International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

OFFENSIVE SECURITY FOR ATM DATA SECURITY USING MACHINE LEARNING FOR PASSWORD AUTHENTICATION

J.Noorul Ameen[1], V.Maheswari[2], R.Nanthini Bharathi[3] , S.Punitha[4]

[1]Assistant professor, Dept of CSE , E.G.S.Pillay Engineering College ,Tamil Nadu, India
[2]UG student, Dept of CSE , E.G.S.Pillay Engineering College ,Tamil Nadu, India
[3]UG student, Dept of CSE, E.G.S.Pillay Engineering College ,Tamil Nadu, India
[4]UG student, Dept of CSE, E.G.S.Pillay Engineering College ,Tamil Nadu, India

---

Abstract - *The human face is an important entity which plays a crucial role in our daily social interaction, like conveying individual's identity. Face recognition system is also able to recognize the person from a specific distance without touching or any interaction with the person. This face recognition method is applied in ATM system. Recognized face is matched then the system will allow using, otherwise this system pass the intimation to concern card holder's mobile and if that holder accepts the request the process can be proceeded for further transactions , if denied the entire process will be surpassed. Also a Personal Identification Number (PIN) is a sequence of digits that confirms the identity of a person when it is successfully presented. The maturity of PIN authentication is a result of its continuous usage for years in a wide range of everyday life applications, like mobile phones and banking systems. PIN authentication is susceptible to brute force or even guessing attacks. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. To overcome shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits. The visibility algorithm forms the core of our work and we would like to examine whether it can be used to assess the visibility of images other than hybrid keypads. Visibility algorithm could be used to assess the visibility of general images, but its parameters have to be appropriately tuned for the particular task at hand.*

***Key Words*: Password, Brute force attack, Shoulders Surfingattack, Authentication system, Usability, Security, ATM, Camera, Local binary patterns**.

1.INTRODUCTION

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines too.

Image processing basically includes the following three steps.

- Importing the image with optical scanner or by digital photography.
- Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
- Output is the last stage in which result can be altered image or report that is based on image analysis.

1.1 METHODOLOGY

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc.

Therefore, the quality of system input determines the quality of system output.

Well designed input forms and screens have following properties

 It should serve specific purpose effectively such as storing, recording, and
retrieving the information.

- It ensures proper completion with accuracy.
- It should be easy to fill and straightforward.
- It should focus on user's attention, consistency, and simplicity.
- All these objectives are obtained using the knowledge of basic design principles

regarding –
o What are the inputs needed for the system?
o How end users respond to different elements of forms and screens.

1.2 TYPES

The two types of methods used for Image Processing are Analog and Digital Image Processing. Analog or visual techniques of image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing.

Digital Processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction.

2. IMAGE PROCESSING

In computer science, **digital image processing** is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-today life for various applications. Image processing has a number of applications such as: Remote Sensing, Medical Imaging, Non-destructive Evaluation, Forensic Studies, Textiles, Material Science, Military, Film industry, Document processing, Graphic arts, Printing Industry etc. Keywords- image processing, image enhancement, image restoring, remote sensing.

Image processing is a form of signal processing for which the input is an image and the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques treat the image as a two-dimensional signal. Image processing is computer imaging where application involves a human being in the visual loop. In other words the image are to be examined and are acted upon by people. The major topics within the field of image processing include: Image restoration, Image enhancement, Image compression

Many of the techniques of digital image processing, or digital picture processing as it often was called, were developed in the 1960s at the Jet Propulsion Laboratory, Massachusetts Institute of Technology, Bell Laboratories, University of Maryland, and a few other research facilities, with application to satellite imagery, wire-photo standards conversion, medical imaging, videophone, character recognition, and photograph enhancement. The purpose of early image processing was to improve the quality of the image. It was aimed at human beings to improve the visual effect of people. In image processing, the input is a low-quality image, and the output is an image with improved quality. Common image processing include image enhancement, restoration, encoding, and compression. The first successful application was the American Jet Propulsion Laboratory (JPL). They used image processing techniques such as geometric correction, gradation transformation, noise removal, etc. on the thousands of lunar photos sent back by the Space Detector Ranger 7 in 1964, taking into account the position of the sun and the environment of the moon.

