BioPay: A Secure Payment Gateway through Biometrics

Gurpreet Singh.[1*], Divyanshi Kaushik[2], Hritik Handa[3], Gagandeep Kaur[4], Sunil Kumar Chawla[5], and Ahmed A. Elngar[6]
[1,2,3,4,5]Chandigarh Group of Colleges, Landran, (Mohali) Punjab
[6]Faculty of Computers and Artificail Intelligence, Beni-Suef University, Beni Suef City, 62511, Egypt
[1]gurpreet.3529@cgc.edu.in,[2]divyanshi1815659@gmail.com,[3]hritikhanda4@gmail.com, [4]gagandeep.4421@cgc.edu.in, [5]sunil.3550@cgc.edu.in , **[6]elngar_7@yahoo.co.uk**

(Corresponding Author: Gurpreet Singh.[1*] , [1]gurpreet.3529@cgc.edu.in)

Abstract:

Due to emerging technological developments, major enhancements are taking place in the area of a secure and quick transaction. BioPay being a secure payment method is a one-step ahead. In the proposed methodology, there is no involvement of any credit or debit card or any other account information like OTP or CVV; it solely depends upon some unique identifying characteristic of a human known as biometrics. This work proposes a novel method that allows users to complete transactions quickly and securely using face and finger recognition. The transaction initiates with scanning face features and matching it with the database which in turn retrieves all the information associated with that customer account. After that, the system will scan the fingerprints of the subject and verify the transaction. This methodology can be implemented in ATMs and smartphones resulting in enhanced security and flexibility for payment purposes.

Keywords: *Face Recognition, Fingerprint, Fast and Secure Transaction, CVV, OTP, Biometrics.*

1. Introduction

Among the panoply of payment methods available today, credit cards and debit cards are the most used methods. People use cards for online shopping, ticket booking, money transferring, and ATM transactions. As every technological advancement improves the current state, there are also some pros and cons attached to every novel technology and invention so is the case with e-payment methods that offer ease of transactions on one hand while poses several challenges like vulnerability to suspicious activities and attacks on the other hand. People encounter various instances in their everyday lives where cards can be lost, stolen, or theft. Considering these insecurity concerns, the proposed work utilizes biometric to circumvent them, which enhances transaction security. The only pre-requisite is the user's face and fingerprint must be linked with the concerned bank.

There is various research ongoing utilizing facial recognition for transaction purposes, such as Kim et al. [11] researched on biometrics payments replacing cards in the offline payments market and concluded

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

transactions being ubiquitous through mobile phones and biometrics. Surekha et al. [16] proposed a methodology for the transaction through facial recognition.

Stressing our work, it is a two-layered authentication system comprises of face and finger recognition, enabling a secure way of transactions. The payer can carry transactions anywhere, anytime with smartphones, and enables ATM's to work without any card or account information. The device captures the payer's biometrics and verifies it with registered biometrics in the bank's database. Face recognition being beloved and ubiquitous nowadays; many research fields advancing with face recognition systems, such as attendance systems based on facial recognition [7], patient monitoring systems based on face and voice recognition [14], etc. The reasons for biometric systems being superior are enhancing security, faster processing, and automated identification. Along with benefits, face recognition also faces challenges like twin problems, Massive data storage capacity, face spoofing, and expression variation. The proposed system is prepared with insight into all these challenges and to solve them.

1.1 Fingerprint Recognition

There available several methods for Fingerprint Recognition in the computer vision, such as correlation-based matching, minutiae-based matching, and pattern-based (or image-based) matching [19, 22]. In the proposed system, Minutiae-based Fingerprint Recognition [1] is utilized.

