International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 7, July 2020 ||

Face Based Authentication for Monetary Transaction Using LBPH and 7th Bit Steganography

Yashaswini A R[1], Varun M[2], Venkat Prashanth Erragolla[3], Sachin V N[4], Laxmana [5]

Assistant Professor, Department of CS&E, Maharaja Institute of Technology Mysore, Karnataka, India[1]

UG student, Department of CS&E, Maharaja Institute of Technology Mysore, Karnataka, India[2]

UG student, Department of CS&E, Maharaja Institute of Technology Mysore, Karnataka, India[3]

UG student, Department of CS&E, Maharaja Institute of Technology Mysore, Karnataka, India[4]

UG student, Department of CS&E, Maharaja Institute of Technology Mysore, Karnataka, India[5]

ABSTRACT: In today's world as the illegal use of technology or software based is significantly growing and at the same time online banking is getting more popular. As of the most of the online banking applications are using two-way authentication which is a password and OTP sent to the registered user.The credentials are being stolen and being misused. The proposed work is based on facial recognition for both login and also monetary transaction.As in face recognition spoofing or faking the face comes into picture.Faking can be done by displaying photograph copy of a picture or video in front of the authenticating device. Considering these faking or spoofing techniques, the system also uses Eye blink recognition to overcome these issues.And the system is also providing a good solution on POS point of Sale using image steganography.Using this we can complete successful transaction by verified person in a way that it is proven to the executing party, that the transaction was in fact initiated and confirmed by an identified person.

In this work, we endeavor to make a stride towards detection of face using LBPH algorithm.LBPH algorithms is better compared to other algorithms in low light condition and has achieved exceptional results in various fields including computer vision. We plan to overcome the shortcomings of the present systems and provide an accurate and precise system to detect face thereby saving people from money thefts.

KEYWORDS: Face recognition,Eye blink recognition,Image steganography,LBPH,Computer vision.

I. INTRODUCTION

Banking is a essential part of human life. Customer's information stored by the banks. This information is private and saved securely in the bank database. Customer can perform transactions on both online and offline manner. Bank transaction activities the attack easy to hack the details. In this situation we have to protect the bank account. At the point when user input their passwords in an open place, they might be chances of attackers taking their secret word. A hacker can catch a secret word by direct perception or by recording the individual's transactions.

It is very essential to integrate biometric facial recognition software with online banking software. Well,there are more positives to this than is the case with more conventional methods used in the past. In fact, using passwords comes with a rather serious problem. People create passwords based on what they know and there behaviour. So it is easy for a hacker to employ a number of tactics to hack the password. Another major flaw is that people can have too many passwords eg. for social media accounts, emails, and e-wallets as well. Also, creating a complex password might result in forgettingthe password and when a banking customer requests for a temporary code the means reseting a new password via email to reset it, then a hacker can intercept in between the bank and the users inbox.

Objectives:

- Solution for the floss in POS services (Point Of Sale)in which the redirecting or masking of QR should be authenticated by image steganography.
- A second level authentication using a eye blink password using simple EAR (Eye Aspect Ratio) which does not involve complex image processing.
- A 7th bit steganography used in POS which is better than the classical steganography approach.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 7, July 2020 ||

