Cancelable Face Template Protection using Transform Features for Cyberworld Security

Firdous Kausar
Electrical and Computer Engineering Department
College of Engineering, Sultan Qaboos University
Muscat, Oman

***Abstract*—Cyber world becomes a fundamental and vital component of the physical world with the increase of dependence on internet-connected devices in industry and government organizations. Provision of privacy and security of users during online communication offers unique cybersecurity challenges for industry and government. Intrusion is one of the crucial issues of cybersecurity, which can be overcome by providing the vigorous authentication solutions. Biometrics authentication is used in different cybersecurity systems for user authentication purpose. The cancelable biometric is a solution to rid of privacy problems in traditional biometric systems. This paper purposes a new cancelable face authentication method, which uses Hybrid Gabor PCA (HGPCA) descriptor for cyberworld security. The proposed method uses the wavelet transform for the extraction of the features of the face images by using Gabor filter and Principal Component Analysis (PCA). Later, both types of features have been ensemble by using the simple concatenation scheme. Then scrambling has been applied to the fused features by using the random key generated by the user. So finally, scrambled fused features has been stored in the database which are used for the cancelable biometric authentication as well as recovery. HGPCA achieves "cancelability" and increases the authentication accuracy. The proposed method has been tested on three standard face datasets. Experimental results of the proposed method have been compared with existing methods by using standard quantitative measures that show superiority over existing methods.**

Keywords*—Cancelable biometrics; face authentication; feature extraction; Gabor filter; Principal Component Analysis (PCA); wavelet transformation

I. Introduction

The number of internet connected devices will reach to 75.44 billion worldwide by 2025 [1] which intensify the risk of cybersecurity breaches such as identity theft, stealing or manipulation of data, credit card frauds, cyber bullying, ransomware and cyberterrorism. Cyber attacks are growing and evolving in prominence every day, causing major damages to industry and government. Most of cyberattacks can be combated by identifying the intruders with proper user authentication. Biometric authentication is considered as one of the most effective user authentication method in cyberworld applications. The biometric can be defined as computerized identification of behavioral or physical uniqueness (e.g. face, gait, fingerprint, voice, iris, etc.) of any person and it must fulfill the standards of universality, uniqueness, collectability, acceptability, and permanence [25]. Currently the existing systems of biometrics (Fig. 1) require further information for some comparisons for generating the templates. The templates generated by biometric systems contain same characteristics across the databases. For example, if some minutiae based system extract the minutia sets of face, these remain similar in different systems.

The biometric data has constant association with specific users, which creates a critical problem. In case of biometric data is compromised from a database by un-authorized users, the original owner of his/her data lose control forever and lose the identity. This makes the biometric templates stand out as a vulnerability of the authentication system because the templates in all databases of related applications have identical characteristics and using similar algorithms. If in one application, a template is compromised, it can be accessed in another application. Further, it is possible, the stored features of templates can be used for the creation of replica demonstration of biometric attributes and can be easily used to access the system. A replica face can be developed from a face template. The compromised biometric template cannot be reissued and discarded. To control this critical problem, the templates are replaced with some biometric features because a person has a specific amount of biometric characteristics. Further, in case the biometric templates are stolen, the attackers can easily attack some other authentication applications which are using the same biometric templates. Due to a person's physical features, the biometric characteristics cannot be effortlessly changed just like keys and passwords [2,3].

The authentication system has vulnerable properties for the biometric templates stored in the databases. The biometric templates in the database have the following risks due to the successful attacks:

1) The attacker can replace the biometric template by an imposter's template for gaining an unauthorized access.

2) The access can be got to the system(s) as per same biometric trait by creating a physical fake from the template available in the database.

3) The attacker can replay the stolen template to the counterpart for gaining the unlawful access.

Therefore, keeping in view the above serious issues, the cancelable biometric has become a prerequisite and has been presented to improve the security of biometric templates. The cancelable biometrics add some additions or alteration to the templates keeping with original biometric data for identification process. If some sets of biometric templates are

compromised, these can be easily removed and new biometric templates can be added to the database. The biometric templates can be protected with following properties:

- Template Diversity: It is very necessary that the different templates of a specific user must be used for different applications and should not match each other. The template diversity property should contain the privacy of the data of the user and it shouldn't allow the cross matching between more than one database.
- Template Revocability: The specific template can be easily revoked if it is compromised. In the place of compromised template, the new template can be issued to the user by using the same biometric. It is very important to remember that the new template must not be matched with compromised template. The revocability property mean to cancel the old compromised template, issue the new one template and as well as to cancel the authentication rights of old authenticator associated with compromised template.
- Template Security: The template security property protects the privacy of the biometric data. It must be impossible to get the original biometric template from the secured template. This property should ensure the physical deceiving of biometric and it cannot be theft the template.
- Performance of the System: The system should ensure the identity of the user with high level of confidence. The system should resist the denial attempts. The performance of the system should not be degraded in case of replacement of the templates.

This paper proposed a hybrid rotation invariant features based on random key for face authentication. The scrambling has been applied on hybrid features to secure templates and hybrid rotation invariant features has been selected by applying Gabor and Wavelet Transform based principle component analysis. The paper is structured as follows: in Section 2 (related work), we explained the current developments in the cancelable biometrics field. In Section 3, we applied the Discrete Wavelet Transform on original images for extraction the features by using the Gabor filter and PCA. After extraction of the Gabor and PCA features, we did the fusion of Gabor and PCA features, scrambled the coefficient vectors, and normalized the features and feature matching. In Section 4, there is results and discussion. Finally, the conclusions and perspectives are given in Section 5.

