Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 6 (2018) pp. 040-047

Secured Biometric Template matching by using Linear Discriminant Analysis

Surbhi vijh[1], Deepak Gaur [2]

[1]Department of Computer Science and Engineering, Amity University
Sector 125, Noida, Uttar Pradesh
Surbhivijh428@gmail.com

[2]Department of Computer Science and Engineering, Amity University
Sector 125, Noida, Uttar Pradesh
dgaur@amity.edu

***Abstract*: Now a day's biometric template matching is of great concern in forensic science. There are different technical classifiers to find out the matching between these templates such as Naïve Bayes classifiers, PCA algorithm, SVM classifier etc. Different classifier gave the different level of accuracy results. All of above these classifiers, Linear Discriminant analysis (LDA) is the classifier which always give best direction of projection for number of classes of features. So, in our experimental result, we use the Linear Discriminant analysis (LDA) to find out the matching between biometric templates. We took the data set of fingerprints; make these fingerprints secured by using Logistic Mapped encryption algorithm. Apply the pre-possessing and post-processing on these encoded fingerprints and matched the fingerprints to the data set by using LDA. Simulated model was found to measure the accurate percentage results of biometric templates.**

***Keywords*:** Biometric Template, Logistic Mapped Encryption Algorithm, Security, Fingerprint, Linear Discriminant analysis (LDA)

I. Introduction

In forensic science, biometric is the common process to find out the attribute of the individual. As an attribute, biometric characteristics can be the biological features which are used for computerized authentication process [1]. Identify the individual is the task to associate individual identity to the system. So, task of resolving the individual personal identity can be categorized in following two steps, verification and identification. So, generally verification is the term refers to find out the personal identity i.e. problem of identify the one's identity from the known or unknown database. Whereas recognition is the process which does not necessarily applied the verification process. In recognition we are much focused on the matching between the two identities from the database. All biometric authentication system is based on this recognition step where all the individuals are previously enrolled in the system and we matched these enrolled templates to the unknown biometric template. Biometric system where this recognition is of high accuracy is termed as "Positive personal identification". In complex modern era, process of identification is more demanding in various areas which become very important to identify the individual in efficient manner [2]. Characteristics of biometric system are the most important issue in forensic science [3]. Further biometric system comes under the number of modalities [4]. These modalities include Voice base recognition [5], Fingerprint based recognition [6], Facial recognition [7], Iris based recognition [8] and signature-based recognition [9], Fast Minutiae-Based Fingerprint Recognition [39], Teeth image Recognition system [26]. Due to time variation, sample of the biometric trait system are changed continuously. This variability changed among biometric feature classes is known as intra user feature variations. For example, in case of fingerprint recognition, different factors such as finger pressure, skin changes and ages variation lead to error generation to the biometric system. So, this variation dramatically affects the performance of the particular biometric system. We have to maintain the feasibility of these system for biometric trait recognition due course of long time [10]. The crypto-biometric system is buoyant to many attacks [41] so it provided efficient solution by using session based cryptographic key for insecure network channel during transmission of message. Singh and Kant [42] proposed the technique of steganography for secure biometrics template system. Rani and Singh [43] presented a combined algorithm for identification of user along with comparatively high degree of security using surf, mser and Harris features.

In this research paper, we use the Linear Discriminant analysis (LDA) to find out the matching between biometric templates [12] as compare to Principal Component Analysis algorithm [24]. We took the data set of fingerprints; make these fingerprints secured by image encryption algorithm where position of pixels in the original image is shuffled and gray values are encrypted using Logistic Map generated [11]. Here we calculate textural statistical features for fingerprint feature extraction of biometric fingerprint template. Once image is encoded, this encoded image is used for pre- processing and post- processing by image enhancement techniques. Finally enhanced encoded image is matched with the data set. The

Simulated model was found measure the accurate percentage result of fingerprints. Cappelli et al. [29] proposed approach for reconstruction of fingerprint image through the use of standard template and matched the original and reconstructed image. Haraksim et al. [44] presented the different fingerprint detection techniques for performance evaluation.

This paper is structured as follows: Section 2 discuss about the related work done on various cryptographic algorithms, biometric technique, and authentication technique. Section 3 discusses about the proposed methodology and algorithm of secured biometrics template matching using LDA. Section 4 describes about the experimental simulated result which contains image encryption algorithm result and image matching simulated result. Further it describes about the Linear Discriminant algorithm. Finally, section 5 concludes about the related work.

II. Literature Survey

A. Comparison of various cryptographic algorithms

Cryptographic algorithm analysis includes overview of the various cryptographic techniques [13]. Generally symmetric key cryptographic algorithm uses two types of ciphers, one is stream cipher and second one is block ciphers. Both ciphers are used to secure application of different types. Stream cipher works on the bit or byte steams formation whereas block cipher works on size block of the data. Following table gives the comparison between the different cryptographic algorithms. Zheng et al. [38] presented the paper which shows cryptographic key generation using lattice mapping.