II. RELATED WORK

Aftab Ahmed et al [1] Automatic individual face recognition is the most challenging query from the past decade in computer vision. However, the law enforcement agencies are not efficient to identify and recognize any person through the video monitoring cameras further efficiently; the blur conditions,resolution, illumination and lighting are some of the major problems in face recognition. there proposed system operates better at the minimum low resolution of 35px to identify the human face in various situations like different angles, side poses and tracking the face during human motion.This paper employs the Local Binary Patterns Histogram (LBPH) algorithm architecture to address the human face recognition in real time at the low level of resolution.Melike GUNAY et al [2] Identification and authentication methods have developed into a main technology in various areas, such as entrance control in building and access control for computers. Most of these methods have a drawback with their legitimate applications.Rather than human and voice recognition, these methods almost requires the user to remember a password, or human action in the process of identification or authentication. However, the corresponding means are potential being lost or forgotten, whereas fingerprints and retina scans suffer from low user acceptance rate. Face recognition has a high recognition rate of more than 90% for huge face databases with proper pose and lighting conditions. This high rate can be used for replacement of lower security requirement environment and could be successfully employed in different kind of issues such as multi-media. Automatic recognition of face is a vast research area of computer vision technology, reaching from face detection, face localization, face tracking, extraction of face orientation and facial features and facial expressions. These will need to tackle some technical problems like illumination, poses and occlusions.Candra Irawan et al [3] If you were to use *steganography* in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages, cryptography. Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover files.H M Rehan Afzal et al [4] In this paper,the proposed method which takes a single 2D image as input and outputs a 3D reconstructed image. This method is fast and robust. It consists of three steps. First step consists on feature extraction. For feature extraction we have used SDM which is computationally efficient. Face is detected at first, then facial features like nose, eyes and mouth are extracted. This image was in 2D dimension, so we applied multivariate Gaussian distribution to find its depth which added one more dimension in our examined image. To overcome the problem of huge computations, PCA was implemented to reduce dimensions. Finally, the data gained from above two steps were aligned with 3D Basel face model to reconstruct 3D face. Result section shows the final outcome of 3D face reconstruction. This method had been tested on a number of images taken from LFW database and its accuracy was checked. Most of previous algorithms used multiple images as input to train algorithms which are computationally costly. However, the proposed method only takes a single 2D image and efficiently reconstructs 3D image.K Sunil manohar Reddy et al [5] Face recognition is a challenging problem in the field of Image processing and computer vision. Because many of the Application in different fields the face recognition have become more popular because of easy and fast process.In this paper different face recognition algorithms are mentioned with their advantages and disadvantages. You can use any ofthem as per your requirement and application. Future work can be done to improve efficiency of discussed algorithmsand improve performance.Tereza Soukupovaet al [6] A real-time algorithm to detect eye blinks in a video sequence from a standard camera is proposed. Recent landmark detectors, trained on in datasets exhibit great robustness against a head orientation with respect to a camera, varying light and face expressions. We show that the landmarks are being detected precisely to reliably estimate the level of the eye opening. The proposed algorithm uses the landmark positions to extracts a single scalar quantity – eye aspect ratio (EAR) – characterizing the eye opening in each frame. Finally,the decrease in ear detects eye blinks as a pattern of EAR values in a temporary window. The simple algorithm outperforms the state-of-the-art results on two standard datasets.Kamaldeep joshi et al [7] As the internet has become the medium for transferring the sensitive information, the security of the transferred message has become the topmost priority. Image steganography has emerged out as the effective tool of information hiding that provides the security of the transmitted data. Image files provide more capacity, and their frequency of availability in the internet is also high. In this paper, a method of image coding is proposed that hides the information in a selected pixel and on the next value of that selected pixel, that is, pixel + 1. One bit is hidden at the selected pixel, and the another bit is hidden on the pixel +1 value. On the basis of the 7th bit of the pixels of an image, a mathematical function is applied on the 7th bit of the pixels, which generates a temporary variable taht is (pixel + 1). The 7th bit of the selected pixel and 7th bit of pixel + 1 are used for information hiding and extracting. On the basisof these two values, two bits of the message can be hidden on each pixel. After implementation, the efficiency of the method is checked on the basis of parameters such as PSNR and MSE, and then comparison with some already proposed techniques. This proposed image steganography showed promising results when compared with other classical and existing techniques. Sevierda Raniprima et al [8] The proposed steganography system that is combined with encryption based on rubik's cube principle can keep information secret. Secret image can be perfectly hidden in

cover image. If somehow secret image is extracted, it would be hard to decrypt secret image due to confusion and diffusion properties of the encryption algorithm and also its large key space. The proposed steganography systems are tested using visual attack and Chi square analysis.

III. METHODOLOGY

This project is implemented using three different techniques which is integrated into our project.

