Fusion based Multimodal Biometric Security for Social Networks Communication

Jayanthi N. M.
Research Scholar,
Bharathiar University, Coimbatore – 641046,
TamilNadu, India

C. Chandrasekar, PhD
Associate Professor,
Dept. of Computer Science, Periyar University,
Salem – 636 011, TamilNadu, India

ABSTRACT
As modern means of communication increase in their potential and receptiveness, they instigate additional demands in terms of security. Therefore, communication between users via social network becomes complicated, that increases possibility of threats with respect to user authentication. With the objective of ensuring security in social networks, different user authentication and cryptographic mechanism were designed. But, with different heuristic and computational algorithm, user authentication through single modal biometric is easily broken and vulnerabilities of multimodal approaches in social network still remain unexplored. This paper proposes a novel Fusion based Multimodal Biometric Security (FMBS) method utilizing Face and Fingerprint features of human individuals on social networks. Feature extraction for FMBS is performed utilizing combination of Binomial Feature Distribution Algorithm and Neighborhood Dominant Attribute Identification for both face and fingerprint features. Then, dominant attributes are stored in spatial vector for both the modalities to form biometric fusion template. Finally, Structural Biometric Fusion Template Matching algorithm designed to compute matching accuracy of test data to available training data. Experimental evaluation with Biometric Research Repositories is conducted. Performance evaluation show that the method significantly improve matching accuracy of human biometric samples, compared to conventional biometrics user authentication that only make use of single modal biometrics. The result shows that the method has low social network authentication time and network space complexity suited for deployment in real time social network sites.

Keywords
Social Network System, Cryptographic Security, Multimodal Biometric, Neighborhood Dominant Attribute, Spatial vector, Template matching

1. INTRODUCTION
The plethora of functionalities offered by social media enables users to communicate through internet where the presence of malicious user behavior causes security threats, letting the whole community of users get compromised easily. In recent years, both single and multimodal biometrics user authentication have been explored extensively in addressing this challenge. A collaborative Face Recognition [1] framework using social graph model provided an insight into hit rate and therefore improving the authentication rate. On the other hand, most existing online social network supports face recognition, though considered to be time consuming and caused collision. Game theoretic strategies were applied in [2] using multimedia fingerprinting to reduce the collision in a time sensitive manner. A series of studies have highlighted the use of single and multimodal biometric model. A multimodal biometric system was introduced in [5] that used behavioral characteristics to track the students in virtual classes. As reported in [6], providing multimodal user authentication using face and gestures has improved considerably over the last decade. On the other hand, considerable work was contributed in [7] based on keystroke behaviors to improve the identity authentication system.

In this paper, the focus of the work is to use multimodal biometrics user authentication by illustrating the model and analysis of user behavior in social networks. The multimodal biometrics user authentication extracts the multimodal features (i.e. face and fingerprint) using Neighborhood Dominant Attribute Identification that reduces social network authentication time by eliminating redundant information (i.e. eliminating the points nearer using the Euclidean distance). As a second outlined contribution, this paper presents a novel Spatial Vector Representation to store the neighborhood eliminated features. Finally, the normalized image obtained through min max [3] performs a fusion template matching by applying Structural Biometric Fusion Template Matching algorithm.

The rest of the paper is organized as follows. Section 2 reviews the related works in the field of multimodal biometric authentication. Section 3 overviews the method of Fusion based Multimodal Biometric Security (FMBS) and goes through details about the method of biometric authentication system on social network and performance measures. Section 4 presents our experimental design, data collection, and experimental results. The performance of the system based on the proposed method is also evaluated. Section 5 concludes our research.

2. RELATED WORKS
In recent years, multimodal biometrics for social network has been an active research area and successfully applied in practice. Few research efforts have thus far been dedicated to address the problem of biometric authentication using multimodal behavioral aspects ensuring security. An adaptive intrusion detection framework [8] used multimodal behavioral models to improve the network detection rate. However, security remained a major concern. To address security in social network, multimodal biometric system based on palmprint and finger knuckle was designed in [9]. A biometric authentication system with the objective of providing security to the sites was designed in [10]. Cryptographic level fusion [11] was applied using K-Means algorithm to improve overall authentication and security via fingerprint, knuckle and iris images.

In recent years, theories of Sparse Representation (SR) have emerged as powerful methods for efficient data processing and securing in the social network. In [12], sparse representation that used correlations and coupling information was investigated for multimodal biometrics recognition.

However, anomaly detection remained unsolved. To address this issue, Collaborative Information Systems (CIS) [13] was deployed in social network to detect insider threats based on the access logs. In [14], another face recognition model was designed using demographic attributes that resulted in the accuracy of intruders being detected. A comprehensive study on recognition of facial expression using local binary patterns was presented in [15]. One of the important sources of forensic evidence is obtaining latent fingerprints where automatic matching of latent fingerprints plays a significant role in social networks. In [16], in order to refine the features extracted, top-down information was used to improve the identification accuracy. However, security with respect to increase in the features remained greater concern. In [17], to provide security, fingerprint-based crypto-biometric system was designed with concatenation-based feature level fusion technique to ensure secured transmissions of data. Another fusion based model using face and fingerprint was presented in [18] for robust recognition system. A robust multimodal face and fingerprint fusion was investigated in [19] to mitigate against anti spoofing attacks. With the objective of ensuring continuous authentication, behavioral biometrics [20] was studied with respect to intruder detection time, however compromising rate of accuracy.