1) Table

Algorithm Name	**Structure**	**Rounds**	**Key Size (In Bits)**	**Block Size (In Byte)**	**Block Modes**
AES	Substitution-permutation network	10, 12, 14	128, 192, 256	16	ECB, CBC
DES	Balanced Fiestel Network	16	56	8	CFB
Triple DES	Fiestel Network	48	112, 168	8	OFB
RC2	Source heavy Fiestel Network	18	40–1024	8	CTR
Blow Fish	Fiestel Network	16	32-448	8	PCBC
Skipjack	Unbalanced Fiestel Network	32	80	8	PCBC
RC4	---------	256	40-2048	----	Stream Cipher

Table 1. Comparison analysis of cryptographic algorithms

B Biometric Encryption Techniques

Biometric template can be secured by using various encryption techniques. These biometric encryption techniques are categorized on various parameters like key generation, key binding structure, key release method etc. Secure biometric templates are always need better encryption techniques before enroll the biometric traits to the system [14]. There are generally three type of biometric encryption techniques are in practice i.e. biometric encryption based on key release [15], biometric encryption based on key binding [16] and biometric encryption based on key generation [16]. Among these techniques key generation is the best techniques as one cannot find out the random location of key generated at every time. The chaotic map lattices are considered as another technique for biometrics encryption [25].

C. Fingerprint Authentication Techniques

In past few years, there are number of methods developed for fingerprint authentication to achieve the accurate results [18]. The performance of Artificial neuron network (ANN), Support vector machine (SVM) and Multivariate Adaptive Regression Splines (MARS) are measured for intrusion detection in to obtain accuracy during classification [32]. The two feature selection algorithm performance is calculated using Bayesian networks (BN) and Classification and Regression Tress (CART). They constructed hybrid architecture by merging the different feature selection algorithm for developing the intrusion detection system in real world [33]. The fingerprint identification in Biometric Security Systems is performed using enrollment and authentication of the input image. The optimal algorithm is used for matching in order to obtain the specified accuracy and performance [34]. The paper presented the enrollment and verification process for biometrics recognition system [37]. Different available techniques for fingerprint authentication are as follows: -

1. Threshold Based Authentication

In this authentication process, input image is divided into number of shares using the visual cryptography technique [19]. After generating the shares, input images are being compressed. So, only one share is stored in the server whereas rest of all shares are stored to user machine. Final biometric template can be reconstructed by super imposing of the shares. The main purpose of this authentication method is to reduce the error rate.

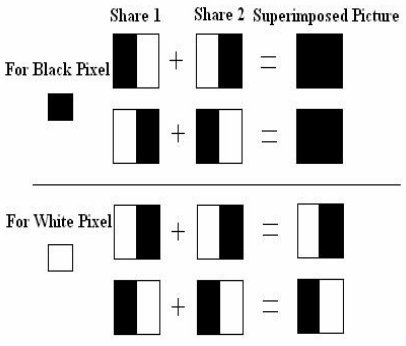


Figure 1. Threshold based authentication

Final biometric template can be reconstructed by super imposing of the shares. The main purpose of this authentication method is to reduce the error rate. Merit of this method is that system is secured from all the attacks from server machine. Demerit of this method is that there is no privacy to biometric template data set. Figure 1 shows how this authentication process generates the shares of images and matches these shares to complete the authentication process.

2. Hough Descriptor Based Technique

This technique is based on the descriptors which bring the biometric template to a line by considering the minutiae and orientation field between the biometric traits [20]. This technique is generally used to authenticate fingerprint modalities. Here sample images contain large number of the descriptors which are basis for Hough descriptor based technique. This process increases the toughness and distortion in the input fingerprint image. Process of matching used in this method is shown in figure 2. In this process, mutual marking is performed on fingerprint images to extract the minutiae location by means of automated extraction. Recognition of unknown image is done by means of aligning the minutiae features for the extracted fingerprint image. The most advantage of Hough descriptor technique is that partial fingerprint can also be identified in this process.

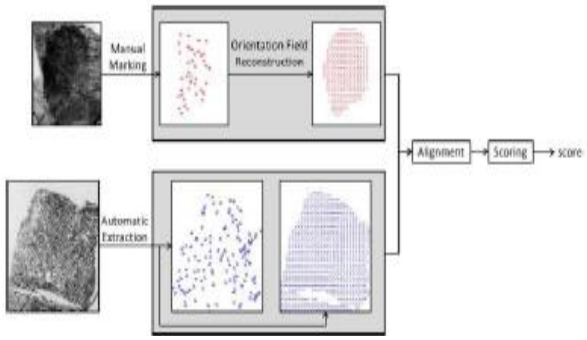


Figure. 2.Hough descriptor cryptography technique

3. Fuzzy Vault Cryptography Techniques

Fuzzy vault cryptography technique is the most accurate technique for identification with secured key generation [21]. This technique matched the unknown pattern to fingerprints image which stored the transformed type of the biometric template. This process also used the multiple biometric score value for matching purpose which improves the efficiency and quality of the biometric system. Key generation is the part which makes this technique more secure with high level accurate score value for the biometric templates. Extracted features are matched to the dataset with generated key values to implement the biometric system.

