Multimodal Cancelable Biometrics

Conference Paper · August 2012

DOI: 10.1109/ICCI-CC.2012.6311208

2 authors, including:

Padma Polash Paul
University of Oxford
54 PUBLICATIONS **867** CITATIONS

Multimodal Cancelable Biometrics

Padma Polash Paul & Marina Gavrilova, Department of Computer Science, University of Calgary, Canada

ABSTRACT

Multimodal biometric systems have emerged as highly successful new approach to combat problems of unimodal biometric system such as intraclass variability, interclass similarity, data quality, non-universality, and sensitivity to noise. However, one major issue pertinent to unimodal system remains. It has to do with actual biometric characteristics of users being permanent, and their number being limited. Thus, if user's biometric is compromised, it might be impossible or highly difficult to replace it in a particular system. Cancellable biometric for individual biometric has been a significantly understudied problem. The concept of cancelable biometric or cancelability is to transform a biometric data or feature into a new one so that users can change their single biometric template in a biometric security system. However, cancelability in multi-modal biometric has been barely addressed at all. In this paper, we tackle the problem and present a novel solution for cancelable biometrics in multimodal system. We develop a new cancelable biometric template generation algorithm using random projection and transformation-based feature extraction and selection. Performance of the proposed algorithm is validated on multi-modal face and ear database.

Keywords: Template Security, Pattern Recognition, Decision Making, Multimodal Cancelable Biometrics

1. INTRODUCTION

Secure access to information, smart devices and network can be ensured by using several types of credentials. Passwords and tokens are traditionally used credentials to authenticate the users. Complexities of the credentials ensure the system security level (Feng, Yuen, & Jain, 2010). However, a password-based system may not be efficient or reliable for several reasons. Sometime it may be difficult for the users to remember the password. There are number of techniques to gain an authorized access to password-protected systems. In addition, passwords can be easily stolen using different spyware by hackers. Unlike passwords or ID cards, biometric characteristics of a person cannot be borrowed, stolen, or forgotten. Thus, the use of biometric technologies in physical and logical access control system is one of the most broadly commercialized sectors of biometrics. Another broad category of biometric technology usage is forensic or criminal investigation system.

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses (Prabhakar, Pankanti, & Jain, 2003). Commonly used biometric traits include fingerprint, face, signatures, iris, palm-print, fingerprint, hand geometry, ear, voice etc. A typical biometric system usually consists of four basic components, a) acquisition of biometric data, b) feature extraction, c) feature matching, and d) decision-making). Figure 1 shows the general architecture of a biometric authentication system

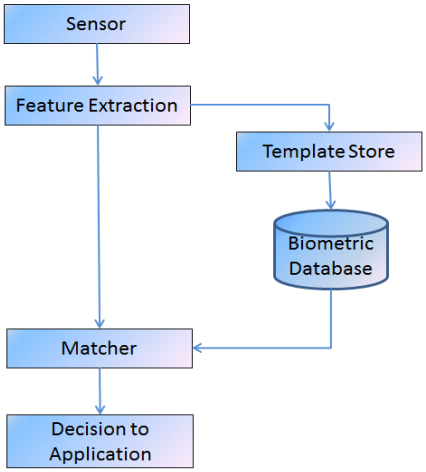


Figure 1: General block diagram of traditional biometric system.

In biometric system both verification and identification are two important way of person recognition (Jain, Flynn, & Ross, 2007). Each is intended to be used under different conditions and in different security application. In verification the person's identity is claimed (Jain, Flynn, & Ross, 2007), on the other hand, in identification system recognize a person from a template database containing certain number of persons. Identification is a more challenging and computationally expensive problem because it involves the matching with the database where verification is one by one matching. (Jain A. K., 2007). Multimodal Biometric System is relatively new to Unimodal Biometric System. Multimodality can be achieved in different ways: such as combining multiple biometric traits, selecting different feature set from same source of biometric etc. In our system we have use same source of biometric but different feature set. From the literature, it is found that multimodal biometric system outperform compared with unimodal biometric system (Ross, Nandakumar, & Jain, 2006). It also solve some problem of unimodal biometric system such as intra-class variability, interclass similarity, data quality, non-universality, sensitivity to noise and other factors. It can improve the performance of a biometric system in a number of aspects, including accuracy, circumvention, resistance to errors and spoof attacks (Ross, Nandakumar, & Jain, 2006; Jain & Pankanti, 2006). Multimodal biometric systems are more secure compared with unimodal systems in term of authentication accuracy (Down & Sands, 2004). However, multibiometric system and technology become vulnerable because of terrorists and criminals.

