Hybrid Approach for Template Protection in Face Recognition System

Sheetal Chaudhary[1] Rajender Nath[2]

GJCST Computing Classification
I.2.10, I.2.7, I.4.6

***Abstract*-Biometrics deals with identifying individuals with the help of their biological (physiological and behavioral) data. The security of biometric systems has however been questioned and previous studies have shown that they can be fooled with artificial artifacts. Also biometric recognition systems face challenges arising from intra-class variations and attacks upon template databases. To tackle such problems, a hybrid approach for liveness detection and protecting templates in face recognition system is proposed. Here, the system captures input face image in three different poses (left, front, right) based upon the order chosen by the random select module. This approach will perform live face detection based upon complete body movement of the person to be recognized and template protection by randomly shuffling and adding the components of feature set resulting after fusion of three poses of input face image. It overcomes the limitations imposed by intra-class variations and spoof attacks in face recognition system. The resulting hybrid template will be more secure as original biometric template will not be stored in the database rather it will be stored after applying some changes (shuffling and addition) in its components. Thus the proposed approach has higher security and better recognition performance as compared to the case when no measures are used for live face check and template protection in database.**

Keywords-Liveness detection, template protection, face recognition, multiple sample fusion, eigen-coefficients

I. INTRODUCTION

The term biometrics is derived from the Greek words bios and metron which translates as life measurement. Biometrics are not secrets and therefore should be properly protected. A good biometrics system should depend not only on security of biometric data but the authentication process must also check for liveness of the biometric data. People leave fingerprints behind on everything they touch, and the iris can be observed anywhere they look. Our facial images are recorded every time we enter a bank, railway station, and supermarket [1]. Once biometric measurements are disclosed, they cannot be changed (unless the user is willing to have an organ transplant). The only way how to make a system secure is to make sure that the data presented came from a real person and is obtained at the time of authentication. Liveness detection in a biometric system means the capability for the system to detect, during enrollment and identification/verification, whether or not the biometric sample presented to the system is alive or not. It must also check that the presented biometric sample belongs to the live human being who was originally enrolled in the system and not just any live human being. It is well known that fingerprint systems can be fooled with artificial fingerprints, static facial images can be used to fool face recognition systems, and static iris images can be used to fool iris recognition systems [2].

Multimodal biometric systems consolidate the evidence presented by multiple biometric sources of information and are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence [3]. Intra-class variations in face recognition system can be overcome with multimodal biometric systems. Figure 1 is showing intra-class variation associated with an individual's face image. Due to change in pose, face recognition system will not be able to match these 3 images successfully, even though they belong to the same individual [4]. A Multibiometric system can be classified into five categories (multi-sensor, multi-algorithm, multi-instance, multi-sample and multimodal) depending upon the evidence presented by multiple sources of biometric information. Multi-sample system can be used to tackle intra-class variations. Here, a single sensor is used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait. It is an inexpensive way of improving system performance since this system requires neither multiple sensors nor multiple feature extraction and matching modules [5] [6].

Fig.1: Intra-class variation associated with an individual's face image

One of the properties that make biometrics so attractive for authentication purposes is their invariance over time. One of the most vulnerabilities of biometrics is that once a biometric image or template is stolen, it is stolen forever and cannot be reissued, updated or destroyed [7]. One of the most potentially damaging attacks on a biometric system is

About-[1]University Research Scholar, Department Of Comp. Sc. & App. K.U., Kurukshetra, Haryana, India (e-mail;Sheetalkuk@Rediffmail.Com)
About-[2]Associate Professor, Department Of Comp. Sc. & App. K.U., Kurukshetra, Haryana, India (e-mail;rnath_2k3@rediffmail.com)

against the biometric template database. Attacks on the template can lead to the following three vulnerabilities: (i) A template can be replaced by an impostor's template to gain unauthorized access, (ii) A physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait) and (iii) The stolen template can be replayed to the matcher to gain unauthorized access [8].

The proposed hybrid approach provides three main advantages: handles intra-class variation, performs live face check and provides protection against attacks on template database. The rest of the paper is organized as follows. Section 2 addresses the literature study. In section 3 face feature set extraction using PCA is discussed. In section 4 architecture of the proposed approach is presented. Section 5 discusses the advantage of proposed approach. Finally, the summary and conclusions are given in last section.

