COMPARATIVE SURVEY ON FACE BIOMETRIC SYSTEM AND DNA PATTERN FOR SECURE AUTHENTICATION

B.Poorani

PG Scholar, ME(CSE)

Sona college of technology,

S.Sakthivel,

Assistant Professor, CSE

Sona college of technology,

1. ABSTRACT

Authentication is the process which is used to securing the documents from unauthorized access and also to provide the security in confidential areas such as airports, banks &financial areas, railway stations, business sectors and national security areas. To enhance the secure authentication, various systems and methods are implemented from the past. From that biometric system plays an important role for secure authentication, because it uses the physiological and behavioral features of the human. In this paper we discussed that to avoid the duplicating the authorized person's feature which can be easily cracked the biometric system. To resolve such problem, authenticate a person by using face biometric system with their DNA-VNTR pattern. Face biometric system recognized the facial features of human using principle component analysis and DNA-VNTR pattern can be analyzed through PCR-STR technique. Due to this secure authentication is highly enhanced and also yield 90% of accuracy in face biometric and 97% accuracy in DNA-VNTR can be analyzed.

Keywords: face biometric system, PCA, DNA-VNTR pattern, PCR-STR technique.

2. INTRODUCTION

Authentication is the process to enhance the security in various fields such as banks, public sector, colleges, hospitals, banks and financial sectors with the law enforcement. Various types of authentication such that making user name and password, making OTP etc are implemented in the past. Even though there may some security issues in authentication process. To improve the secure authentication biometric systems are evolved which measures the physiological and behavioral features of human. The physiological features such as face pattern of human, iris pattern ,fingerprint pattern etc. the behavioral features is based on the persons particular behavioral characters such that voice of the human . According to the measure of the features various types of biometric system are evolved. From that face biometric system are widely used in many confidential areas as above mentioned.

Face biometric system is the automated computing system which computes the facial features of the authorized person. This system used widely in airports, science analysis, crime analysis according to law enforcement[9]. In the system extract the unique features of face such that length between eyes, nose, distance between nose column to mouth tip, and overall structure of the face. Face biometric system process the face recognition in step by step process. Firstly, captures the authorized person's face using camera. Then extracting the unique features of the face from the digital information which is captures through camera. Compare the extracted features with the already collected information (called database) finally matched person are authenticate to access.

Various algorithms such as PCA using Eigen faces, linear discriminate analysis, hidden markov model; multilinear subspace learning is the traditional techniques to recognize the facial features of individual.
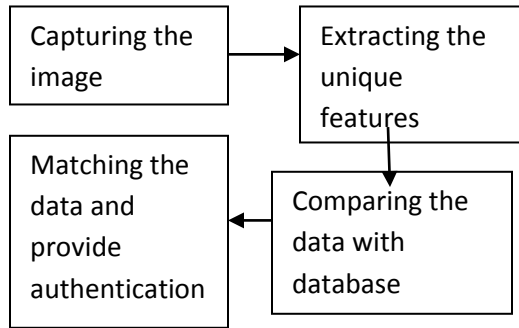
Figure 1: Face Recognition Steps.

Since there may occur some security issues in face biometric system. Duplicating the unique features of face is used to crack the security in face biometric system.

DNA is De-oxy ribonucleic Acid which is present in the chromosome of organism can be for secure authentication which cannot be duplicated easily and also provide high unique to one another.

DNA consists of four bases components there are adenine, quinine, thynamine, cystonine. These four components are consequently arranged in sequence called DNA sequence. Each and every person has different allele sequence. Allele sequence is the certain sequence of DNA is similar and those sequences are varying one another. Such sequences are identified through PCR-STR technique.

A tandem repeat is a sequence of two or more DNA base pairs that are repeated in such a way that the repeats lie adjacent to each other on the chromosome. Tandem repeats are generally associated with non-coding pattern of DNA.

VNTR pattern of the DNA is the identical to individuals. Variable number tandem repeat (VNTR) is a location in genome where SNP is organized as a tandem repeat. These can be found on many chromosomes, and often show variations in length between individuals.

