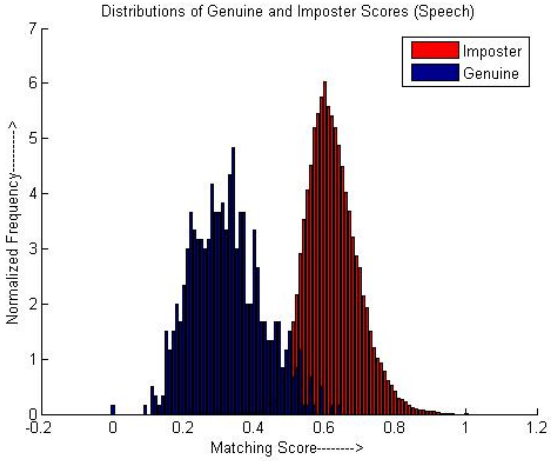
Another set of experiments are reported using the XM2VTS database from face and speech [32]. It contains the synchronized databases of frontal face and speech from 295 users. The database is divided into three sets: 200 genuine and 25 evaluation impostors while the rest 70 are the test impostors. In [38], the training and evaluation approaches called as Lausanne Protocol I and II are reported on different combinations of baseline systems. There are 8 samples per user out of which 3 are used for the training the baseline experts, the remaining 3 are used for evaluation [38] and the rest 2 are for testing.

In this work we employed the baseline system with Lausanne Protocol I. The Discrete Cosine Transform (DCTb) features extracted from bigger size face images (80×64 pixels) are used to the generate genuine and imposter scores using the Gaussian mixture model (GMM). The Linear Filter-bank Cepstral Coefficients (LFCC) speech features are computed using 24 linearly-spaced filters on each frame over a window length of 20 milliseconds. The genuine and imposter scores are generated using GMM. We utilized fusion development set of genuine and imposter scores containing 600 (200×3) genuine and 40,000 (25×8×200) imposter scores. The histograms of both the matching scores corresponding to face and speech matching scores are shown in Fig 7 (a) and 7 (b) respectively. The combined ROC of both the scores appears in Fig. 7 (c). The improvised ACO vs. PSO plot of the average of the minimum errors for the score level fusion is

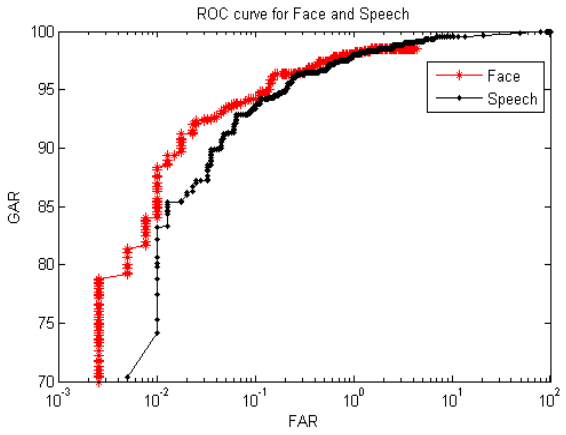
given in Fig. 7 (d) and SD of the errors in Fig. 7 (e). The probability of each rule being selected out of 4 score level fusion rules using ACO is portrayed in Fig. 7 (f).



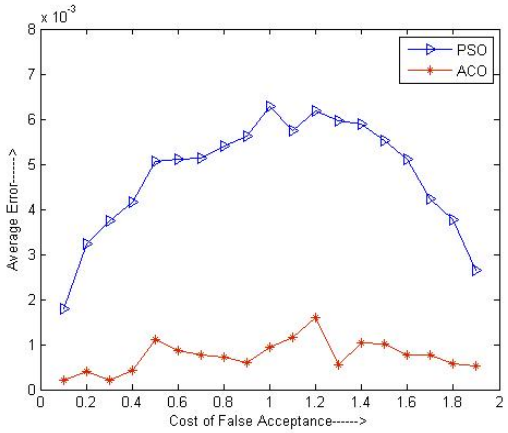
(a)