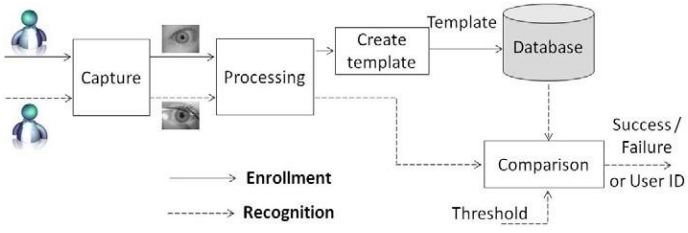


Fig. 1. Architecture of Cancelable Biometric System.

II. Related Work

Cancellable biometric consists in applying an intentional irreversible transformation on the biometric feature, then storing the distorted template in the database. This provides an individual with different biometric templates for different application. Ratha et al. presented the principle of cancelable biometrics in [25]. Lots of solutions can be found in the literature regarding cancelable biometric systems. These systems use some transformation process on the biometric data.

Cancellable multi-biometric approach was investigated in [2]. Multi-biometric is the fusion of different types of biometric information. The main goal of using a multi-biometric is to overcome the limitations such as the non-universality on unimodal biometric systems. Securing distinctive formats of a user independently is not empowering approach in term of security. Therefore, cancellable multi-biometric was designed in a manner to produce a single feature from a mixture of biometric features by applying an irreversible mixture transform. A multi-biometric approach using fuzzy vault scheme was designed and developed in [3] by Nandakumar et al. Their technique was based on two main steps. First, they use an individual template to derive a single multi-biometric template. Securing distinctive formats of a user independently is not empowering approach in term of security. They demonstrated that multi-biometric gives better acknowledgment execution and higher security in contrast with a solitary biometric fault. They have based their experimental tests multi-biometrics vaults on fingerprint and iris.

In [2] Genetic algorithms are applied for multi-biometric cancellable identification. The proposed system was tested via two different biometric face, modalities and voice separately. Use of genetic algorithms shows certain flexibility, since they involved in different part of a biometric authentication system. For more proficiency in their work they connected an upgraded framework in light of the primary combination association to consolidate the diverse data sources. For the transformation methods, we cite BioHashing of Jin et al. [4], in which proposed a two component authenticator in light of the cycle of the inward items between a pseudo-irregular number and the individual unique mark include. The BioHashing provide zero false accept rates.

Connie et al. [5] produce unique palmhash code by applying the hash function on a combination of the palmprint feature and a set of pseudo randomly generated keys. The use of pseudo random keys in the process of generating palmhash code can produce several sets of palmhash codes to be used in multiple applications. It also helps in revocation of biometric keys. Non-invertible property of the palmhash codes make it feasible to be stored in tokens and smartcards for authentication purpose without the threat of retrieving original biometric template from it.

Savvides et al. [6] propose a method to generate cancelable face biometrics by encrypting the biometric template using random convolution kernels. The minimum average correlation energy (MACE) sort relationship channels are utilized to produce the single biometric channel from these convolved encoded formats. The biometric layout can be effortlessly

repudiated or re-issued by utilizing diverse arbitrary convolution piece.

Boult et al. [7] use fingerprints template to generate cryptographically secure biotokens. Keeping in mind the end goal to upgrade security in biometric frameworks, biotokens, which they allude to as Biotope™, are embraced to existing acknowledgment plans. Wei-jing et al. [8] presented a strategy to produce particulars dispersion based cancelable unique finger impression layout known as multi-line codes. A multi-line code is created by speaking to the unique mark layout as a number string which is made out of various exceptionally composed minutia codes. The performance of this scheme is ideal with zero percent of equal error rate (EER) as long as secret key remain secure, however accuracy of system deteriorates considerably in the case of a compromise of secret key.

Christian et al. [9] perform score fusion based comparison during the feature alignment process of cancelable iris biometric templates. A biometric framework is upgraded with score level combination by consolidating the correlation scores of numerous comparators. This method also improves the overall accuracy by overcoming the unavoidable degradation in the accuracy of these systems caused by cancelable iris biometric systems.

Marta et al. [10] propose a method to generate non-invertible face templates established on the adaptive bloom-filters. Gabor-based features are extracted from the face image after preprocess it. These extracted features are encoded and binarized. Then binarized features are used to compute Bloom filters which are compared to a reference template in order to calculate the final scores for comparison with a threshold value. Faster authentication is achieved because of the reduced size of templates generated by using bloom filters.

Salman et al. [11] propose a two-factor authentication system consist of password and handwritten signature. The secure biometric templates are generated by applying random projections to signatures templates using secure random keys which are derived from user entered passwords. These irreversible secure biometric templates can be stored in portable devices to provide user authentication for different applications.