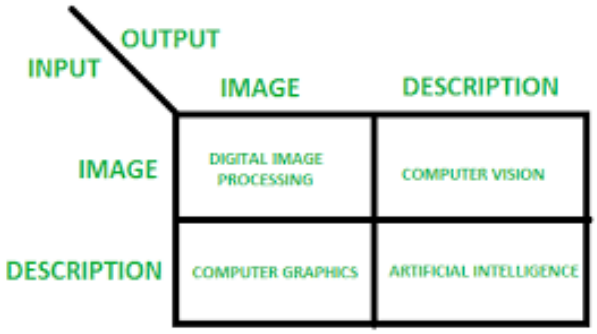


Fig 1: Overlapping Fields With Image Processing

The impact of the successful mapping of the moon's surface map by the computer has been a huge success. Later, more complex image processing was performed on the nearly 100,000 photos sent back by the spacecraft, so that the topographic map, color map and panoramic mosaic of the moon were obtained, which achieved extraordinary results and laid a solid foundation for human landing on the moon. roliferate as affordable computers and dedicated hardware were becoming available. This led to images being processed in real-time, for some dedicated problems such as television standards conversion. As general-purpose computers became faster, they started to take over the role of dedicated hardware for all but the most specialized and computer-intensive operations. With the fast computers and signal processors available in the 2000s, digital image processing has become the most common form of image processing, and is generally used because it is not only the most versatile method, but also the cheapest.

Digital image processing technology for medical applications was inducted into the Space Foundation Space Technology Hall of Fame in 1994

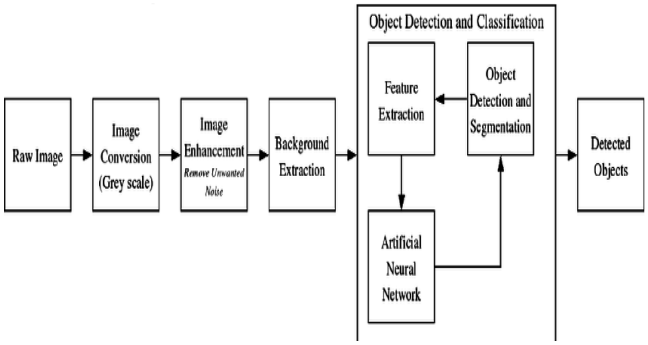


Fig 2: **Overview of Image Processing**

2.1 Digital Image Processing

Digital image processing is the use of computer algorithms to perform image processing on digital images. There are three major benefits to digital image processing: a consistently high quality of the image, a low cost of processing, and the ability to manipulate all aspects of the process. In digital photography, the image is stored as a computer file. This file is translated using photographic software to generate an actual image. The colors, shading, and nuances are all captured at the time the photograph is taken, and the software translates this information into an image. The principle advantage of Digital Image Processing methods is its versatility, repeatability and the preservation of original data precision.

2.2 Image Enhancement

Sometimes images obtained from satellites and conventional and digital cameras lack in contrast and brightness because of the limitations of imaging sub systems and illumination conditions while capturing image. Images may have different types of noise. In image enhancement, the goal is to accentuate certain image features for subsequent analysis or for image display [1, 2]. Enhancement methods tend to be problem specific. For example, a method that is used to enhance satellite images may not suitable for enhancing medical images. Although enhancement and restoration are similar in aim, to make an image look better. They differ in how they approach the problem. Restoration method attempt to model the distortion to the image and reverse the degradation, where enhancement methods use knowledge of the human visual systems responses to improve an image visually.

3. LITERATURE REVIEW

3.1 Title: Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected

Authors: Taekyoung Kwon ; Sooyeon Shin ; Sarang Na

When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concern. To cope with this problem, previous methods presumed limited cognitive capabilities of a human adversary as a deterrent, but there was a pitfall with the assumption. In this paper, we show that human adversaries, even without a recording device, can be more effective at eavesdropping than expected, in particular by employing cognitive strategies and by training themselves. Our novel approach called covert attentional shoulder surfing indeed can break the well known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution in this paper is the formal modeling approach by adapting the predictive human performance modeling tool for security analysis and improvement. We also devise a defense technique in the modeling paradigm to deteriorate severely the perceptual performance of the adversaries while preserving that of the user. To the best of our knowledge, this is the first work to model and defend the new form of attack through human performance modeling. Real attack experiments and user studies are also conducted.