4. Minutiae Based Technique

In this technique, new biometric template is being constructed from the minutiae of both fingers values [22]. So, combined fingerprint template is constructed in two steps, in first step images are captured from both fingers of identity. So, after that a reference value from the first fingerprint is taken out and this value is combined with the minutiae features of both the fingerprints to produce the new biometric template. This constructed biometric template is than stored in the dataset. With the help of this technique, combined new template is reconstructed from the both two fingerprints value. This makes the technique quite secured for template matching. When applied these minutiae based technique on different matching algorithm, it is found that error rate is very low. This means false matching rate ratio gets reduced to large extent and system is more secured from the unauthorized person. Figure 3 illustrate how two fingerprints 'A' and 'B' are stored in the dataset. These fingerprints are stored in dataset with consideration of the reference value and minutiae location of the both the images. With the help of both these parameters new template is being constructed in efficient manner. Database stored the new template image in secured and feasible positon for matching purpose. The fingerprint image taken as an input is usually measured on the basis of minutiae [36], the performance is evaluated using orientation based spectral minutiae and location based minutiae representation. Prabhakar et al. [28] has improved the matching performance through feedback approach for feature extraction and feature refinement stage. Orientation is considered as crucial step for fingerprint recognition system [30].

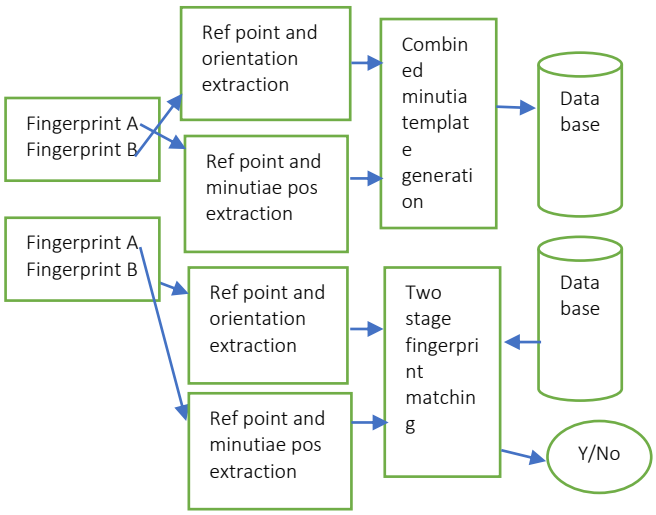


Figure 3. Minutiae based recognition system

5. Moodle Based Algorithm

This algorithm used the minutiae based technique for authenticates the biometric templates. Figure 2.5 shows the Moodle based process for fingerprint recognition [23]. Moodle also designed the software which is used for creating the new web sites, where login to these web sites include the concept of minutiae base authentication for the user. Because Moodle concept is based on minutiae based technique, so here firstly we construct the new fingerprint template with the help of reference value of first image and minutiae features values of another fingerprint image. Here we then include the binarization process followed by direction analysis of the minutiae points. This binarization involves the quantization of the image, which is the most advantage of the Moodle based technique. Following figure 4 shows the concept of minutiae based technique

D. Comparative Analysis of Techniques

Following table 2 shows the comparative study of various techniques depending upon false rejection rate (FRR) ratio:

1) Table

Technique Used	**Objective**
Matching technique [1o] .	Design voting system with matching technique with FRR as parameter. FRR ration is >15%. The system lags with high FRR ratio.
Minutiae based algorithm [11]	Design algorithm for privacy and security reason. The FRR ration is quite low i.e. o.4%.
Threshold cryptography technique [7] .	Developed the technique to divide in small number of technique [7] shares. FRR ratio is o.3 %. Compression is required for reconstruction of fingerprint image.
Fingerprint matching	Developed the technique to acceptance rate. GAR ratio is Gabor filter [8] 91 %. Compression is required for reconstruction of fingerprint image.

Table 2. Literature survey of various cryptography techniques

III. Proposed Methodology

Initially we take data set of sample fingerprint images, apply logistic mapped security algorithm on each of sample image. Than pre-process the encoded images and finally matched the processed image to data set by using linear discriminant analysis. The image preprocessing consists of image enhancement which uses histogram analysis [27] and fast Fourier transformation methods followed by the binarization process. In FFT method the factors considered are from 0-10 which can be applied on it. The image histogram equalization is the process to enhance or expand the pixel's value distribution of the image. Image segmentation is an approach of partitioning of image into a collection of connected set of pixels. It is the operation of organization of the objects into the group based upon its attribute. It can be region based, edge based etc. Thinning reduces the amount of data and time which is required to process the image by extracting the important features. It performs pixel by pixel operation until a specific pattern is determined. Some morphological operations such as removing the H breaks and spikes are used for filtering the thinned maps. Minutia marking is done through cross number. It is a method which is applied in order to extract the minutiae. It helps in locating the minutiae points. It is the process which determines the properties of a pixel by calculating the black and white transition to the neighbouring pixels (p) which are being processed. In this burification [31], termination and triple counting branch functionalities are used. The average inter ridge width is also calculated. It referred to the average distance between the two neighbouring ridges. The post processing consists of removal of false minutia. It improves the minutia extraction accuracy and improves the matching performance. The following figure 5 shows the simulated flow diagram for our experimental simulation.