Kanagalakshmi et al. [12] presents another method comprising of building distinctive stages, for example, preprocessing, details extraction, post preparing and cancelable and unavoidable layout era. A cancelable format is created utilizing biometrics unique mark highlights. The new technique is tried in view of numerous angles, for example, cancelability, unavoidability and security. Some execution components were utilized also like coordinating time and layout memory utilization. The trial comes about demonstrate that the proposed RMCCP change strategy plays out a decent execution.

Radha et al. [13] introduced the new technique for biometric analysis called BioHashing to generate the cancellable biometrics by using the fingerprints. The advantage of this method is that it does not involve any re-alignment of fingerprints similar to other techniques. The fingerprint translated into pre-defined two dimensional space. Then the Biohashing method is used to achieve the one-way property of the biometric template. This method is highly resistant to any negligible translation error and rotation distortion. The obtained result shows an Equal Error Rate (EER) of less than1%.

Polash et al. [14] presented the cancellable biometrics system, which based on transforming biometric data and feature in order to achieve cancelability. This technique is based on three main steps. The first step consists of performing a twofold random selection of the signals. The got overlap is then anticipated arbitrarily utilizing a projection strategy. Second step comprises of decreasing the element measurement of the arbitrarily anticipated folds utilizing the Principal Components Analysis (PCA). Creating a single template for face biometrics, using K-mean clustering for dimension reduction. Finally, a Linear Discriminant is used to the feature in order to enhance discriminability. The obtained feature is then passed through a classifier to acquire the ultimate authentication performance.

Dwivedip et al. [15] exploit the concept of randomized look-up table mapping for the generation of cancelable iris template. After pre-processing of iris images, the feature vectors are generated in binary matrix form using a 1-D Log Gabor filter. Decimal vectors are generated by using consistent bit vector and perform the decimal encoding. Finally, the cancelable templates are generated by using the lookup table and decimal encoded vector. Experiment results carried on different iris dataset shows that it preserves the transformation properties of the concealable iris templates.

Sree et al. [16] utilized the fluffy vault to create cancellable multimodal biometric layout for face and fingerprints. The details highlight from unique mark are separated by utilizing the crossing number idea and the nearby double example calculation is utilized to extricate the face elements and both are consolidated by highlight level combination. Fluffy vault is made by including copy values and having a mystery key to bolt and open the framework. Execution examination demonstrates that the fluffy vault enhances the execution of the cancelable authentication framework.

Edlira et al. [17] proposed the biometric format assurance conspire by utilizing sprout channels and the idea of engineered layouts, keeping in mind the end goal to delude aggressors called nectar formats. From the input biometric template, feature vector is extracted, then the feature re-arrangement is done by structure-preserving and finally the bloom filter computation is performed on it. The proposed scheme is implemented by conducting experiments on facial authentication. The analysis shows that it achieves the properties of unlinkability, irreversibility and detection of stolen templates of a cancelable biometric system, but it needs to improve templates indistinguishability, pseudonymity, and unobservability. Rathgeb et al. [18,19] propose cancelable biometric template protection schemes based on bloom filter. Binary Feature vectors are extracted from different Iris authentication systems and then transform is applied based on the generic adaptive Bloom filter. Analysis results show that it provides the properties of irreversibility and unlinkability of

biometric templates. Further, a high level of security with acceptable authentication rate can be achieved by using the rotation-invariant Bloom filter-based transform.

Jin et al. [20] combines the notion of biometric cryptosystem and cancellable biometrics, and present a key binding scheme for minutiae-based fingerprint bio-metrics. They exploit the idea of chaffing and winnowing (CWS) [21] to confuse the eavesdropper in order to distinguish between real and bogus data and provide confidentiality without using encryption which actually reduces the overall performance of the system.

Yang et al. [26] propose a multimodal cancelable biometric system based on fingerprint and fingervein by using enhanced partial discrete Fourier transform. They design feature level fusion scheme with three different fusion options and provide revocability and irreversibility. Murakami et.al [27] presents the permutation based indexing search scheme for generating cancelable templates. They applied their scheme on face, finger and finger vein datasets to show its performance. The finger vein based templates outperform in term of accuracy as compared to face and finger based templates. Another approach to non-invertible and revocable cancelable face template generation is presented by Wang et al. [28] in which extracted face features are applied repeatedly with random orthonormal transformation (ROT) to generate the cancelable face template. It does not perform well in case of stolen key scenario.

III. Proposed Method

After Keeping in mind the end goal to accomplish the specified cancelable biometric prerequisites, we proposed a Hybrid Gabor PCA (HGPCA) based feature descriptor for cancelable biometric authentication. Fig. 2 demonstrates a general overview of the proposed cancelable biometric framework. The proposed method has been divided into two different phases known as an enrollment and authentication process.

During the enrollment process, the image of a face is captured and feature extraction process has been performed to extract rotation scale invariant features. For features extraction, we have extracted two different types of features by using Gabor filter and wavelet based PCA features and combined. Then these hybrid features have been scrambled by using random key to protect the face template and normalization has been applied to the scrambled features. These features are stored as templates in the database for authentication. If a specific image is compromised, it can be changed by creating a new template. Finally, these features can be used for the authentication process.

During the authentication process, the same steps are performed on the unknown test face image. In this process, first features extraction is performed, then key based scrambling is performed. From that point onward, by using some matching measures, the features compare with the features stored in the database. Detail of the process has been given below step by step.