1.2 Minutiae-Based Fingerprint Recognition

A preprocessed (Noise cleared, Binarised, and thinned) fingerprint image is fed to Feature Extractor which scans the local neighborhood of each pixel in the thinned image and computes the Crossing Number (CN) using:

$$CN = \frac{1}{2} * \sum_{i=1}^{8} |P_i - P_{i+1}|, \qquad where\ P_i\ is\ the\ pixel\ value\ in\ the\ neighborhood\ of\ P$$

Every crossing number corresponds to a different ridge structure resulting in the extraction of different sets of minutiae points. For each Minutiae point, there will be (x, y) coordinate, Orientation factor (θ) type factor (CN). The extracted set is shown below:

Fig 1: Minutiae points extraction of fingerprints

Then this image will be passed to minutiae matcher which will iterate over every minutiae point and find the closest image-based orientation and distance difference between minutiae point in the database fingerprint image and test minutiae image.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

For distance computation:

$$sd_j = \begin{cases} 1 & if\ \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \leq r_0\ ,\ where\ r_0\ is\ the\ distance\ threshold \\ 0 & otherwise \end{cases}$$

For orientation computation:

$$dd_j = \begin{cases} 1 & if\ \min(|\theta_j - \theta_j|\ , 360 - |\theta_j - \theta_j|) \leq \theta_o \\ 0 & otherwise \end{cases}, where\ \theta_o\ is\ orientation\ threshold$$

Based on these observations the matrix MarkScore will be marked and the Match score with the formula:

$$Matching\ Score = \frac{number\ of\ minutiae\ marked\ as\ 1\ in\ MarkScore}{maximum\ number\ of\ minutiae} * 100\ \%$$

1.3 Face Recognition

For face as well, several methods are available and after a comparative study of all these different face recognition techniques in the cited paper [6,20,21,23,24], LBPH is found to be having better results than other techniques like PCA and LDA. In the proposed system, the LBPH classifier, a feature-based face recognition technology is utilized.

1.4 Local Binary Pattern Histogram (LBPH)

(LBPH) is a type of visual descriptor that works on grayscale images to recognize facial features. LBP is an ordered dataset (x_i, y_i) made with the comparisons of neighboring intensities of eight pixels with the central pixel intensity and given as:

$$LBP(x_c, y_c) = \sum_{n=0}^{7} s(l_n - l_c)2^n$$

Where l_n corresponds to the intensity of neighboring pixel, l_c denotes the intensity of central pixel and s is the threshold function and given as:

$$s(k) = \begin{cases} 1 & if\ k \geq 0 \\ 0 & k < 0 \end{cases}$$

The first step by the LBP classifier is to create a compressed image that can represent the original image, the LBP algorithm uses the concept of sliding with neighbor and radius as parameters to create the central compressed image. After that, the compressed image is divided into blocks, each block represents a histogram and aggregating all the histograms create a larger histogram, which can represent the original image. Now, This histogram will be compared with one in the database, and distance difference is determined using Euclidean distance (D)

$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$ that can be used to determine the confidence level of the model.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

2. Literature Sirvey

Biometric is becoming beloved and ubiquitous day by day, many kinds of research are going on enhancements of biometrics. One field is e-payment systems require extra endeavors, so embedding biometrics with payment methods for authentication can be a better practice. Many researchers investigating methods for authentication utilizing biometric. N. Badovinac et al. [2] proposed a multimodal biometric authentication system, that generates the required pin for card payments with the help of biometrics, without any involvement of the bank. Also, they have mentioned that the distance between the eyes and pupil will determine whether the person uses 4 digit pin or 6 digit pin and the one finger can generate at most 2 digit pin. So, the whole pin will be generated with the correct combination of multiple fingers. Now suppose if the person is using a 6 digit pin and has a small face for which their algorithm determines the person uses 4 digit pin, so transaction cancels or by some means of an accident, the person got scratches on one of these fingers, it will cancel the transaction. Also enlightening the accuracy of their system, Suppose if a finger matches with a 90% confidence level with the database, then the pin generated will be wrong as the whole procedure depends on the 100% accuracy of biometrics which is practically impossible.