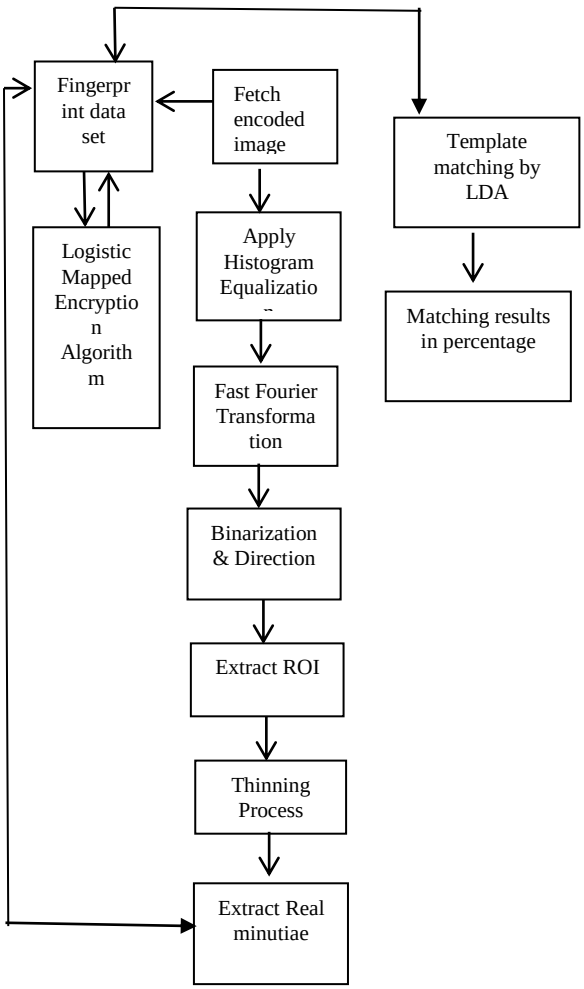


Figure 5. Secured fingerprint authentication using LDA

The flow chart of proposed methodology is shown as follows

Algorithm: ***Secured Fingerprint template matching by LDA***

Our proposed methodology follows the following steps:

1. Find out the encoded image from the fingerprint data set by applying the logistic mapped security algorithm.
2. Calculate the histogram equalization of encoded fingerprint image.
3. Apply Fast Fourier Transformation to get the sampling and quantization of encoded image.
   Apply binarization, direction to find out the region of interest for encoded image.

4. Apply thinning process to find out the enhanced image. Remove H break and extract the real minutiae values of the encoded image.
5. Save the pre-processed image to data set
6. Now apply linear discriminant analysis for matching this saved biometric template to data set. Which will give us the matching percentage value.

IV Experimental Simulated Results

A. Image Encryption Algorithm Results

Depending upon the strength parameter of encryption algorithm we achieved the following results: -

1. Histogram Analysis

The input image, corresponding to its encoded image and histogram formation of both images are shown in figure 6. From the formation of histogram of the encoded image it is being clear that we got the equalized histogram which means we have secure formation of encoded image. This encrypted biometric template does not provide any pixel information of the inputted image, which makes the attacker to difficult to hack the system. Hence, we got the secured biometric template.

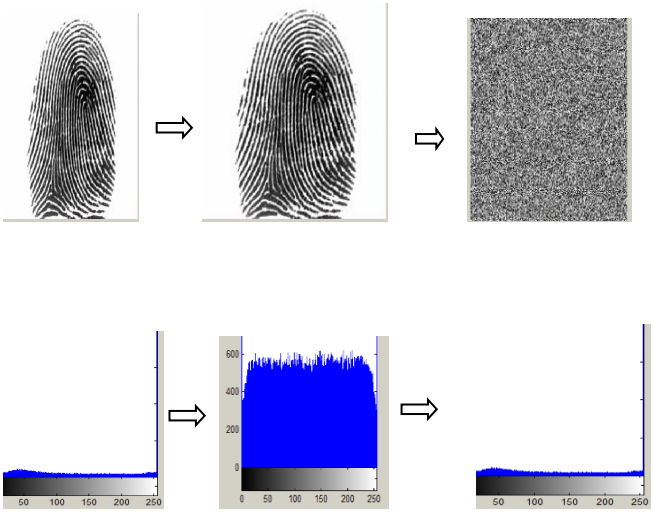


Figure 6. Input image, encoded image and histogram m formation

2. Image Entropy, Correlation and Mutual Information Analysis Results

Different images have been tested by the proposed image encryption procedure and the resulting entropy, horizontal and vertical correlation coefficients are shown in the Table 3 below. The input image is taken which is encoded by implemented certain function. The entropy of input image and encoded image is calculated. Correlation analysis is performed to examine the associated set of images.