Physical and logical access control system is commercialized sector of biometric using emerging technologies of biometric (Jain, Flynn, & Ross, 2007). Individual's biometric traits are stored in template database during the training session of biometric system. The most important parts of the biometric system are template database because of the security and privacy concern of individual. Biometric characteristics are unique and cannot be changed. If they are compromised, the loss of the privacy is permanent for an individual. That is why template security is most crucial part in biometric system. To deal with the privacy and protection of template data, the notion of Cancelable Biometrics has been introduced (Feng, Yuen, & Jain, 2010). Biometric systems are also being developed for many other applications (Jain & Pankanti, 2006) such as banking, credit cards, border control, employee's registration, amusement parks entrance etc. With the growing use of biometrics, there is now a concern about the security and privacy of the biometric data itself (Prabhakar, Pankanti, & Jain, 2003). Person's biometrics are unique, if one or more biometrics are compromised there are no way of replacing the biometrics for that person (Prabhakar, Pankanti, & Jain, 2003). Therefore, biometric data (template)

security (Prabhakar, Pankanti, & Jain, 2003; Uludag, Pankanti, Prabhakar, & Jain, 2004) is one of the most important issues in developing a practical biometric system. Recent studies (Alder, 2003; Uludag, Pankanti, Prabhakar, & Jain, 2004) have shown that the raw biometric data can be recovered from the biometric template stored in the database. As a result, protection of biometric template in biometric system applications is crucial.

A common approach to deal with biometric security, privacy is to store the transformed version of original template (Alder, 2003). In (Alder, 2003), author represented the dependency of cancelable biometric algorithm such as security, discriminability, recoverability and diversity. It is computationally hard to reconstruct the original template from the Transformed template. The discriminability of the original biometric template should not be degraded after the cancelable transformation. On the other hand, the revocability and diversity are two most important characteristics of Cancelability. If the transformed biometric template is stolen or lost, the algorithm should be able to generate another transformed template from the original template. Moreover, the algorithm should be able to generate different transformed templates of an individual for different applications.

Authors of (Darrell & Indyk, 2005) emphasize that a biometric template protection algorithm should satisfy the following three requirements:

1) Security: Reconstruction of the original biometric template from the transformed biometric template should be computationally hard.

2) Discriminability: The discriminability of the original biometric template should not be degraded after the transformation.

3) Cancelability: Revocability and Diversity are two most important characteristics of Cancelability

The concept of cancelable biometric or cancelability is a new trend that focuses on how to transform a biometric data or feature into a new one so that users can change their single biometric template in a biometric security system. However, cancelability in multi-modal biometric has not been addressed at all, to the best of our knowledge. In this paper, we tackle the problem and present a novel solution for cancelable biometrics in multimodal system. We develop a new cancelable biometric template generation algorithm using random projection and transformation-based feature extraction and selection. Performance of the proposed algorithm is validated on multi-modal face and ear database.

The methodology is briefly described as follows. At the first step, the two-fold random selections are made for each biometric trait. A feature level fusion scheme is used to generate the two-fold feature set from the single biometrics. Each fold is then randomly projected using random projection technique. In the second step, the Principal Components Analysis (PCA) is used to reduce the feature dimension of the randomly projected folds. After the PCA, a dimension reduction feature-based fusion using k-mean clustering is applied to create single templates for individual biometrics. In the third step, to enhance the discriminability, the Linear Discriminant Analysis is applied to the features. These features are then used in a classifier to get the final authentication performance. The system is tested on virtual multimodal databases for face and ear biometrics, considering both cancelability and performance. The results are presented in experimentation section with conclusions drawn and future directions outlined.

2. RELATED WORK

According to (Jain, Nandakumar, & Nagar, 2008), the template protection scheme can be categorized into two broad categories: transformation based system, biometric cryptosystem. We have found that there are some methods called hybrid system that uses both transform based system and biometric cryptosystem. From the literature review, we can categorize the cancelable biometric system into three broad categories transformation based system, biometric cryptosystem and hybrid system. In term of biometric system, we can also divide cancelable biometric system into two categories, unimodal cancelable biometrics and our proposed multimodal cancelable biometrics. Similar as unimodal biometric system, multimodal biometric system can be categories into transformation based system, cryptosystem and hybrid system. Multimodal cancelable biometric system can be achieved by applying information fusion of different biometric traits. In (Jain, Nandakumar, & Nagar, 2008) they also mentioned that transformation based approach can be categorized into two categories, noninvertible transformation and salting. Matching of the transform-based system is performed in transformed domain (Alder, 2003). There are different levels of attack (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002; Matsumoto, Hirabayashi, & Sato, 2004; Harrison, 1981; Wretling & P, 2007) may take place in biometric system such as input level (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002; Matsumoto, Hirabayashi, & Sato, 2004), module level (Ross, Shah, & Jain, 2007), matching level, database level, feature extraction level attack etc. Transform based cancelable biometric approach able to resolve the problem of database level attack. Ratha et al 2007 (Ratha, Chikkerur, Connell, & Bolle, 2007) first proposed the concept of cancelable biometrics (or cancelable template). He provided the basics of the cancelable biometrics but author did not address the discriminability issues. Later salting of biometrics is introduce by the researcher to combine a user defined key or password to increase the between-class variation and enhance the discriminability. However, a transform-based approach also takes the original biometric template and the user-specific key to enhance the discriminability of the transformed templates (Teoh, Ngo, & Goh, 2004). The advantage of the transformed template is cancelability. The transformed templates can be cancelled or replaced by changing the key which is also known as bio-hashing algorithm (Goh & Ngo, 2003). In (Teoh, Ngo, & Goh, 2004), Teoh et al. 2004 proposed a two-factor authentication algorithm and a random Multi-space Quantization algorithm for fingerprint and face biometric respectively. Another approach called biometric cryptosystem such as fuzzy commitment scheme and fuzzy vault scheme (Juels & Wattenberg, 1999) can be used to improve the intraclass variability (Jain, Nandakumar, & Nagar, 2008). Since the output of biometric cryptosystem is encrypted and it is highly secure. Hybrid systems are designed based on biometric cryptosystem and transformation based approach (Jain & Pankanti, 2006; Feng, Yuen, & Jain, 2010; Jain, 2007) designed and developed method based on random projection, discriminability preserving (DP) transform, and fuzzy commitment scheme. Their proposed approach retains the advantages of both the transform-based approach and biometric cryptosystem approach. The hybrid algorithm consists of random projection, discriminability preserving (DP) transform, and fuzzy commitment scheme. Jain et. al., 2006, presented cancelable biometric using Multi-space random projection. In their paper, they have subsequently re-projecting the same feature onto a number of random subspaces. In our proposed method, we have presented multimodal approach to achieve the cancelable face biometric template.

