Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 3, (Special Issue) March-2019, ISSN 2230-7540

Multimodal Biometric Authentication System for Automatic Certificate Generation

Sandeep Kumar[1]* A. Sony[2] Rahul Hooda[3] Prof. Yashpal Singh[4]

[1] Professor, ECE, Sreyas Institute of Engineering & Technology, Hyderabad, India

[2] B.Tech Student, ECE, Sreyas Institute of Engineering & Technology, Hyderabad, India

[3]Assistant Professor, Govt. College Jind, Haryana, India

[4] Professors, Department of ECE, OPJS University, Rajasthan, India

Abstract – The Biometric systems are successfully being used in many diverse fields like identification, forensic, authorization and security systems. The multimodal biometric system uses two or more human body characteristics which results in a much higher security and authentication level. The aim of this paper is to think about different methods utilized for security to automatic certificate generation for events. The proposed methodology used to generate certificates for workshops, conferences, college events with the secured system and robostic algorithms by using multimodal authentication. Conventionally, educational institutes and companies use specialized tools for generating a certificate on a large scale which minimizes time consumption. This work can be extended to generate an analysis report for large data sets as well. The major steps involved in this project are a base image, candidate face images, fingerprints should be in tif, jpg or png format for more secured. The image generated by the program retains the properties of the base image. Source code given here only inserts text on the image. Data (Names awarded to the candidates) to be written can be either in xls or xlsx format. MS Excel is preferred as it's a powerful mathematical and statistical tool. It allows data to be internally computed and analyzed within the file.

Keywords: Face Recognition, Haar Features, Finger Recognition, Chaff features, Excel.

----------X----------

I. INTRODUCTION

Robust personal authentication is becoming ever more important in computer-based applications. Among a variety of methods, biometric offers several advantages, mainly in embedded system applications. Data security, complete system control, and missed storage and computing opportunities in personal portable devices are some of the major limitations of the centralized cloud environment (Xueyi, et. al., 2015), (Hidano, et. al., 2008, Kikuchi, et. al., 2007, Arun and Jain, 2004). Among these limitations, security is a prime concern due to potential unauthorized access to private data. Biometrics, in particular, is considered sensitive data, and its use is subject to the privacy protection law. To address this issue, a multimodal authentication system using encrypted biometrics for automatic certificate generation. Human has used body characteristics to recognize each other for thousands of years. In the late nineteenth century, Alphonse Bertillon, a French policeman, introduced the science of identifying a person based on his anatomical and behavioral features (Ghimire and Joonwhoan, 2013), (Zulfiqar, et. al., 2018, Mario, 2015, Kumar, et. al., 2018). He developed a system, called Bertillonage, which is used to identify criminals based on a number of body measurements. Based on the behavioral features, we classified in addition to fingerprints, other personal traits like face, iris, palm etc. are also developed for identification. These body traits used for identifying an individual came to be known as biometric traits. With the use of biometric traits being automated, biometric-based authentication systems are now preferred to traditional authentication systems (Haghighat, et. al., 2016), (Kumar, et. al., 2018, Srikrishnaswetha, et. al., 2018). Traditional authentication systems are dependent on something you know like a password or something you have like smartcards which can easily be forgotten, lost or stolen. Currently, biometric recognition systems are extensively used in a wide range of applications. These systems work in two modes: identification, in which there are one-to-one matching and verification in which there is one-to-many matching.

In the proposed work, we used multimodal biometrics means a combination of face and finger recognition.