3.2 Title: Graphical Password Authentication: Cloud Securing Scheme

Authors: Shraddha M. Gurav ; Leena S. Gawade ; Prathamey K. Rane ; Nilesh R. Khoch

Graphical password is one of the alternative solution to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication.

3.3 Title: DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices

Authors: Toan Van Nguyen a, Napa Sae-Bae b, Nasir Memon

PIN authentication is widely used thanks to its simplicity and usability, but it is known to be susceptible to shoulder surfing. In this paper, we propose a novel online finger-drawn PIN authentication technique that lets a user draw a PIN on a touch interface with her finger. The system provides some resilience to shoulder surfing without increasing authentication delay and complexity by using

both the PIN as well as a behavioral biometric in user verification. Our approach adopts the Dynamic Time Warping (DTW) algorithm to compute dissimilarity scores between PIN samples. We evaluate our system in two shoulder surfing scenarios: 1) PIN attack where the attacker only knows the victim's PIN but has no information about it's drawing characteristic and 2) Imitation attack where an attacker has access to a dynamic drawing sequence of a victim's finger-drawn PIN in the form of multiple observations. Experimental results with a data set of 40 users and 2400 imitating samples from two attacks yield an Equal Error Rate (EER) of 6.7% and 9.9% respectively, indicating the need for further study on this promising authentication mechanism.

3.4 Title: Enhancing security and privacy in biometrics-based authentication systems

Authors: N. K. Ratha, J. H. Connell, R. M. Bolle

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as ecommerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

3.5 Title: A Novel Touchscreen-based Authentication Scheme Using Static and Dynamic Hand Biometrics

Authors Mengyu Qiao ; Suiyuan Zhang ; Andrew H. Sung ; Qingzhong Liu

The booming of smart phone and high-speed wireless networks in recent years, applications and data have been shifting from desktop to mobile devices at a vigorous pace. Although mobile computing provides great convenience in daily life, it becomes vulnerable to various types of emerging attacks. User authentication plays an indispensable role in protecting computer systems and applications, but the development of touch screen hardware and user habit change post requirements for new authentication methods for mobile and tablets devices. In this paper, we present a robust user authentication scheme using both static and dynamic features of touch gestures. Discriminative features such as distance, angle, and pressure are extracted from the touch-point data, and used in statistical analysis for verification. We tested our scheme in a variety of experiments that involved multiple volunteers to perform various gestures. The analysis of experimental results and user feedback indicate the proposed scheme delivers comprehensive measurements and accurate pattern classification for touch gestures.

4. EXISTING SYSTEM

Now a days most of the criminal activities are performed in ATM machine. The unwanted peoples are using an ATM card without knowledge of authorized user. Also the jammer is used to fetch the card details and also the shoulder suffer technique is used to fetch the secret passwords. So the attacker can easily fetch the ATM details. These are the drawbacks in this existing system. Our Proposed method is used to reduce these drawbacks

4.1 Disadvantages

- Face detection and loading training data processes just a little bit slow.
- It can only detect face from a limited distance.
- It cannot repeat live video to recognize missed faces.
- The instructor and trainingSet manager still have to do some work manually.