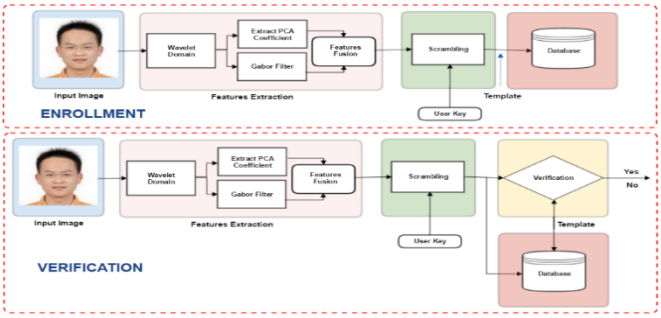


Fig. 2. Block Diagram of Proposed Method.

A. PCA Feature Extraction using Discrete Wavelet Transform (DWT)

First the face image is applied with 2D-DWT, which reduces its dimensionality and is helpful in reducing computational overhead. Further, it also provides the multi-resolution data approximation and insensitive feature extraction, which is desirable for security sensitive applications, and transform domain. Then the 2D matrices of face image are converted into 1D image vector for face authentication techniques based on PCA. High-dimensional image vector space is produced by the 1D image vector. The large size and less number of training samples of this high-dimensional image vector space makes the evaluation of covariance matrix more hard.

1) Discrete Wavelet Transform (DWT)): DWT is applied on 1D image vector. The image is passed over a sequence of filter bank stages in order to create its wavelet transform. Afterwards, down sampled is performed in the horizontal direction on these filtered outputs by a factor of 2. Then an identical filtered pair is applied in the vertical direction on each of these signals. We use the symbol of LL, HL, LH and HH to represent the image after decomposition into 4 sub-bands. The unique image characteristics are represented by these sub-bands and are considered as a tinier version of the image. Workflow of DWT is shown in Fig. 3.

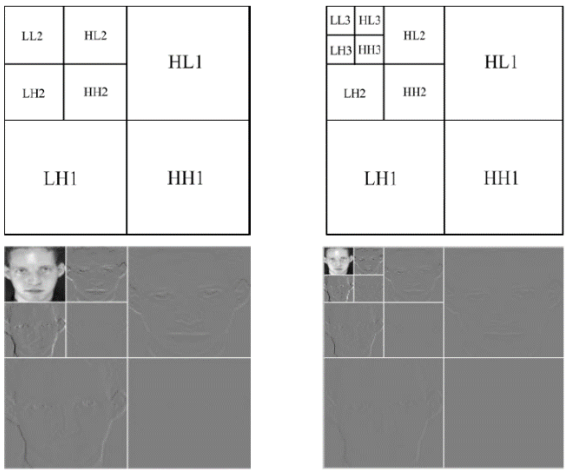


Fig. 3. Wavelet Transform Process.

After applying a 1-level DWT on an image, we get the approximation sub-band LL, the horizontal sub-band LH, the vertical sub-band HL, and the diagonal sub-band HH. Moreover, if we apply a 2-level DWT on the image, we just simply apply another 1-level DWT on the approximation sub-band LL. After applying a 2-level DWT, we also get the approximation sub-band LL2, the horizontal sub-band LH2, the vertical sub-band HL2, and the diagonal sub-band HH2 of the approximation sub-band LL other than sub-bands LH, HL, HH. Applying IDWT to LL, HL, LH, and HH, we get four different frequency's images that are low frequency image, middle-low frequency image, middle high frequency image, high frequency image separately. In this paper, we also apply 2-level DWT so that image dimensions can be reduced. For features extraction, we use the approximation component.

2) Principal Component Analysis (PCA): Although, DWT also reduced the dimensions, but still it has bigger dimensions. We have an image of 256x256 dimensions, then after applying 2D-level, we get an image of 64x64=4096 features that is huge to use for security applications. Therefore, we have used PCA to reduce it further with only significant features. In our proposed enrollment phase, 2-D wavelet is applied at suitable LL subband and then applied 2DPCA to extract most suitable features. During authentication a face image, 2-D wavelet decomposition is applied till specific level and then 2DPCA is applied to extract the features of the face. The Euclidian distance is measured between the mean values of authenticated image and enrollment image in each class to recognize the face.

B. Gabor Filter

We use the Log-Gabor filters (Field, 1987) in our proposed method instead of Gabor (1946) because it is more appropriate for natural image coding as it is more uniform for human visual system quantities. A set of Gabor wavelets is convolved with the input face image. The resulting images are then utilized to extract feature, which produce the salient representation. We illustrate the example of this process in Fig. 4. The original face image shown in Fig. 4(a) is convolved with the Gabor wavelets set of size 4 × 8 shown in Fig. 4(b). Gabor wavelets are used to extract the rotation invariant texture features where we calculated the mean and variance of the Gabor filtered images to find these features. An image feature is used to produce the feature vector.