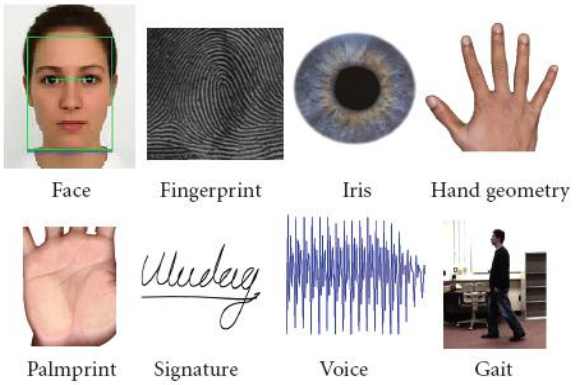


Figure 1. Various Biometric Traits

For face recognition, we used haar features selection and haar features are used as a features detector and it will compute the integral image which is of rectangular type. Every people has unique parts like eyes, nose, and mouth but the eyes region are darker nose and mouth will be in different shape these are compared based upon this. In the next step constructing an integral image: The rectangular boxes are computed to construct an image at(x,y). After constructing the image, we are providing AdaBoost training: It is used to find the visual features from large to small set (Valiollahzadeh, et. al., 2008), (Alam, et. al., 2018, Srikrishnaswetha, et. al., 2018). Finally cascading classifiers used for combine all the above and discards the background. For feature extraction can be performed by using a technique called PCA. The term PCA denotes Principle Components Analysis is a useful statistical technique that has found application in the field such as face recognition and image compression and is a common technique for finding a pattern in data of high dimension. It is the dimensionality reduction of data set process by finding a new set of variables smaller than the original set of variables. Retains most of the input data information.PCA introduces mathematical concepts which include standard deviation, covariance, eigenvectors, and eigenvalues. It is a way of identifying patterns in data and expressing the data in such a way as to highlight their similarities and differences. Since patterns in data can be hard to find in data of high dimension, where the luxury of the graphical representation is not available, PCA is a powerful tool for analyzing data. Steps involved in PCA are:

- Get the data from an image and subtract the mean.
- Calculate the covariance matrix.
- Calculate the eigenvectors and eigenvalues of the covariance matrix
- Choosing components and forming a feature vector
- Deriving the new data set
- Getting the old data back

K-Means clustering is one of the most used algorithms for classification. Basically, it is an unsupervised learning algorithm with several data analysis applications, the main goal is to classify data into groups of information (Srikrishnaswetha, et. al., 2018), (Kumar, et. al., 2017, Kumar, et. al., 2017). This process basically consists of several iterations of a specific process, designed to get an optimal minimum solution for all data points. Let's look at this process in detail: First, we need to establish a function of what we want to minimize, in our case the distance between every data point and the correspondent Centroid.

$$J = \sum_{i=1}^{k} \sum_{j=1}^{n} \left\| X_j - C_i \right\|^2$$

With this function well defined, we can split the process into several steps, in order to achieve the wanted result (Alam, et. al., 2018). Our starting point is a large set of data entries and a K defining the number of centers. The first step is to choose randomly K of our points as partition centers.

- Next, we compute the distance between every data point on the set and those centers and store that information.
- Supported by the last step calculations, we assign each point to the nearest cluster center. This is we get the minimum distance calculated for each point, and we add that point to the specific partition set.
- Update the cluster center positions by using the following formula:

$$c_i = \frac{1}{|k_i|} \sum_{x_{j \in k}} x_j$$

- If the cluster centers change, repeat the process from

Otherwise successfully computed the K means clustering algorithm and got the partition's members and centroids.

For finger recognition, we used the fuzzy vault and which is based on the infeasibility of the polynomial reconstruction problem. Fuzzy vault also has the

ability to deal with the intraclass variations in the biometric data and also capable to work with unordered sets. Whereas difference of a single bit in the key of a classical cryptosystem (e.g. AES, RSA) hinders decryption completely, the fuzzy vault allows some minor differences between the encryption and the decryption sets, where the sets are unordered and is used to lock and unlock the vault (Juels and Sudan, 2002), (Hooda and Gupta, 2013, Hooda and Kaur, 2015). This fuzziness is necessary for use with biometrics, since different measurements of the same biometrics often result in quite different signals, due to a noise in the measurement or non-linear distortions. For instance, two impressions of the same fingerprint can have substantial distortion (displaced minutiae points) and the number of features may vary between the two impressions (e.g. missing spurious minutiae).