3) Table

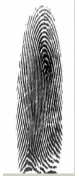
Input Image	**Encoded Image**	**Entropy Input Image**	**Entropy Encoded Image**	**Correlation Coefficient value**	**Mutual Information**
		4.6497	7.9571	0.00385	-1.74
		3.2882	7.9571	0.00096	-1.81
		2.9487	7.9571	0.00088	-1.84
		4.2054	7.9571	0.00665	-1.74
		2.6083	7.9571	-0.0001	-1.87

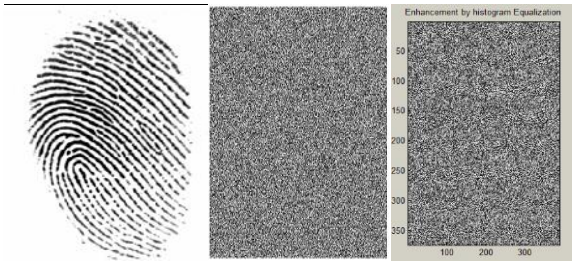
Table 3 Images with their corresponding Entropy, correlation coefficient & MI values

B. Fingerprint Matching Simulated Results

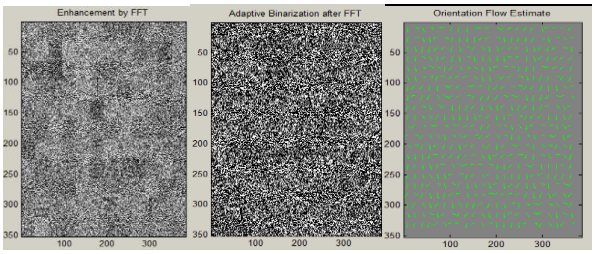
1. Simulated Results

Following is the achieved results by our experimental results: - Figure. 7 a: Input image, b: Encoded image, c: Histogram Equalization, d: FFT image, e: Binarization, f: direction, g: Thinned image, h: ROI, **i:** Extracted minutiae

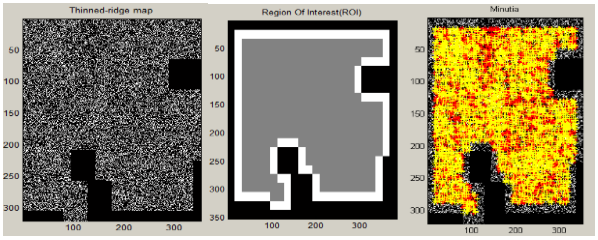
Fingerprint sample template '1' results:



(a) (b) (c)

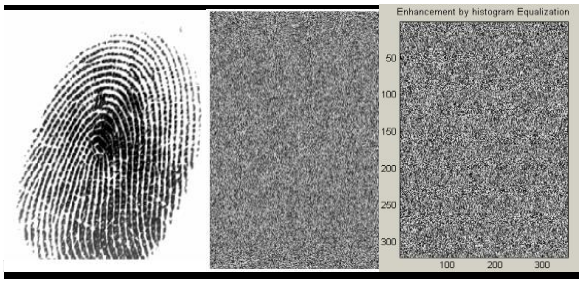


(d) (e) (f)

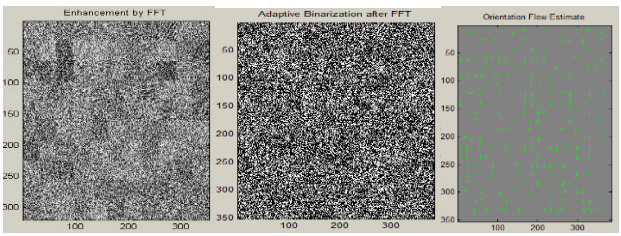


(g) (h) (i)

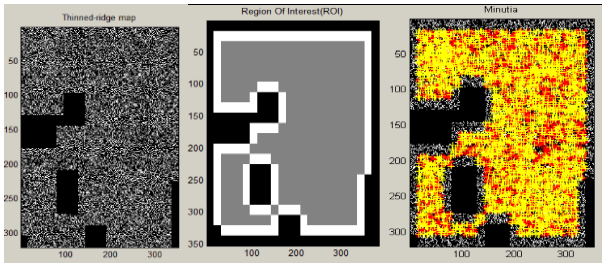
Fingerprint sample template ‘2’ results:



(a) (b) (c)



(d) (e) (f)



(g) (h) (i)

Figure 7: Simulated results on fingerprint sample template ‘1’ and ‘2’

In the above fingerprint sample template 1 and template 2 results:

a. Take the input image from the fingerprint data set.
b. The input image is encoded by applying logistic mapped security algorithm.
c. The histogram equalization is applied on the encoded fingerprint image to make the pixels of image equivalent.
d. The factors are taken from 0-10 in fast Fourier transformation which calculates the discrete Fourier transforms and its inverse.
e. In the image the binarization is applied by implementing adaptive threshold method.
f. The orientation flow estimation of the encoded image is calculated.
g. Some morphological operations such as removing the H breaks and spikes are used for filtering the thinned maps.
h. The Region of interest of the encoded image is calculated.
i. The extracted minutiae value real image, after this the matching is performed using linear discriminant analysis to obtain the percentage value.