II. Related work

In recent years face recognition has received substantial attention from both research communities and the market, but still remained very challenging in real applications. A lot of face recognition algorithms have been developed during the past decades. Face recognition consists in localizing the most characteristic face components (eyes, nose, mouth, etc.) within images that depict human faces This step is essential for the initialization of many face processing techniques like face tracking, facial expression recognition or face recognition. Among these, face recognition is a lively research area where a great effort has been made in the last years to design and compare different techniques [9]. Hong and Jain [10] designed a decision fusion scheme to combine faces and fingerprint for personal identification. Brunelli and Falavigna [11] presented a person identification system by combining outputs from classifiers based on audio and visual cues. Face recognition algorithms are categorized into appearance based and model-based schemes. For appearance-based methods, three linear subspace analysis schemes are presented (PCA, LDA, and ICA) [12].The model-based approaches include Elastic Bunch Graph matching [13], Active Appearance Model [14] and 3D Morphable Model [15] methods. Among face recognition algorithms, appearance-based approaches are the most popular. These approaches utilize the pixel intensity or intensity-derived features.

The template protection schemes proposed in the literature can be broadly classified into two categories, feature transformation approach and biometric cryptosystem approach [8]. In the feature transformation approach, a transformation function is applied to the biometric template and only the transformed template is stored in the database. The same transformation function is applied to query features and the transformed query is directly matched against the transformed template. Depending on the characteristics of the transformation function, the feature transform schemes can be further categorized as salting and non-invertible transforms. In a biometric cryptosystem, some public information about the biometric template is stored. This public information is referred to as helper data and hence, biometric cryptosystems are also known as helper data-based methods. While the helper data does not reveal any significant information about the original biometric template, it is needed during matching to extract a cryptographic key from the query biometric features. Matching is performed indirectly by verifying the validity of the extracted key. Biometric cryptosystems can be further classified as key binding and key generation systems depending on how the helper data is obtained [16].

Liveness detection can be performed either at the acquisition stage, or at the processing stage. There are two approaches in determining if a biometric trait is alive or not; liveness detection and non-liveness detection [2]. Liveness detection, which aims at recognition of human physiological activities as the liveness indicator to prevent spoofing attack, is becoming a very active topic in field of fingerprint recognition and iris recognition, but efforts on live face detection are still very limited though live face detection is highly desirable. The most common faking way is to use a facial photograph of a valid user to spoof face recognition systems. Most of the current face recognition works with excellent performance are based on intensity images and equipped with a generic camera. Thus, an anti-spoofing method without additional device will be preferable, since it could be easily integrated into the existing face recognition systems [17] [18].

III. Feature extraction

Facial recognition is the identification of humans by the unique characteristics of their faces. It has attracted a lot of attention because of its potential applications. Among face recognition algorithms, appearance-based approaches (PCA, LDA, and ICA) are the most popular. These approaches utilize the pixel intensity or intensity-derived features [12].

In this paper, the PCA method using eigenfaces was adopted for face recognition. PCA is a way of identifying patterns in data, and expressing the data in such a way as to highlight their similarities and differences. The main idea of the principal component analysis (or Karhunen-Loeve transform) is to find the vectors which best account for the distribution of face images within the entire image space. These vectors define the subspace of face images, which we call "*face space*". Because these vectors are the eigenvectors of the covariance matrix corresponding to the original face images, and because they are face like in appearance, we refer to them as "*eigenfaces*". Eigenfaces are a set of eigenvectors used in the computer vision problem of human face recognition. The eigenfaces are the principal components of a distribution of faces, or equivalently, the eigenvectors of the covariance matrix of the set of face images, where each image with NxN pixels is considered a point (or vector) in N^2-dimensional space [19]. The idea of using principal components to represent human faces was developed by Sirovich and Kirby [20] and used by Turk and Pentland [21] for face detection and recognition. Eigenfaces are mostly used to:

(a) Extract the relevant facial information, which may or may not be directly related to face features such as the eyes,

nose, and lips. One way to do so is to capture the statistical variation between face images.
(b) Represent face images efficiently. To reduce the computation and space complexity, each face image can be represented using a small number of dimensions.
Mathematically, it is simply finding the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images, treating an image as a point or a vector in a very high dimensional space. Each eigenvector is accounting for a different amount of the variations among the face images. These eigenvectors can be imagined as a set of features that together characterize the variation between face images [19]

IV. Proposed Approach

Figure 2 shows the block diagram of the proposed approach for template protection in face recognition system. The main idea behind the proposed approach is to generate secure hybrid templates by integrating three different views (left, front and right) of input face image and then changing the components of resulting face feature set.

