IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Enhanced PAD security Mechanism Using Fingerprint and Face Scanning

Surinder Pal Kaur[1*], Anil Kumar[2]

[1,2]Department of Computer Engineering &Technology, Guru Nanak Dev University Amritsar, India

Corresponding author: spk.rcf@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.506509 | Available online at: www.ijcseonline.org

Accepted: 09/Mar/2019, Published: 31/Mar/2019

Abstract- Biometric techniques are utilized to provide authentication to prevent unauthorized access and it handle physical or behavioral that identifies the identity of a person. In our proposed paper the security mechanism named PAD is proposed that provides more accuracy than the existing system. In this technique first of all sensor capture the biometric images and then it is utilized to identify one or more characteristics of a person like face, fingerprint and other feature. Results section shows that it gives better accuracy and recognition rate utilizes various combination of biometric technique.

Keywords- Biometric, PAD security mechanism, Security, Sensors.

I. INTRODUCTION

The term Biometric refers to the physical / logical attributes of the human body that uniquely identify the person. These details may differ from person to person and can be used as security purposes for unique identification of the person. The biometric system is the one that collects various data from attributes and then store it for recognizing the identification of person. Biometric systems are the access control system that gives specific data to the person that is identifiable by system.

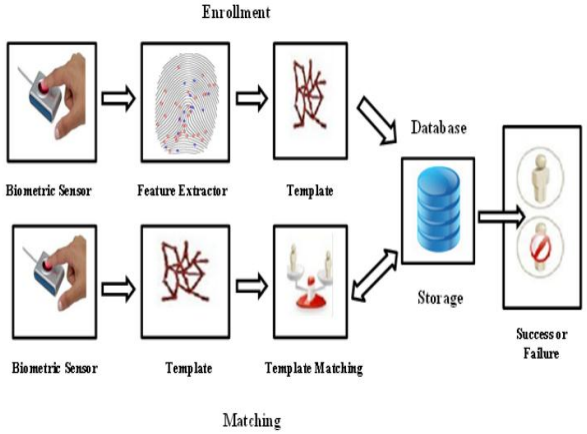


Figure 1: Biometric System

So as to get to the biometric security framework, an individual should give their special qualities or attributes which will be coordinated to a database in the framework. In the event that there is a match, the locking framework will give access to the information to the client. The locking and catching framework will actuate and record data of clients who got to the information. The connection between the biometric and biometric security framework is otherwise called the lock and key framework. The biometrics security framework is the lock and biometrics is the way to open that lock.

Application areas of Biometric

The biometrics is mainly utilized for physical and logical access control. The physical access control is the one that requires the properties which physically exists and logical access control is the one that utilizes techniques, schemes and procedures in the system.

1. Physical access control:
   It gives identity control process that utilizes users for providing physical attributes. The location like hospitals, military and police stations are used because these are highly secured areas. The physical access controls are utilized at doors or computers for confidentiality and ensuring high level security.
2. Logical access control : It gives control over the data files or computer programs to ensure the security of system. It utilizes private information of various users for providing authentication. The logical access control is mainly used for computer networks and access controls in various systems. It is more secure and effective with the advantage of saving money and time.

1.2 Problems in Biometric System

Biometric framework get motion from just a single biometric framework known as unimodal. However, each biometric has its own upsides and downsides so it isn't hard to take a biometric, make a duplicate and utilize the phony quality to assault on biometric frameworks. This a difficult

issue on the grounds that to upgrade the system security individuals nowadays are utilizing biometric. [1]

Moreover, powerless attacks can be put to break the security of systems like satire assault, replay assault, substitution assault, Trojan steed assault and transmission assault and so forth. Diverse advances have been connected to overcome these attacks like biometrics, however it isn't mystery so it can't be secured like passwords. With no mindfulness individuals leave their biometrics all over the place so data can without much of a stretch be caught, duplicated or produced. Another test before a biometric framework is the speed for example the framework must settle on a precise choice progressively.

A large portion of the accessible strategies for face Presentation Attack Detection (PAD) are either founded on investigating surface or the movement data that can be additionally prepared to identify the face antiquities. The possibility of the movement put together methodologies is based with respect to the supposition that, the typical (or genuine/live) face produces diverse movement which is to a great extent fixated on the nose when contrasted with the relic test. The greater part of the current movement based PAD plans depend on evaluating the optical stream from the recorded video which is additionally broke down to recognize the presentation attacks.