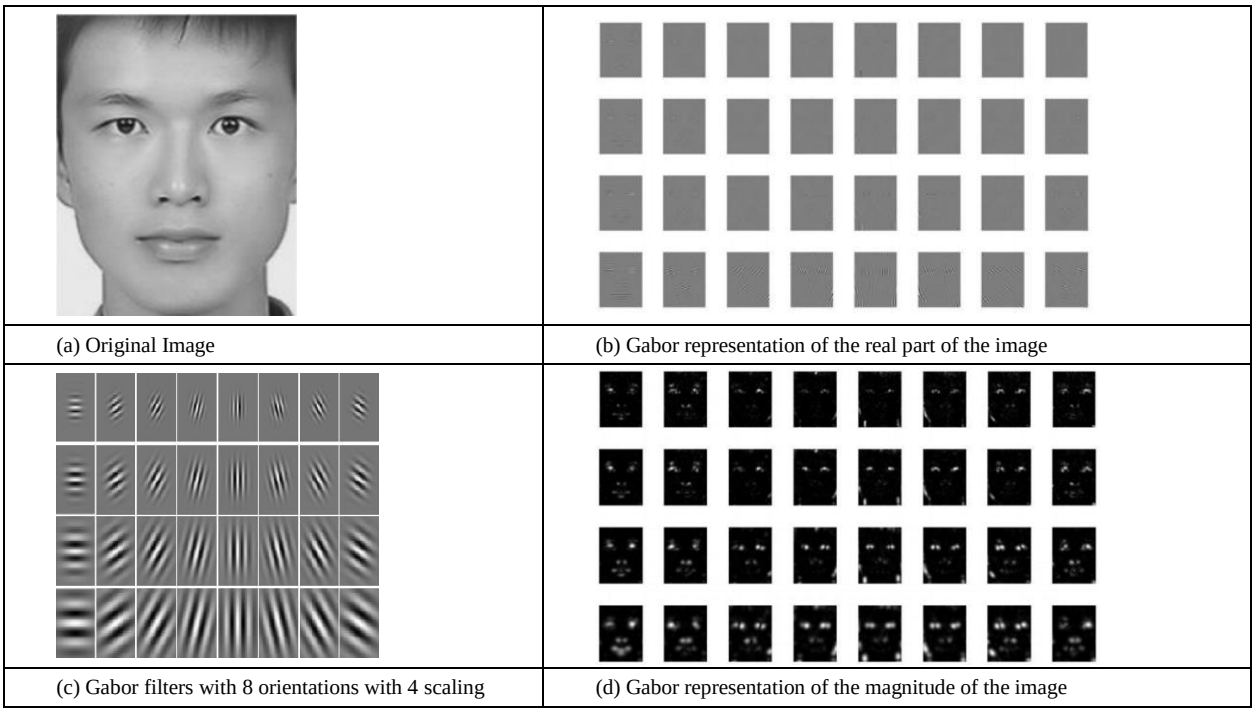
C. Fusion of Gabor and PCA Features

In the previous section, we have extracted Gabor features and wavelet based PCA features. In this section, we have to combine both these types of features. The process of fusion is depicted in Fig. 5. We use a simple process to combine both feature types. We concatenate both types of features and use to store in the database for training and later used for authentication purpose.

GPCA = {Gabor Features, PCA Features}

D. Scrambling the Coefficient Vectors

During the scrambling phase, a random scrambled function depends on the user ID is applied on each weighted coefficient vector. In this scheme, we are using two scrambling functions naming PCA SID and Gabor ID. The weighted normalized PCA coefficient vector p is scrambled by PCA SID while the weighted normalized Gabor coefficient vector ‘i’ is scrambled by applying Gabor ID.



(a) Original Image

(b) Gabor representation of the real part of the image

(c) Gabor filters with 8 orientations with 4 scaling

(d) Gabor representation of the magnitude of the image

Fig. 4. Gabor Wavelet Representation of a Face Image.

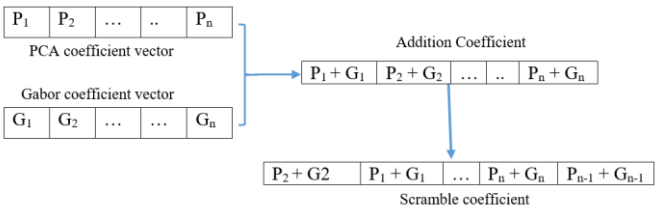


Fig. 5. Fusion of Gabor and PCA Features.

E. Normalization Features

To normalize the features, we use min-max normalization process that is applied on scrambling features. Following method has been used to normalize the features for matching

$$norm_{data} = \frac{(bla - \min(bla))}{\max(bla) - \min(bla)} \quad (1)$$

F. Incorporating the Key Information to the Templates

In our research, we use the 4-digit key, which has been obtained from the user as a password. It is very critical to incorporate key data into the biometric templates. We have used the statistic that the key information can be reflected by ring information, which is non-revocable. The feature descriptor converts to 65 length vector (64 bins plus the ring information) as per the new feature information. The two digits from 4-digit key is taken as two parameters for orientation and scaling. The orientation covers the large variety of conditions with different facial expressions. The scaling covers the different sizes of the face because the practical implementation of face detection system, the system must be able to recognize the face in different sizes. Further, for the enhancement of security, the feature vectors are different for each template of every individual.

G. Feature Matching

During the enrollment process, all features of the faces are stored in the database as a template. During authentication, features of the test image are calculated. The test image is compared with the feature template and calculates a score.

In the coordinating procedure, there could be four conceivable situations: the two patterns for coordinating could be from:

1) The two templates match perfectly in case same user with the same key.