By investigating methods for fetching the features of face for face recognition, the paper starts with is facial recognition. In [10], Olszewska et al. proposed system stated that Biometric technology is the automatic method to identify a person which we can use as a key step for our system, but their process depends on the physiological characteristics of a person which can not differentiate the twins. So to overcome that, we have used the iris recognition system along with face recognition. Also considering the credit card frauds, M. Chavan et al. [4] proposed a method for credit card authentication using face recognition by local binary pattern algorithms. In their method, they divided the facial recognition process into two categories: processing before detection where face detection and the alignment take place and afterward recognition that occurs through feature extraction and matching, but this system is cornered within credit cards due to the low-security level. So our system overcomes this limitation by adding extra biometric features like fingerprint recognition. With this biometrics combination, this system can push its limits from only use with credit cards to use in every payment that does not matter whether it's on a mobile phone, ATMs, or at shopping windows.

As the panoply of techniques available today for Biometric recognition and various researches are going on these techniques to improve their accuracy and success rate. Some of the cited papers dealing with these kinds of researchers are [6, 9, 15, 18, 24].

S.Sawhney et al. [18] proposed a method for Smart attendance by making the use of face recognition techniques, like eigenfaces, Principle Component Analysis (PCA), and Convolutional Neural Network (CNN). After this, the communication of a respected face should be accessible by comparing the database with the student's face. Also, P. Wagh et al. [15] proposed an attendance system based on face recognition techniques based on Principle component analysis (PCA) and eigenfaces. Narayan et al. [12] discussed and classified various face recognition techniques based on success rates. He accomplished this in two stages. In the First stage, His model detects the image of the human face by Viola-Jones Algorithm but it is not quite effective in detecting tilted or turned faces. So, in the Second stage detected face is recognized by the fusion of Principle Component Analysis (PCA), Artificial Neural Network (ANN). It provides better accuracy in the face recognition system.

3. Proposed System

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

3.1 Architecture

This method requires a camera for face recognition and a fingerprint scanner. As there are no specific pre-requisites, so there is no special architecture for the proposed payment method. This method can be utilized in smartphones and ATM's.

3.2 Methodology:

To develop and use our BioPay system, the steps required to be followed are given below:

- **Registration of the face and fingerprint data with the bank account**

Our proposed system comprises two main components, face recognition and fingerprint authentication that is required to be registered in the bank one time, so that registered data can be used as reference data during account fetching and fingerprint verification.

- **Face Recognition**

The first phase of the system is face recognition, which extracts the facial features like nodal points, retina structure, and iris structure and matches data with the database reference data by feeding facial data to the trained model at the server-side (LBPH classifier) so that it fetches the bank accounts linked with the particular face.

- **Fingerprint Recognition**

The second phase of the system is fingerprint recognition, which requires fingerprint from the user, this fingerprint will be preprocessed and filtered and extract the minutiae points of the input fingerprint with the help of fingerprint processing algorithm, then it matches it with the database. If a match succeeds, then the transaction is carried further.

- **Confirmation of transaction from the bank servers**

Every bank has its own rules, like maintaining some minimum balance, so before carrying the transaction the bank servers will check all the formalities for a successful transaction like amount must be less than the funds in the bank account, Minimum balance is maintained, etc. After that Servers allow the transaction.

Flow Chart of Proposed System:

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

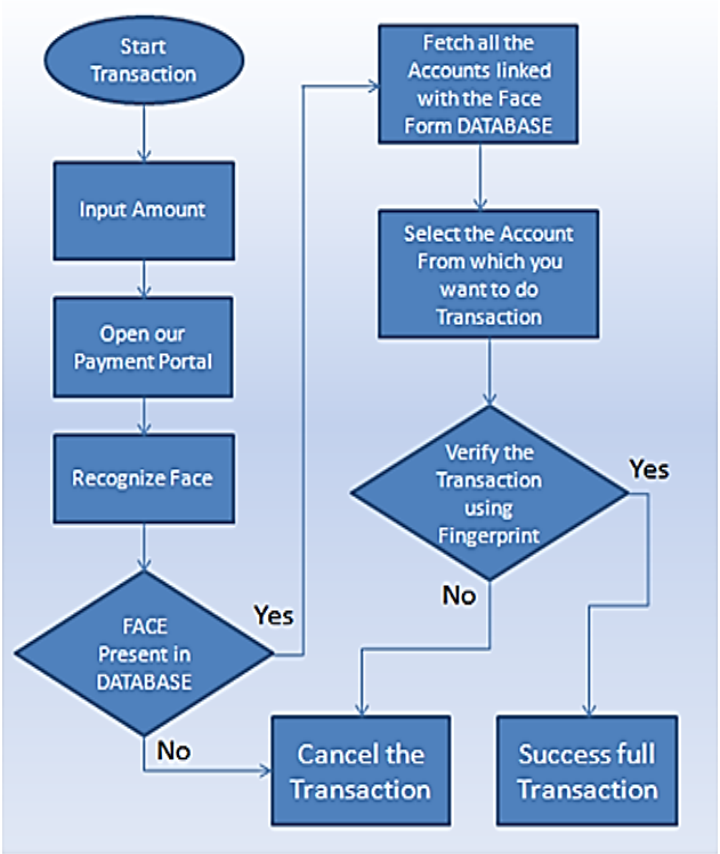

Fig 2: Flowchart of proposed system

Technology Used: We have created a prototype of BIOPAY payment System using:

Table 1: Technology Details

Technical Language	Python
Environment	Python 3.7
IDE	Pycharm Community Edition 2019
Libraries	Image -Processing Libraries -OpenCV [8], Machine learning libraries- Tensorflow, Keras
Graphical User Interface	Tkinter

- **Login**

We have created a login System for Admin to login and set the Model and data of the users (Including their Account balance, Facial Features, and fingerprints) a customer can log in and can do the transaction.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

Fig 3: Login window

❖ **Face recognition for verification**

At this stage, we have used the Viola-Jones Algorithm to train our Classifier and now it can detect the face in real-time and fetch the Accounts associated with that face.

Fig 4: Face recognition

❖ **Fingerprint recognition for transaction**

In this Section, a Real-time fingerprint is matched with Fingerprint in the database associated with the user database.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

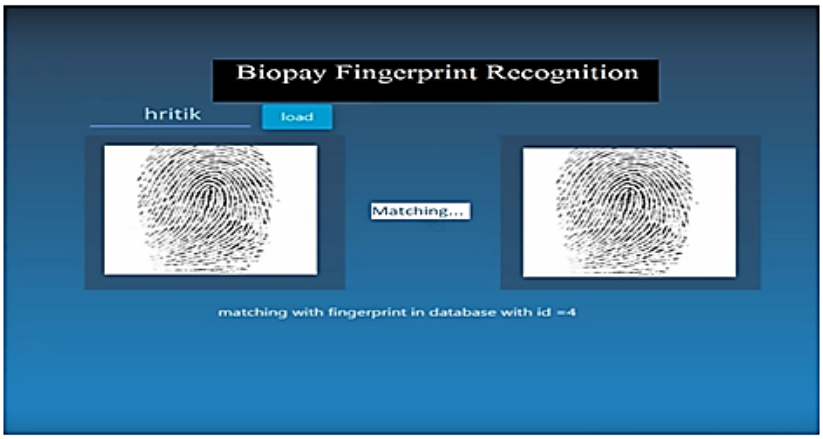

Fig 5: Fingerprint Recognition

❖ **Advantages of Proposed System**

- Enhanced security and payment exchange in a brief span preventing money robbery.
- Proposed System work without any card, Bank Documents, furthermore there is no overburden of recollecting OTP, all they need to utilize their biometrics for recognizable proof, which is an extremely protected alternative than current methods.
- LBP classifiers have the important property of adjustment against varying illumination and simple computation, which allows the LBP classifier for real-time Applications.