2 Matching Results

After generating these two secured template values, LDA is being applied to find out the matching percentage between these two generated files. And matching percentage between these two fingerprint images is 44.9541%.

C. Linear Discriminant Analysis (LDA)

It is generalized form of Fisher discriminant analysis which has its application in machine learning, pattern recognition and artificial intelligence in order to determine the linear grouping of attributes that characterizes the different classes of events. Linear Discriminant analysis technique in relevance to principal component analysis obtain certain advantages such as LDA determines the differences between the different classes of data, however PCA does not take the account to distinguish between the different classes. Linear Discriminant is a linear classification as well dimensionality reduction method.

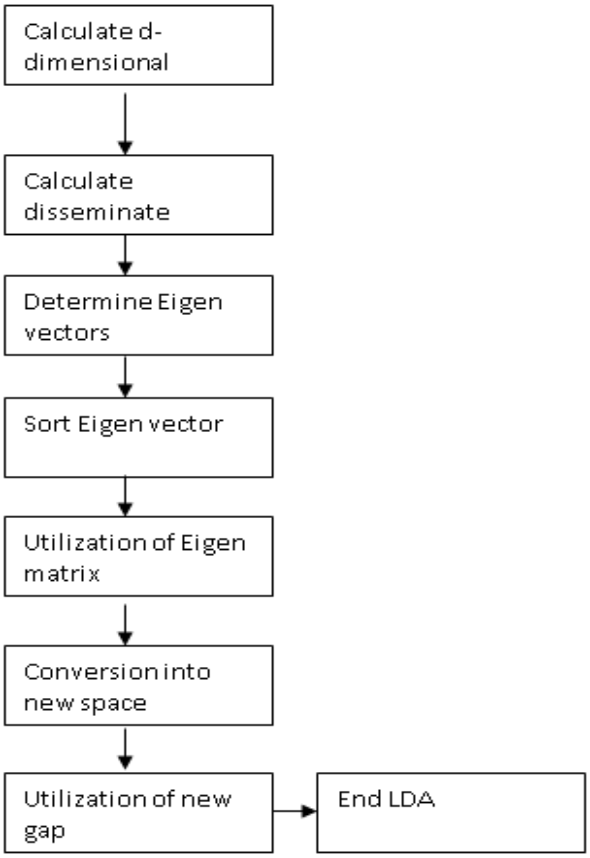


Figure 8. Flow representation of Linear Discriminant analysis

V Conclusions

Linear discriminant analysis is most powerful classifier for pattern matching. Results obtained from our simulation shows the feasibility of this classifier. Further we simulated our experiment on number of fingerprint images and every execution gave us accurate results. Matching percentage ration is quite high in our experiment. However, to secure biometric template, further one can use the more efficient algorithm to achieve different results values. Lastly, we conclude that based on current results, secured biometric template matching with help of linear discriminant analysis classifier represent a feasible and efficient authenticate system.

Acknowledgement

Authors will like to acknowledge the support provided by the Amity university, Noida

Reference

[1] Park, Unsang & Reddy Jillela, Ragha vender & Ross, Arun & K. Jain, Anil., "Periocular Biometrics in the Visible Spectrum", *IEEE transaction on Information Forensics and Security*, vol. 6, no.1, pp. 96-106, 2011.

[2] S. C. Eastwood, V. P. Shmerko, S. N. Yanushkevich, M. Drahansky and D. O. Gorodnichy., "Biometric-Enabled Authentication Machines: A Survey of Open-Set Real-World Applications", *IEEE Transactions on Human-Machine Systems*, vol .46, no.2, pp. 231-242, 2016.

[3] Prabhakar, Salil & Ivanisov, Alexander & Jain, A.K., "Biometric recognition: Sensor characteristics and image quality", *IEEE Instrumentation & Measurement Magazine*, vol.14, no.13, pp. 10-16, 2011.

[4] Buhan, Ileana & Kelkboom, Emile & Simoens, Koen., "A Survey of the Security and Privacy Measures for Anonymous Biometric Authentication System", Sixth *international conference on Intelligent Information Hiding and Multimedia Signal Processing* (IIH-MS), pp. 346-351, 2010.

