Pak. J. Biotechnol. Vol. 13 special issue II (International Conference on Engineering and Technology Systems (ICET'16) Pp. 138 - 142 (2016)

SIMULATION OF MULTIMODAL BIOMETRICS WITH CRYPTOSYSTEM IN HOSPITAL SUITES

[1]Lalithamani, N. and B. Sruthi[2]

Department of Computer Science and Engineering Amrita School of Engineering, Coimbatore
Amrita VishwaVidyapeetham, India. E-mail : [1]n_lalitha@cb.amrita.edu; [2]bsruts@gmail.com

ABSTRACT

Objectives: To apply Multimodal Biometrics in the authentication process in hospital suites, fusing two Biometric traits namely face and fingerprint at the feature level to improve the security.

Methods/Statistical analysis: This paper deals with using face and fingerprints, which are fused at the feature level and processed further. Majorly, techniques for pre-processing include Histogram Equalization for face, and Skeletonizing and thinning for fingerprints. In the next stage, Feature Extraction techniques like PCA (Principal Component Analysis) for face and Ridge Endings and Bifurcation extractions for fingerprint are used. Then once fused at feature level, shuffling is done and the fusion vectors are encrypted. These are used for authentication in hospital suites.

Findings: In general, Multimodal Biometrics offers higher security than Unimodal when implemented efficiently. This concept can be used in hospital suites, where security is prime importance and a breach of the same can endanger the lives of patients.

Application/Improvements: As mentioned, this concept can be highly useful in hospital suites, where close monitoring of access to VIP suites is necessary. Since a breach of security can be very sensitive in such places, it is important to employ maximum protection for the authentic-cation process. Areas where it could be improved further can be in increasing the number of traits for tighter security, and exploring apt fusion methods for the same to improve efficiency. Also, in future different encryption algorithms can be tested and tried.

Keywords*: *Multimodal Biometrics, Feature level fusion, Cryptosystem, Hospitals

1. INTRODUCTION

Multimodal biometrics[1] is the use of multiple characteristics in conjunction to identify an individual. Some characteristics include, finger prints, iris, voice, facial recognition, facial structure, handwriting, retina, gait, scent, gesture, ear height, etc.[2]. These, on their own, can be faked by a determined person but when they are used *in conjunction*, they identify you in a secure way. Adding a cryptographic module[3,4] will only strengthen the level of security.

In this paper, we aim to use two of these traits, namely face and fingerprint, for feature level fusion[5] and to simulate the authentication process in hospital suites. The images of the traits are taken from the existing database. Face prints are obtained from AT&T database and fingerprints from CAS IA[6]. Once the images are obtained, pre-processing techniques are applied on them to remove any noise that might be present. Then the features from both the traits are extracted and fused at the feature level to obtain fused vectors for face and fingerprint respectively. Shuffling algorithms[7] are applied to the fused vectors and they are encrypted. The encrypted form of vectors is stored in the hospital server for comparison.

The images of face and fingerprint are pre-processed. For face, Histogram Equalization[8] is used and for fingerprint Skeletonizing and thinning[9] are used. Once pre-processing is done, features are extracted by applying certain feature extraction techniques like PCA (Principal Component Analysis) for face and ridge endings and bifurcation extractions for fingerprint. Shuffling algorithms are applied before fusing, feature level fusion is performed, and again Shuffling algorithms are used to encrypt the fused vectors.

Feature level fusion is preferred because it improves the accuracy of the system. As compared to match level and decision level fusion[10], more raw information is obtained at this stage which improves the efficiency.

The cryptographic module uses Shuffling algorithms which contain a revocable logic for encrypttion. These shuffling algorithms provide an extra layer of security. Generally, a shuffle key is generated the vector is mapped per a logic with the shuffle key. This process is revocable. For any Biometric System, pre-processing, feature extraction is done before the actual processing of the images to improve its quality.

A. Fingerprint processing: Fingerprints are mainly characterized by their ridges and valleys. The cuts and bruises present may cause ridge discontinuities, which degrades the quality of finger print images. In[11] describes the pre-processing methods for finger print which includes extraction of ridges and bifurcations. Minutiae points can be extracted from the skeleton of the fingerprint images. The process of thinning is applied on a binary image which is based on thresholding of the input image, and the skeleton is obtained after the skeletonization[9].