The presentation attack identification calculations as indicated by the ISO/IEC WD 30107-3 as far as: (1) False accept Rate (FAR), which is characterized as an extent of attack presentation erroneously named typical (or genuine) presentation (2) False Reject Rate (FRR) which is characterized as extent of ordinary presentation mistakenly delegated attack presentation. At long last, the execution of the general PAD calculation is exhibited as far as Failure to Enrollment Rate (FTR) with the end goal that,
FTR =(FAR+ FRR)

The lower the estimations of ACER, the better is the PAD execution.
While utilizing biometrics a few issues come before us which are given beneath:
1.Noise in detected information.
2.Intra-class variety in the example information.
3.Inter-class likeness in the example information.
4.Spoof attacks.
5.Distinctive Ability.
To overcome these problems of [2] unimodal biometrics PAD security mechanisms system was introduced.

1.3 PAD security mechanisms
[3] PAD security instruments is rising decision to verify verification of client. PAD security instrument alludes to converging of at least two biometric modalities for improving the execution of the individual frameworks, acknowledgment rate and unwavering quality. For the most part, the term multimodal shows the utilization of more than one biometric viewpoint (methodology, sensor, example or potentially calculation) and some an opportunity to join these and make a predetermined biometric check/distinguishing proof choice.

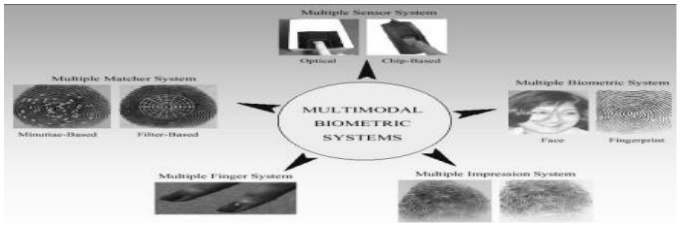


Figure 2: Types of multimodal system

The main objective of multimodal is to reduce the following:
1. False Accept Rate (FAR)
2. False Reject Rate (FRR)
3. Failure to Enroll Rate (FTE)
4. Susceptibility to Artifacts or Mimics

Multimodal are progressively indispensable to deceitful advancements, since it is so hard to produce numerous biometric qualities than to manufacture a solitary biometric trademark in this manner give higher precision rate and higher assurance from satirizing. [4]PAD security instrument frameworks additionally give hostile to caricaturing measures by making it troublesome for an interloper to at the same time parody the different biometric qualities of a client. Besides, contingent upon the characteristics, [5]sensors and highlight sets a wide range of sorts of multimodal frameworks are given underneath:

1. Presenting a clever thought of investigating the natural qualities of the light field camera to recognize the face presentation attacks by assessing the variety of center from various profundity pictures.
2. Analyzing broadly 26 distinctive center measure administrators and their effect on the proposed face PAD strategy.
3. Introducing three unique techniques to ascertain the variety of the concentration from the numerous profundity face picture that thus can be investigated to distinguish the nearness of face presentation attacks. [6]
4. Presenting a broad investigation on a recently developed light field face relic database to think about the defencelessness of the standard face acknowledgment framework on three diverse presentation attacks.
5. Benchmarking the proposed plan with 10 diverse all around received best in class plans. Acquired outcomes have exhibited the adequacy of the proposed plan for hearty face PAD utilizing camera.

Next section presents literature survey of existing techniques used PAD mechanism. Section 3 presents the proposed mechanism. Section 4 gives the results. Section 5 gives conclusion and future scope, section 6 gives the references