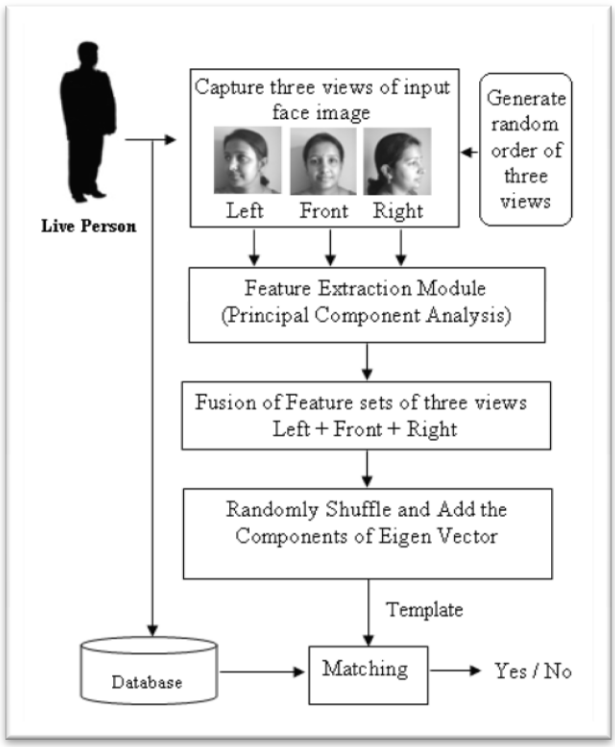

Fig. 2: Architecture of proposed approach for template protection in face recognition system

The proposed approach can be roughly divided into the following four steps:
A. Random selection of three Facial views (Left, Front, Right) to perform Liveness Detection.
B. Extraction of Feature sets of three Facial views
C. Fusion of Feature sets of three Facial views (Left + Front + Right).
D. Random shuffling and addition of components of Eigen vector (resulting after fusion).

A. Random selection of three Facial views

This step is responsible for performing liveness detection. Here, the person to be recognized is required to stand in front of camera which is focused upon full height of the person. Based upon the random order (LFR or LRF or FLR or FRL or RFL or RLF, L: Left; F: Front; R: Right) generated by the random select module as shown in fig. 2, the person is asked to move left or right or look at front. The camera is focused upon the entire body to examine the actual body movement but it will capture only the images of face in the order selected by the module. The module which generates random order of three views will detect whether the person is live or not by instructing the person to move left or right or look at front. Complete body movement is examined through camera and face images will be captured only if the person is live. To perform liveness detection, the random select module can be equipped with the following decision process which first checks liveness and then performs person recognition
if data = live
perform acquisition and extraction
else if data = not live
do not perform acquisition and extraction

B. Extraction of Feature sets of three Facial views

performs feature set extraction of three views (Left, Front, Right) of input face image by using PCA (appearance based) face recognition technique. PCA method is applied individually on each view of the face image to extract the corresponding feature set. When using PCA, each face image is assumed to be a 2-dimensional array of intensity values. It is represented as 1-dimensional vector by concatenating each row (or column) into a long thin vector. By projecting the face vector to the basis vectors, the projection coefficients are used as the feature representation of each face image. The PCA method using eigenfaces consists of the following two stages [10]

1) Training stage, in which a set of N face images are collected; eigenfaces that correspond to the M highest eigenvalues are computed from the data set; and each face is represented as a point in the M dimensional eigenspace, and
2) Operational stage, in which each test image is first projected onto the M-dimensional eigenspace; the M dimensional face representation is then deemed as a feature vector and fed to a classifier to establish the identity of the individual.
For each face image, we obtain a feature vector by projecting image onto the subspace generated by the principal directions of the covariance matrix. After applying the projection, the input vector (face) in an n-dimensional space is reduced to a feature vector in an m-dimensional subspace (M<< N) [9].
Thus, the feature vectors of three individual face views can be represented in terms of eigen vectors as described below
eigen vector for left face view $V_L = [a_1, a_2, a_3, a_4 \ldots a_m]$
eigen vector for front face view $V_F = [b_1, b_2, b_3, b_4 \ldots b_m]$

eigen vector for right face view $V_R = [c_1, c_2, c_3, c_4 \ldots c_m]$ where V_L, V_F, V_R represent the feature sets in terms of eigen-coefficients of three views of face image respectively.