The three main parameters in the fuzzy vault scheme are:

i) The number of points in the vault that lie on the polynomial and it depends on the number of distinct features that can be extracted from the template (e.g. a number of minutia points in the user's fingerprint).

ii) The number of chaff points that are added and this parameter influences the security of the vault. As more chaff points are added, the security increases.

The degree of the encoding polynomial which controls the tolerance of the system to errors in the biometric data. Generally, the degree of the polynomial is less than the minimum number of minutia points extracted from biometric data (Clancy, et. al., 2003, Hidano, et. al., 2008). During the encoding phase of the fuzzy vault chaff generation method is used to generate random points. These chaff points, also known as noise points, are used to hide the genuine minutiae points and therefore also secure the secret crypto-key. Any generated chaff points must satisfy a few conditions. Firstly they should not lie on the polynomial on which genuine points lie. Secondly, all chaff points should be distributed randomly without any pattern (Kumar, et. al., 2018, Srikrishnaswetha, et. al., 2018). Thirdly, each chaff points must be a δ distance away from each other member of fuzzy vault member.

II. LITERATURE SURVEY

Several efforts have been made to improve the security level of personal unauthorized access to private data. Several papers have been published on face and finger recognition to provide the security level.

Ye, Xueyi et al. [1] proposed a Deep Learning Network method for Face Detection. In the proposed methodology Skin color (YCbCr) segmentation is used for face detection and Deep Learning or Artificial Neural Network Classifier (4 hidden layers) was used. In the proposed method the LFW dataset (7000) & CAS-PEAL dataset (4000) used for experiments. According to experimental results system performance increased in the form of correction rate CR, missing detection rate (MDR) and false detection rate (FDR).

Ghimire et al. [2] proposed a robust face detection method based on skin color and edges. Firstly in pre-processing step Image Enhancement was done after the pre-processing Skin Segmentation is conducted by YCbCr and RGB space. The Edges (Canny Edge) of the Input image are combined with Skin Segmentation to identifying the face. In this proposed methodology The FRGC dataset (302 Frontal Image Sample) used for experiments. According to experimental results system improved in the form of Correct Detection Rate (CDR) is 80.1%, False Positive Rate (FPR) is 3.31%, and Missing Rate (MR) is 19.8%.

Abdul Rahman et al. [3] proposed a face detection model. In this proposed methodology RGB-H-CbCr Skin Colour Model used for segmentation of Human Face Detection. It was experimentally proved that good detection success rates for near-frontal faces were achieved so that system performance improved. Outcomes in the form of False Detection Rate (FDR) is 28.29 %, Detection Success Rate (DSR) is 90.83%.

Seyyed et al. [4] proposed an Edge-Based Efficient Method of Face Detection and Feature Extraction. In the proposed methodology Multi-Layer Feed-Forward NN used as classifier between faces and non- faces. The output of this classifier is then used as an input to the Viola-Jones algorithm for face detection. Features Extraction performed through Canny Edge detection. According to experimental results detection rate of Neural Network with Adaboost is 94.1% and False Positive Rate is 6.5%. The disadvantage of this proposed methodology was these techniques applied only 5 images of samples.

Originally the fuzzy vault was proposed by Juels & Sudan [5]. They used the example of Alice and Bob where Alice encloses secret S in the fuzzy vault and lock it using an unordered set A. Bob also having an unordered set B can unlock the vault only if set B substantially overlaps with set A. Based on secret key chosen by Alice, a polynomial P is formed. Set A constitute the points which lie on that polynomial and then some chaff points are added which do not lie on the chosen polynomial.