5 PROPOSED SYSTEM

Face recognition system is also able to recognize the person from a specific distance without touching or any interaction with the person. This face recognition method is applied in ATM system. Recognized face is matched then the system will allow using, otherwise this system pass the intimation to concern card holder's mobile and if that holder accepts the request the process can be proceeded for further transactions , if denied the entire process will be surpassed. Shoulder-surfing is a big threat for PIN authentication in particular, because it is relatively easy for an observer to follow the PIN authentication process. PINs are short and require just a small numeric keypad instead of the usual alphanumeric keyboard. In addition, PIN authentication is often performed in crowded places, e.g., when someone is unlocking her mobile phone on the street or in the subway. Shoulder-surfing is facilitated in such scenarios since it is easier for an attacker to stand close to the user while escaping her attention. Illusion PIN is a PIN-based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of Illusion PIN is based on the simple observation that the user is always

viewing the screen of her device from a smaller distance than a shoulder-surfer. Based on this, the core idea of Illusion PIN is to make the keypad on the touch screen to be interpreted with a different digit ordering when the viewing distance is adequately large. This way, when the shoulder surfer is standing far enough, he is viewing the keypad as being different from the one that the user is utilizing for her authentication, and consequently he is unable to extract the user's PIN. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. To overcome shoulder-surfing attacks on authentication schemes by proposing Illusion PIN (IPIN), a PIN-based authentication method that operates on touch screen devices. Also, the keypad is shuffled in every authentication attempt to avoid disclosing the spatial distribution of the pressed digits. We create the keypad of Illusion PIN with the method of hybrid images and we call it a hybrid keypad.

5.1 ADVANTAGE

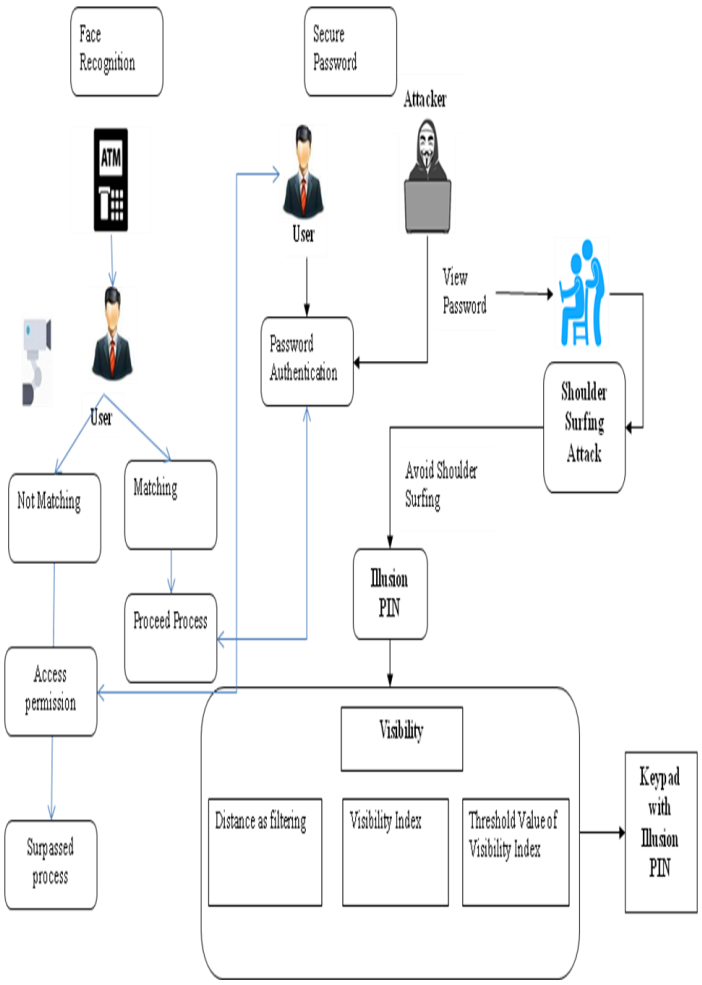
- The system stores the faces that are detected and automatically pass the intimations to card holders.
- Provide authorized access.
- Ease of use.
- Multiple face detection.

5.2 DATAFLOW DIAGRAM

A data-flow diagram is a way of representing a flow of a data of a process or a system. The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow, there are no decision rules and no loops.

The visual representation makes it a good communication tool between User and System designer. Structure of DFD allows starting from a broad overview and expand it to a hierarchy of detailed diagrams. DFD has often been used due to the following reasons: ... Determination of physical system construction requirements.