A. FACE RECOGNITION

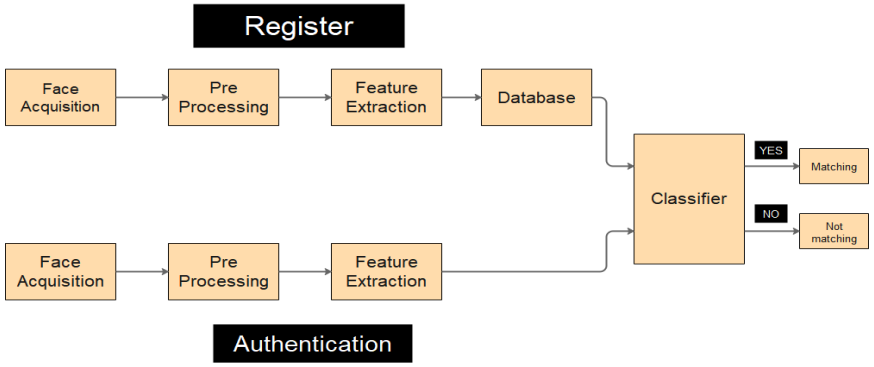

Fig 1:Face Recognition Process

Face Detection

We have used OpenCV which presents a Haar cascade classifier , which is used for face detection. The Haar cascade classifier uses the AdaBoost algorithm to detect multiple facial features. First, it reads the image to be detected and converts it into the gray image, then loads Haar cascade classifier to decide whether it contains a human face. If so, it proceeds to examine the face features and draw a rectangular frame on the detected face. Otherwise, it continues to test the next picture.

Feature Extraction

The LBP operator is applied on the image to describe the contrast information of a pixel to its neighborhood pixels.Normally LBP operator is defined in the window of 3*3. Using the median pixel that is central pixel value as the threshold of the window,it compares with the pixel value with gray value of the adjacent 8 pixels. If the neighborhood pixel value is larger or equal compare to the median pixel value, the value of pixel position is marked as 1, otherwise marked as 0.In this way, 8 points in the3*3 neighborhood are compared to generate 8-bit binary numbers. Changing it to decimal numbers, the LBP values of the middle pixel points of the window are obtained, which is used to display the texture features of the region. The current LBPH algorithm uses an improved circular LBP operator.The gray value GP of P neighborhoods of the pixel C, theradius of which is R. GC is the graypixel value C (xc,yc). This algorithm makes the LBP operator no longer limited to fixed radius and neighborhood and can meet the needs of more different size and texture features. For each pixel of an image, it computes its LBP eigenvalues. Then these eigenvalues can form the LBP feature spectrum. The LBPH algorithm uses the histogram of the LBP spectrum as the feature vector for classification and comparison.It divides a picture into several sub regions, then extracts LBP feature from each pixel of the sub-region, establishing a statistical histogram of the LBP characteristic spectrum in each subregion, so that each sub region can using a statistical histogram to describe the whole picture through a number of statistical histogram components. The advantage is to reduce the error that the image is not fully aligned with a certain range.

1. ALGORITHM USED

LBPH- Local Binary Pattern Histogram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 7, July 2020 ||

Firstly the face image input is given to the algorithm.The face image is divided into blocks called grids.On applying the local binary operator on those grids a histogram will be created on each grid.At last all those histograms of each grid is combined and used for face recognition.

B. EYE BLINK RECOGNITION

$$\mathrm{EAR} = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|}$$

EAR refers to the aspect ratio of the eye region, which is often used to calculate the temporal consistency and speed of left and right eye blinks and in fatigue detection . There has been no results of the application of EAR to the assessment of facial paralysis. In this study, EAR was used to characterize the displacement changes of the eye landmarks of facial paralysis patients in the movement image series of frames, and the difference in bilateral eye movements of facial paralysis patients was evaluated according to the changes in EAR.

In both the normal face images and facial paralysis face images, the landmarks of the nasal root and the nose tip on the face changed slightly during the movements (displacement changes of less than 2 pixels. To raise the difference in bilateral eye movements and to improve the performance of the difference in EAR characteristics and based on the observation that the movements of the bilateral eyebrows are also inconsistent during the process of eye opening and closing in facial paralysis patients, the Euclidean distance from the centre of the eyebrows to the tip of the nose divided by length of the nose is used as an amplification factor for EAR.

C. 7TH BIT LSB TECHNIQUE

Image steganography has emerged out as the important tool of information hiding that make sure the security of the transmitted data. Image files provide more capacity, and their frequency of availability in the internet is also high. In this paper, a method of image coding is proposed that hides the information in a selected pixel and on the next value of the selected pixel, that is, pixel + 1. One bit is hidden at the selected pixel, and the next bit is hidden on the pixel +1 value. On the basis of the 7th bit of the pixels of an image, a mathematical function is applied on the 7th bit of the pixels, which generates a variable (pixel + 1). The 7th bit of the selected pixel and 7th bit of pixel + 1 are used for information hiding and extracting. On the basis of a combination of two values, two bits of the message can be hidden on each pixel P. After implementation, the efficiency of the method is checked based on the parameters like PSNR and MSE, and then comparison with some already proposed techniques.