Clancy et al [6] proposed a fingerprint vault based on the fuzzy vault of Juels and Sudan. In this paper, multiple minutiae locations are used as elements of locking set. This paper proposed the

concept of using random points known as chaff points which do not lie on the polynomial. These chaff points and genuine points, which lie on the polynomial, together with forms the fuzzy vault. The fuzzy vault is made public and the chaff points are used to conceal the minutiae points and prevent the misuse of the vault. The security of the vault increases with the number of chaff points. This method assumed that fingerprints required to form vault and for the query are pre-aligned.

Seira Hidano et al [7] propose a technique for template security using fuzzy vault scheme. This scheme stores the user template after encryption and fuzzy vault scheme is used to generate the secret data from the user template and the query biometric data. It incorporates a measure to only provide sufficient information so to prevent the secret data and the user template used to obtain the secret data from being recovered, and also to enable the secret data to be generated from the user's biometric data. In this paper, a fingerprint authentication system is simulated to evaluate the template security of the proposed technique. This method is also applied to a fingerprint matching system and determined that the secret data can be recovered at a high probability if it is an authorized person, by setting the number of elements 'k' and the number of parity code elements 'g' to suitable values. Since this method generates secret data from a registered template and submitted biometric data, it seems to provide extremely good confidentiality, not just of the template but also the secret data.

Hiroaki Kikuchi et al [8] found that typical feature extracted from a fingerprint, known as minutiae, is assumed to tolerate against re-ordering minutiae. In order to address the issue, a new scheme of the fuzzy vault for the fingerprint is proposed that assigns an identification number to all minutiae and chaff (fake minutia) and determines correct order in greedy short distance algorithm. The main idea is to assign identification to both genuine and chaff minutiae so that reordering is made possible, which then allows efficient error-collecting code to be used to resolve the uncertainty of biometric information. The proposed scheme is also compared with some existing schemes in terms of accuracy and performance.

III. PROPOSED METHOD

A multimodal biometric system is mainly a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database as shown in Figure 2.

i) **Biometric Sensor Module:** A biometric sensor is used for obtaining identifiable information from the users. The sensor module has a quality checking module which performs quality estimation to ensure that the acquired biometric can be reliably processed by a feature extractor. If the sample does not meet the quality criteria, this module will ask the user to try again.

ii) **Feature extractor module:** This module extracts a set of salient features from the acquired biometric data. This feature set will now be the new identity of the person as shown. It will be stored in the system as a biometric template for future verification. The template is expected to be capable of tolerating intra-user variability and be discriminatory against inter-user similarity.

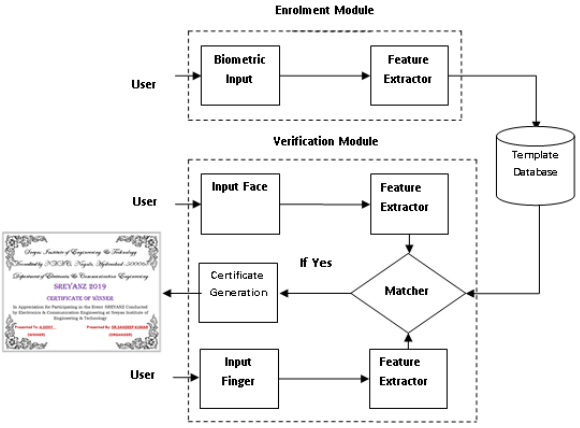
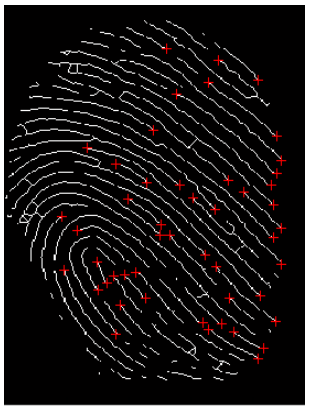


Figure 2. Flow Chart of Proposed Methodology

(a)

(b)

(c)



(d)

Figure 3. (a) An input image of Face (b) Face detector through V-J Method (c) Input image for Finger (d) Feature Extractor for finger

iii) **Template database:** The database is used for storing user templates captured during the enrolment stage. The scale of the database depends on the application.

iv) **Matching Module:** This module compares a query or tests biometric data with the pre-stored template. The output is a matching score between query and template which tells about the degree of similarity. For example, in minutiae-based fingerprint verification, the matching score is the matched minutiae between the query and the template fingerprint. In the same way, we are matching the face score.

v) **Decision-making module**: This module decides on the identity of the user based on the matching score. If both of the matchings will complete and result will come as an authentic person then automatically all the certificate will generate as shown in Figure 4.