The main motivation of the multimodal biometric system is to enhance the security and reliability of the multi-modal biometric system as well as its performance using novel Multimodal Cancelability methodology. Applying the multimodal technique in feature level, the proposed Cancelable

Multibiometric System can enhance the interclass variability and thus improves the performance of the system. Furthermore, the main complications of multimodal biometric system are memory and computational complexity during the training and testing. In the traditional multibiometric system, all of the biometric traits are stored in the database and used for computation. Proposed Cancelable Multibiometric System is able to fuse all the templates (for example face, ear, palm print etc.) into one single multimodal biometric trait that can reduce the database size and computation during the identification and verification process.

3. PROPOSED METHOD

3.1 Multiple Biometric Traits Fusion

In this paper, we proposed to achieve the cancelability using random projection method. We furthermore applied it for the first time to multimodal biometric system to achieve cancelability in the presence of multiple biometrics. Feature fusion of multiple biometric traits is a highly important step for multifold random projection. Raw biometric features are divided into two equal parts. A pseudorandom number generation algorithm is used to split the raw features into two parts. Face biometric template is divided into Face-Fold 1 and Face-Fold 2. Similarly, ear template is divided into Ear-Fold 1 and Ear-Fold 2. Finally, we have combined Face-Fold 1 and Ear-Fold 1 to achieve the Face-Ear Fold 1 and Face-Ear Fold 2. Finally, we have similar sized image for each fold. Therefore, the Face-Ear Fold 1&2 are in same size as the template size i.e., 100x100. These folds are then processed using proposed cancelable templates generation algorithm. Figure 2 depicts the process described above.

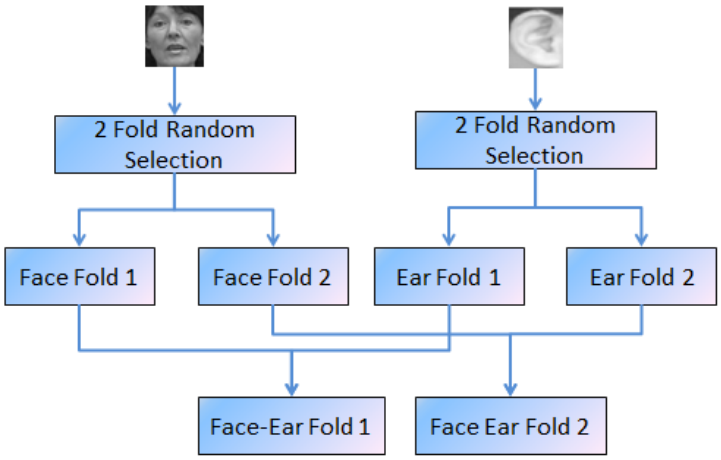


Figure 2: Cross folding of two biometric traits face and ear for proposed two-fold cancellable system

3.2 Proposed Cancelable Biometrics

Proposed cancelable biometric system is divided into three parts: a) Two Fold Random projection based transformation, b) Projection of Transformed features using Principal Components (PCs) and combining two fold features using k-means clustering, c) Application of Linear Discriminant Analysis (LDA) to enhance the interclass variability. Finally, the cancelable template is used to model the k-NN classifiers. Following figure 3 shows the block diagram of the random transformation based cancelable biometric template generation.