Reported work in the literature shows that collaborative Face Recognition [1] can have a positive impact on online social networks. However, the collaborative Face Recognition using multiple FR engines perform well for personal photo collection, they perform poorly with multimodal biometrics. This happens mainly due to the fact that these algorithms were not designed to work well with other features other than the face annotation. Also, the lack of publicly available multimodal datasets is another challenge that needs to be overcome in the future. Multimedia fingerprinting using game theoretic strategies and equilibriums though studies the time sensitive bargaining equilibrium are geometrically normalized as a non-cooperative game, the method cannot be used due to the effect that the users either behave in an honest or semi honest manner. Therefore, an efficient multimodal biometric system needs to be designed, developed, and applied to reduce the social network authentication time and space complexity in social networks. The following section explains the proposed method in detail.

3. MULTIMODAL BIOMETRICS USER AUTHENTICATION

A Fusion based Multimodal Biometric Security (FMBS) method of human individuals is introduced by extracting the face and fingerprint features to the social network domain area. Our proposed method for social networks communication consists of three main modules: feature extraction through binomial feature distribution, fusion using spatial vector representation and template matching using a biometric fusion template matching algorithm as shown in fig 1.

3.1 System model for Multimodal Biometrics User Authentication

Let us consider a social network communication system model of 'n' users where '$n = 100\,users$' and let '$\varphi^1, \varphi^2, \dots, \varphi^n$' denotes the templates of the '$n\,users$' in a biometric system. Let us further assume that 'n' user communicate with each other in social network settings to create, share or exchange information (Facebook, Twitter, Instagram, etc) with each enrolled user possessing only one template stored in the biometric system. Hence, the '$ith\ user$' template is of the form '$\varphi^i = \{\varphi_1^i, \varphi_2^i\}$' comprising of two elements, where 'φ_1^i, φ_2^i' are the templates for face and fingerprint respectively. Our problem is then defined as follows: Given a social network setting with an assumption of '$100\ users$' behaving in an honest manner where '$20\ users$' are considered as malicious user behavior who behaves in a semi-honest manner. The objective lies in designing a model where a matcher is introduced to detect the misbehavior of users in social networks using multi modal (i.e. face and fingerprint features of human individuals) biometric system. Fig.1. shows the block diagram of Fusion based Multimodal Biometric Security method to be followed on social network with Face, and Fingerprint features of human individuals.

As shown in the figure, in order to establish the social network communication, three steps are followed in Fusion-based Multimodal Biometric Security (FMBS). In the first module, preprocessing of face/fingerprint images is performed to extract the vital portion using Neighborhood Dominant Attribute Identification for both face and fingerprint features. The second module performs the fusion process to combine face and fingerprint features. Dominant attributes are stored in a spatial vector for both the modalities and form biometric fusion template (i.e. fingerprint abstraction and face abstraction) of the human individuals.

The third module carries out fusion template matching. At this stage, with preprocessed face/fingerprint images of users (social media), process of fusion template matching is performed to find the matching accuracy. A Structural Biometric Fusion Template Matching algorithm is developed to find the matching accuracy of test data to the available training data (i.e. from fusion templates) extracted from the benchmark/real dataset. With successful matching of the test and trained dataset (obtained from fusion template), efficient social network communication takes place. On the other hand, no communication takes place between the users upon unsuccessful matching.

3.2 Binomial Feature Distribution

To start with the process, the FMBS method initially extracts the user's features entering into the social media (Facebook, Twitter, Instagram, etc). Binomial Feature Distribution Algorithm (BFDA) extracts the features via Neighborhood Dominant Attribute Identification for both face and fingerprint features by matching their neighborhood structures. Preprocessing of features is highly required for better identification result. Fig.2. shows the structure of binomial feature distribution for fingerprint and face image. The first step in the design of the proposed method is to preprocess the multimodal features by identifying the dominant attributes of both face and fingerprint features. The proposed method uses Neighborhood Dominant Attribute Identification for both the face and fingerprint features.

3.2.1 Fingerprint Feature Extraction

To register fingerprint features, a unique ID is generated for each user represented by 'ID_u', for a user 'u'. In a similar manner any number of users registers their fingerprint in the biometric system and obtains a unique ID. In a similar manner, multiple fingerprint impressions of the same user are obtained and stored in '$FP_i\ , where\ i = 1, 2, \dots, n$', and '$n$' symbolizes the number of fingerprint impressions for user 'i'. Fingerprint feature extraction in the proposed method is performed using the minutia features [9]. A minutia for fingerprint impression is denoted as given below.