6. BLOCK DIAGRAM



6.1 SNEAKPEEKS OF IMPLEMENTATION

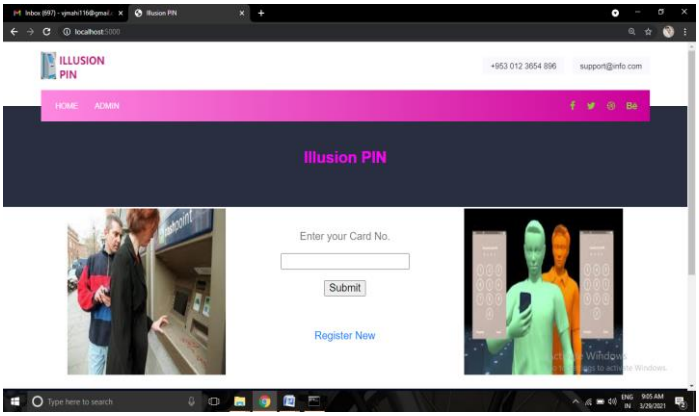


Fig 3 Homepage

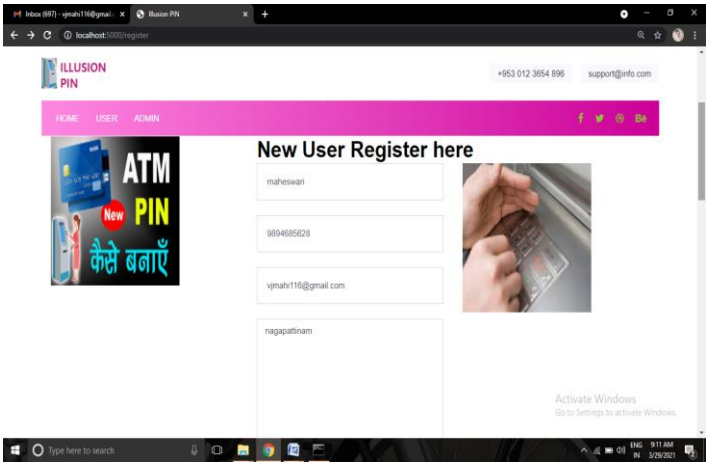


Fig 4 New user registration

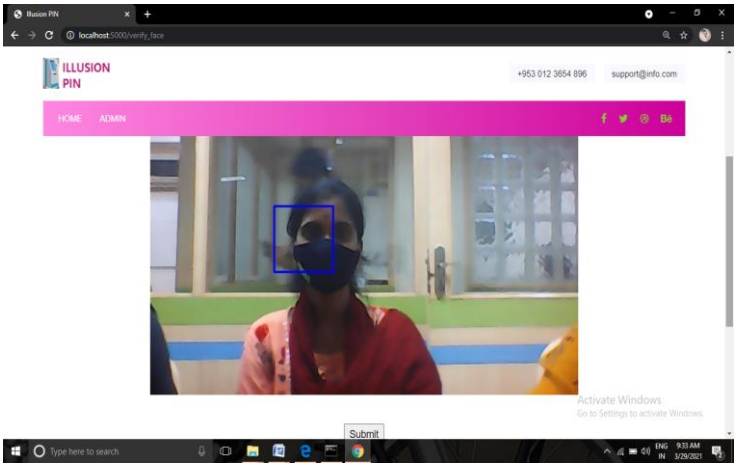


Fig 6.1

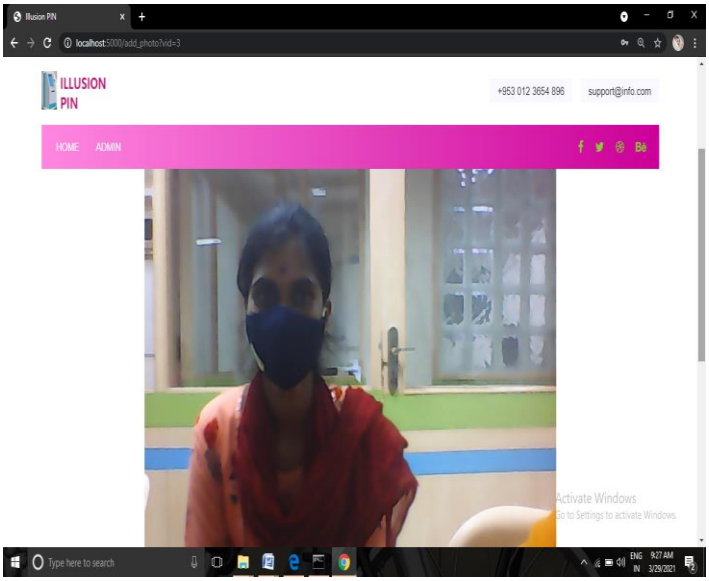


Fig 5 Face Recognition

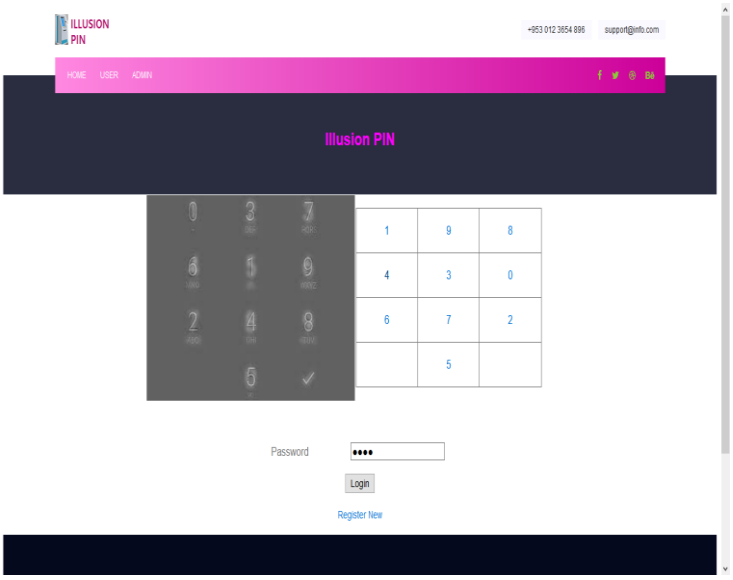


Fig 7 Illushion Pin

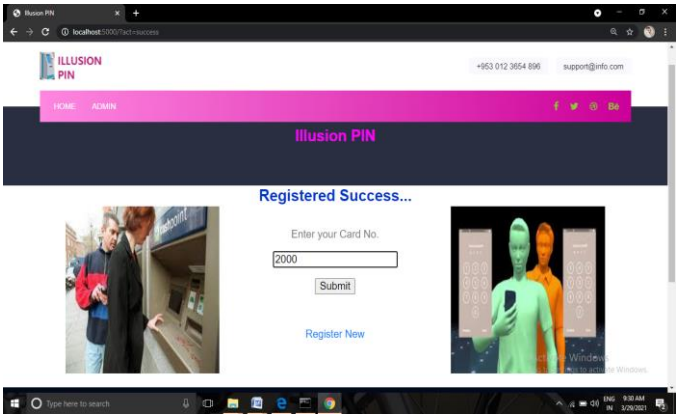


Fig 6 Pin Registration

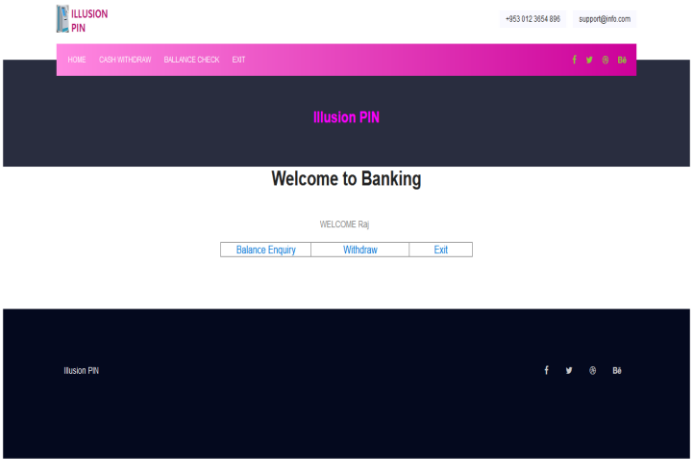


Fig 8 Transactions

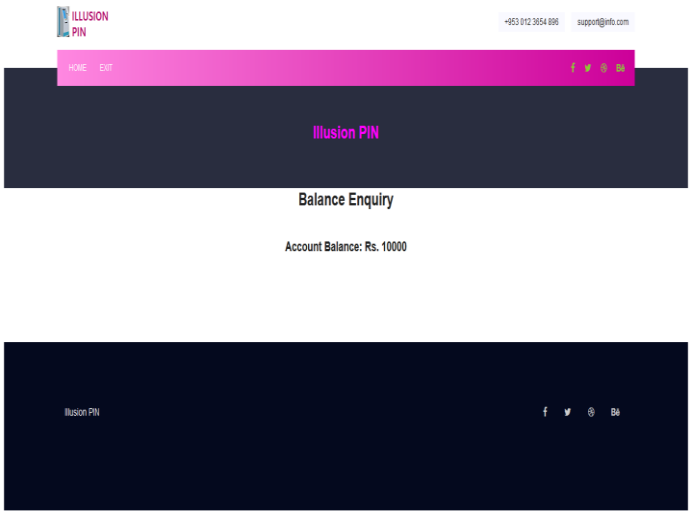


Fig 9 Balance Enquiry

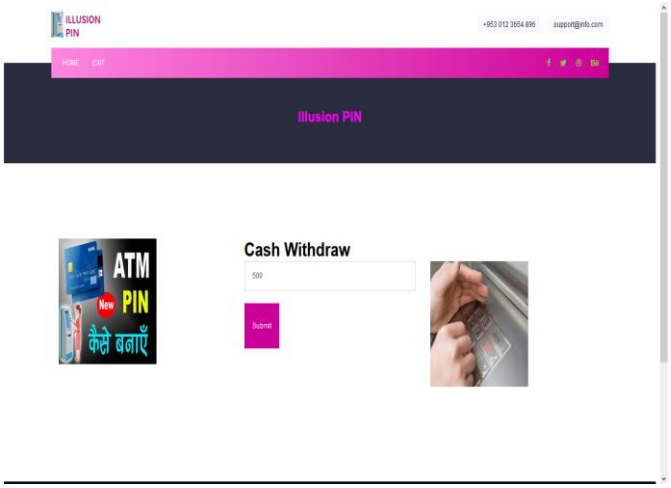


Fig 10 Cash Withdraw

7. CONCLUSION

The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we created Illusion PIN. We quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance, which we estimated with