4. Comparison and Analysis

Comparison with Patent Lifeng et al. [2] discussed the application of face for the transactions and payment exchanges. They set up a framework for enabling payment exchange through facial recognition. The disadvantage of their work is that their framework is equipment availability place dependent and transactions can be carried out during shopping etc, where verified employes of the organization carry the transaction. The proposed transactional system is more secure as there is double-precision due to multimodal biometrics e.g. face and fingerprint. The proposed system is also flexible; in the sense that the payments can be carried out from anywhere, using a smartphone.

Comparison with Patent Hoyos et al. [3] also proposed a strategy for transactions based on biometrics. Hereafter the distinguishing proof of the face and fingerprint, a transaction code is created in the enrolled portable number. After embeddings that code into the machine, the transaction is successful, but in our system, there is no code, PIN, and CVV involvement.

A comparison with Bhuvaneshwari et al. [5] proposed the strategy wherein biometric is utilized for security purposes in ATMs. For security purposes, they utilized Aadhar numbers as client IDs rather than ATM cards, and fingerprint identification is used for passwords. For that, they need to convey the Aadhar card or recall the Aadhar number for ID. There is no need to remember anything in our system as there is no enrollment of numbers and the whole transaction is carried out with the help of biometrics only.

Comparison with Adegboye et al. [13] researched on the secure online transaction through Biometrics and came up with the combined solution of biometrics and password. In biometrics, the fingerprint is used as an id, and a password is used as a confirmatory key. In our system, there is no requirement for a password.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

Comparison with P Sharma et al. [17] proposes a payment system only with the use of face recognition, which is practically less secure. Also, their system requires a password for the transaction which makes it a slow method.

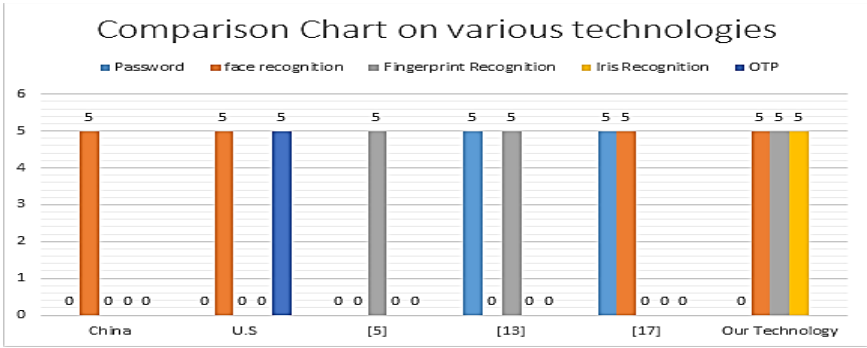

Fig 6: Comparison chart

Comparison with existing state of art:-

The current system of payment is very advanced, UPI is in trend, but card payments have their place. So when we compare the current system with our proposed system, we come to some points that:

Table 2: Comparison Between Current Technology and Future Planned Technology

S. No.	Existing state of Art	Disadvantages of existing state	Overcome
1	Card is necessary	The card can be stolen	No need for a card
2	Need to remember the pin	The pin can be forgot	No need of pin code
3	Transaction requires Code	Less Secure	The more secure transaction requires biometrics

5. Experimental Results

For facial recognition, after demonstrating the LBPH algorithm, below mentioned are the first 10 iterations and corresponding accuracies in Table 3 and overall accuracy of the facial recognition model in Table 4:

Table 3 : First 10 Model Iterations vs Accuracies

Iteration number	Accuracy
1	90.99
2	89.95
3	90.45
4	89.67
5	91.70
6	92.74
7	90.81
8	91.44