$$M = (A, B, \theta) \qquad (1)$$

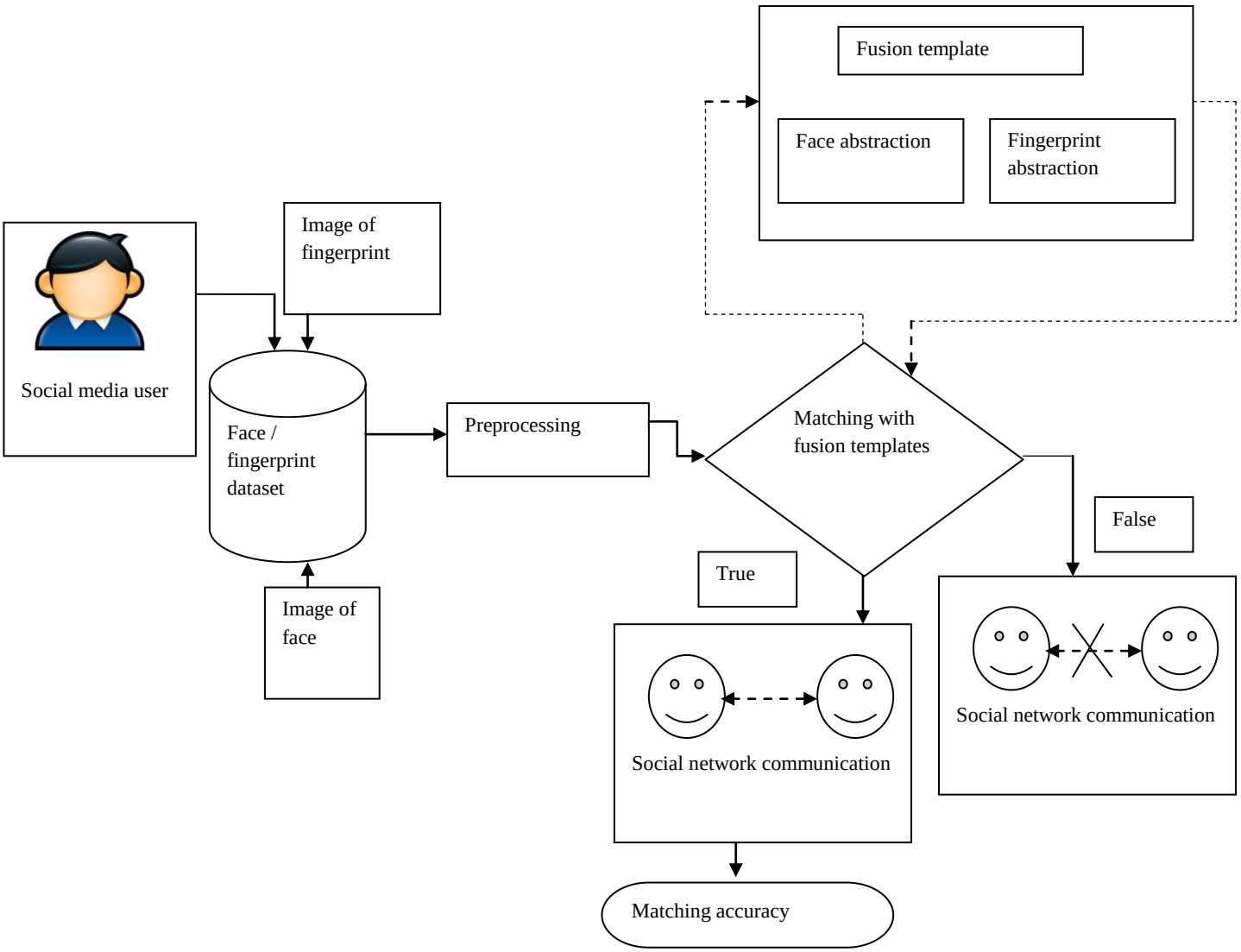

Fig.1. Block diagram of Fusion-based Multimodal Biometric Security method

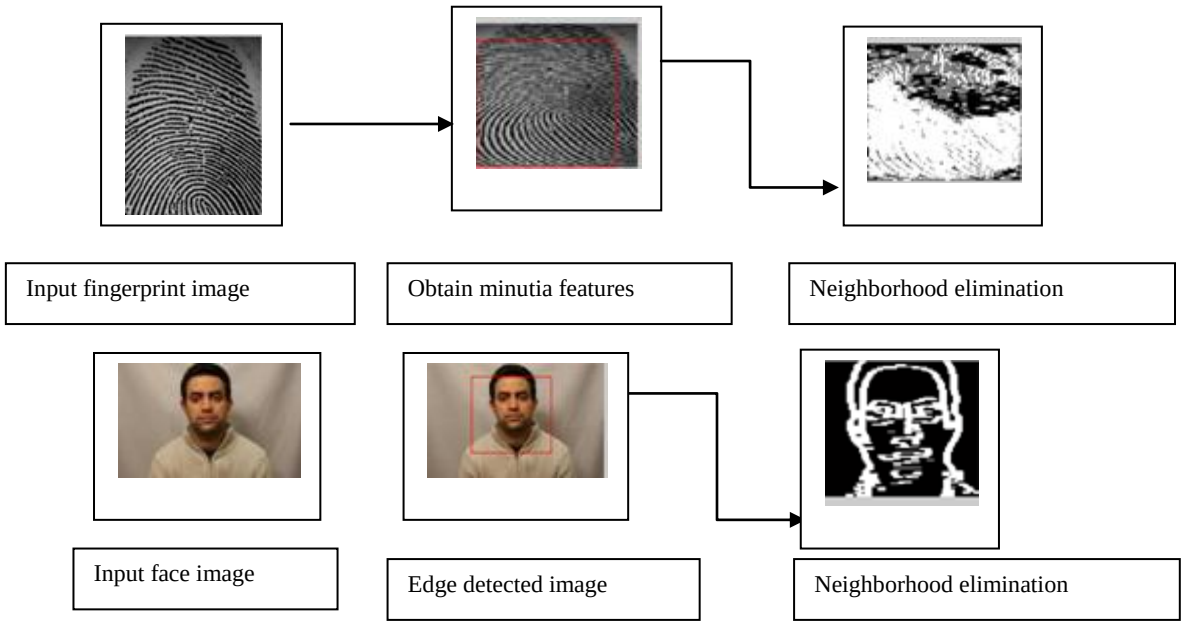

Fig.2. Binomial feature distributions

From (1), 'M'represent the minutia with 'A, B' symbolizing the locations where orientation is denoted as 'θ'. In a similar manner, for each fingerprint impression, features are generated as given below