Once the skeleton of the image is obtained, minutiae can be extracted from it. Minutiae can be based on two forms namely ridge endings and ridge bifurcations[12,13,14]. Thus these are extracted from the skeletonized image. In[9] it is described as an algorithm which can detect a maximum number of minutiae points from the skeletonized fingerprint using Rutovitz crossing number.

After the pre-processing stage, the ridge endings and bifurcations are extracted, and stored as a finger print minutiae template. Shuffling is then performed on these templates before the fusion process. A shuffle key is gene-rated, which is a pattern of zeroes and ones. A revocable logic is applied to the corresponding template vector, and a shuffled vector is obtained.

B. Faceprint processing: Facial features can be pre-processed and extracted in numerous ways like Histogram Equalization, LOG, GIC (Gamma Intensity Correction), SQI, etc.[8] discusses pre-processing methods like Gamma Correction, DOG (Difference of Gaussian) filtering, contrast equalization.

i. Histogram Equalization: This is a normalization technique that deals with redistributing the different levels of the image to obtain an increase in the contrast of the image. So, Histogram Equalization adjusts the intensity levels to enhance the contrast of the image[15]. It results in a histogram that is constant for all intensity levels thereby providing an intensity distribution where all the values will be equally probable.

For a grayscale image $\{x\}$ and let n_i be the number of occurrences of gray level i. The probability of an occurrence of a pixel of level i in the image is

$$p_x(i) = p(x = i) = \frac{n_i}{n}, 0 \le I \le L$$

L being the total number of gray levels in the image (typically 256), n being the total number of pixels in the image, and $p_x(i)$ being in fact the image's histogram for pixel value i, normalized to [0,1].

ii. LOG (Laplacian of Gaussian): The Laplacian of an image highlights the regions of rapid intensity change and is therefore often used for edge detection[16]. Generally, this operator is applied to images that have been already smoothed using smoothening techniques.

iii, GIC (Gamma Intensity Correction): Gamma Intensity Correction controls the overall brightness of the image.

iv. SQI (Self Quotient Image): SQI is based on the reflectance-illuminance model. It uses a weighted Gaussian filter that convolutes with only the large part in edge regions. Thus, the halo effects can be reduced.

Results show that Histogram Equalization and GIC are better than the other two methods, as they don't involve too much of complexities. Once pre-processing is done for the face images, various algorithms are available for feature extraction like PCA (Principal Component Analysis), LDA (Linear Discriminant Analysis), Gabor Wavelet, etc. Both Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) are linear transformation techniques that are commonly used for dimensionality reduction. Shuffling algorithm is applied to the face vector and stored in the database.

C. Fusion: Fusion can be as simple as concatenating the obtained shuffled vectors or using an algorithm for the process, at the feature level. Three levels of fusion are possible, namely, Feature Level, Match Level and Decision Level[17,18,19,20,21,22]describes the various levels of fusion, the techniques used in each level for improving the performance at each level.

Feature level, Match level and Decision level fusion involve combining the vectors at the feature stage, matching stage (once a score is generated) and decision stage (where the decision to accept or reject is combined) respectively. One more type of fusion that can be performed is the sensor level fusion, where the raw data of the traits from the sensors are combined[23]. But not always will the data obtained from sensors be compatible as images might be from different resolution cameras. In general, the sensor level and feature level fusion are termed as Pre-classification fusion[22] as the integration of data happens before classification or matching. The others are called Post-classification fusion.

Fusion at feature level[5] involves the integration of feature sets corresponding to multiple information sources. The feature set contains richer information about the raw biometric data than the match score or the final decision, integration at this level is expected to provide better authentication results.

D. Shuffling: Shuffling involves using an algorithm that is reversible to encrypt the feature vectors to enhance the security. These shuffling algorithms make use of a shuffle key that is generated to shuffle the vectors.

In[24] it explains how to use shuffle based feature level fusion, where they combine feature vectors based on a Shuffling Algorithm.