C. Fusion of Feature sets of three Facial views

Fusion involves consolidating the evidence presented by two or more biometric feature sets of the same individual. This step performs fusion of feature sets of three face views of the same image at feature level [6]. Here, the three feature sets originate from the same feature extraction algorithm (PCA). Fusion of three face views is performed by just averaging them as given below

$$X = (VL + VF + VR)/3 \quad (1)$$

The resulting fused eigen vector can be represented as X = [x1, x2, x3, x4…xm].

D. Random shuffling and addition of components of Eigen vector

This step in the proposed approach is responsible for performing changes in the eigen vector that is obtained after fusion of three feature sets. It will make the resulting template more secure. This step is illustrated in fig.3 below

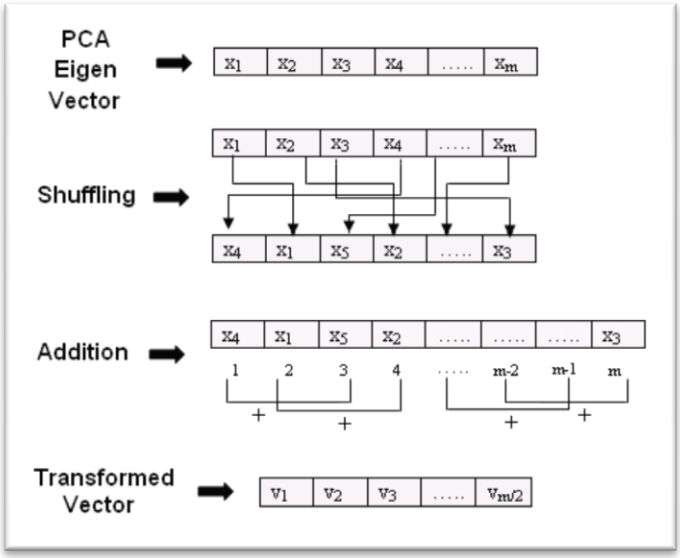

Fig. 3: Steps to generate secure hybrid template from input face images

The coefficients of eigen vector X are randomly shuffled. By shuffling, randomly chosen columns are interchanged and every time we can generate a new eigen vector.

$$X' = Hshuffle\ (X) \quad (2)$$

where Hshuffle is the function which performs shuffling on the eigen vector X and X′ is the shuffled eigen vector. The number of coefficients in both X and X′ are same, shuffling just changes the order of columns. After that, addition among coefficients of shuffled eigen vector is performed in some order. Addition function is described below:

$$Addition = \sum_{p=1}^{p=m-2} [x_p + x_{p+2}], \quad (3)$$

after every two iteration p is incremented with 3.

Random shuffling of coefficients in the eigen vector that is obtained after fusion of three feature sets and addition among coefficients of shuffled eigen vector will generate the hybrid template that would be finally stored in the system database. The resulting hybrid template will contain half the no. of coefficients in the original eigen vector that was obtained in the previous step. The no. of coefficients are reduced by addition function. This approach will make the template more secure against spoof attacks and will take less memory in the database.

V. Advantage of Using Proposed Approach

basic idea of the proposed approach is that instead of storing the original template in database, it is stored after performing fusion, shuffling and addition in the coefficients of eigen vector. The proposed approach offers advantage in terms of liveness detection, intra class variation, and template security by providing the ability to discard the stolen template information. Here, multiple samples of the same biometric trait (face) are captured in order to account for the intra class variations that can occur in the trait and for checking liveness of acquired biometric sample. This approach for liveness detection is natural, non-intrusive and no extra hardware is required. But it requires user collaboration by instructing the user to move left, right or stand in front of camera.