$$M_i = M_1, M_2, \dots, M_n \quad (2)$$

From (2), 'n' denotes the total minutia in a fingerprint impression that is called as the normalized fingerprint impression. Once the normalized fingerprint impression is obtained, the proposed method uses Neighborhood Dominant Attribute Identification to remove redundant information. The objective behind the application of Neighborhood Dominant Attribute Identification is not only to eliminate redundant information but also retain the most vital information. The points are eliminated which are very near using the Euclidean distance, to a specific point. Another factor is that because of being in vicinity, these redundant points do not provide any additional information. So, the purpose behind applying Neighborhood Dominant Attribute Identification is to take into consideration only those points that belong to highly unique region. The Euclidean distance [4] between minutia '$M_i = (A_i, B_i, \theta)$' and '$M_j = (A_j, B_j, \theta)$' is given as below.

$$Dis\,(M_i, M_j) = \sqrt{(A_i - A_j)^2 + (B_i - B_j)^2} \quad (3)$$

Once the distance between minutiae is obtained using (3), Neighborhood Dominant Attribute Identification is applied to the resultant value. Let us assume the fingerprint threshold be considered as 'FP_t'. Two minutia of a user are considered neighbors if the Euclidean distance between them is less than or equal to 'FP_t'. That is, for each fingerprint impression, those impression are considered to be neighbors that lie within the neighborhood of a limit or if the Euclidean distance (obtained from) between them is less than or equal to 'FP_t'. So, the fingerprint impression lying within the neighbors are removed giving 'M_i^{red}', the reduced fingerprint impression and is formulated as given below.

$$Dis\,(M_i, M_j) \le FP_t \rightarrow redundant\ information \quad (4)$$

$$Dis\,(M_i, M_j) \ge FP_t\ store\ the\ information\ in\ M_i^{red}(FP_i) \quad (5)$$

From (4) and (5), if the distance between the minutiae is less than the fingerprint threshold value, then it is considered as redundant information and eliminated. On the other hand, if the distance is greater than the fingerprint threshold, then the resultant information is stored as reduced fingerprint impression.

3.2.2 Face feature extraction

Face feature extraction is considered to be a tedious process, due to environment change, light effects, varied face expressions and poses of the face. In order to extract the inherent face features, initially edge is detected and histogram equalization is applied to the detected edge and finally Neighborhood Dominant Attribute Identification is applied to remove the noise present in the face. Let the face be denoted as '$F(A, B)$' with size of the face represented by '$M * N$' rows and columns respectively and let us split the whole face into 'C' columns.

$$I = (F_1, F_2, \dots, F_C) \quad (6)$$

Now edge detection [6] for the input face 'I' is given as below.

$$D = \sum_{i=1}^{C} I_i \quad (7)$$

From (7), 'D' symbolizes the edge direction, and to which Histogram Equalization is applied to normalize face. The mean estimation of inter 'H_w' and intra class 'H_b' of histogram equalization is obtained as given below.

$$H_w = (a - f_i)\, h\, (a - f_i) \quad (8)$$

$$H_b = n_i(f - n)(f_i - f) \quad (9)$$

Where '$f_i = \frac{1}{n_i} \sum f$' is the mean of the '$ith\ class$' of face image '$f_i$' and '$f = \frac{1}{n} \sum f$ ' is the global mean of the overall face image 'f'. Though histogram equalization for face feature extraction is highly reliable, the actual density value of the face is eradicated during inter and intra class mean estimation, resulting in certain amount of noise. In this paper, Neighborhood Dominant Attribute Identification is proposed which handles produced noise with highest recognition rate and is formulated as given below.

$$F_{red} = f_i(M, N)\, red(a - M, b - N) \quad (10)$$

From (10), the face reduced image with redundant information is removed. Here, '$F_{red} = f_i(M, N)$' represents the actual face image with '$M * N$' rows and columns and '$F_{red}\,(a, b)$' is the reduced face image obtained where 'red' shows the interpolation for reduced face image, '$(M, N), (a, b)$ ' represents the points of original face image and interpolated reduced face image respectively. Algorithm 1 summarizes the process followed by the Binomial Feature Distribution.

Algorithm 1: Binomial Feature Distribution

Input: User 'u', ID for a user 'ID_u', Fingerprint Impression 'FP_i', face '$F(A, B)$'

Output: Optimal features extracted

Begin

For each user 'u'

Provide with unique ID

Obtain multiple fingerprint impressions

Obtain minutia using (1)

Obtain normalized fingerprint impression using (2)

Measure Euclidean distance between minutia using (3)

Measure reduced fingerprint impression using (5)

If '$Dis\,(M_i, M_j) \le FP_t$ '

Eliminate the redundant information

Else

Store the information in $M_i^{red}(FP_i)$

End if

Perform edge detection for the input face 'I' using (7)

Perform inter class 'H_w' mean estimation using (8)

Perform intra class 'H_b' mean estimation using (9)

Obtain reduced face image using (10)

End for

End

As shown in the above algorithm, the BFDA performs feature extraction with the aid of Neighborhood Dominant Attribute Identification for both the face and fingerprint features. The proposed method by applying neighborhood attribute investigates the effect of biometric user authentication scheme with multi-modalities (i.e. using fingerprint and face features) for secured and reliable social network communication.