2. **PROPOSED SYSTEM:** Figure 1 shows the flow chart of the proposed system that outlines the major areas of the work.

It gives the general flow of the process of enrollment and verification, both of which uses the Biometric module for its processing. Fig. 1. Flow chart representing the Enrollment and Authentication Process. In this paper, we propose to create a simulation software for Fusion based Multimodal Biometric Crypto- system for Hospital Suites. We are employing the following methods and algorithms for processing the images of the traits: Histogram Equalization for face, thinning and skeletonizing for fingerprint in the pre-processing phase; PCA for face, Ridge endings and Ridge Bifurcation extraction in the feature extraction phase.

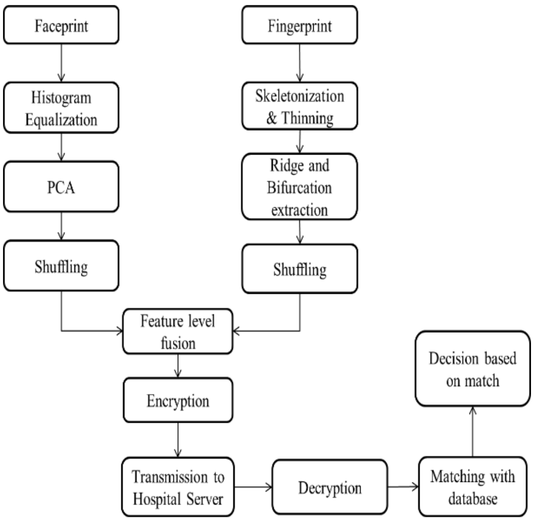


Fig. -1: Flowchart representing the Enrollment and Authentication Process.

Once the feature vectors are obtained they are shuffled separately and fused at the feature level by concatenation. The fused vector is again shuffled and stored in the database. The input image is taken and processed the same way and compared with the stored templates.

A. Pre-Processing: *Face:* In the pre-processing stage, the images obtained from the database are fed as input for the registration process. After a standard sequence of cropping and converting it to a binary image, Histogram Equalization is applied on the images and stored in the database[24].

Fingerprint: For fingerprint first thinning is performed to obtain a skeleton of the image. Thinning invlves adaptive frequency thresholding of the gray images. After thinning, skeletonizing is done to obtain the pre-processed image for minutiae extraction.

B. **Feature Extraction:** *Face:* PCA algorithm is employed for feature extraction in face images. This algorithm tries to reduce the dimensionality of the data while retaining the non-redundant information. It allows us to compute a linear transformation that maps data from a higher dimensional space to a lower dimensional sub-space. For this we need to compute the eigen faces using the covariance matrix[25].

The following steps are used in general:

- Compute the average face vector (φ)
- Subtract the mean face (ϕ_i)
- Compute the covariance matrix, C
- Compute the eigen values

Once the eigen faces are computed, they are stored as a linear combination of eigen vectors in the database as shown in Figure 2.

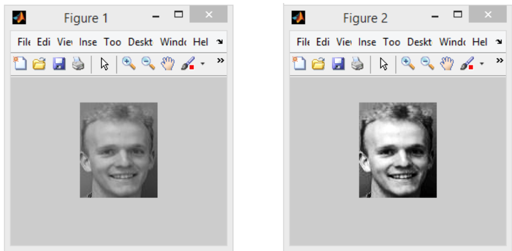
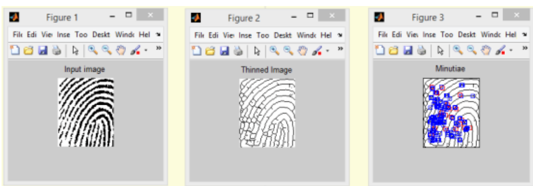


Fig. 2. Preprocessing of face image (a) Input face image (b) Image after Histogram Equalization

Fingerprint: For fingerprints, we extract the minutiae points by finding the region of interest (ROI), and extracting the ridge endings and ridge bifurcations. The extracted features are stored as feature vectors in the database as shown in Figure 3.



