e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Highly Secure Authentication Scheme: A Review

Rahul Bora[1], Madhuri Zawar[2]
[1]*Computer Engineering, GF's G.C.O.E, Jalgaon*
[2]*Computer Engineering, GF's G.C.O.E. Jalgaon*

Abstract— The usability security has unique challenges because the need for highly secured authentication means identification and personal verification for strong system. The usability goal of highly secured authentication system is to provide better password by combining the graphical password using persuasive cued click points and biometric authentication using finger nail plate surface. To modifying the scheme of graphical password along with biometric authentication we can use only three fingers (Index, middle and Ring) by acquiring the low resolution images from digital camera from the outermost part of nail surface. Contour and texture is the main characteristics of nail plates which are represented shape based and their appearance features. For implementation of this we use the matching score level rules by employing decision and supporting vector machine. Here is the objective which provide highly secure authentication scheme to use the personal ID with graphical password using persuasive cued click point and biometric authentication using finger nail plate surface. In this there is limit of three fingers which is the scope of this paper. For better and strong password we use only three fingers for highly authentication for the purpose of some applications like banking, military, in forensic labs and civilians etc.
Keywords- Graphical Password, Biometric Authentication, Persuasive Cued Click Points, Security, Finger Nail Plate.

I. INTRODUCTION

In the modern era of computer system security is very important factor in the world of electronic. The secure system is the need of highly security to the number of ways to present the authentication like as biometric authentication, password authentication, token based authentication and text-based authentication for the secure computer system. But for all this types of authentication does not provide the high security where is the security required like in security agencies, banking, military, animal evolution and in forensic labs etc. Hence in the text-based password users can create the passwords which are remembering and it is easy for attackers to guess and also having the possibility to forget the text-based password for that information can be easily stolen by the hackers or attackers.

We are using the biometric authentication in that having some limitations in the existing system like in the finger knuckle which are more difficult to forge and in face recognition the characteristics of face can be changes with the age of an individual and in fingerprint technology the people can leave their fingerprint unconsciously wherever they touch an object and thus increasing the possibilities of imposter attacks and impersonation. So here we use the combination of two types of authentication for the system to increase the level of security. And we provide here high security level by combining and integrating the biometric authentication by using finger nail plate surface and graphical password by using the persuasive cued click points to reach the highly security level as each of the both methods can provide the high secure authentication.

II. RELATED WORK

A. PERSUASIVE CUED CLICK POINTS

In the previous models of click based graphical passwords it shown problems of hotspots, to reduce the space for effective password which can simplify the improving dictionary attacks. By adding the CCP features into Persuasive Cued Click Points it generates the password. We analyze that passwords choice influenced by user to select random clicks for maintaining the usability. For the generating password, PCCP uses the some requirements like viewport and shuffle. In this model of PCCP when certain image shown randomly selected block known as viewport and other portion of image shaded except the viewport and for this user can select the particular portion of viewport in the image (see Figure 1). For creating the secure graphical password the system can choose images randomly from selecting viewport of each image. User can select or click anywhere in the image of view port and they are having another option to change the position of view port which is known as "Shuffle". For attackers it is very complex to guess the click points in all images because the limitation of changing the position of view port. The viewport and shuffle button will be appearing at the time of registration process [2].

Fig1: PCCP creates Password hint.The viewport highlights part of the image

B. BIOMETRIC AUTHENTICATION USING FINGER NAIL PLATES

Now a days, the biometric system is received the hand based biometric authentication which can uses the various features which can be discrete and consultative. In this paper we examine that the real performance and some capabilities from the biometric finger nail plates which can be definite character achieved for the personal authentication system. In the biometric authentication of nail plate surface the ridge pattern is available on the nail which is highly uncommon in case of single and in twins and also other fingers of hand. Before that there is no attempt is utilized of texture and appearance based feature of finger nail plate for the personal authentication as like that it is very challenging characteristics of finger nail plate from hand it become visible as a guarantying fundamental of biometric study [2]. This new system is based on the outer part of finger nail and nail plate is challenging biometric device for military, forensic and civilian applications. The tongue-in-groove arrangement of the dermis and epidermis layers of the nail bed is referred to as arched and valley portion in Fig. 2(b) and it forms a structure that is unique, closely parallel and irregularly spaced. This grooved spatial arrangement of the nail bed is observed on the upper (convex) nail plate surface as longitudinal ridges/striations.

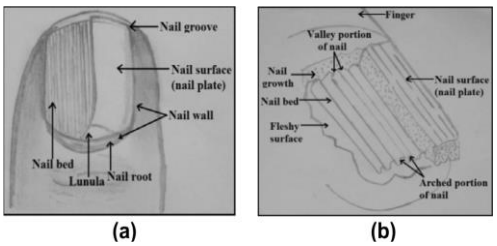

Fig 2: Finger nail surface in (a), magnification of the nail bed structure in (b)

These longitudinal striations simulated on the nail plate surface are highly unique for every individual for personal authentication. Thus, the individuality in the uniqueness of nail plate is based on biometrics which is completely depending on the essential anatomic characteristics of the nail organ [2].