3.3 Spatial vector representation

As mentioned in the first section, the features obtained by applying Neighborhood Dominant Attribute Identification for both the fingerprint and face has to be combined to create a joint feature vector. Thus vector representation is used to create a joint feature vector, which then forms the basis for the matching process. One of the main problems while creating a joint feature vector during fusion process is the formation of very high dimensional feature vector. In this work, dominant attributes are stored in a spatial vector for both the modalities integrating fingerprint and face forms biometric fusion template of the human individuals.

Let '$P = p_1, p_2, \dots, p_m$' and '$Q = q_1, q_2, \dots, q_n$' represents the spatial vector representing information extracted from two different modalities namely, fingerprint and face respectively. In order to obtain the new feature vector 'R', vectors 'P' and 'Q' are enlarged. With the resultant enlarged value, feature selection is performed on the resultant vector 'R' with the objective of reducing the dimensionality.

The individual fingerprint and face values of the vectors 'P' and 'Q' significantly differ in terms of their range. So, to ensure that the resultant feature vectors obtained for both fingerprint and face features are comparable, min max normalization [3] is performed in the proposed method. Let us denote the feature score obtained from fingerprint and face features as 's' from the set of all scores 'S', the corresponding normalized score '$Norm_S$' is as given below.

$$Norm_S = \frac{s - Min\,(S)}{Max\,(S) - Min\,(S)} \qquad (11)$$

Where 'S'comprises of the reduced features of fingerprint and face '$M_i^{red}(FP_i), F_{red}$' respectively. Once the min max normalization is performed, the modified fingerprint and face spatial vectors are denoted as '$P' = p_1', p_2', \dots, p_m'$' and '$Q' = q_1', q_2', \dots., q_n'$' respectively with the resultant vector in the form '$Z' = p_1', p_2', \dots, p_m', q_1', q_2', \dots., q_n'$'. However, by applying min max normalization, the dimensionality of values is large in size. To reduce the dimensionality, the proposed method applies Maximum Relevance Feature Selection [4]. Here, the relevance of a feature set 'FS'for a user 'ID_u' is defined by the average value of all mutual information values between the individual features 'Z''' and the user 'ID_u' as follows:

$$(FS, C) = \frac{1}{|FS|} \sum_{Z' \in FS} (Z', ID_u) \qquad (12)$$

From (12), '$FS \in (P', Q')$', a new feature vector or score '$R = r_1, r_2, \dots., r_o$' is obtained. With the resultant feature vector, matching accuracy of the data is performed which is concentrated in the following section.

3.4 Biometric Fusion Template Matching Algorithm

Finally, with the resultant vector obtained through spatial vector representation, a Biometric Fusion Template Matching algorithm is designed to find the matching accuracy of test data to the available training data. The matching tasks for both modalities (i.e. fingerprint and face) are carried out using Biometric Fusion Template Matching algorithm.

To perform biometric fusion template matching, the proposed method calculates the matching score using the sum rule [18]. The result of the measurement is then compared with an experimental threshold to decide whether or not the two representations (i.e. fingerprint and face) belong to the same user. The fused score '$Fused_{score}$' for fingerprint and face using sum rule is as given below.

$$Fused_{score} = (weight_1 * scores_{FP}) + (weight_2 * scores_F) \qquad (13)$$

Where '$weight_1$' and '$weight_2$' symbolizes the weights assigned to multimodal biometrics fingerprint '$scores_{FP}$' and face '$scores_F$' respectively. These final matching fused scores '$Fused_{score}$' are then compared with a certain threshold to recognize the person as genuine or an impostor. Algorithm 2 summarizes the Biometric Fusion Template Matching.

Algorithm 2: Biometric Fusion Template Matching

Input: User 'u', Fingerprint Impression 'FP_i', face '$F(A, B)$'

Output: Improved matching accuracy

Begin

For each User 'u' provided with Fingerprint Impression 'FP_i' and face '$F(A, B)$'

Extract fingerprint and face features based on Neighborhood Dominant Attribute Identification

Reduced fingerprint and face features are obtained using (5) and (10)

Reduced fingerprint and face features are stored in spatial vectors

Scores obtained are normalized using (11)

Scores are then converted to obtain maximum relevance using (12)

Measure fused score for fingerprint and face using (13)

Compare against a threshold value to recognize user as genuine or an imposte

End for

End

As shown in the above algorithm 2, the fusion template to perform Biometric Fusion Template Matching algorithm includes 100 user's unique face and fingerprint abstraction separately extracted from benchmark/real dataset. Face and fingerprint abstraction includes 100 faces and fingerprints extracted from 100 individual user's and stored as fusion templates forms biometric fusion template matching. The multimodal biometric system for the proposed method is developed by integrating two traits i.e., fingerprint and face. Based on the proximity of feature vector and template, matching score is evaluated. These individual scores are finally combined into a fused score '$Fused_{score}$' to perform efficient matching.

4. EXPERIMENTAL SETTINGS

The experimental evaluation is conducted with Biometric Research Repositories (i.e. Association Biosecure) on the face and fingerprint subcorpora included in the multimodal

Biosecure database with various training and test dataset. The biometric samples are extracted from the BioSecure [21] datasets which are distributed by Association BioSecure. The samples contain data of two persons (male and female). It is publicly available through the BioSecure foundation. The training dataset is of the size 100 face and fingerprint images whereas the test dataset include 35 images of user's face and fingerprint for social network communication. The experiments were implemented in MATLAB. The proposed method is compared with two existing methods namely novel collaborative Face Recognition (FR) [1] and Multimedia Fingerprinting (MF) [2]. Multimodal biometrics user authentication focuses on the aspects of matching accuracy and social network authentication for social network. The proposed method is evaluated in different aspects such as fusion template size, density of human biometric samples, matching accuracy, social network authentication time and space complexity.