Figure 4. (a) Sample Certificate (b) After Verification Winner Certificate

IV. EXPERIMENTAL RESULT

MATLAB is an interactive system whose basic data element is a matrix. This allows formulating solutions to many technical computing problems, especially those involving matrix representations, in a fraction of time. Today, MATLAB incorporates state of the art numerical computation software that is highly optimized for the modern processor and memory architectures. The processing of any type of images like stored images, live time images etc. by the help of MATLAB. It is the language which gives the information regarding removing noise, geometric and images transformation, texture feature extraction, compression of images or to segment the image related to select the region of interest. In the proposed scheme image processing tool and image acquisition tool of MATLAB is used.

For evaluation of our proposed module, we used own database as shown in Figure 5. First, we acquired the face input image for authentication with the proposed methodology. After verification of face again, we are going for finger authentication. When both the verification will over then only Matlab read the excel sheet and excel sheets provide the list of participants and winners to whom

we have to provide the certificates. Finally, this proposed module will generate the entire certificate for mention list in excel file. This module will do our work so easy and it will take very less time as compared to manual work.

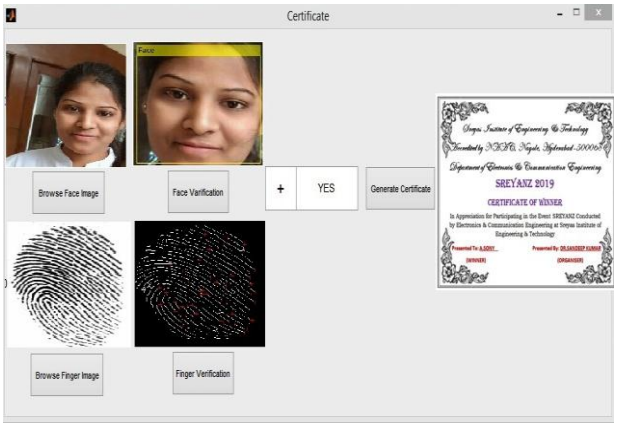


Figure 5. GUI overall module for Proposed Methodology

V. CONCLUSION & FUTURE SCOPE

This proposed methodology gives a wonderful result to generate automatic certificate during any kind of big events i.e. Conferences, Tech fest etc. In the proposed method simple mathematical operations are used to generate random chaff points in finger recognition and Haar features, PCA features extraction technique for face recognition. After verification of the authentic person automatically certificate will generate for all list of winning participate in the events. The accuracy of both methods comes out to be high and processing time is also very less. Thus it can be said that the developed method is better than for generating the certificate in big events. The motto of designing any system is accuracy, time consumption, the effort of work and power consumption.

In the future, this work can be extended to generate an analysis report for large data sets in the companies or any kind of organization.

REFERENCES

1. Ye, Xueyi, Xueting Chen, Huahua Chen, Yafeng Gu, and Qiuyun Lv (2015). "Deep learning network for face detection." In 2015 IEEE 16th International Conference on Communication Technology (ICCT), pp. 504-509. IEEE, 2015.

2. Ghimire, Deepak, and Joonwhoan Lee (2013). "A robust face detection method based on skin color and edges." Journal of Information Processing Systems, vol. 9, No. 1, pp. 141-156.

3. Haghighat, Mohammad, Mohamed Abdel-Mottaleb, and Wadee Alhalabi (2016). "Fully automatic face normalization and single sample face recognition in unconstrained environments." Expert Systems with Applications 47, pp. 23-34.