IV. RESULTS AND DISCUSSION

The main aim of our project is to provide a better solution on online monetary transactions. Our system overcomes existing system drawbacks by providing

1. Cost effective solution.
2. Application can be accessed remotely anywhere at anytime.
3. More accurate.
4. User friendly solution.

Our system checks weather the user is authenticated or not to make transactions.
Now comparing Fisher Face , Eigen Face and LBPH algorithms that we used in the system

Feature	Fisher Face	Eigen Face	LBPH
Light variation	70-75%	83-85%	85-90%
Distance Variation	68-73%	83-88%	88-93%
Pose Variation	70-75%	78-83%	88-90%

Table.1:Algorithm accuracy comparison

The results showed that LBPH is best algorithm to choose for our work and it gave better results on various conditions like light,distance and pose.

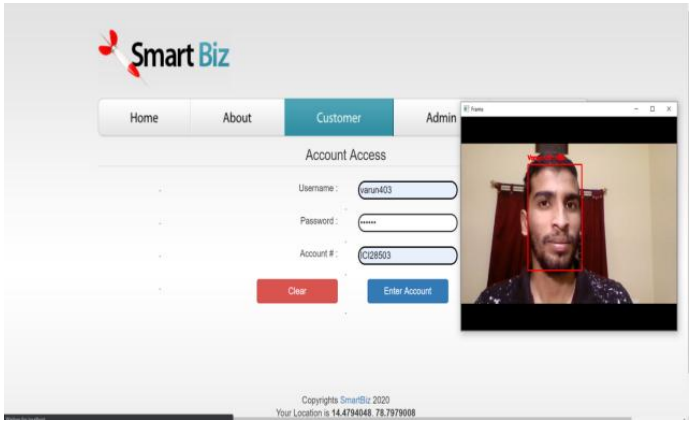

Fig.2:Face Recognition.

In this figure the person is authenticating himself to the online banking system using facial recognition.

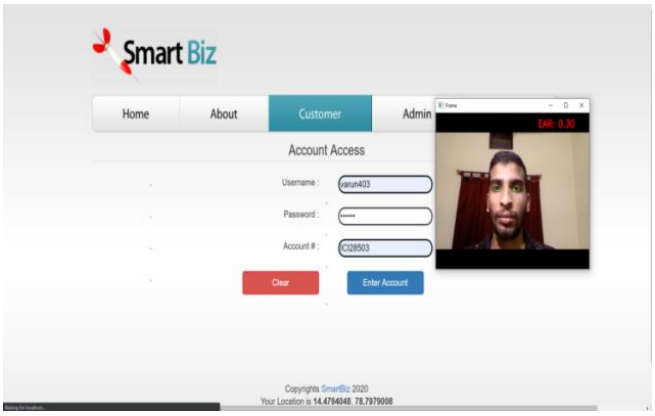

Fig.3:Result Pages.

In this figure the person is authenticating himself to the online banking system using eye blink password.

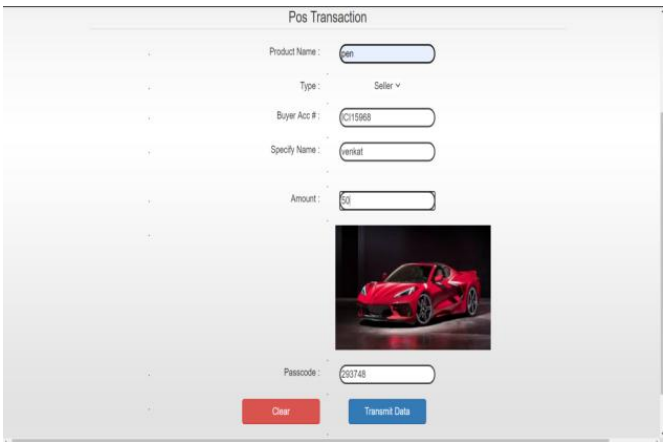

Fig.4:Result Pages.