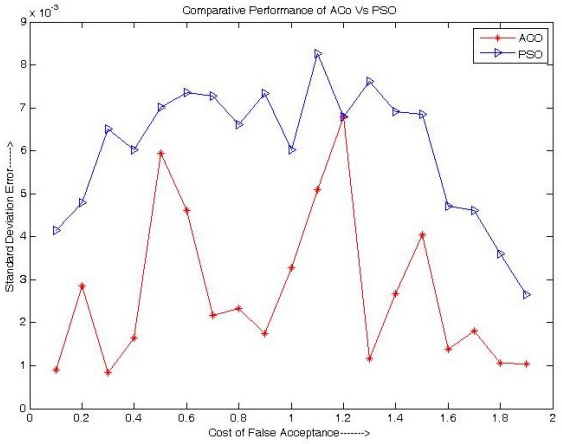
(b)



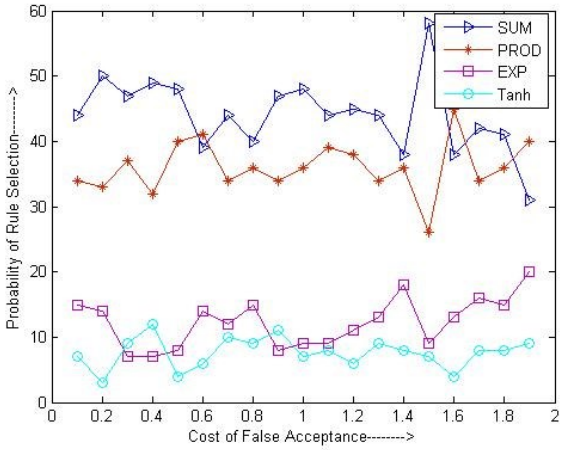
(c)



(d)



(e)



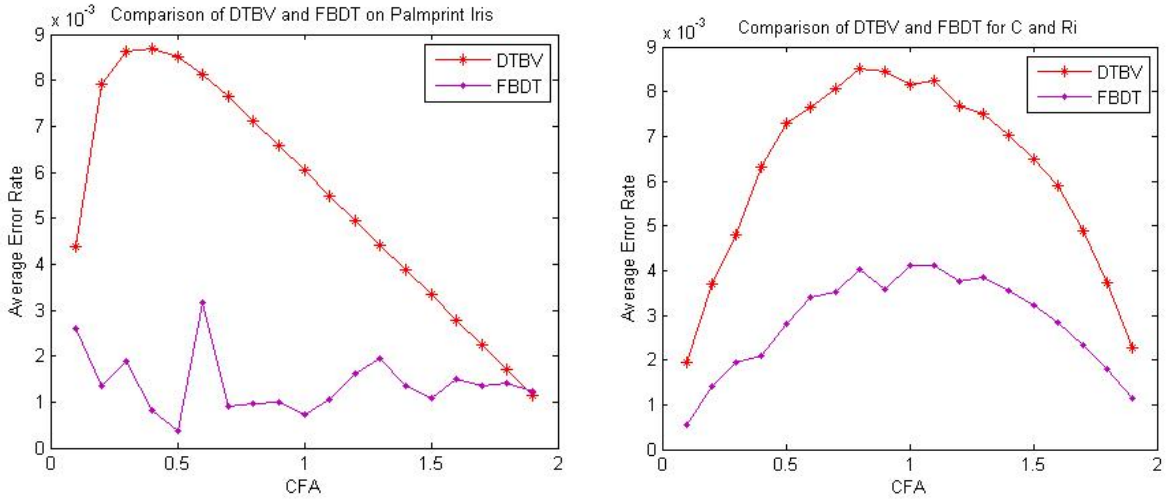
(f)

Fig.7: The histogram of the matching scores from the face and speech databases are given in (a) and (b) respectively; ROCs corresponding to both modalities are given in (c); PSO verses ACO plot for the score level fusion corresponding to the average and SD of error are given in (d) and (e) respectively; and the plot of probabilities of selection of score level rules corresponding to each CFA is given in (f).