[5] Gałka, Jakub & Mąsior, Mariusz & Salasa, Michał., "Voice Authentication embedded solution for secured access control", *IEEE transactions on Consumer Electronics*, vol.60, no.4, pp. 653-661, 2014.

[6] C. Gottschlich, T. Hotz, R. Lorenz, S. Bernhardt, M. Hantschel, and A. Munk., "Modelling the Growth of Fingerprints Improve Matching for Adolescents", *IEEE transaction on Information Forensics and Security*, vol.6, no.3, pp. 1165-1169, 2011.

[7] Shangfei Wang, Zhilei Liu, Siliang Lv, Yanpeng Lv, Guobing Wu, Peng, Fei Chen and Xufa Wang "A natural Visible and Infrared Facial Expression Database for Expression Recognition and Emotion Inference", *IEEE transaction on Multimedia*, vol.12, no.7, pp. 682-691, 2010.

[8] Si, Y., et al., "Novel Approaches to Improve Robustness, Accuracy and Rapidity of Iris Recognition Systems", *IEEE transaction on Industrial Informatics*, vol.8, no.1 pp.110-117,2012.

[9] Munich, Mario & Perona, Pietro, "Visual Identification by Signature Tracking", *IEEE transaction on Pattern Analysis and Machine Intelligence*", vol.25, no.2, pp.200-217, 2003.

[10] N. A. Schmid and J. A. O'Sullivan., "Performance Prediction Methodology for Biometric Systems using a large Deviations Approach", *IEEE transaction on Signal Processing*, vol.52, no.10, pp.3036-3045, 2004.

[11] Ai-hong Zhu, Lian Li, "Improving the Chaotic Image Encryption Algorithm based on Logistic Map", *IEEE International Conference on ESIAT*, vol.3, pp.211-214, 2010.

[12] I. W. H. Tsang, A. Kocsor and J. T. Y. Kwok, "Large Scale Maximum Margin Discriminant Analysis Using Core Vector Machines", *IEEE transaction on Neural Networks*, vol.19, no.4 pp. 610-624, 2008.

[13] Chandra, S., Paira, S., Alam, Sk.S., Sanyal, G., "A Comparative Survey of Symmetric and Asymmetric Key Cryptography", *IEEE International Conference on ICECCE*, pp. 83-93, 2014.

[14] Eng, A.; Wahsheh, L.A., "Looking into My Eyes: A Survey of Biometric Security", *IEEE Tenth International Conference on ITNG*, pp. 422-427, 2013.

[15] A. Askarov and A. Sabelfeld, "Gradual Release: Unifying Declassification, Encryption and Key Release Policies", *IEEE Symposium on Security and Privacy*, pp. 207-221, 2007.

[16] Minhthang Bui, Francis & Martin, Karl & Lu, Haiping & Plataniotis, Konstantinos & Hatzinakos, Dimitrios, "Fuzzy Key Binding Strategies Based on Quantization Index Modulation (QIM) for Biometric Encryption (BE) Applications", *IEEE transaction on Information Forensics and Security*, vol.5, no.1 pp. 118-132, 2010.

[17] L. Wu, X. Liu, S. Yuan and P. Xiao, "A Novel Key Generation Cryptosystem based on Face Features", *IEEE Tenth International Conference on Signal Processing Proceedings*, pp. 1675-1678, 2010.

[18] V. J. Rathod, N. C. Iyer and Meena S M., "A Survey on Fingerprint Biometric Recognition System", *IEEE International Conference on ICGCIoT*, pp. 323-326, 2015.