While authenticate the person using face biometric system with DNA pattern yield high security in the authentication process.

3. RELATED WORK:

Various researches are happened on both faces biometric authentication and DNA pattern analysis are done separately.

M A Imran, M S miah ,et al (2015) proposed that face recognition and detection are done by appearance based approach .they recognized the face by using PCA based algorithm. Detection of face done by matching the Eigen values of recognized person with training datasets. They provide 80% accuracy to detect and recognize the face of authorized person.

Wen-hui lin, ping wang ,et al(2016) proposed that recognizing the face using SVM classifier for online user authentication. In this user authentication SVM classifier is used to recognized and classify the digital image data in datasets .cross-validation done with user layer to dataset which provide 97% accuracy and also provide higher precision of facial recognition to existing system it gives 89% accuracy.

Ramya Krishnan,renuka ,et al(2016) proposed that attendance marking system using face recognition .author uses the RFID tag to automatically tracks the student while entering the classroom and also initiates camera to capture the student and marked into attendence.ultrasonic sensor are used to automatically triggering the camera to and off . Facial feature extraction author uses the SURF algorithm and authors analysis in face features in three main parts namely interest point detection, local neighborhood description and matching.

Anil k.jain ,karthick nandakumar ,et al (2016) paper deals about the evolution of biometric system research and says about challenges accomplished with that. They proposed that all the biological and behavioral characteristics such as fingerprint, face, iris, and voice. From that survey, fingerprint matching is first evolved automated biometric system. Duplicating authorized person's fingerprint pattern made to enhance the security access voice of authorized person is used for authentication .since there is problem that voice pattern analysis not used May confidential areas and voice of authorized person also duplicated easily. Thirdly, iris pattern of authorized person is used for secure authentication after that face feature

recognition biometric is evolved which is used in many highly confidential areas.

Tsai L.C ,Lee CC et al (2016) says about the crime source DNA is tested through STR typing quantification. Fingerprint process is held to evolve for analysis the epithelial cell deposited on surface of porous. Author explains that the sample of DNA is subjected to silver nitrate and quantify the subjected DNA sample which enhancement DNA allele in STR typing. Fingerprint process to analyze using PCR-STR manner and it shows results for particular gene pattern.

Alexeeva V, D'souza et al (2016) proposed that the how the embroyonic stem cell are engineered using TALEN-based genome editing. Author explained about green fluorescent protein are enhanced in embryonic cell by analyzing the MIXL1 gene pattern. MIXL1 gene expressions are analyzed through PCR technique. Using the MIXL1 gene pattern authenticate the valid embryonic stem cell to the person.

Mark F. Tannian, Christina schweikert et al(2017) proposed that protecting the birth certificate of the person using their respective DNA pattern. To provide identification in the birth certificate records add the DNA profile biometric. In that profile consists their respective mother and father DNA pattern and much it will contributed to the child. Using the mother contributed gene pattern is used to protect the birth certificate document from duplicating.

Comparative analyses of facial features of authorized person with DNA pattern analysis procedure are used for secure authentication and also for securing the confidential documents. This way of authentication can't be duplicated easily and it will provide the more uniqueness, adaptable to the society.

4. PROPOSED METHODOLOGY:

In real world authentication various algorithm such HMM, genetic algorithm ,neural networks are used which they produce efficient results but ,we proposed PCA using eigenfaces algorithm is efficient for analysis the facial features of human with the DNA of the specified person.

Because, PCA using Eigen faces is the traditional method which can be easily measure the features human face and verified the DNA pattern along with the facial features are performed easily and effectively.

Capture the face of authorized person using the camera and the extract the unique features from the captured image .facial features are recognized by PCA with Eigen faces. This algorithm follows three steps: 1. converting the 2-d images into 1dimensional images and the subtract with the mean of the image which is used analysis features of the captured images,2.calculate the covariance matrix for the images which are subtracted with the mean value.3.calculate the eigen value and eigen matrix for covariance matrix. Classify the faces according to the Euclidean distance of facial features pattern. using wavelet decomposition such that DWT and DCT are used to improved the feature regonition pattern.it is widely used to recognize the multiresolution images[6][10]. In this method ,author proposed that using wavelet transformation along with wavelet transformation .calculate and classify the pattern according to their weight. due to this low-contrast image features are enhanced.