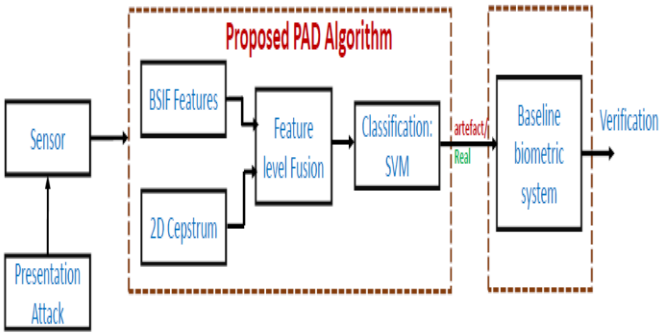
II. LITERATURE SURVEY

This section presents a comprehensive analysis of the security mechanisms that could be used in order to prevent attacks. [7] proposed a watermarking mechanism of security. The images are combined together in this case. As the images are combined the original image is difficult to fetch for unauthorized user. The overall process of combining multiple images into a single one is known as visual cryptography. [8] proposed a visual cryptography on the basis of watermarking in the fog edge computing. The images used in this case are logo and main image. Logo image is pasted over the main image. This process is known as encryption. This encrypted image is transmitted over the network. Overall security process yield complex key and hence security is enhanced. [9] proposed iris biometric security mechanism to be included before transmission of information over the network. Visual cryptography and watermarking images are combined together. The combined process efficiently detects the intrusion if any within the image. [10] proposed efficient multimodal security process in which fingerprint and iris scan mechanism is considered for evaluation. Initially biometric image is used and investigated against the pre-build dataset. In case fingerprint are matched successfully than iris scan is on the way. The result is presented in the form of false matching and false negative rate. [11] proposed a watermarking mechanism for forgery detection. The security mechanism of this sort enhance security but feature extraction on area of interest is missing that could increase the classification accuracy further. [12] proposed motion adaptive security mechanism for video processing. Motion adaptive security mechanism can handle static video frame but motion handling mechanism incorporated with motion adaptive mechanism is termed as Motion handling temporal mechanism. Trajectory handling mechanism is employed in this mechanism to handle motion and filtering mechanism is included to tackle noise within the video frame. This filter is capable of handling occlusion effect. [13] proposed a mechanism to tackle abnormalities form the extracted MRI image. Kurtosis based mechanism is the optical flow analyser that could be further processed in order to obtain accurate video processing model. Active pixel regions could be obtained accurately by including clipping procedure within this mechanism. [14] proposed a candidate selection mechanism for face recognition. This algorithm is novel local motion based algorithm to determine the static and motion within the video frame. Candidate selection algorithm strictly employs candidate vectors at each site where motion detection is desired. This algorithm was formed under Bayesian framework to yield minimum possible estimation error. [15] proposed a mechanism to handle healthcare issues. Propagation mechanism is employed to tackle the problem of mean square error. Propagation mechanism adjusts the input vectors in order to obtain modified input in order to obtain the output which lies between the threshold limits. [16] and [17]proposed a local and global feature extraction mechanism from videos integrated with machine learning mechanisms. Local motion detection mechanism employs local valuators and vectors that checks for the motion of object within the scene. This detection mechanism uses the static motion detector since frame changes to small extent using this model. Global detection includes detection of motion due to the camera movement. The noise handling mechanism must be integrated within such model to eliminate noise that could be present due to capturing mechanism. Temporal redundancy is explored using this modeling process.

III. PROPOSED WORK

In the current framework to coordinate the score of pictures catching from finger and face print we was just utilizing details coordinating and edge recognition. There is no real way to deal with the clamor that happens amid catching. In our proposed paper we are utilizing PAD security component frameworks which catch unique finger impression and face pictures from an informational collection. In the wake of catching pictures for recognizable proof of individual we coordinate the score by utilizing details coordinating and design coordinating procedures. The execution of the above proposed work will be improved by utilizing middle sifting to evacuate the commotion that happens amid picture catching procedure. The exactness of the framework is improved by limiting the PSNR, FAR, FRR and MSE and so forth.

Flow chart of proposed work



IV. RESULTS

False Match Rate (FMR): It is an estimation of incorrectly identified sample that claimed to identify the sample. These samples may belongs to different subject.

Table 1: False Matching Rate (FMR)

	Result	THRESHOLD=0.4
Image	FMR_EXISTING	FMR_PROPOSED
Img1	0.003234	0.003124
Img2	0.003451	0.003057
Img3	0.003203	0.002898
Img4	0.002787	0.0026032
Img5	0.002968	0.0025890

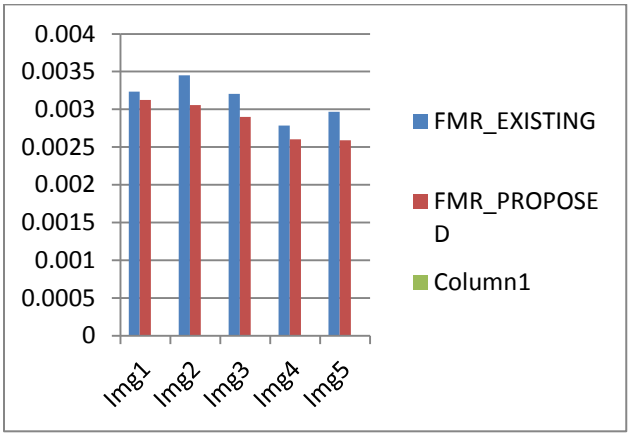


Figure 3: False Matching Rate (FMR)

False Non-Match Rate (FNMR):
It is estimation of the samples that are rejected by incorrectly and claimed when sample actually belongs to that subject.

Table 2: False Negative matching Rate (FNMR)

	FNMR_EXISTING	FNMR_PROPOSED
Img1	0.02676	0.02546
Img2	0.02534	0.02365
Img3	0.02336	0.02184
Img4	0.02262	0.02012
Img5	0.02873	0.02234