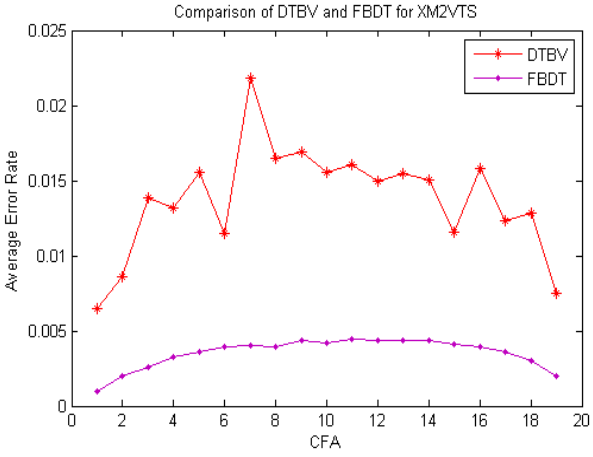
D. The Experiments on FBDT

The experimental results for the biometrics verification are presented in this section using FBDT and ACO. The construction and classification of FBDT in this work are the same as in [23]-[25]. The experimental results in the earlier works show that, the learning of FBDT is done from four membership functions: *Same*: (Gaussian, Gaussian), (Trapezoidal, Trapezoidal) and *Different*: (Gaussian, Trapezoidal), (Trapezoidal, Gaussian) and two tree-nodes computation criteria: fuzzy information gain, fuzzy Gini index. It can be observed that, the change in membership function and the tree-node computation criteria provide a tradeoff in the error rates (FAR/FRR). However, as the FBDT is trained as per the different values of security level (varying FAR and FRR) only (Gaussian, Gaussian) membership function and fuzzy Gini index are sufficient for providing the optimal results and hence used for FBDT. The ACO framework using FBDT has also been proposed in the earlier work for multimodal knuckle verification [25]. However, this work entirely focuses on ACO-FBDT framework (for knuckle verification) while the work in this paper investigates decision threshold based biometrics verification (DTBV) using ACO and evaluates performance on variety of multimodal biometrics systems. In this paper we provide a comparison of the ACO-FBDT [25] with ACO-DTBV to illustrate that ACO based biometrics verification framework can be utilized in majority of the pattern classification problems.

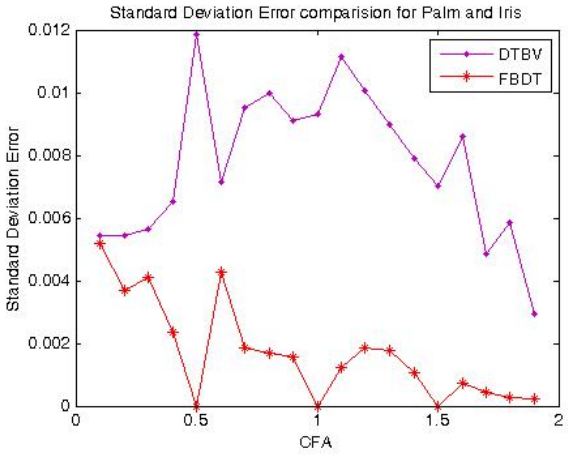
The matching scores and the experimental protocol for the FBDT based approach in this section is the same as detailed in *Section IV-A*, *Section IV-B*, and *Section IV-C* for palmprint and Iris, BSSR1 (C and Ri) and XM2VTS multimodal biometrics databases respectively. The approach detailed in earlier sections of this paper is referred to as the decision threshold based biometrics verification (DTBV) as the biometrics verification in that approach is dependent on decision threshold for the final decision. We show the comparison between the FBDT (detailed in this section) and the DTBV approaches. The average error corresponding to each CFA for the two approaches in the BSSR1 multimodal system (C and Ri) is shown in Fig. 8 (a) while for the XM2VTS is shown in Fig. 8 (b). A comparison of the standard deviation on these two multimodal databases is shown in Fig. 8 (c) and Fig. 8 (d) respectively. The average error plots from Fig. 8 (a)-(b) show that, the approach using FBDT yields considerably less error rates while the standard deviation plot show that the FBDT approach is more stable than DTBV approach and requires very few run of the algorithm for computation of the reliable/stable results. The plots of the frequency of the four score-level rule selection using FBDT approach corresponding to each CFA are shown in Fig. 8 (e) for BSSR1 (C and Ri) while for XM2VTS in Fig. 8 (f).