4. Valiollahzadeh, Seyyed Majid, Abolghasem Sayadiyan, and Mohammad Nazari (2008). "Face detection using adaboosted SVM-Based component classifier." arXiv preprint arXiv:0812.2575.

5. Ari Juels and Madhu Sudan (2002). “A Fuzzy Vault Scheme”, in IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408.

6. T Clancy, D Lin, and N Kiyavash (2003). “Secure smartcard-based fingerprint authentication” in Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications, Berkley, CA, pp. 45-52.

7. Seira Hidano, Tetsushi Ohki, Naohisa Komatsu and Masao Kasahara (2008). “On Biometric Encryption using Fingerprint and It’s Security Evaluation”, in 10th International Conference on Control, Automation and Robotics and Vision, pp. 950-956.

8. Hiroaki Kikuchi, Yasunori Onuki and Kei Nagai (2007). “Evaluation and Implementation of Fuzzy Vault Scheme using Indexed Minutiae”, Proceedings of IEEE, pp. 3709-3712.

9. Ross, Arun, and Anil K. Jain (2004). "Multimodal Biometrics: an overview." In 2004 12th European Signal Processing Conference, pp. 1221-1224. IEEE, 2004.

10. Ali, Zulfiqar, M. Shamim Hossain, Ghulam Muhammad, Ihsan Ullah, Hamid Abachi, and Atif Alamri (2018). "Edge-centric multimodal authentication system using encrypted biometric templates." Future Generation Computer Systems 85: pp. 76-87.

11. Malcangi, Mario (2015). "Developing a Multimodal Biometric Authentication System Using Soft Computing Methods." In Artificial Neural Networks, pp. 205-225. Springer, New York, NY.

12. Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar (2018). “Live Detection Of Face Using Machine Learning with Multi-Feature Method” in Wireless Personal Communication Springer Journal (SCI)

Published DOI: 10.1007/s11277-018-5913-0.

13. Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar (2018). "Automatic Live Facial Expression Detection Using Genetic Algorithm with Haar Wavelet Features and SVM" in Wireless Personal Communication Springer Journal (SCI) Published DOI: 10.1007/s11277-018-5923-y.

14. Kone Srikrishnaswetha, Sandeep Kumar and Prashant Johri (2018). "Comparision Study on Various Face Detection Techniques" in 4th International IEEE Conference on Computing Communication and Automation (ICCCA-2018), December 14-15, 2018.

15. Sony Alam, Sandeep Kumar, and Kone Srikrishnaswetha (2018). "Automated Non-Supervised Detection of Dental Caries using PCA and K-Means" in 2nd International Springer/Elsevier Conference on Nano Science & Engineering Applications, 4th to 6th, October 2018.

16. Kone Srikrishnaswetha, Sandeep Kumar and MD Rashid Mahmood (2018). "A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IOT" in 7th (Springer) International Conference on Innovation in Electronics and Communication Engineering (ICIECE-2018).

17. Sandeep Kumar, Sukhwinder Singh & Jagdish Kumar (2017). "A Study on Face Recognition Techniques with Age and Gender Classification" In IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1001-1006, May 2017.

18. Sandeep Kumar, Sukhwinder Singh & Jagdish Kumar (2017). "A Comparative Study on Face Spoofing Attacks" In IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1104-1108, May 2017.

19. Hooda, Rahul, and Sahil Gupta (2013). "Fingerprint fuzzy vault: a review." International Journal 3, No. 4: pp. 479-82.

20. Hooda, Rahul, and Manavjeet Kaur (2015). "Novel chaff generation for fingerprint fuzzy vault." British Journal of Mathematics & Computer Science 10, No. 3: pp. 1-9.

Corresponding Author

Sandeep Kumar*

Professor, ECE, Sreyas Institute of Engineering & Technology, Hyderabad, India

drsadeepkumar@sreyas.ac.in