2) The matching of two templates produces high distance in case of the same user with different keys because of different transformations. As a result, these two templates would not be matched.

3) In the third case where we have different users with same key produces high distance because of Gabor Descriptors are different for different faces.

4) In the fourth case of different users with different keys, the transformations would be different and produces a high distance, which considerably reduce the false acceptance rate.

IV. Results and Discussion

A. Dataset

In this paper, the AR, Yale, and FERET Face databases [22, 23, 24], have been used for the evaluation of authentication performance as shown in Fig. 6.

AR database [22] has more than 3200 images and it has all frontal view of 126 subjects, which has captured in the large variety of conditions with different facial expression e.g. smile, anger, neutral expression, right-light on, left-light on, all lights on, scream, wearing scarf, wearing scarf and left-light on, wearing scarf, wearing scarf and right-light on, wearing sun glasses, wearing sun-glasses and left-light on, wearing sun-glasses and right-light on. In this database, the image consists of "81 x 81" array of pixels and second session (same conditions as all expressions). The number of pictures of per person is 26, which have been recorded over the span of two weeks in two different sessions.

Fig. 6. Sample Images from different Datasets.

Yale database [23] consists of 165 images of 15 persons in grayscale and GIF format. Each person or subject has 11 images one per different facial expression or configuration: center-light, w/glasses, happy, left-light, w/no glasses, normal, right-light, sad, sleepy, surprised, and wink.

The FERET [24] database consists of total 14,126 images of 1199 persons with 1564 sets of images and 365 duplicate sets of images.

B. Performance Evaluation

The performance of our proposed method is assessed by measuring the two important parameters including the false acceptance rate (FAR) and false rejection rate (FRR). False acceptance rate is defined as the measure of percentage of accepting the unauthorized user as an authenticated user. On the other hand, the false rejection rate is a measure of percentage of not authenticating the legitimate user. The two parameters together are used to measure the error rate of the system and play an important role to measure the overall accuracy in biometric systems. When FAR and FRR are equal, then it is referred as the equal error rate (EER). We have to minimize this EER in order to achieve high accuracy of the system.

For our experiment, we use the database comprises of 20 samples of each subject. The process consists of two phases i.e. enrollment and authentication. For enrollment phase, 16 images of each subject are used to create the enrollment set while in the authentication phase remaining 4 images of each subject is used to create the authentication set. Authentication process is 1:1 comparison of biometric templates in database as compare to identification, which is 1:n comparisons and requires more time and effort. We performed the authentication instead of identification for our experiments. We perform the comparison of each of the 4 images in the authentication set with the 16 corresponding images in the enrollment set to calculate the false-rejection. Overall, it computes total of 64 comparisons for calculation of FRR of each subject. Thus, for 10 subjects the total number of comparisons is 640.

The false rejection rate is computed by using the following equation:

$$FRR = \left(\frac{no\ of\ false\ reject}{number\ of\ comparisons}\right) x100\% \quad (1)$$

Next, we approximate the mean FRR after computing the FRR for all the classes. We calculate the FRR for all the subjects on for three databases and found the average values for Yale 0.3, AR 0.671 and FERET 0.753. The number of false rejection and the false rejection rate for each subject class on different data set is shown in Table I.

We compute the false acceptance by perform the 1:1 comparison among each enrolled subject with the rest of 9 authentication subjects set. For each subject, it requires to perform total of 576 (9 x64) comparisons and for overall 10 subject it would require 5760 comparisons.

FAR for each subject is computed by using the following expression.

$$FAR = \left(\frac{no\ of\ false\ accept}{number\ of\ comparisons}\right) x100\% \quad (3)$$

TABLE. I. FRR RESULTS ON DIFFERENT DATASETS

	YALE Database		AR Face database		FERET Database	
Subject#	**False Reject**	**False Reject Rate %**	**False Reject**	**False Reject Rate %**	**False Reject**	**False Reject Rate %**
0001	0	0	1	1	0	0
0002	0	0	0	0	0	0
0003	0	0	0	0	2	1.45
0004	0	0	0	0	0	0
0005	0	0	2	1.32	3	1.89
0006	0	0	0	0	1	1
0007	1	1	3	1.87	2	1.3
0008	0	0	2	1.52	0	0
0009	1	1	1	1	3	1.89
0010	1	1	0	0	0	0

Experiments results are shown in Table II. We found that FAR is 0.52%, 0.61%, and 0.58% for AR, YALE, FERT database respectively. Similarly FRR is 0.89%, 1.52%, and 1.23% for AR, YALE, FERT database respectively. It is possible to achieve slightly different results if the input images are of low quality because quality of image plays an important role in the accuracy of biometric systems. Number of test subjects may also produce variation in achieved results. Further, the security of system can be enhanced by adding more biometric feature dimensions but it decreases the authentication accuracy.

Table III shows the comparison of EER of our proposed method with some other face based cancelable biometric schemes. Average EER of our proposed method for all three databases is 0.39 which is better than other methods [10][28].

C. Revocability Analysis

The revocability is most imperative property of the cancelable biometrics scheme. The revocability means to cancel the old compromised template, issue the new one template and as well as to cancel the authentication rights of old authenticator associated with compromised template. In any case, the relationship among the templates issued from a similar user ought to be kept negligible so that the invader can barely take in any helpful data from numerous templates. We utilized the normalized mutual information (NMI) to show the relationship between two templates explained a

$$NMI(X;Y) = \sum_x \sum_y P(x,y) \log\left(\frac{P(x,y)}{P(x)P(y)}\right) \quad (4)$$

where P(x, y) is the joint probability of x and y, and P(x) and P(y) are the marginal probabilities of x and y respectively.