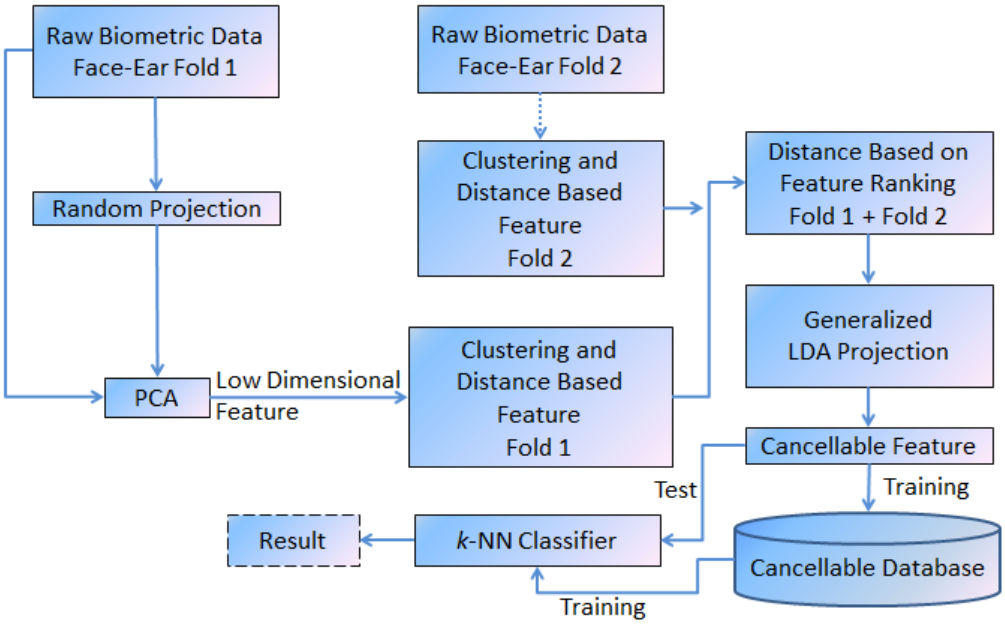


Figure 3: Block Diagram of proposed system Cancelable Template generation algorithm using transform based approach.

We have applied the same cancelable transformation on both fold (Fold1 and Fold2). Each fold is then projected using random projection that transforms the original m-dimensional data to n-dimensional. The random projection is not an orthogonal transformation. It is a linear mapping of the feature set to new dimension. We have applied Principal Component Analysis on the projected features to reduce the dimensionality of features. Low dimensional features are then clustered using k-means cluster to get the cluster centroid to generate new domain feature called distance based feature. New features from two folds are then combined together for linear discrimination analysis (LDA). Projected feature using LDA are cancelable because it comes from the random projection and initial cross folding between face and ear template. If we change the indices of cross-folding and random projection matrix, we can achieve the cancelable template for multiple biometrics.

3.3 Principal Component Analysis

PCA is a standard tool in modern data analysis in different fields such as biometrics, image processing - because it is a simple, non-parametric method for extracting relevant information from confusing data sets (Randall & Martinez, 2003). Benefit of PCA arises from quantifying the importance of each dimension for describing the variability of a dataset. In particular, the measurement of the variance along each principle component provides a mean for comparing the relative importance of each dimension. The goal of PCA is not only dimensionality reduction. A simple approach to PCA is to use singular value decomposition (SVD) which enhances the features by reducing noise (Statheropoulos, Pappa, Karamertzanis, & Meuzelaar, 1999).

Generally, a linear orthogonal transformation v = Wu (where u is the observation vector) is used such that the retained variance is maximized (Statheropoulos, Pappa, Karamertzanis, & Meuzelaar, 1999). Alternatively, PCA is viewed as a minimizer of reconstruction error. It turned out that these principles (variance maximizer or reconstruction error minimizer) leads to a symmetric eigenvalue problem. The

row vectors of W correspond to the normalized orthogonal eigenvectors of the data covariance matrix. Let us denote the data covariance matrix by $R_u = E\{uu^T\}$ where the superscript T denotes the transpose of vector or matrix. Then the SVD of R_u has the form

$$\boldsymbol{R}_u = \boldsymbol{U}_u \boldsymbol{D}_u \boldsymbol{U}_u^T \tag{1}$$

Where U_u is the eigenvector matrix and D_u is the diagonal matrix whose diagonal elements correspond to the eigenvalues of R_u. Then the linear transformation W for PCA is given by

$$\boldsymbol{W} = \boldsymbol{U}_u^T \tag{2}$$

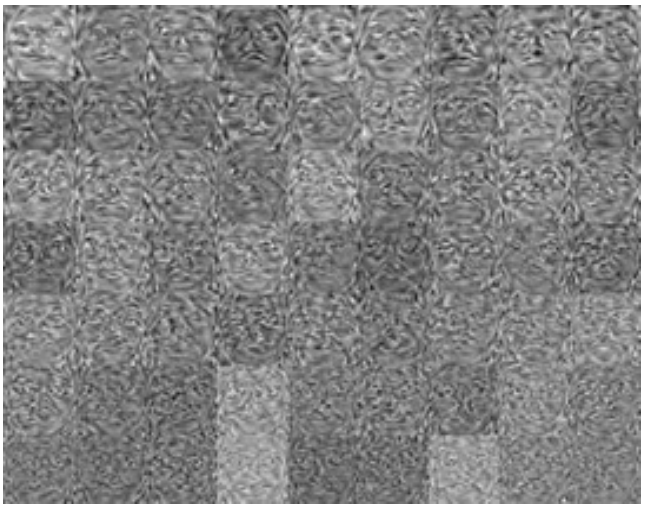


Figure 4 shows the impact of projection using different number of principal component for experimental data.