It provides template security by performing fusion of feature sets of three facial views (Left, Front, Right), random shuffling of eigen-coefficients in the fused eigen vector and addition among the shuffled eigen-coefficients. If the template is found to be compromised, the proposed approach provides the ability to discard it and reissue with new shuffling rules. In this way, with shuffling a number of eigen vectors can be generated. Also it is impossible for the attacker to convert the stolen template into the original face data (PCA eigen vector). It is well known that each eigenface represents certain characteristic features of faces and any original image can be reconstructed by combining the eigenfaces in right proportion. Hence, the original eigen vector is not stored in the database rather it is stored after applying shuffling rules and then adding the shuffled coefficients according to the addition function as discussed in the previous section. Addition reduces the size of the eigen vector by half and hence the final hybrid template generated will be compact and more secure. Thus the proposed scheme provides higher template security and better recognition performance as compared to the case when no measures for liveness detection and template protection are taken as in existing face recognition system using eigenfaces approach.

VI. Conclusion

Biometric template protection has become one of the important issues in deploying a practical biometric system. In this paper, a hybrid approach for template protection in face recognition system is proposed. This approach is based on the fusion of three different views (left, front, right view captured randomly) of input face image, random shuffling of coefficients in the eigen vector (extracted using PCA

method) obtained after fusion and addition among coefficients in the shuffled eigen vector. On the theoretical basis, it has been proved that the proposed approach provides better template protection against spoof attacks as compared to the existing method. One of the weaknesses of biometrics is that once a biometric data or template is stolen, it is stolen forever and cannot be reissued, or discarded. Thus template security has become very critical in these systems. The proposed scheme provides new measures (shuffling and addition) for template protection by giving the ability to discard the lost template and reissue a new one.

VII. References

1) Bori Toth, "Biometric Liveness Detection", Information Security Bulletin, October 2005, Volume 10, pages 291-297.
2) International Biometric Group. Liveness detection in biometric systems, 2003. White paper. Available at http://www.biometricgroup.com/reports/public/reports/liveness.html.
3) A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4–20, Jan 2004.
4) Arun Ross and Anil K. Jain, "Multimodal biometrics: An overview", appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.
5) Arun Ross, "An Introduction to Multibiometrics", EUSIPCO, 2007.
6) A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, New York, Springer, 2006.
7) B. Schneier, "The uses and abuses of biometrics", Communications of the ACM, vol. 42, no. 8, pp. 136, Aug. 1999.
8) A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, January 2008.
9) Lu, X., Wang, Y. & Jain, A.K. (2003). Combining Classifiers for Face Recognition, In IEEE Conference on Multimedia & Expo, Vol. 3, pp. 13-16.
10) L. Hong and A.K Jain, "Integrating faces and fingerprint for personal identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295–1307, 1998.
11) R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955–966, Oct. 1995.
12) [12] Xiaoguang Lu, "Image Analysis for Face Recognition – A brief survey", Dept. of Computer Science & Engineering, Michigan State University, personal notes, May 2003.
13) L. Wiskott, J.M. Fellous, N. Kruger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 775–779, 1997.
14) G.J. Edwards, T.F. Cootes, and C.J. Taylor, "Face recognition using active appearance models," in Proc. European Conference on Computer Vision, 1998, vol. 2, pp. 581–695.
15) V. Blanz and T. Vetter, "A morphable model for the synthesis of 3D faces," in Proc. ACM SIGGRAPH, Mar. 1999, pp. 187–194.
16) U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges," vol. 92, no. 6, pp. 948–960, June 2004.
17) Gang Pan, Zhaohui Wu and Lin sun, "Liveness Detection for Face Recognition", Recent Advances in Face Recognition, pages 109-123, December 2008, I-Tech, Vienna, Austria.
18) Jiangwei Li, Yunhong Wang, Tieniu Tan, A.K. Jain, "Live Face Detection Based on the Analysis of Fourier Spectra", Biometric Technology for Human Identification, Proceedings of. SPIE, Vol. 5404.
19) Y. Vijaya Lata, Chandra Kiran Bharadwaj Tungathurthi, H. Ram Mohan Rao, A. Govardhan, L. P. Reddy, "Facial Recognition using Eigenfaces by PCA", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
20) L. Sirovich and M. Kirby, "Low-dimensional procedure for the characterization of human faces", Journal of the Optical Society of America A 4: 519–524, 1987.
21) M.Turk and A. Pentland, "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, March 1991.