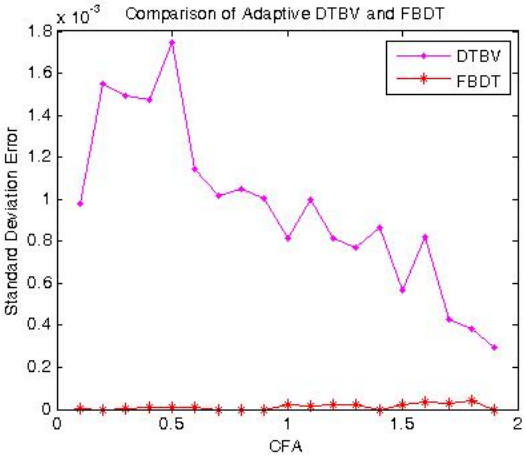
(a) (b)


Comparison of DTBV and FBDT for XM2VTS
Average Error Rate
CFA
DTBV
FBDT

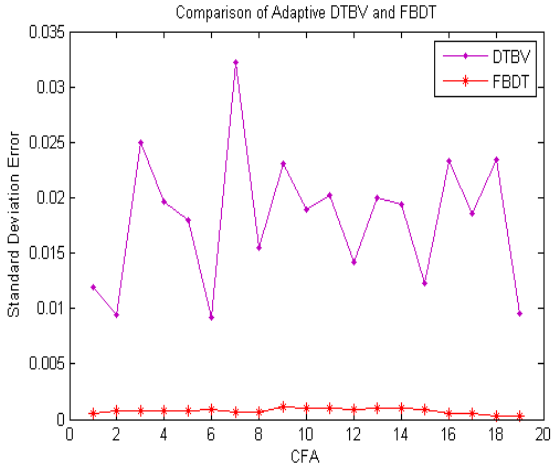
(c)


Standard Deviation Error comparision for Palm and Iris
Standard Deviation Error
CFA
DTBV
FBDT

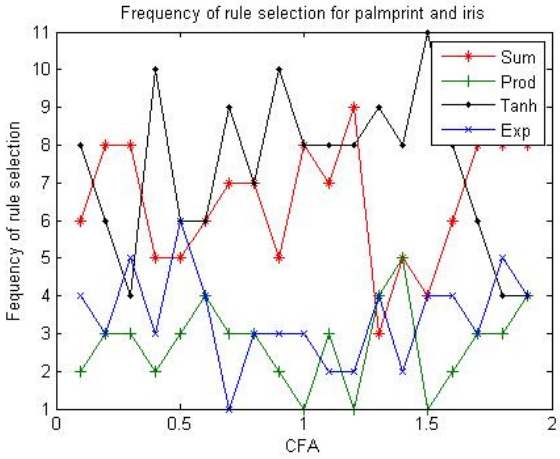
(d)


x 10^-3
Comparison of Adaptive DTBV and FBDT
Standard Deviation Error
CFA
DTBV
FBDT

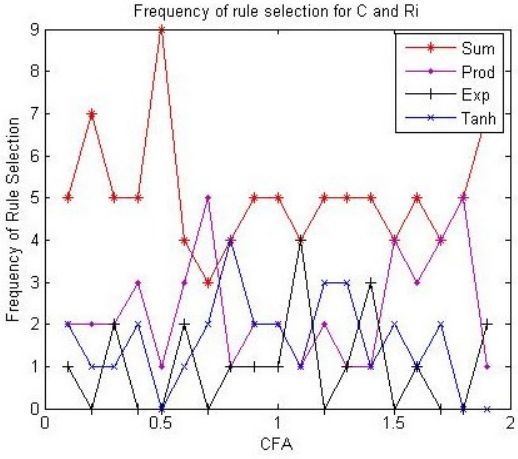
(e)