Table IV shows the NMI values of fixed-length binary MLC for all tested datasets. In average for all three datasets, the NMI value is approximately 0.114, meaning that two templates generated from the same fingerprint using different random keys share 11% of mutual information and are slightly correlated.

TABLE. II. RESULTS ON DIFFERENT DATABASES

Database	FRR	FAR	EER%	GAR at FAR 0.1	GAR at FAR 0.01
AR	0.89	0.52	0.36	97.782	96.253
YALE	1.52	0.61	0.24	98.328	97.185
FERET	1.23	0.58	0.58	96.316	94.371

TABLE. III. EQUAL ERROR RATE (EER) OF DIFFERENT CANCELABLE BIOMETRICS

Cancelable biometric schemes	Equal error rate (%)
Bin Scheme II [10]	5.41
PCA based ROT-O [28]	2.09
Proposed Method	0.39

TABLE. IV. REVOCABILITY OF FIXED-LENGTH BINARY MLC TEMPLATE MEASURED IN NMI

Dataset	NMI
YALE	0.061
AR	0.120
FERET	0.162

D. Real-Valued Templates

The execution of genuine key case for all datasets is perfect (zero EER). Though, on account of compromised random keys, the execution decays of course. Table IV reports the real valued templates under stolen-key situation. We used both Dice's likeness and inner product to watch the pattern of execution for various comparability measures. Table V shows that proposed method achieve good dice coefficient as well as inner product.

E. Non-Invertible Transformation

The transformation process is a non-invertible spatial transformation consisting of a random re-mapping of the 72 features to shuffle the original location. Therefore, theoretically 72! (big value) different transformations can be obtained. We have used random based scrambling that also shuffle the original features. In this way, even the features are not in original form, features are shuffled randomly so that attacked should not know the original position of the features. Random seed is used by the key that has been taken from the user. So, at different level security has been added to secure the template. The transformation procedure is a non-invertible spatial change comprising of an irregular re-mapping of the components to rearrange the first location. In our research, we scrambled the features of the images for changing the original position of the features. We have taken one digit from 4-digit key as a seed point to generate pseudorandom number for the purpose of security and this process scramble the positions of the features. This non-invertible spatial transformation process ensures the security of the system.

TABLE. V. PERFORMANCE OF THE PROPOSED METHOD IN STOLEN-KEY SCENARIO OVER DIFFERENT DATASETS

Similarity measure	YALE	AR	FERET
Dice's coefficient	3.417	3.772	4.352
Inner Product	2.942	3.214	4.014

F. Perform Face Authentication using the Key Incorporated Templates

To match two feature point maps, which we taken from 4-digit key from the users, for the purpose of orientation and scaling, the average of the gap scores between all covering highlight focuses is computed and utilized as the coordinating score between two element point maps as shown in Table VI. Further, we altered the Euclidean distance based coordinating calculation by mulling over the transformation. The exceptional transformation mapping is the same for both enrolled and test image from a specific user by his/her same key. We check the feature point area data before computing the Euclidean distance. We see the two formats as being from various users and proceed onward to the following examination, if some chunks are observed to be too far away. An assailant can't recuperate the first change with just the radius location information. Thus, we added orientation and scaling information, which can accept correct acceptance and can reduce the matching time with keeping the security of the templates.

Table VII shows the results after effecting rotation and scaling factors. Like we have experimented by rotating the images at different angles and find the accuracy and then test the performance after making scale factor as well and check the accuracy results. These results show that proposed method perform well even in rotation as well scaling effect. Occasionally, we have to take pictures that are rotated or at different angles. So, we also need to check whether proposed method works well in these cases or not. But we have extracted rotation and scale invariant features therefore proposed method works in these cases well.

TABLE. VI. AUTHENTICATION PERFORMANCE OF THE PROPOSED METHOD

Dataset	PCA + Gabor	PCA	Gabor
YALE	95.6	92.24	93.42
AR	94.25	81.58	91.23
FERET	91.23	84.19	87.56

TABLE. VII. EFFECT OF ROTATION AND SCALING ON AUTHENTICATION USING THE KEY INCORPORATED TEMPLATES

Dataset	Accuracy (Rotation)	Accuracy (Scaling)
YALE	93.152	93.312
AR	91.252	91.143
FERET	90.051	91.352

V. CONCLUSIONS

The proposed method has aims to introduce face authentication cancelable biometric system with high rate of privacy and accuracy. The cancelable biometric is solution to ride of privacy problems in biometric systems as well as a desirable solution to ensure the revocability and alternative of face template when compromised. The traditional cancelable biometrics approaches often compromise the authentication accuracy. In this paper, we propose a new cancelable face authentication method using Hybrid Gabor PCA (HGPCA) descriptor, which can not only achieve "cancelability", but also

increase the authentication accuracy. We apply wavelet transform on original images till the second level for extraction the features via a Gabor filter and PCA coefficient vectors and in next step scramble the same. The produced templates are restored in the database and can be recognized/authenticate with an extraordinary rate of precision. Further, if some restored template is compromised, it can be easily cancelled and replaced. As per the results of our proposed method, the authentication accuracy and privacy are improved as compared to the traditional schemes. Consequently, our proposed method satisfies all conditions of an ideal cancelable biometrics system keeping with high rate of accuracy and security.