4.1 Comparison with the Existing Methods

The main goal of our experiments is to determine the rate of matching accuracy for biometric user authentication using evolutionary algorithms. 35 faces and fingerprint images of the same user were randomly selected out of 100 images. With this experimental setting the rate of matching accuracy is defined as given below. Matching accuracy is one of the performance metrics to measure the accuracy or determine the proportion of the biometric samples that were matched correctly to the density of human biometric samples provided as input during experimentation The matching accuracy 'A' for biometric user authentication on social network of an individual person '$size$' depends on the number of samples correctly matched and is evaluated by the following formula.

$$A = \sum_{size=1}^{n} \frac{Fusion\ template\ correctly\ matched}{u_{size}} * 100 \qquad (14)$$

From (14), the accuracy 'A' is measured with respect to the total number of human biometric samples 'u_{size}' and measured in terms of percentage (%). Table 1 presents the results of matching accuracy and social network space complexity of an exploratory experimentation on BioSecure dataset by presenting the matching accuracy and social network space complexity using FMBS, FR and MF. The experiment was conducted to gain insights on the matching results of the datasets, to measure the performance of matching accuracy, social network space complexity and to measure the effect of multimodality biometric user authentication in social network scenario.

Table 1 Comparison of matching accuracy

Density of human biometric samples	Matching accuracy (%)		
	FMBS	FR	MF
5	91.45	84.89	78.35
10	93.14	86.18	78.10
15	94.28	87.32	79.22
20	89.17	82.21	73.11
25	92.48	85.52	78.42
30	94.29	88.34	80.34
35	95.17	90.21	82.11

As shown in the table above, the matching accuracy and social network space complexity for biometric authentication in social network with density of human biometric samples in the range of 5 to 35 are presented. The decision point of seven different biometric samples (face and fingerprint) was selected in a random manner that achieved a substantial improvement in ratings from the previous decision. The results show better performance of the proposed FMBS method, but however not seen to be linear due to the presence of noise in biometric images. The last values in the table seem to confirm the working hypothesis that the matching accuracy for biometric authentication in social network increases with the increase in the density.

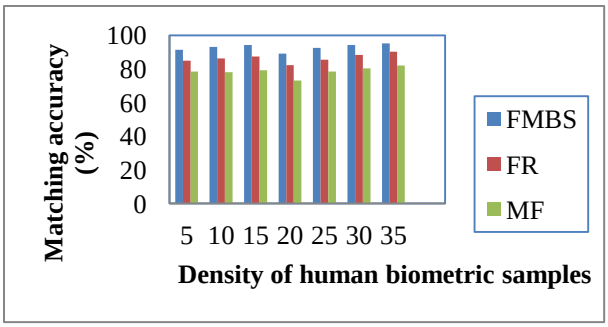

Fig. 3 Measure of matching accuracy

As illustrated in figure 3 when compared to two other methods FR [1] and MF [2], the FMBS method substantially improved the accuracy for biometric authentication using the extensive Biometric Fusion Template Matching algorithm. This is because the FMBS method adapted a dynamic sum rule and the resultant value (fused score) was compared with the threshold to decide upon the factor whether or not the two representations belong to the same user, resulting in the improvement of matching accuracy. Furthermore based on the resultant fused score, to obtain maximum relevance they were converted based on the mutual information values (i.e. face and fingerprint) on social network improves the matching accuracy by 6.98% compared to FR and 15.45% compared to MF.

Table 2 Comparison of social network space complexity

Density of human biometric samples	Social network space complexity (KB)		
	FMBS	FR	MF
5	1954	1996	2018
10	2098	2139	2198
15	2122	2249	2287
20	2015	2085	2105
25	2247	2318	2490
30	2815	3015	3095
35	3125	3248	3398

Next, the second goal of the experiments (Table 2) with respect to social network space complexity showing the comparison between FMBS, FR and MF are defined as follows. Social network space complexity is a measure of the

amount of working storage required to perform biometric template matching (algorithm). In other words, social network space complexity measures the memory required to execute the algorithm at any point.

$$SN_{sc} = u_{size} * Mem\ (Fused_{score}) \qquad (15)$$

From (15), the social network space complexity 'SN_{sc}' is obtained using the density of human biometric samples 'u_{size}' and memory for obtaining fused scores (face and fingerprint). It is measured in terms of Kilo Bytes (KB). For all scenarios as shown in table 1, social network space complexity is increasing with biometric samples considered from different users. Seven unique experiments were conducted for each review size.