Comparison of Adaptive DTBV and FBDT
Standard Deviation Error
CFA
DTBV
FBDT

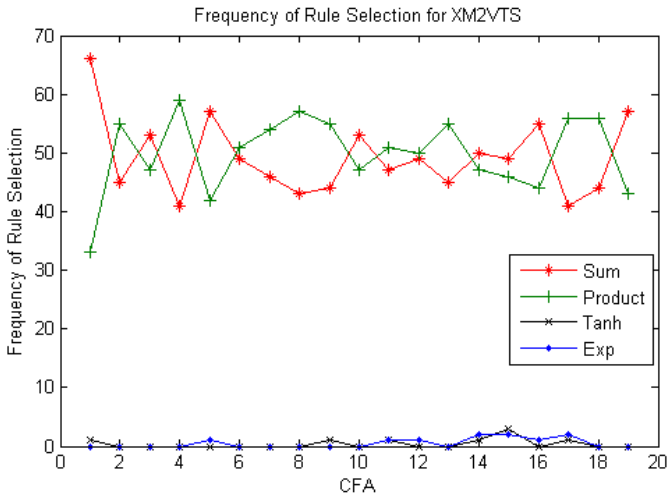
(f)


Frequency of rule selection for palmprint and iris
Fequency of rule selection
CFA
Sum
Prod
Tanh
Exp

(g)


Frequency of rule selection for C and Ri
Frequency of Rule Selection
CFA
Sum
Prod
Exp
Tanh

(h)



(i)

Fig. 8: (a) Comparison of the FBDT and DTBV approach for adaptive biometrics verification: (a) average error for palmprint and iris (b) average error rate for C and Ri (c) average error for XM2VTS (d) standard deviation error for palmprint and iris (e) standard deviation error for C and Ri (f) standard deviation error for XM2VTS (g) frequency of rule selection for Palmprint and iris (h) frequency of rule selection for C and Ri (i) frequency of rule selection for XM2VTS.

IV. DISCUSSION AND CONCLUSIONS

There has been very little attention on the adaptive selection of the verification parameters required to ensure varying security requirements during the deployment of a typical multimodal biometrics system. Most of the work in available references does not provide any mechanism to automatically select the optimal verification parameters according to the different security requirements set by the system administrator. This paper has focused on such problem and investigated the adaptive biometrics verification using ACO. The main contributions of this paper are: (1) proposition of a discrete domain evolutionary technique using ACO for the computation of the verification parameters in a multimodal biometrics system to meet the changing security requirements. The experimental results presented using on various multimodal

databases (Sections IV-A and Section IV-B) have shown that the verification parameters selected using ACO incur significantly smaller average and standard deviation of the error (Equation 3) than those from the popularly used PSO; (2) The proposed framework is generalized using FBDT based supervised classification for the biometrics verification. The FBDT is learned during the training phase from the available/generated matching scores. The trained FBDT is then utilized for making a two-class classification of the claimed identity to accept (genuine) or the reject (imposter) an unknown user. The experimental results reported in Section IV-C show that, the FBDT based framework illustrates smaller average error rate in comparison to DTBV based approach, and (3) comparative evaluation of the score-level and the decision-level fusion approaches for the adaptive biometrics verification using ACO. It is observed that the score-level fusion offers superior performance in comparison to the decision-level fusion (See Fig. 5 (e) and Fig. 5 (f)) which is also supported by earlier work in [4] but using PSO.

In this work, we have systematically evaluated ACO for the adaptive management of multimodal biometrics modalities to meet varying security requirements during the deployment. The requirement of discrete domain evolutionary approach in [4] motivated us to explore ACO over PSO. It may be noted that the other evolutionary techniques like GA [20] use crossover and mutation operations which are quite random in comparison to the ACO where ants follow the best path favored by the majority. The GA might offer better exploration of the solution space but it is constrained by the limitations like expensive fitness function, convergence to local minimum, and divergent solutions on dynamic data set [39]. Similarly, bacterial foraging optimization (BFO) [40] can also be subjected to so much of exploration by the way of swimming and tumbling in the four stages: *chemotaxis*, *swarming*, *reproduction*, and *elimination and dispersal* steps. Therefore the use of GA and BFO is constrained by the lack of adequate exploration; the only exploitation is through the optimization function.