As a future work, we would like to apply our proposed method on multi model biometric systems to find out its implication for different cyberworld security applications.

REFERENCES

[1] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ : accessed 25 July 2019.

[2] Canuto AMP, Pintro F, and MC Fairhurst, "Genetic Algorithm and Ensemble Systems for Multi-biometric Cancellable Authentication," Journal of Biometrics and Its Applications, vol. 1, no. 1, 2015.

[3] K. Nandakumar and A. K. Jain, "Multi biometric Template Security Using Fuzzy Vault," in 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, pp. 1-6.

[4] Andrew Teoh Beng Jina, David Ngo Chek Linga, and Alwyn Gohb, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," vol. 37, no. 11, pp. 2245–2255, 2004.

[5] T Connie, A Teoh, M Goh, and D Ngo, "Palmhashing: A Novel Approach for Cancelable Biometrics.," Information Processing Letters, pp. 1-5, 2005.

[6] M Savvides, B Kumar, and P Khosla, "Cancelable biometric filters for face authentication.," in 17th International Conference on Pattern Authentication, 2004.

[7] T Boult, W Scheirer, and R Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis.," in IEEE Computer Society Conference on Computer Vision and Pattern Authentication, 2007.

[8] W Wei-jing, DW Mou-ling, and K Yau-hee, "Multi-line code: A low complexity revocable fingerprint template for cancelable biometrics.," Journal of Central South University, vol. 20, no. 5, 2013.

[9] R Christian R and B Christoph B, "Comparison Score Fusion Towards an Optimal Alignment for Enhancing Cancelable Iris Biometrics," in Fourth International Conference on Emerging Security Technologies., 2013.

[10] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez and C. Busch, "Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters," 2014 22nd International Conference on Pattern Recognition, Stockholm, 2014, pp. 4483-4488.

[11] H Salman, M. A Akbar M. A, S Farrukh, F Mudassar F, and K Zeashan , "Secure biometric template generation for multi-factor authentication, Pattern Authentication," Pattern Authentication, vol. 48, no. 2, pp. 458–472, 2015.

[12] K. Kanagalakshmi & Dr. E. Chandra" A Novel Technique for Cancelable and Irrevocable Biometric Template Generation for Fingerprints", Global Journal of Computer Science and Technology Graphics & Vision. Volume 13 Issue 6 Version 1.0 2013.

[13] N.Radha, S.Karthikeyan "An Evaluation of Fingerprint Security Using Noninvertible Biohash", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[14] Padma Polash Paul and Marina Gavrilova" Cancelable Biometrics: Securing Biometric Face Template", International Journal on Artificial Intelligence Tools 4(1), pp. 25-34, June 2012.

[15] Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping", Computers & Security, Elsevier, Available online 24 October 2016.

[16] R. Soruba Sree and N. Radha, "Cancellable multimodal biometric user authentication system with fuzzy vault", 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, pp. 1-6, 2016.

[17] Martiri Edlira, Gomez-Barrero Marta, Yang Bian, Busch Christoph, "Biometric template protection based on Bloom filters and honey template", IET Biometrics, 2016.

[18] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On the application of bloom filters to iris biometrics," IET J. Biometrics, vol. 3, no. 4, pp. 207–218, 2014.

[19] Christian Rathgeb and Christoph Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters", Computers & Security, Volume 42, Pages 1–12, May 2014.

[20] Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi, Yong-Haur Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation", Pattern Authentication, Volume 56, Pages 50-62, August 2016.

[21] R.L. Rivest, Chaffing and Winnowing, "Confidentiality without Encryption", MIT Lab for Computer Science, Massachusetts, Cambridge, USA, 1998. http://people.csail.mit.edu/rivest/pubs/Riv98a.pdf

[22] A.M. Martinez and R. Benavente. The AR Face Database. CVC Technical Report #24, June 1998.

[23] Yale face database: cvc.cs.yale.edu/cvc/projects/yalefaces/yalefaces.html

[24] K. Delac, M. Grgic, S. Grgic, Independent Comparative Study of PCA, ICA, and LDA on the FERET Data Set, International Journal of Imaging Systems and Technology, Vol. 15, Issue 5, pp. 252-260.

[25] J. Connell, and R.M. Bolle N. Ratha, "Enhancing security and privacy in biometrics biased" IBM systems, pp. 614 - 634, 2001.

[26] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli. , "A fingerprint and finger-vein based cancelable multi-biometric system" in Pattern Recognition, vol. 78, pp.242-251, June 2018,

[27] T. Murakami, R. Fujita, T. Ohki, Y. Kaga, M. Fujio and K. Takahashi, "Cancelable Permutation-Based Indexing for Secure and Efficient Biometric Identification," in *IEEE Access*, vol. 7, pp. 45563-45582, 2019.

[28] Wang Y, Plataniotis K: Face based biometric authentication with changeable and privacy preservable templates. Proc of the IEEE Biometrics Symposium 2007, 11-13.