Using HMM model ,facial features are recognize globally in 3-D manner. In feature pattern extraction uses the DCT to capture expression in low-contrast images[2]. The algorithm constitute the Eigen values to capture the feature pattern and then using the local identifier to identify the expression of the person.

Algorithm used to recognize the facial feature	Performance accuracy	disadvantage
PCA+eigenfaces	80%	Low-contrast imaged features are not enhanced
PCA+wavelet transformation	91%	Used for 2D images
Hidden markov	95%	High memory

model   needed

Table 1: comparison on the facial feature recognition algorithm

Face recognized person are valid then proceed to DNA analysis of the person. Variable number of tandem repeats (VNTR) pattern of person are used to identify the person and parental identification. Most widely forensic departments are crime identification.

4.1 DNA SAMPLE AND EXTRACTION

Biological factors such as blood, saliva, buccal swab, hair are used as the samples for DNA. Moreover blood samples are used for DNA extraction. Blood samples are collected on the FTA cards. When blood samples are concentrate on silver nitrate, double stranded DNA are separate into fragments.
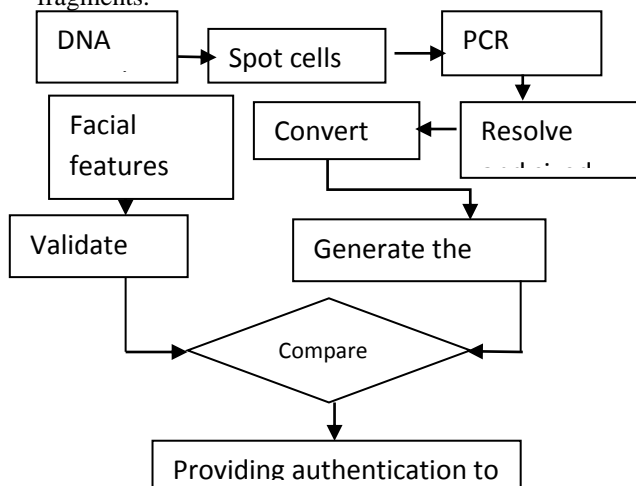
Figure 2 Flow Diagram for Face Recognition with DNA pattern.

4.2 DNA QUANTIFICATION AND AMPLIFICATION

PCR is polymerase chain reaction technique which is used to amplify the DNA fragments and it is used to amplify the tandem repeats of DNA fragments. In this technique, heating and cooling the fragments about for 30 cycles. Each and every cycle a copy of DNA sequence is generated. Single tandem repeats of DNA can be amplified about 16 patterns

are generated. After that using STR alleles are differ by only one base-pair.

STR shows that repeats of the specified region of genome and these repeated sequences are designated by core repeat unit called VNTR pattern. For efficient authentication, chromosomal loci of DNA-VNTR pattern which will be differ among persons.

To provide the personal DNA identification by following steps are done: 1.Calculate the VNTR repeats at each locus.

2. Compute the STR count values of the allele in the pattern.

3. Generate DNA ID according to the count.

Consider that a person has following allele at specified loci as,

D3S1358 and D21S11and D18S51 and...D16S539 are number as (12, 11) and (8, 12) and (13, 15)…. (10, 10) .marked the numeric values in the sequence make an id for that sequence. Validate the DNA ID and facial identification for secure authentication process.

5. EXPERIMENTAL RESULTS

In the past, face biometric system are implemented and they provide the better results in the authentication process. The better accuracy results yield in face biometric system. When duplicating the authorized person facial features then system will authenticated wrongly. Authenticate the person along with the DNA pattern yield high security and high uniqueness.

	Accuracy	wrongly authenticate
face biometric	80%	70%
face biometric other biometric	90%	70%
face biometric+ DNA pattern	90%	10%

Table 2: secure authentication accuracy in biometric system.