In this figure the POS transaction is being initiated by the seller.

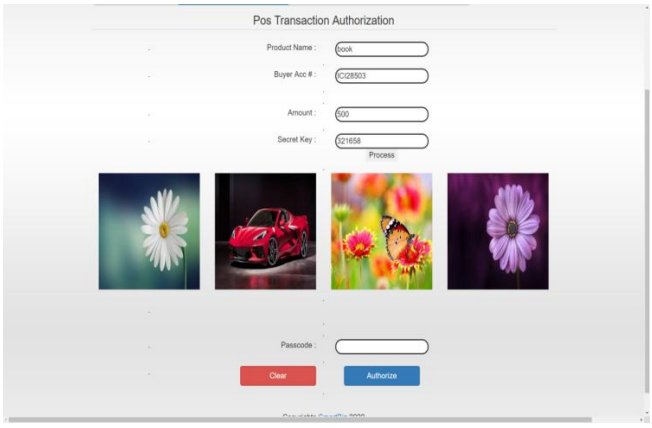

Fig.5:Result Pages.

In this figure the POS transaction is being verified by the buyer.

V. CONCLUSION AND FUTURE WORK

The motivation for the project is to provide security for all types of monetary transactions.Facial Recognition software has a livenliess detection which prevents hackers from using a picture of the customer for impersonation purposes. It also applies to other biometric modalities such as eye blink where the liveliness detection does exactly that – it assesses the 'liveliness' of the facial image to guarantee that it is a live image and not a (still) picture or a spoof as it is known. The recognition system also allows users to access their bank accounts from computers or laptops. It is possible by the means of webcams which are built-inin laptops. While logging into their account, facial biometrics is an additional layer of security.And Avoiding the spoofing attack using eye blink recognition.LBPH algorithm is the best and works good on low light conditions and posture problems compared to Eigenface and FisherFace. Coming to the application on the whole, it works in real-time and has the ability to send alert emails along with offering a user-friendly graphical interface. It's cost-effective, reliable robust,accurate compared to existing opto-electronic hardware and software-based systems in the market.

Proposed system uses "Eye blink Recognition" for Anti spoofing Attacks so by using Convolutional Neural Network for Face Anti-Spoofing.The application only detects the wrong attempt to access the account and gives only alert so by the help of picture of wrong person try to attack the account and by using geocoding in the application can lodge complaint against them. The application has manual process for POS transaction so it replaced with QR.

REFERENCES

[1]."LBPH Based Improved Face Recognition At Low Resolution"Aftab Ahmed,Jiandong Guo,Fayaz Ali and Farha Deeba.
[2]."Comparision of Various Face Recognition Algorithms", Melike GUNA.
[3]."Hiding and Securing Messages on Edge Areas of Image using LSB Steganography",Candra Irawan,De Rosal Ignatius Moses Setiad,Christy Atika Saari and Eko Hari Rachmawanto.
[4]'Reconstruction of 3D facial image using a single 2D image",By H. M. Rehan Afzal, Suhuai Luo and M. Kamran Afzal.
[5]"Comparison of Various Face Recognition Algorithms",K. Sunil Manohar Reddy and Dorina Kabakchieva .
[6]."Real-TimeEye Blink Detection using Facial Landmarks".Tereza Soukupova and Jan Cech
[7]."A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image",Kamaldee Joshi
[8]."Digital Image Steganography with Encryption Based on Rubik's Cube Principle",Sevierda Raniprima and Bambang Hidayat.
[9]".OTP-Based Two-Factor Authentication Using Mobile Phones",By Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan.
[10]."Implementation of Graphical Passwords in Internet Banking for Enhanced Security",SALMA ABID RAZVI ,S.NEELIMA and G.YUVASREE.
[11]."Mobile Banking Transaction Using Fingerprint Authentication",By Lokesh Sharma and Manish Mathuria.
[12]. "Online Banking Authentication System using Mobile-OTP with QR-code",Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee.
[13] Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., & Ma, M. (2019). Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics. IEEE Access, 7, 158481-158491.
[14]."Secure User Authentication in Internet Banking: A Qualitative Survey", Janardan Choubey and Bhaskar Choubey.