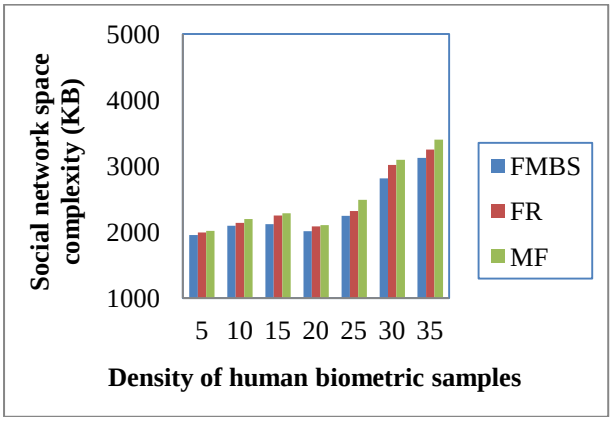

Fig. 4 Measure of Social Network Space Complexity

As shown in fig 4, substantial experimental results to measure social network space complexity versus the density of human biometric samples considered for experimentation. The targeting results of social network space complexity using FMBS method is compared with two state-of-the-art methods [1], [2]. Our method differs from the FR [1] and MF [2] in that spatial vector is incorporated for both the modalities integrating fingerprint and face of the human individuals. Here the dominant attributes are stored using spatial vector representation that reduces the dimensionality factor. With the resultant feature vectors obtained for both fingerprint and face features, min max normalization [3] followed by this Maximum Relevance Feature Selection [4] is applied to the resultant normalized image based on the mutual information of the individual features. This in turn reduces the space complexity arising during social network communications. Therefore the space complexity in social network for biometric authentication using multimodal features (face and fingerprint) is reduced by 3.96% compared to FR and 7.11% compared to MF respectively.

Table 3 Comparison of Social Network Authentication Time

Fusion template size (KB)	Social network authentication time (ms)		
	FMBS	FR	MF
350	708	809	912
700	1120	1230	1290
1050	1250	1360	1405
1400	1304	1414	1498
1750	1298	1398	1425
2100	1308	1418	1739
2450	1315	1425	1510

Finally, to clearly compare the features of both FMBS and existing Face Recognition (FR) [1] and Multimedia Fingerprinting (MF) [2], the social network authentication time (table 3) involved in authenticating the users is defined. The social network authentication time involved during feature extraction is the time required to measure the attributes with respect to the fusion template size and is as given below. It is the product of fusion template size considered and the time taken for feature extraction.

$$SNA_{time} = FT_{size} * Time\ (Att\ identification) \quad (16)$$

Where 'SNA_{time}' is the social network authentication time and 'FT_{size}' refers to the fusion template size considered during each iterations. For all scenarios as shown in table 3, social network space complexity is increasing with biometric samples considered from different users. Seven unique experiments were conducted for each review size.

Finally, to clearly compare the features of both FMBS and existing Face Recognition (FR) [1] and Multimedia Fingerprinting (MF) [2], the social network authentication time (table 3) involved in authenticating the users is defined. The social network authentication time involved during feature extraction is the time required to measure the attributes with respect to the fusion template size and is as given below. It is the product of fusion template size considered and the time taken for feature extraction.

$$SNA_{time} = FT_{size} * Time\ (Att\ identification) \quad (16)$$

Where 'SNA_{time}' is the social network authentication time and 'FT_{size}' refers to the fusion template size considered during each iterations. For all scenarios as shown in table 3, social network space complexity is increasing with biometric samples considered from different users. Seven unique experiments were conducted for each review size.

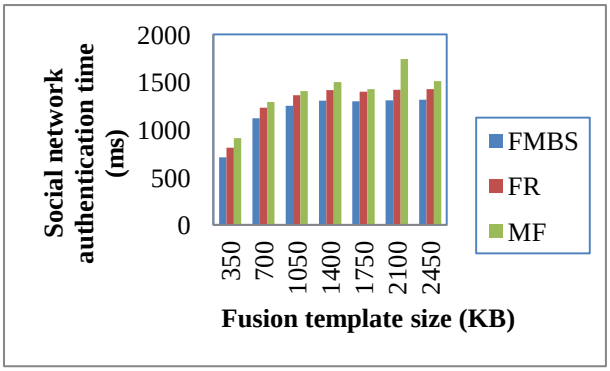

Fig.5. Measure of Social network authentication time

Results are presented for different fusion template sizes (Fig.5.). Higher, the fusion template size, higher the social network authentication time is. This is because with higher fusion template size, the size of individual images grows exponentially, and therefore the authentication time for increased template size also increased. But from the figure it is evident that the social network authentication time is

comparatively observed to be lower using the proposed FMBS method. By applying Neighborhood Dominant Attribute Identification in FMBS method, fingerprint and face images are extracted, comparing their corresponding neighborhood structures. This in turn removes the redundant information present in the fingerprint and face images of a user resulting in minimizing the social network authentication time. The process is repeated with fusion template size of 350KB to 2450KB for conducting experiments. The results reported here confirm that with the increase in the fusion template size, the social network authentication time also increases, though betterment achieved using FMBS method.

As shown in the figure, when compared to two other methods FR [1] and EF [2], the FMBS method had better changes using the extensive Binomial Feature Distribution algorithm. This is because the Binomial Feature Distribution algorithm applied in FMBS method symbolizes the mean estimation of inter and intra class reducing certain amount of noise present in face and fingerprint. This in turn reduces the social network authentication time by 9.40% compared to FR and 18.40% compared to EF.

5. CONCLUSION

One of the complex tasks in social network is user authentication through Biometric due to the intrinsic features of these networks and presence of malicious user. Due to this, a surge to safeguard these social network networks and to propose an efficient method to provide security to the social network users is the need of the hour. In this paper, Fusion based Multimodal Biometric Security (FMBS) method is provided that can be employed as a safe communication method in social networks. Initially, the features were extracted using Binomial Feature Distribution Algorithm for both the face and fingerprint. With the extracted features, dominant attributes were stored in a spatial vector form which resulted in the improvement of social network authentication time for several users. The evaluation of the template matching is performed finally using the Biometric Fusion Template Matching algorithm to authenticate the users in social network. Through the experiments using real traces, we observed that our multimodal biometric authentication method reduced social network authentication time and space complexity compared to the existing biometric authentication methods.