While duplicating the biological pattern authenticate the incorrectly may occurred but compared with other biometric authentication DNA based authentication provide better result
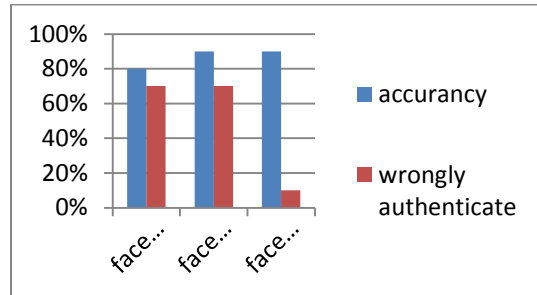
6. CONCLUSION

Authentication using the DNA with the facial recognition yield better accuracy and secure authentication. DNA based authentication are used widely various national security sectors to avoid the culprits who can crack the security system. And this type of authentication can be used in airports, railways etc. to avoid the hijacks. Fault authentication will be reduced. It will provide high uniqueness one another so we can easily identify the personal who is culprits or not.

7. REFERENCES:

[1] M. A. Turk and A. P. Pentland, "Face recognition using Eigen faces," in Proc. IEEE Computer Society Conf. Computer Vision and Pattern Recognition, Maui, Hawaii, pp. 586-591, 1991.

[2] Sheng H.Kung and Mohammed A Zohdy,"3D HMM-based facial expression recognition using histogram of oriented optical flow"Trasaction on machine learning and aritificial intelligence,vol 3,issue 6,pp 41-69,ISSN 2054-7390,2015.

[3] Abhishek Bansal, Kapil Mehta and Sahil Arora," Face Recognition Using PCA & LDA Algorithms", Second International Conference on Advanced Computing & Communication Technologies, IEEE, 978-0-7695-4640-7/12, 2012.

[4]M A Imran , M S U Miah, et al" Face recognition using Eigenfaces",International journal of computer application,vol 118,issue 5,pp 12-19,ISSN 0957-8887,2015.

[5] M. Kirby, L. Service, "Application of Karhunen–Loeve procedure for the characterization of human faces", IEEE Transactions on Pattern Analysis and Machine Intelligence vol. 12, pp. 103–108, 1990.

[6] S. Sakthivel and M. Rajaram, "Improving the Performance of Machine Learning Based Multi Attribute Face Recognition Algorithm Using Wavelet Based Image Decomposition Technique", Journal of Computer Science, vol 7,issue 3,PP 366-373, ISSN 1549-3636, 2011.

[7]R.Ramya Krishnan, R.Renuka, c.swetha,R.Ramakrishanan,"Effective automatic attendance marking system using face recognition with RFID".IJSRST volume 2 ,issue 2, pp.2395-6011,2014.

[8] Mark F. Tannian ,Christina Schweikert, Ying Liu,"Securing birth certificate documents with DNA profiles",Hawaii international conference on system Science,ISBN:978-0-9981331-0-2,pp 2398-2407,2017.

[9]S.Sakthivel And Dr.R.Lakshmipathi, "Enhancing Face Recognition Using Improved Dimensionality Reduction And Feature Extraction Algorithms –An Evaluation With Orl Database", International Journal of Engineering Science and Technology, Vol 2,issue 6,pp 2288-2295,ISSN: 0975-5462, 2010

[10] Wen-hui Lin,pingwang,chen-Fang tsai."Face recognition using support vector model for user authentication" electronic commerence research and application volume 18,pp-71-82,2015.

[11] S.Sakthivel And Dr.R.Lakshmipathi, "Weighted Attribute Fusion Model for Face Recognition", International Journal of Computer Science and Information Security, VOl 8, Issue 3, PP 122-128, ISSN 1947-5500, 2010.

[12].Anil K.Jain ,Karthick Nandakumar,Arun Ross,"50 years of biometric research:Accomplishments,challenges,and opportunities",pattern recognition letters Elsevier,pp1-26,ISSN:0617-8655,2016.