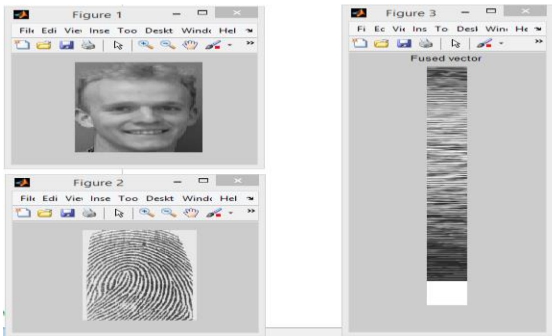
a b c

Fig. -3: a) Input fingerprint image b) Fingerprint image after thinning c) Minutiae extracted from the fingerprint image

C. **Shuffling & Fusion:** Once the feature vectors are obtained we shuffle them separately using a shuffling algorithm. For that a shuffle key is generated:

- Generate a shuffle key, K, consisting of ones and zeroes
- Group all the values corresponding to zeroes in the front
- Group all the values corresponding to ones in the back
- Store the resulting vector, V_i, in the database for comparison

Once the shuffled vectors are obtained, they are concatenated and the fused vector, f_i, is obtained. The shuffling algorithm[26] is again applied to the fused vector before storing it in the database for further comparisons as shown in Figure 4.



(a) (b)

Fig. -4: (a) The input traits – face and fingerprint (b) The fused vector of the input traits

D. **Comparison:** The input images are taken in for comparisons, and the same pre-processing and feature extraction techniques are applied on them. Shuffling is performed and the resulting fused vector is considered for comparisons. We use Euclidean distances to measure the extent of match between the input and the stored images. The general method for calculating the Euclidean Distance is:

$$d(x,y)=\sqrt{\sum_{1}^{n}(x_i-y_i)^2}$$

where x and y belong to the vectors fused vectors X and Y.

Based on the result of the comparison, FAR (False Accept Rate) and FRR (False Reject Rate) are computed. FAR is calculated as a fraction of impostor scores exceeding a threshold. FRR is calculated as a fraction of genuine scores falling below a threshold as shown in Figure 5.

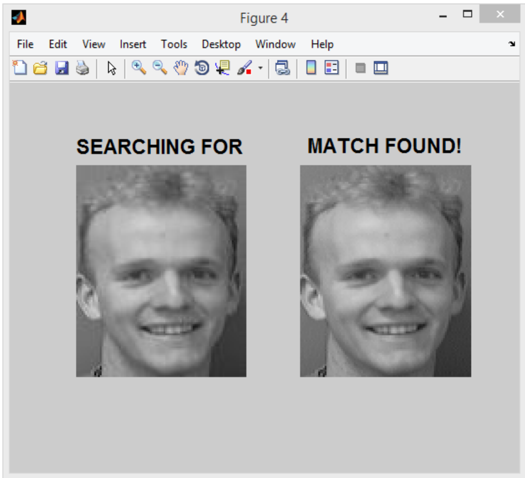


Fig. -5: Generating a match for the individual

3. RESULTS AND DISCUSSIONS

After registering for 100 images, we found our efficiency to be 96.12%. The False Acceptance Rate was computed to be 3.39%. Thus, we simulated the software, that allows or denies the authentication process to take place in the hospital suite.

4. CONCLUSION

This simulation was done in Matlab R2010a. The images were obtained from the existing databases and successfully registered as a training set after pre-processing, feature extraction, fusion and shuffling. The input image was fed and the same procedures were applied on it. And a match was generated based on which the simulation for the authentication in a hospital suite was performed.

This system can be used for various other applications where security is an issue that needs to be taken care of. Some application areas include Digilocker, Airport Security System (Immigration), Pension schemes (to avoid false acquisition) and Gas Connection subsidy.

REFERENCES

1. Komal, S. and Y. Bansal, Concept of Unimodal and Multimodal Biometric System. International Journal of Advanced Research in Computer Science and Software Engineering 4(6): 394-400 (2014)
2. Prasad, M. and K.L. Sudha, Chaos Image Encryption using Pixel shuffling. Computer Science & Information Technology 169–179 (2011).
3. Kekre, H. B., T. Sarode and P. Halarnkar, Image Scrambling using R-Prime Shuffle. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2(8): 2320–3765 (2013).