The proposed framework using ACO can also be generalized for various pattern classification approaches whereas the pattern classification problems need to address two-class classification. The implementation of FBDT in this work is an important attempt to illustrate that the proposed framework using ACO can be generalized for any classification technique. However, in this paper, the ACO based framework is used for biometrics verification. Its usage in the computation of parameters biometrics identification (close/open) is part of our future work. It may be noted that the ACO as a discrete evolutionary technique may be more relevant to the biometrics identification using the rank-level fusion which is only option when scores from multiple classifiers are not available. This is mainly because of the fact that, unlike decision thresholds (which are the normalized values between 0 and 1), ranks are the natural numbers representing the best match in the decreasing order of confidence.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "An Introduction to biometric recognition," *IEEE Trans. Circuits & Sys. Video Tech*., vol. 14, no. 1, pp. 4-20, 2004.

[2] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[3] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney, "An Adaptive Multimodal Biometric Management Algorithm", *IEEE Trans. On Systems, Man, and Cybernetics—Part C: Applications and Reviews*, vol. 35, no. 3, Aug. 2005.

[4] A. Kumar, V. Kanhangad, and D. Zhang, "A New Framework for Adaptive Multimodal Biometrics Management", *IEEE Trans. Information Forensics & Security*, vol. 5, no. 1, pp. 92-102, Mar. 2010.

[5] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE Trans. Patt. Anal.Machine Intell.*, vol. 20, pp. 226-239, Mar. 1998.

[6] R. W. Frischholz and U. Deickmann, "BioID: A multimodal biometric identification system," *Computer*, vol. 33, no. 2, pp. 64–68, Feb. 2000.

[7] K. Nandakumar, Y. Chen, S. C. Dass and A. K. Jain, "Likelihood ratio based biometric score fusion", *IEEE Trans. Patt. Anal. Machine Intell.*, vol. 30, no. 2, pp. 342-347, Feb. 2008.

[8] F. Roli, S. Raudys, and G. L. Marcialis, "An experimental comparison of fixed and trained fusion rules for crisp classifier outputs," *Proc.3rd Int. Workshop on Multiple Classifier Systems* (MCS 2002), Cagliari, Italy, Jun. 2002.

[9] K. Nandakumar, A. Jain, and A. Ross, "Fusion in multibiometric identification systems: What about the missing data?" *Proc. ICB 2009*, Alghero, Italy, Jun. 2009.

[10] A. Kumar, "Dynamic security management in multibiometrics", *In Multibiometrics for Human Identification*, B. Bhanu and V. Govindaraju (*Eds*.), Cambridge University Press, 2011.

[11] M. Beattie, B.V.K. Vijaya Kumar, S. Lucey, and O. Tonguz. "Combining verification decisions in a multi-vendor environment", *Lecture Notes in Computer Science, Springer-Verlag Heidelberg*, vol. 3546, July 2005.

[12] M. Vatsa, R. Singh, A. Noore, and A. Ross, "On the dynamic selection of biometric fusion algorithms," *IEEE Trans. Information Forensics & Security,* vol. 5, pp. 470-479, 2010.

[13] D. Mery and K. Bowyer, "Face recognition via adaptive sparse representations of random patches," *IEEE Workshop on Information Forensics and Security* (WIFS), Atlanta, Dec. 3-5, 2014.

[14] R. M. Ramadan and R. F. Abdel – Kader, "Face Recognition Using Particle Swarm Optimization-Based Selected Features", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 2, No. 2, June 2009.

[15] M. Konrad, H. Stögner, and A. Uhl, "Evolutionary optimization of radial basis function classifiers for data mining applications" *IEEE Proc. 6th Intl. Symp. Image and Signal Processing and Analysis*, pp. 534-539, Salzburg, Austria, September 16-18, 2009.

[16] J. Adams, D. L. Woodard, G. Dozier, and P. Miller, "Genetic-Based Type II Feature Extraction for Periocular Biometric Recognition: Less is More," *IEEE 20th International Conference on Pattern recognition (ICPR)*, Istanbul, Turkey, Aug 23, 2010 - Aug 26, 2010.

[17] H. R. Kanan and K. Faez, "An improved feature selection method based on ant colony optimization (ACO) evaluated on face recognition system," *Applied Mathematics and Computation*, vol. 205, Issue 2, pp. 716–725, 15 November 2008.