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

9	91.46
10	91.80

Table 4: Overall Facial Recognition Model Accuracy

Average Accuracy	88.73
Maximum Accuracy	92.74

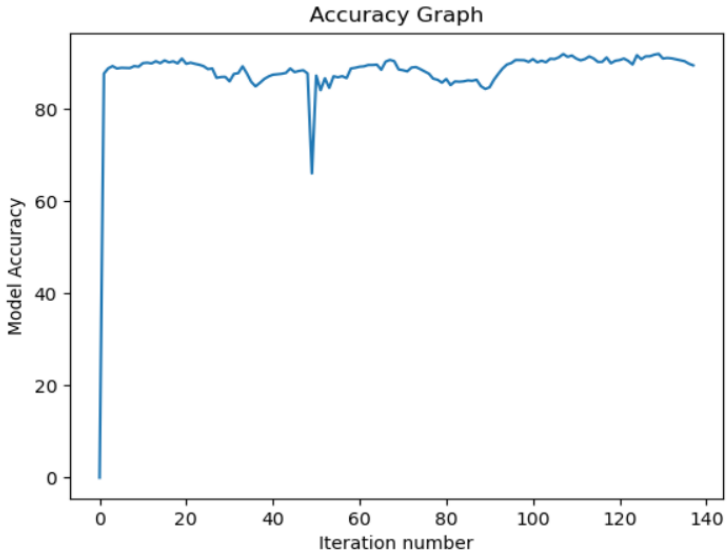

Fig 7: Face recognition model accuracy graph

Accuracy of the facial recognition system depends upon three factors:

1. Quality of Image
2. Illumination effect
3. Facial Expression

In the proposed system, image is captured utilizing a webcam which is considered as a low-quality camera, also due to improper light causing illumination effect degrades the accuracy of the model. So they can be overcome by using a high-quality camera and proper lighting.

6.Conclusion & Future Scope

The proposed system manages payments utilizing biometrics such as fingerprint and face. This system. It initially scans the user's face and fed it to the proposed algorithm which will extract facial features and matches it with the database. Then, the window will show all the Bank accounts linked with that particular person, then the user has to select the transactional account. The system will demand for the fingerprint of the client to verify the transaction. If all biometrics matches, the transaction would proceed. As we are utilizing biometrics, it's a highly protected way to do a transaction. Also, it does not require any information regarding the bank accounts like card number, PIN, CVV, or bank account number. In the proposed

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

prototype, the LBPH face recognizer has posses accuracy of 92.74% when 120 training samples per person are fed to the classifier, which can be further enhanced by proper illumination and high-quality camera.

The proposed system can be used in various perspectives. As cybercrime is increasing day by day, it is significant that our bank accounts must be safe. If this system is implemented in ATMs and other payment portals this will make every transaction quick and secure. Also, it will prevent frauds and theft. The combined System of the face and fingerprint recognition can also be used to protect homes, offices, lockers, and much more, but as there is no robust facial recognition technology with 100% accuracy, So it is required to use a threshold value till the fingerprint and face recognition techniques becomes robust. The proposed system will be very beneficial in the sectors of security and advancements.

References

[1] Mouad. M.H. Ali, V. H. Mahale, PravinYannawar, A.T. Gaikwad. "Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching", IEEE 6th International Conference on Advanced Computing (IACC), 2016

[2] N. Badovinac and D. Simic, "A Multimodal Biometric Authentication (MBA) in Card Payment Systems", International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI), Belgrade, Serbia, pp. 23-236, doi: 10.1109/IC-AIAI48757.2019.00011, 2019.

[3]Hoyos; Hector (New York, NY)," Systems and methods for biometric authentication of transactions", United States Patent US9208492B2, Nov 13, 2014

[4] M.Chavan, D.Sawant, S.Nalawade, "Credit Card Authentication Using Facial Recognition", International Research Journal of Engineering and Technology (IRJET), Volume: 06, Issue: 04,4th April 2019

[5] AJ, Bhuvaneshwar, "Secure and enhanced ATM with Biometric Authentication", 2019.

[6] P. Kamencay, T. Trnovszky, M. Benco, R. Hudec, P. Sykora, and A. Satnik, "Accurate wild animal recognition using PCA, LDA, and LBPH," 2016 ELEKTRO, StrbskePleso, pp. 62-67, doi: 10.1109/ELEKTRO.2016.7512036, 2016.