4. Somdip, D., SD-EI: A Cryptographic Technique To Encrypt Images. IEEE Journal 28-32(2012)
5. Yogesh, H.D. and S.R. Inamdar, Fusion Based Multimodal Biometric Crypto-system. International Conference on Industrial Instrumentation and Control (2015)
6. Lalithamani, N. and K.P. Soman, An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates. International Journal of Computer Science and Network Security 9(3): 183-193 (2009).
7. Ahmad, M.L., W.L. Woo and S.S. Dlay, Multimodal Biometric Fusion at Feature Level: Face and Palmprint. IEEE Pp. 537 - 541 (2010).
8. Anila, S. and N. Devarajan, Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions. Global Journal of Computer Science and Technology Graphics & Vision. Version 1.0 12(11): 13- 18 (2012).
9. Zhao, F. and X. Tang, Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. Pattern Recognition Society Pp. 1270 – 1281 (2007).
10. Taruna, P. and A. Singh, Multimodal Biometric System. International Journal of Advanced Research in Computer Science and Software Engineering 3(5): 1360-1363 (2013).
11. Patel, U., A Study on Fingerprint (biometrics) Recognition. International Journal of Engineering and Sciences 1(2): 1- 6 (2015).
12. Ross, A. and A.K. Jain, Information Fusion in Biometrics. Pattern Recognition Letters 24 (13): 2115-2125 (2003).
13. Shubhangi, D.C. and B. Bali, Multi-Biometric Approaches to Face and Fingerprint Biometrics. International Journal of Engineering Research & Technology 1: 1-7 (2012).
14. Barman, S., D. Samanta and S. Chattopadhyay, Fingerprint-based crypto-biometric system for network security. EURASIP Journal on Information Security (2015).
15. Pankesh, B., Image Encryption Using Pixel Shuffling. International Journal of Advanced Research in Computer Science and Software Engineering 2(12): 279-282 (2012).
16. Prabhakar, S. and A.K. Jain, Decision-level fusion in fingerprint verification. Pattern Recognition 35: 861-874 (2002).
17. Omaima, N. and M. Abdel-Mottaleb, Fusion of Matching Algorithms for Human Identification Using Dental X-Ray Radiographs. IEEE Trans-actions on information forensics and security 3(2): 586 - 591 (2008).
18. Mohamad Abdolahi, Majid Mohamadi and Mehdi Jafari, Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic. International Journal of Soft Computing and Engineering 2(6): 504-510 (2013)
19. Sireesha, V. and K. Sandhyarani, Overview of Multimodal Biometrics. Publications of Problems & Application In Engineering Research 4: 170-173 (2013).
20. Nageshkumar, M., P.K. Mahesh and M.N.S. Swamy, An Efficient Secure Multi-modal Biometric Fusion Using Palmprint and Face Image. International Journal of Computer Science 2: 49-53 (2009)
21. Dapinder, K. and G. Kaur, Level of Fusion in Multimodal Biometrics: A Review. International Journal of Advanced Research in Computer Science and Software Engineering 3(2): 242-246 (2013)
22. Ross A. and R. Govindarajan, Feature Level Fusion Using Hand and Face Biometrics. SPIE Conference on Biometric Technology for Human Identification II. 5779, Pp. 196-204 (2005).
23. Agarwal, N. and H. Sharma, An Enhanced Pixel-Shuffling based Approach to Simultaneously Perform Double-DCT Image Compression, Encryption and Secondary Steganography. International Journal of Computer Applications 75(7): 376-385 (2013).
24. Jeng, R.-H., W.-S. Chen and L. Hsieh, An Efficient Feature-Level Fusion Scheme in Multimodal Biometrics. International Conference on Machine Vision Applications (2013)
25. Turk, M. and A. Pentland, Eigenfaces for recognition. Journal of Cognitive Neuroscience 3: 71–86 (1991)
26. Shivsubramani, K. and K.P. Soman, Implementation and Comparative Study of Image Fusion Algorithms. International Journal of Computer Applications. 9(2): 25-35 (2010).