[18] S. Nemati, M. E. Basiri, "Text-independent speaker verification using ant colony optimization-based selected features," *Expert Systems with Applications*, vol. 38, Issue 1, pp. 620–630, January 2011.

[19] E.S. Peer, F. Van Den Bergh, A.P. Engelbrecht, "Using neighborhoods with the guaranteed convergence PSO", *IEEE Proc. Swarm Intelligence*, pp. 235-242, USA, Apr. 2003.

[20] A. Ross, and A. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters*, vol. 24 pp. 2115–2125, 2003.

[21] A. Kumar, and D. Zhang, "Personal Recognition Using Hand Shape and Texture", *IEEE Transactions on Image Processing*, vol. 15, Aug. 2006.

[22] P. Verlinde and G. Cholet, "Comparing decision fusion paradigrams using k-NN based classifiers, decision trees, and logistic regression in a multi-modal identity verification application," *Proc. 2nd International Conference on AVBPA*, pp. 188-193, Washington, DC, USA, Mar. 1999.

[23] A. Kumar, M. Hanmandlu, A. Das, and H. M. Gupta, "Biometric Based Personal Authentication Using Fuzzy Binary Decision Tree", *Proc. 5th IAPR Intl. Conf. Biometrics*, ICB 2012, pp. 396-401, New Delhi, India, Mar-Apr. 2012.

[24] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Fuzzy binary decision tree for biometric based personal authentication", *NeuroComputing*, vol. 99, pp. 87-97, June 2012.

[25] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Ant Colony Optimization Based Fuzzy Binary Decision Tree for Bimodal Hand Knuckle Verification System", *Expert Systems with Applications,* vol. 40, no. 2, pp. 439-449, 2012.

[26] R. E. Banfield, L. O. Hall, K. W. Bowyer, and W.P. Kegelmeyer, "A comparison of decision tree ensemble creation techniques" *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 1, Jan. 2007.

[27] X. Liu, L. O. Hall, and K. W. Bowyer, "Comments on A parallel mixture of SVMs for very large scale problems", *Neural Computation,* vol. 16, no. 7, pp. 1345-1351, July 2004.

[28] M. Dorigo, G. Di Caro and L. M. Gambardella "Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem*" IEEE Trans. Evolutionary Computation*, vol. 1, no. 1, Apr. 1997.

[29] A. Kumar, "Incorporating cohort information for reliable palmprint authentication," *Proc. ICVGIP*, Bhubneshwar, India, pp. 583-590, Dec. 2008. Available at: http://www.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm

[30] IIT Delhi Iris Database, available at: http://www.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

[31] NIST BSSR1 biometric score set, Available at: http://www.nist.gov/biometricscores.

[32] Available at: http://info.ee.surrey.ac.uk/Personal/Norman.Poh/web/fusion/main.php?bodyfile=entry_page.html {with due acknowledgement to Dr. Norman Poh, University of Surrey}.

[33] E. Grosso, L. Pulina, and M. Tistarelli, "Modeling biometric template update with ant colony optimization", *Proc. 5th IAPR Int. Conference on Biometrics*, 29 March - 1 April, 2012.

[34] M. Dorigo, V. Maniezzo and A. Colorni, "The Ant system: Optimization by A colony of cooperating agents", *IEEE Trans. System, Man, and Cybernetics*, *Part B*, vol. 26, no. 1, 1996.

[35] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1041–1050, Sep. 2003.

[36] Z. Sun, T. Tan, Y. Yang, and S. Z. Li, "Ordinal palmprint representation for personal identification," *Proc. CVPR 2005*, pp. 279-284, 2005.

[37] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal identification," *Proc. CVPR 2008*, pp. 21-27, Anchorage, Alaska, June 2008.

[38] N. Poh and S. Bengio, "Database, protocol and tools for evaluating score-level fusion algorithms in biometric authentication", *Pattern Recognition*, vol. 39, no. 2, pp. 223-233, 2006.

[39] *Handbook of Evolutionary Computation*, T. Bäck, D. Fogel and Z. Michalewicz (*Eds*), IOP Publishing and Oxford University Press, New York, 1997.

[40] K. M Passino, "Biomimicry of bacteria foraging for distributed optimization and control", *IEEE Control Systems Magazine*, June 2002.