[7] Y. Kawaguchi, T. Shoji, W. Lin, KohKakusho, M.Minoh, "Face Recognition-based Lecture Attendance System", 2005.

[8] K.Goyal, K.Agarwal, R. Kumar, "Face detection and tracking: Using OpenCV", pp 474-478, doi:10.1109/ICECA.2017.8203730, 2017.

[9] S.Majithia, H. Singh, A. Gupta, N.Sharma."An efficient machine learning method for facial expression recognition", International Journal of Innovative Technology and Exploring Engineering, 8(9 Special Issue), pp. 539–546, 2019.

[10] Olszewska, Joanna, Isabelle," Automated Face Recognition: Challenges and Solutions. Pattern Recognition - Analysis and Applications",doi:10.5772/66013,Dec 14,2016.

[11] M.Kim, S.Kim, J.Kim, "Can mobile and biometrics payments replace cards in the Korean offline payments market? Consumer preference analysis for payment systems using a discrete choice model," Telematics and Informatics, vol.38, pp. 46-58, 2019.

[12] N. T.Deshpande, Dr. S.Ravishankar," Face Detection and Recognition using Viola-Jones algorithm and fusion of LDA and ANN", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 6, Ver. II (Nov. - Dec. 2016), PP 01-06

[13]Adegboye, A. "Secure On-Line Transaction through Augmented Biometrics System". Global journal of computer science and technology,2015.

[14] AtifAlamri," Monitoring System for Patients Using Multimedia for Smart Healthcare" IEEE Access, vol. 6, pp. 23271-23276, 2018, doi: 10.1109/ACCESS.2018.2826525.

[15] P. Wagh, S. Patil, J. Chaudhari, R. Thakare, "Attendance System based on Face Recognition using Eigenfaces and PCA Algorithms, "International Conference on Green Computing and Internet of Things (ICGCloT), 2015.

[16] S.R.Gondkar, Saurab. B, "Biometric Face Recognition Payment System", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, NCESC - 2018 Conference Proceedings, Special Issue – 2018.

[17] P. Sharma, Priyanshu, V. Tiwari, N.Jha, "A Mobile Payment System Based On Face Recognition", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, Vol. 06 Issue: 4, Apr 2019

[18] S. Sawhney, K. Kacker, S. Jain, S. N. Singh, and R. Garg, "Real-Time Smart Attendance System using Face Recognition Techniques," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp 522-525, doi: 10.1109/CONFLUENCE.2019.8776934, 2019.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021

[19] Cynthia D'Souza N, L.J. Rodrigues, and Nausheeda B.S," A survey on fingerprint recognition techniques", International Journal of Latest Trends in Engineering and Technology, pp. 441-447 e-ISSN: 2278-621X, Special Issue SACAIM 2016.

[20] X. Zhao, C. Wei. "A real-time face recognition system based on the improved LBPH algorithm." IEEE 2nd International Conference on Signal and Image Processing (ICSIP) (2017): 72-76, 2017.

[21] F. Deeba, H.Memon, F. A.Dharejo, A.Ghaffar, Aftab Ahmed, "LBPH-based Enhanced Real-Time Face Recognition", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 5, 2019.

[22] K. Nirmalakumari, H. Rajaguru, P. Rajkumar, "Efficient Minutiae Matching Algorithm for Fingerprint Recognition," 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 1-5, doi: 10.1109/ICACCE46606.2019.9079971, 2019.

[23] G. Xiang, Z. Qiuyu, W. Hui, C. Yan, "Face recognition based on LBPH and regression of Local Binary Features," International Conference on Audio, Language and Image Processing (ICALIP, pp. 414-417, doi: 10.1109/ICALIP.2016.7846668, 2016.

[24] S. Gupta and L. Singh, "A study on new biometric approaches," International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, 2017, pp. 306-310, doi: 10.1109/IC3TSN.2017.8284496, 2017.

DOI: 10.5281/zenodo.5224633
Received: February 07, 2021 Accepted: July 19, 2021