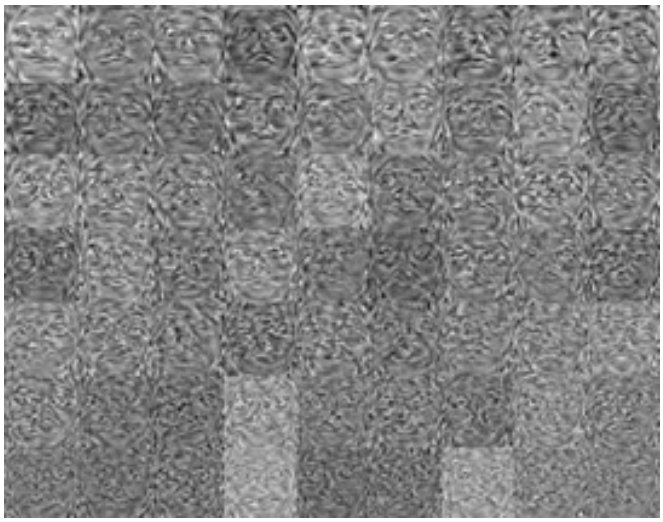


Figure 5: Example of projected image using Eigen vectors of corresponding eigenvalues (from highest to lowest) for our virtual face database for fold 1.

For dimensionality reduction, one can choose p dominant column vectors in U_u which are the eigenvectors associated with the p largest eigenvalues in order to construct a linear transform W.

3.4 *k*-Means Clustering

Features of reduced dimension are then clustered by combining both fold of the random selection. k-mean clustering is used to find clusters of the features. Final features are the distances between the combined clusters and individual clusters. Figure 6 shows the clustered cancelable biometric face template.

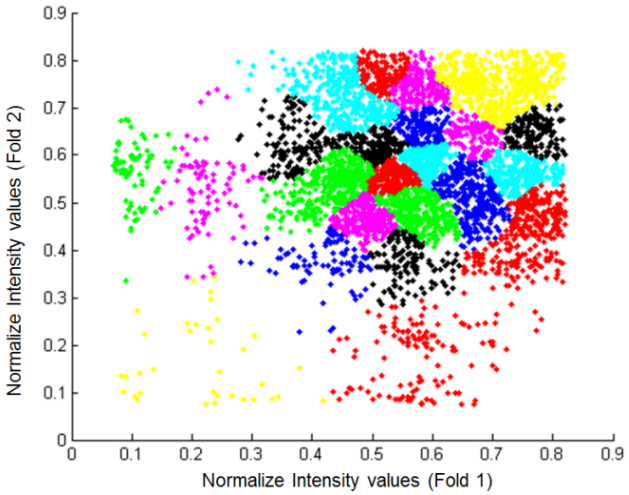


Figure 6: Clustered cancelable template for using k-means clustering.

4. EXPERIMENTS

A performance of the biometric system is highly dependent on the training process. To ensure successful training, database selection and pre-processing is necessary and crucial. In multi-biometric system, it is often that databases used in experiment are not true databases due to the cost and effort associated with data acquisition and processing (Jain, Nandakumar, & Nagar, 2008). The creation of the virtual database is based on the assumption that the different biometric traits of the same person are unique and independent. For testing our premises, we have used a virtual database that contains data form two different unimodal biometric database for face and ear.

For face, VidTIMIT (Sanderson & Paliwal, 2002) and Olivetti Research Lab Database (Samaria & Harter, 1994) are used. The VidTIMIT dataset is comprised of video and corresponding audio recordings of 43 people, reciting short sentences. It can be useful for research on topics such as automatic lip reading, multi-view face recognition, multimodal speech recognition and person identification. The dataset was recorded in 3 sessions, with a mean delay of 7 days between Session 1 and 2, and 6 days between Session 2 and 3. The sentences were chosen from the test section of the TIMIT corpus. In addition to the sentences, each person performed a head rotation sequence in each session. The sequence consists of the person moving their head to the left, right, back to the center, up, then down and finally return to center. The video of each person is stored as a numbered sequence of JPEG images with a resolution of 512 x 384 pixels. 90% quality setting was used during the creation of the JPEG images.

Olivetti Research Lab Database, also known as AT&T database of Faces contains a set of face images taken between April 1992 and April 1994. The database was used in the context of a face recognition project carried out in collaboration with the Speech, Vision and Robotics Group of the Cambridge University. There are ten different images of each of 40 subjects. The images were taken at different times, varying the lighting, facial expressions (open / closed eyes, smiling / not smiling) and facial details (glasses / no glasses). All the images were taken against the same dark background with the subjects in an upright, frontal position. The size of each image is 92x112 pixels, with 256 grey levels per pixel.

Two databases called University of Science and Technology Beijing (USTB) Image Database I & II (Zhichun, Zhengguang, Yuan, & Wang, 2003) for ear are selected to generate virtual multimodal Face-Ear. Subjects are student and teacher from the Department of Information Engineering, University of Science and Technology Beijing. In Image Database I, every volunteer is photographed three different images. They are normal frontal image, frontal image with trivial angle rotation and image under different lighting condition. Each of them has 256 gray scales. Images had already experienced rotation and shearing, but they were without illumination compensation.