a visibility algorithm. In the context of the visibility algorithm, we had to model at a basic level how the human visual system works. Illusion PIN is a Hybrid PIN-based authentication scheme that would be resistant against shoulder surfing attacks. Two keypads are blended in a single key digit that will show different key pad to the attacker. Illusion PIN gives best results when compared to other PIN Authentication scheme. Recognized face is matched then the system will allow using, otherwise this system pass the intimation to concern card holder's mobile and if that holder accepts the request the process can be proceeded for further transactions , if denied the entire process will be surpassed.

REFERENCES

[1] P. Ekman and W. V. Friesen, "Constants across cultures in the face and emotion," *J. Personality Social Psychol.*, vol. 17, no. 2, pp. 124–129, 1971.

[2] A. Kläser, M. Marszalek, and C. Schmid, "A spatio-temporal descriptor based on 3D-gradients," in *Proc. Brit. Mach. Vis. Conf.*, 2008, pp. 99.1–99.10.

[3] P. Scovanner, S. Ali, and M. Shah, "A 3-dimensional sift descriptor and its application to action recognition," in *Proc. 15th Int. Conf. Multimedia*, 2007, pp. 357–360.

[4] L. Ma, "Facial expression recognition using 2-D DCT of binarized edge images and constructive feedforward neural networks," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IEEE World Congr. Comput. Intell.)*, Jun. 2008, pp. 4083–4088.

[5] S. Mohseni, H. M. Kordy, and R. Ahmadi, "Facial expression recognition using DCT features and neural network based decision tree," in *Proc. ELMAR*, 2013, pp. 361–364.