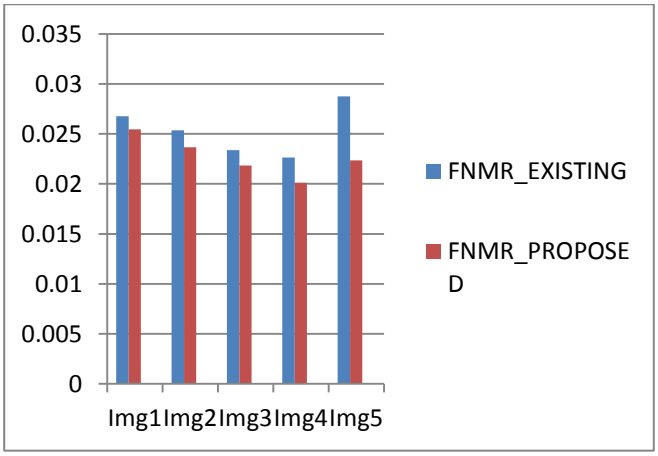


Figure 4: False Negative matching Rate (FNMR)

V.CONCLUSION AND FUTURE SCOPE

Biometric innovation includes another layer of security by giving secure distinguishing proof and confirmation. This innovation prospering in all respects quickly, however biometric verification doesn't give flawless outcomes. To beat this issues biometric verification strategy has been checked on from above dialog that there are two sorts of biometric validation procedure for example unimodal& multimodal. To expand exactness and the dependability of biometric confirmation, PAD security instrument can be utilized. This paper additionally gives results as FAR, FRR, FTE that comes amid information catching. In future to upgrade the multimodal framework we can blend multiple or two biometric tests to show signs of improvement reaction.

REFERENCES

[1] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, K. N. Qureshi, F. Computing, and J. Bahru, "Security Issues and Attacks in Wireless Sensor Network," *World Appl. Sci. J.*, vol. 30, no. 10, pp. 1224–1227, 2018.

[2] D. Karaboga, S. Aslan, and Ü. Ñ. Ò. Ö. Ò. Ü. Ñ. Ü. Ü. Ñ. Ò, "A New Emigrant Creation Strategy for Parallel Artificial Bee Colony Algorithm ØÒ ××," pp. 689–694.

[3] M. A. Jabbar, B. L. Deekshatulu, and P. Chandra, "Classification of Heart Disease Using K- Nearest Neighbor and Genetic Algorithm," *Procedia Technol.*, vol. 10, pp. 85–94, 2013.

[4] X. Yang and A. Hossein Gandomi, "Bat algorithm: a novel approach for global engineering optimization," *Eng. Comput.*, vol. 29, no. 5, pp. 464–483, 2012.

[5] F. Tashtarian, M. H. Yaghmaee Moghaddam, K. Sohraby, and S. Effati, "On Maximizing the Lifetime of Wireless Sensor Networks in Event-Driven Applications With Mobile Sinks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 7, pp. 3177–3189, 2015.

[6] "FaceRecognition." .

[7] P. Anitha, K. N. Rao, V. Rajasekhar, and C. H. Krishna, "Security for Biometrics Protection between Watermarking and Visual Cryptography," *IEEE Access*, no. March, pp. 64–71, 2017.

[8] W. Abdul, Z. Ali, S. Ghouzali, M. S. Hossain, and S. Member, "Biometric Security Through Visual Encryption for Fog Edge Computing," *IEEE Access*, vol. 5, 2017.

[9] W. L. Woo, S. Member, and J. A. Chambers, "A Framework for Iris Biometrics Protection : A Marriage between Watermarking and Visual Cryptography," vol. 3536, no. c, pp. 1–13, 2016.

[10] A. Jameer Basha, V. Palanisamy, and T. Purusothaman, "Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features," *J. Comput. Sci.*, vol. 7, no. 5, pp. 698–706, 2011.

[11] L. R. Haddada, B. Dorizzi, and N. Essoukri Ben Amara, "Watermarking signal fusion in multimodal biometrics," *Int. Image Process. Appl. Syst. Conf. IPAS 2014*, 2014.

[12] N. Dey, "Motion Detection and Tracking in Video Processing Applications (Preface)," *IEEE Access*, no. September, 2016.

[13] R. Snehkunj, A. N. Jani, and N. N. Jani, "Brain MRI / CT Images Feature Extraction to Enhance Abnormalities Quantification," *Springer Int. Publ.*, vol. 11, no. January, pp. 1–10, 2018.

[14] L. Best-Rowden, H. Han, C. Otto, B. F. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2144–2157, 2014.

[15] P. Naraei, V. Street, V. Street, and V. Street, "Application of Multilayer Perceptron Neural Networks and Support Vector Machines in Classification of Healthcare Data," *IEEE Access*, no. December, pp. 848–852, 2016.

[16] A. V. Flevaris, A. Martínez, and S. A. Hillyard, "Attending to global versus local stimulus features modulates neural processing of low versus high spatial frequencies: An analysis with event-related brain potentials," *Front. Psychol.*, vol. 5, no. APR, pp. 1–11, 2014.

[17] S. Africa, "From Local to Global Processing: The Development of Illusory Contour Perception," vol. 4, no. 11, pp. 38–55, 2017.