[19] R. Mukesh and V. J. Subashini., "Fingerprint based Authentication System using Threshold Visual Cryptographic Technique", *IEEE International Conference on ICAESM*, pp. 16-19, 2012.
[20] J. Shin, D. Kim and C. Ruland, "Content based Image Authentication using HOG feature Descriptor", *IEEE International Conference on Signal Processing*, pp. 5292-5296, 2014.
[21] Kholmatov A., Yanikoglu B., "Secure Fuzzy Vault based Fingerprint Verification System", *IEEE International Conference on Signals, System and Computers*,1, pp. 577-581, 2004.
[22] Z. Jin, M. H. Lim, A. B. J. Teoh, B. M. Goi and Y. H. Tay, "Generating Fixed-Length Representation from Minutiae Using Kernel Methods for Fingerprint Authentication", *IEEE transaction on Systems, Man and Cybernetics: System*, pp. 1-14, 2016.
[23] R. Gil, E. Sancristobal, G. Diaz and M. Castro., "Biometric Verification System in Moodle & their Analysis in Lab Exams", *IEEE International Conference on EUROCON*, pp.1-4, 2011.
[24] Zhang, X., Zhang, X., Ren, X., "Two Dimensional Principal Component Analysis based Independent Component Analysis for Face Recognition", *IEEE International Conference on Multimedia Technology*, pp. 934-936, 2011.
[25] Pisarchik, A.N., Flores-Carmona, N.J., Carpio-Valadez, M., "Encryption and Decryption of Images with Chaotic Map Lattices", *International CHAOS Journal, American Institute of Physics*, vol.16, no.3 pp. 3118-3124, 2006.
[26] Jong-Bae Jeon, Jung-Hyun Kim, Jun-Ho Yoon, Kwang-Seok Hong., "Performance Evolution of Teeth Image Recognition System based on Difference Image Entropy", *IEEE International Conference on Convergence and Hybrid Information Technology*, vol.2, pp. 967-972, 2008.
[27] K. Qin, K. Xu, Yi Du and Deyi Li., "An Image Segmentation Approach based on Histogram Analysis utilizing Cloud Model", *IEEE International Conference on FSKD*, pp.524-528, 2010.
[28] Prabhakar, S, Jain, A.K, Jianguo Wang, Pankanti S, Bolle (2002), "Minutia Verification and Classification for Fingerprint Matching", *International Conference on Pattern Recognition*, vol.1, pp. 25-29, 2002.
[29] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni., "Fingerprint Image Reconstruction from Standard Templates," *IEEE Trans. Pattern Analysis and Machine Intelligence*, pp. 1489, 2007.
[30] Luping Ji, Zhang Yi, "Fingerprint Orientation field Estimation using Ridge Protection", *The Journal of the Pattern Recognition*,41, pp. 1491-1503, 2008.
[31] Robert Hastings, "Ridge Enhancement in Fingerprint Images Using Oriented Diffusion", *IEEE Computer Society on Digital Image Computing Techniques and Applications*, pp. 245-252, 2007.
[32] Srinivas Mukkamala, Andrew H. Sung, and Ajith Abraham, Intrusion detection using an ensemble of intelligent paradigms. *J. Netw. Comput. Appl.*, vol.28, no.2 pp.167-182, 2005
[33] Srilatha Chebrolu, Ajith Abraham, and Johnson P. Thomas., Feature deduction and ensemble design of intrusion detection systems. *Comput. Secur.* vol.24, no.4 pp.295-307, 2005.
[34] Mary Lourde R and Dushyant Khosla, "*Fingerprint Identification in Biometric Security Systems*", International Journal of Computer and Electrical Engineering, vol.2, pp.1793-8163, 2010.
[35] W. Shen, R. Khanna, "Special issue on automated biometrics", Vol. 85, No. 9, Sept. 1997, pp. 1343-1492. 32 Information Security Technical Report, vol.3, no.1,1997.
[36] Haiyun Xu, Raymond N. J. Veldhuis, Asker M. Bazen, "Fingerprint Verification Using Spectral Minutiae Representations", *IEEE Transactions on Information Forensics and Security*, vol.4, no.3 2009.
[37] O'Gorman L. Fingerprint Verification. In: Jain A.K., Bolle R., Pankanti S. Biometrics. *Springer*, Boston, MA, 1996.
[38] Zheng, G, Li, W & Zhan, C, "Cryptographic key generation from biometric data using lattice mapping", 18th *International Conference on Pattern Recognition*, 2006 (ICPR 2006), 20-24 August 2006, 4, 513-516.
[39] H. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar and T. A. H. M. Akkermans, "A Fast Minutiae-Based Fingerprint Recognition System," in *IEEE Systems Journal*, vol.3, no.4 pp. 418-427, 2009.
[40] Yagiz Sutcu, Qiming Li, Nasir Memon, "Secure Biometric Templates from Fingerprint-Face Features", *IEEE Conference on Computer Vision and Pattern Recognition*,2007.
[41] Subhas Barman, Debasis Samanta, Samiran Chattopadhyay, "Fingerprint-based crypto-biometric system for network security", *EURASIP Journal on Information Security*, Number 1, pp.1, 2015.
[42] Sukhdev Singh, Chander Kant, "A Novel Approach to Secure Biometric Template with Steganography", *International Journal of Advanced Research in Computer Science*, vol.8, no.5 2017.
[43] Bandhana Rani, Hardeep Singh, "Biometric identification with combined algorithms (surf, harris and mser)", *International Journal of Computer Science and Mobile Computing* IJCSMC, vol.6, no.1 January 2017, pg.228 – 233, 2017.
[44] R. Haraksim, A. Anthonioz, C. Champod, M. Olsen, J. Ellingsgaard and B. Christophe, "Altered fingerprint detection – algorithm performance evaluation,"*4th International Conference on Biometrics and Forensics (IWBF)*, Limassol, pp. 1-6,2016.

Author Biographies

Surbhi Vijh received her B. tech degree in computer science from A.P.J Abdul kalam Technical University (AKTU) in 2016. She started pursuing M. tech in computer science from Amity University, Noida in 2017. She is a research student at Amity University, Noida.

Deepak gaur received B. tech degree in computer science from Himachal Pradesh university in 2002 and M. tech degree in information technology from Punjab engineering college, Chandigarh in 2006. Presently pursuing Ph.D. and working as Assistant professor in Amity University, Noida.