In Image Database II (Zhichun, Zhengguang, Yuan, & Wang, 2003), the subject's head in right hand view is photographed by CCD camera. The distance between subject and camera is fixed to 2 meters. In terms of illumination variations and angle variations, we adopt methods illustrated in the figure 2 and figure 3 respectively. In the figures, S represents the subject, C represents the camera and Lx represents the lamp (L1 represents the one right above the subject and L2 and L3 have certain angle changes from the subject). Every volunteer is photographed four images. They are profile image, two images with angle variation and one with illumination variation. Each image is 24-bit true color image and 300x400 pixels. The first image and the fourth one are both profile image but under different lighting. The second and the third one have the same illumination condition with the first while they have separately rotated +30 degree and -30 degree with the first one. Thus, the main purpose of the image database is to support the research about ear recognition under illumination variations and angle variations. Following table shows the virtual database setup for three sets of virtual database. Sample of virtual multimodal biometric database are shown in Figure 7

Table 1: Randomly created virtual multimodal database, each set is designed using different numbers of subjects from different databases. For each subject three images are taken.

SET	***FACE***		***EAR***		***Total***	***Resolution***
	VIDTIMIT	***AT&T***	***USTB 1***	***USTB 1***	***Samples***	
SET-01	43(3)	40(3)	60(3)	23(3)	249	100x100
SET-02	43(3)	40(3)	43(3)	40(3)	249	75x50
SET-03	43(3)	40(3)	23(3)	60(3)	249	100x80

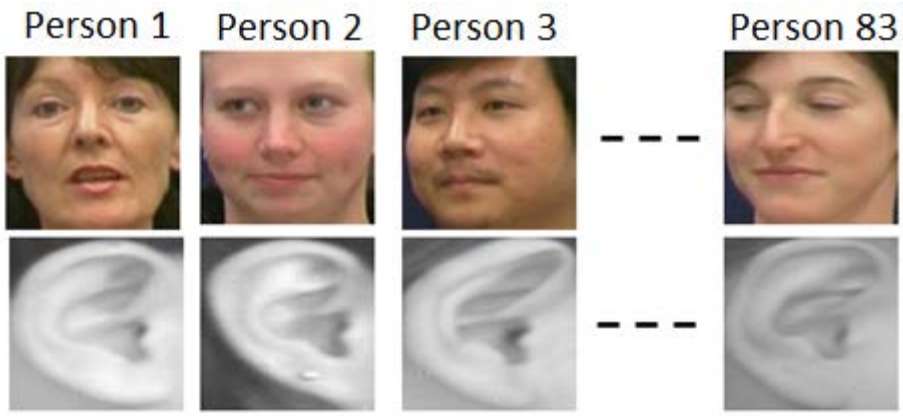


Figure 7. Samples form virtual multimodal database.

4.1 Experimental Setup

We have designed cancelable multibiometric system using MATLAB 2009b on Intel Core i7 2.2GHz Windows 7 Enterprise workstation. Developed system is menu driven Graphical User Interface (GUI) that support both 32-bit and 64-bit version of Windows. Virtual database is preprocessed and saved as MATLAB standard database file with mat extension. Each biometric trait is scaled into 100x100 resolution grayscale bitmap image. GUI includes a button to selection of database for connection. As soon as database is connected, it automatically retrieves all the dimension information and number of samples form the database. Developed system has the capability of processing biometrics of different resolution and this processing is automatic. User can also input number of fold for cross validation process. All the results presented in this paper are from 10-fold cross validation and system can automatically create the dataset for 10 folds to use them in training and testing. In addition, the thresholds for biometric trait recognition and Social Network Analysis can be changed using another configuration GUI module. Virtual database contains about 502 images, 400 images for face and 102 images for ear.

4.2 Performance Measure of Biometric System

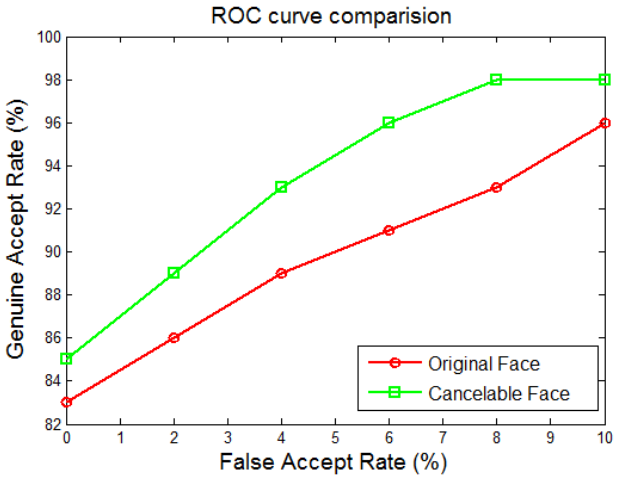
In biometric performance measure, False Acceptance Rate (FAR) and False Rejection Rate (FRR) are two important error rates. According to (Yanushkevich, Gavrilova, Wang, & Srihari, 2007), a decision made by a biometric system is either a “genuine individual” type of decision or an “impostor” type of decision (Yanushkevich, Gavrilova, Wang, & Srihari, 2007). This means for each type of decision true and false are two possible outcomes. The False Acceptance Rate (FAR) is known as the probability of an impostor being accepted as a genuine individual. On the other hand, the False Rejection Rate (FRR) is known as the probability of a genuine individual being rejected as an impostor. Genuine Accept Rate (GAR) can also be used for biometric system performance. The GAR is computed as:

$$GAR = 1 - FRR. \quad (3)$$

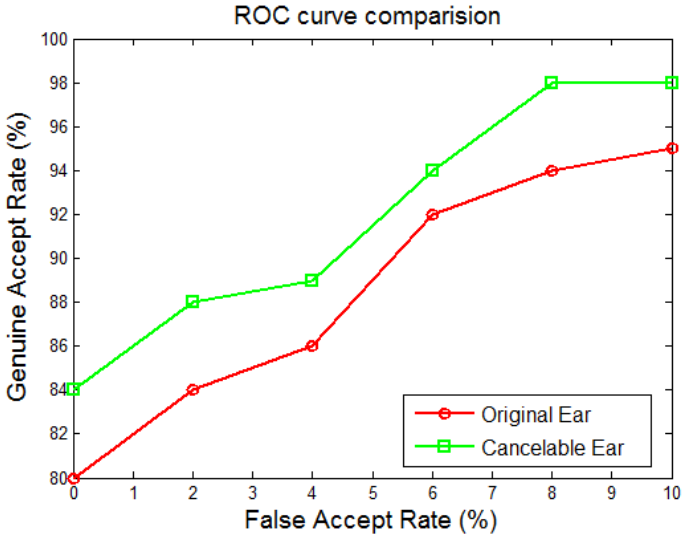
4.3 Experimental Results

In the experiment, we have used ten-fold cross validation on our virtual multimodal database. We have tested the properties of cancelable biometric. In the result, we have shown that using cancelable biometric template achieved performance is better than the original template. We have tested for both unimodal system and multimodal system. Figure 8 (a) shows the ROC curve for cancelable biometric template and the original face template. In Figure 8 (b), we have shown the similar comparative result for

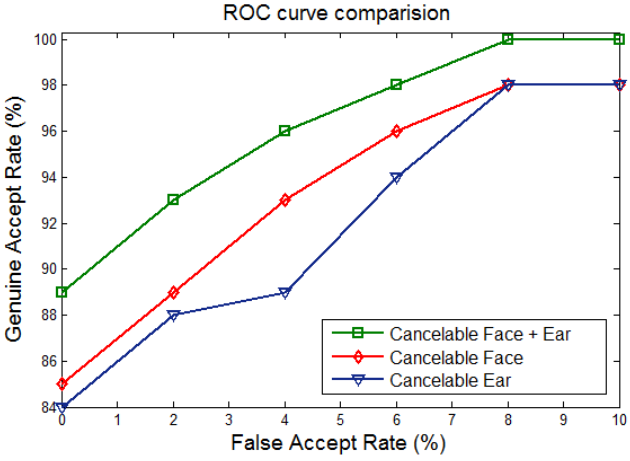
cancelable ear and original ear template. Finally, the performance of multimodal cancelable template and cancelable unimodal cancelable biometric is shown.



(a)



(b)



(c)

Figure 8: (a) ROC curve for original face and cancelable face template. (b) ROC curve for original ear and cancelable ear template. (c) ROC curve for multimodal cancelable biometric template and unimodal cancelable biometric is shown.

From the result, we have found that using cancelable biometric template from unimodal system preserve the interclass and intraclass variability. On the other hand, from the result it is found that multimodal cancelable system improves the performance compared with unimodal biometric system. Our proposed Multimodal Cancelable Biometric System preserves the cancelable property.

Furthermore, if we do not have the randomly selected feature index, cancelable biometric system would not correctly recognize an individual class. We have tested our system using other randomly selected indexes to split the features. We tested under the same experimental conditions, with modifications in random selection of features. We have found that if we change the random selection of feature, then classifier is unable to recognize the person. This performance ensures cancelability of the template. If we open those indices of cross folding it is impossible to reproduce the original face or ear template. Following figure 9 show the result of changed random selection and projection.

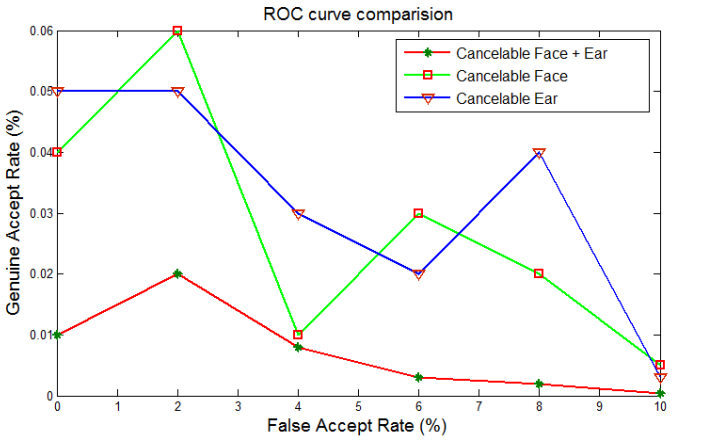


Figure 8: ROC curve for false random selection and projection for Face-Ear, Face and Ear.