Main and important elements of biometric authentication using finger nail plate surface which show in (figure 3) the following block diagram.

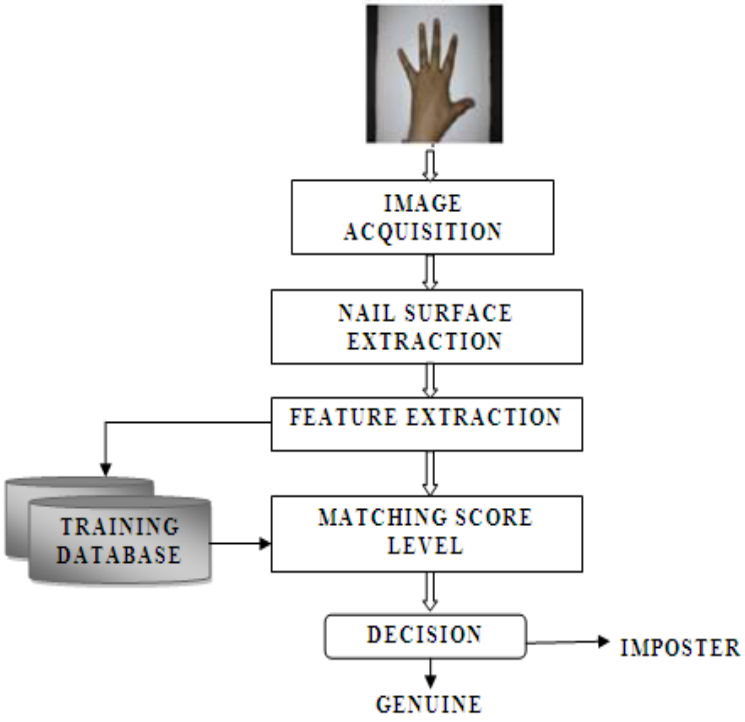

Fig 3: Block diagram of personal identification using nail plate and steps

III. LITURATURE SURVEY

A. CLICK BASED GRAPHICAL PASSWORDS

Mechanisms of graphical passwords are a type of knowledge based authentication that attempts to leverage the human memory for visual information. A precursor to Persuasive cued click points (PCCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click- points on one image, CCP uses one click-point on five different images shown in the sequence. The next image displayed is based on the location of the previously entered cued click-point, creating a path through an image set. Users select their images only to the extent that their cued click-point determines the next image. Creating a new password with different cued click-points it will results in a different sequence of images [1].

B. PERSUASIVE TECHNOLOGY

Persuasive Technology is a technology to motivate and influence people to behave in a desired manner. An authentication method which applies Persuasive Technology should guide and

encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive technology elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a low level (weak) password more tedious and time consuming. The path of least resistance for users is to select a strong password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across various users is minimized since click-points are more randomly distribute. [1].

C. BIOMETRICS

Biometrics means it is the study of automated methods for analyzing human characteristics like fingerprint, facial recognition, voice recognition, eye retina's and irises which used specially for authentication. It is based on "who are you", and "something you are". It is a way of identifying the person by using unique physical characteristics of person like facial or fingerprint scans and iris or voice recognition to identify users [6].

D. FACE RECOGNITION TECHNOLOGY

A facial recognition technique is an application of computer for automatically identifying or verifying a user from a digital image or a video frame from a video source. It is the most natural means of biometric identification. Facial recognition technologies have recently developed into two areas and they are Facial metric and Eigen faces. Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these features) [5].

E. FINGERPRINT TECHNOLOGY

A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmer (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal ". The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Now in modern approach, live finger print readers are used .These are based on optical, thermal, silicon or ultrasonic principles. It is the oldest of all the biometric techniques [5].

IV. CONCLUSION

It presents a fully automated personal authentication system based on finger nail-plate biometrics along with graphical password. It provides highly authentication scheme by integrating graphical password and finger nail-plate. It implements the graphical passwords scheme to improve the difficulty level of guessing it along with the biometric authentication which is very convenient and efficient method by acquiring low resolution images of nail-plate surface which is the outermost part of the nail unit.

REFERENCES

[1] S Chanson, E. Sober, A. Forget, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism,"Proc. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012.

[2] Amioy Kumar, Shruti Garg, M. Hanmandlu, "Biometric authentication using finger nail plates," Proc in Expert Systems with Applications 41 373–386 Elsevier at science direct, 2014.

[3] S. Chanson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[4] X.S. Zhou and T.S. Huang, — Relevance feedback For Image Retrieval: A Comprehensive Review, Multimedia systems, vol.8, no. 6 Apr. 2003.

[5] D. Bhattacharyya, R. Ranjan, F. Alisherov and M. Choi, "Biometric Authentication: A Review," International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009.

[6] S. Sonkamble, Dr. R. Thool, B. Sonkamble, "SURVEY OF BIOMETRIC RECOGNITION SYSTEMS AND THEIR APPLICATIONS," Journal of Theoretical and Applied Information Technology, 2005 - 2010 JATIT.