6. REFERENCES

[1] Jae Young Choi, Wesley De Neve, Konstantinos N. Plataniotis and Yong Man Ro, 2011, Collaborative Face Recognition for Improved Face Annotation in Personal Photo Collections Shared on Online Social Networks, IEEE Transactions on Multimedia, 14-28.

[2] W. Sabrina Lin, H. Vicky Zhao, and K. J. Ray Liu, 2011,Game-Theoretic Strategies and Equilibriums in Multimedia Fingerprinting Social Networks, IEEE Transactions on Multimedia,191-205.

[3] M. Indovina, U. Uludag, R. Snelick, A. Mink, A. Jain, 2003, Multimodal Biometric Authentication Methods: A COTS Approach, Workshop on Multimodal User Authentication, 1-8.

[4] Hanchuan Peng, Fuhui Long, and Chris Ding, 2005, Feature Selection Based on Mutual Information: Criteria of Max-Dependency, Max-Relevance, and Min-Redundancy, IEEE Transactions on Pattern Analysis and Machine Intelligence, 1226-1238.

[5] Mohsen Khademi Dehnavi, Neda Peykanpour Fard, 2011, Presenting a multimodal biometric model for tracking the students in virtual classes, Elsevier, Procedia - Social and Behavioral Sciences, 3456–3462.

[6] Hyunsoek Choi and Hyeyoung Park, 2015, A Multimodal User Authentication System Using Faces and Gestures, Hindawi Publishing Corporation, BioMed Research International, 1-9.

[7] JiyunWu and Zhide Chen, 2015, An Implicit Identity Authentication System Considering Changes of Gesture Based on Keystroke Behaviors", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, 1-17.

[8] Ja'far Alqatawna, 2015, An Adaptive Multimodal Biometric Framework for Intrusion Detection in Online Social Networks", IJCSNS International Journal of Computer Science and Network Security, 19-25.

[9] Esther Perumal and Shanmugalakshmi Ramachandran, 2015, A Multimodal Biometric System Based on Palmprint and Finger Knuckle Print Recognition Methods, The International Arab Journal of Information Technology, 118-128.

[10] Asma Kebbeb, Messaoud Mostefai, Fateh Benmerzoug, and Chahir Youssef, 2015, Efficient Multimodal Biometric Database Construction and Protection Schemes, The International Arab Journal of Information Technology, 346-351.

[11] Muthukumar Arunachalam and Kannan Subramanian, 2015 ,AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print, The International Arab Journal of Information Technology, 431-440.

[12] Sumit Shekhar, Vishal M. Patel, Nasser M. Nasrabadi, and Rama Chellappa, 2014, Joint Sparse Representation for Robust Multimodal Biometrics Recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, 113-126.

[13] You Chen, Steve Nyemba, and Bradley Malin, 2012, Detecting Anomalous Insiders in Collaborative Information Systems, IEEE Transactions on Dependable and Secure Computing, 332-344.

[14] Lacey Best-Rowden, Hu Han, Charles Otto, Brendan Klare, and Anil K. Jain, 2012 , Unconstrained Face Recognition: Identifying a Person of Interest from a Media Collection, IEEE Transactions on Information Forensics and Security, 2144-2157.

[15] Caifeng Shan, Shaogang Gong, Peter W. McOwan, 2009, Facial expression recognition based on Local Binary Patterns:A comprehensive study, Elsevier, Image and Vision Computing , 803-816.

[16] Sunpreet S. Arora, Eryun Liu, Kai Cao, and Anil K. Jain, 2014, Latent Fingerprint Matching: Performance Gain via Feedback from Exemplar Prints, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2452-2465.

[17] Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, 2015 , Fingerprint-based crypto-biometric system for network security, Springer, EURASIP Journal on Information Security ,1-17.

[18] Norsalina Hassan, Dzati Athiar Ramli, and Shahrel Azmin Suandi, 2014, Fusion of Face and Fingerprint for Robust Personal Verification System, International Journal of Machine Learning and Computing, 1-5.

[19] PeterWild , PetruRadu, LuluChen, JamesFerryman, 2016, Robust multimodal face and fingerprint fusion in the presence of spoofing attacks, Elsevier, Pattern Recognition, 17–25.

[20] Lex Fridman , Ariel Stolerman , Sayandeep Acharya , Patrick Brennan , Patrick Juola ,Rachel Greenstadt , Moshe Kamd, 2015, Multi-modal decision fusion for continuous authentication, Elsevier, Computers & Electrical Engineering, 142–156.

[21] Ortega-Garcia, J., Fierrez, J., Alonso-Fernandez, F., Galbally, J., Freire, M.R., Gonzalez- Rodriguez, J., Garcia-Mateo, C., Alba-Castro, J.-L., Gonzalez-Agulla, E., Otero- Muras, E., Garcia-Salicetti, S., Allano, L., Ly-Van, B., Dorizzi, B., Kittler, J., Bourlai, T., Poh, N., Deravi, F., Ng, M.W.R., Fairhurst, M., Hennebert, J., Humm, A., Tistarelli, M., Brodo, L., Richiardi, J., Drygajlo, A., Ganster, H., Sukno, F.M., Pavani, S.-K., Frangi, A., Akarun, L., Savran, A, 2010, The multi-scenario multi environment BioSecure multimodal database (BMDB)", IEEE Transactions on Pattern Analysis and Machine Intelligence 32, 1097–1111.