5. CONCLUSION

We have presented a new cancelable biometric template generation algorithm using random projection and transformation based feature extraction and selection. We have reported the results that satisfy cancelable property of the biometric system. Moreover, we applied the method for the first time to multi-modal system that satisfies cancelable property. Hence, we can conclude that Multimodal Cancelable Biometric system is possible. The current result shows that the proposed method can successfully generate cancelable template for multi-modal biometric system. In future different method of fusion can be tested for the performance analysis. Automatic generation of random indices from user specific data can be analyzed from for the system. Key binding approach adopting with the current system can enhance the cancelability. More analysis for the cancelability measure can address more challenges of Cancelable Biometric system. On the other hand adopting another biometric trait with the system can also enhance the cancelability and security of the system.

ACKNOWLEDGMENT

Authors are grateful for NSERC and GEOIDE partial support of the project.

References

Alder, A. (2003). Sample images can be independently restored from face recognition templates. *Elect. Comput. Eng, 2*, 1163-1166.

Darrell, S., & Indyk. (2005). *Nearest-Neighbor Methods in Learning and Vision.* MIT Press, ISBN 0-262-19547.

Down, M. P., & Sands, R. J. (2004). Biometrics: An overview of the technology, challenges and control considerations. *Jounal of Inf. Syst. Control, 4*, 53-56.

Feng, Y. C., Yuen, P. C., & Jain, A. K. (2010). A Hybrid Approach for Generating Secure and Discriminating Face Template. *IEEE Trans. On Information Forensics and Security, 5*(1), 103-117.

Goh, A., & Ngo, D. C. (2003). Computation of cryptographic keys from face biometrics. *7th IFIP TC6/TC11 Conf. Commun. Multimedia Security, 22*, pp. 1-13.

Harrison, W. R. (1981). *Suspect Documents, Their Scientific Examination.* Chicago, II, USA: Nelson-Hall.

Jain, A. K. (2007). Biometric recognition: Q&A. *Nature, 449*, 38-40.

Jain, A. K., & Pankanti, S. (2006). A touch of money. *IEEE Spectrum, 43*(7), 22-27.

Jain, A. K., Flynn, P., & Ross, A. (2007). *Handbook of Biometrics.* Springer.

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing, 2008*.

Juels, A., & Wattenberg, M. (1999). A fuzzy commitment scheme. *Proc. Sixth ACM Conf. Comp. and Commun. Security* (pp. 26-36). ACM.

Matsumoto, T., Hirabayashi, M., & Sato, K. (2004). A vulnerability evaluation of iris matching. *Proceedings of the Symposium on Cryptography and Information Security*, (pp. 701-706). Iwate, Japan.

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial "gummy" fingers on finger-print systems. *Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV,*, (pp. 275-289). San Jose, Calif, USA.

Perpinan, C. (1995). *Compression neural networks for feature extraction: Application to human recognition from ear images.* Madrid, Spain: M.S. thesis, Faculty Informat., Tech. Univ.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy*, 33-42.

Randall, D., & Martinez, R. T. (2003). The general inefficiency of batch training for gradient descent learning. *Neural Networks, 16*(10), 1429-1451.

Ratha, N., Chikkerur, S., Connell, J., & Bolle, R. (2007). Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell, 29*(4), 561-572.

Ross, A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of Multibiometrics.* New York: Springer-Verlag.

Ross, A., Shah, J., & Jain, A. K. (2007). From template to image: reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4), 544-560.

Samaria, F., & Harter, A. (1994). Parameterization of a stochastic model for human face identification. *2nd IEEE Workshop Appl. Comput. Vis.*, (pp. 138-142). Sarasota, FL.

Sanderson, C., & Paliwal, K. (2002). Polynomial Features for Robust Face Authentication. *IEEE International Conference on Image Processing, 3*, 997-1000.

Statheropoulos, M., Pappa, A., Karamertzanis, P., & Meuzelaar, H. L. (1999). Noise reduction of fast, repetitive GC/MS measurements using principal component analysis (PCA). *Analytica Chimica Acta, 401*(1-2), 35-43.

Teoh, A., Ngo, D., & Goh, A. (2004). Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition, 37*(11), 2245-2255.

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: Issues and challenges. *Proc. IEEE, 92*, 948-960.

Wretling, P., & P, E. (2007). How flexible is the human voice? A case study of mimicry. *Proceedings of the European Conference on Speech Technology*, (pp. 1043–1046). Rhodes, Greece.

Yanushkevich, S., Gavrilova, M., Wang, P., & Srihari, S. (2007). *Image Pattern Recognition: Synthesis and Analysis in Biometrics* (Vol. 67). World Scientific Publishers.

Zhichun, M., Zhengguang, X., Yuan, L., & Wang, Z. (2003). A New Technology of Biometric Indentification-Ear Recognition. *The 4th Chinese Conference on Biometric Recognition*, (pp. 286-289). Beijing.