Highly Secure Authentication Scheme

Ushir Kishori N
Department of Computer Engineering MMCOE, Pune

R.B. Joshi
Department of Computer Engineering MMCOE, Pune

ABSTRACT
The increased level of effective security control and transaction fraud in the world of electronic and internet commerce, demands for highly secured identification and personal verification systems. The Knowledge based authentication system encourage to user in selecting password for high security. For high security application the proposed scheme presents an integrated evaluation of the graphical password scheme by using persuasive cued click points, including usability and security evaluations, and implementation considerations along with the biometric authentication using finger nail plate surface. It implements the graphical passwords scheme to improvise 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. The contour and texture characteristics of nail plates from three fingers (Index, Middle and Ring) are represented by the appearance and shape based feature descriptors. To implement these we use the technique of score level rules for fusion and classifier based fusion of matching scores by employing decision tree and support vector machine. The objective is to provide highly secure authentication scheme by using user name with graphical password using persuasive cued click points along with biometric authentication using finger nail plate. The scope of the scheme is limited to three fingers only and also for high security purpose where it is very important to keep tight security like military application, forensic labs, civilian, banking applications, etc.

Keywords
Biometric Authentication, Graphical Password, Finger Nail Plate, security, Persuasive Cued Click-Points.

1. INTRODUCTION
In current state it is very important to secure system where the need of high security for that there are various ways to available authentication like password authentication, token based authentication and biometric authentication. But this all types of authentication cannot provide alone high security where required high securities like in military, banking, forensic lab etc. Because in textual password generally users create most memorable passwords which are easy to guess for attackers and also there is possibility to forget textual password that's why information can easily stolen by attacker. And in biometric authentication there are various limitations in existing devices i.e. in fingerprints in this people leave their fingerprint unconsciously wherever they touch an object and thus increasing the possibilities of imposter attacks and impersonation and also face characteristics changes with the age of individuals in face authentication. So that integration of

two types of authentication system is needed to increase the security level. So we provide the high security level by integrating the graphical password using persuasive cued click points and biometric authentication based on nail plate surface to reach a higher security level than each of the both methods can provide alone.

1.1 Motivation
Graphical password with Biometric authentication using finger nail plates motivates us to work on this because, There are various application where they required the highly secure authentication scheme for that there are various type of authentication which provides the security but out of them like textual password in that there is possibility to forget textual password by user and also can easily guess by attacker and also in biometric authentication there is some limitation in face, palm etc. So this scheme motivates us to increase the security level of fooling the access control system by using two different authentication methods in combination like graphical password with biometric authentication using finger nail plate. It combines the biometric and the graphical password based authentication methods to reach a higher security level than each of the both methods can provide alone. In addition it motivates the use of the biometric system in the verification and identification mode.

Also in nail plate authentication only the nail plate is regenerated as new cells are made, the ridge pattern which is present on the nail plate surface is highly unique and also stability. And the structure of nail plate surface is highly unique of the individual and also in case of twins and also different finger nails of the hand. Thus unlike face characteristics which changes with the age of an individual, these characteristics of the nail surface can be very useful for identification over the entire lifespan of the individual. Also there has not been any attempt in utilizing the texture and the appearance based information of the nail-plate along with graphical based password authentication for human authentication and verification in literature. This has motivated us to explore the combination of these two types of authentication for security applications.

2. RELATED WORK
In Graphical based password authentication Pass Point, Cued Click Points technique in literature**.** In pass-point [3] graphical password scheme consists of a sequence of 5 different click points on given image. To create password user can selects any pixel in the image as a click-points for their password. The limitation of this method is the HOTSPOTS and attackers can easily guess the password because user forms certain pattern to remember the secret code so that pattern formation attacks are easily possible. Cued Click Point [4] in that CCP uses one click-point on five different images in sequence instead of five click points on one image. The next image displayed is based on the previously entered the click point on the image. Limitation of this method is false accept (system can be accept incorrect click point) and false reject (system can be reject correct click point).this method reduced the pattern realization attack but HOTSPOT problem is still present. And also in biometric authentication there are various biometric scheme in the literature such as face, retina,

fingerprint/palm print Iris, etc. but in hand based biometric scheme like in palm print [5] and finger print [6] the palmer part of the hand is more susceptible to spoof attacks and also people unconsciously leave their palm and finger prints on the object whenever they touch. And also in finger knuckle [7] which are more difficult to forge and in face recognition [8] the face characteristics changes with the age of an individual.

3. PERSUASIVE CUED CLICK POINTS

Persuasive Cued Click Points [2] create the password by adding CCP features into it. In previous password scheme hackers can easily guess the password and also most of user clicks on the hotspots in each selected image without the system guidance. The system influence in this method is that the user can select more random clicks, and also it maintains the user's memorability. For password generation PCCP uses requisites like viewport & shuffle. In this method at the time of registration the randomly selected block of the image called the view port and only this view port clearly seen out and all the other parts of the image are shaded, so that the user can select click point only inside the view port of the image. (see Figure 1)The system is randomly selecting the view port of the image for each image to create a graphical password. The users can click anywhere in the view port of the image and also they have option to change the position of viewport called as "Shuffle". There is a limit to change the position of view port. So that for attacker it will be very difficult to guess the click point in all images. Only at the time of registration process the viewport and shuffle button appear. During login process the images are displayed normally, without shading or the view port, and the users can click anywhere on the images.

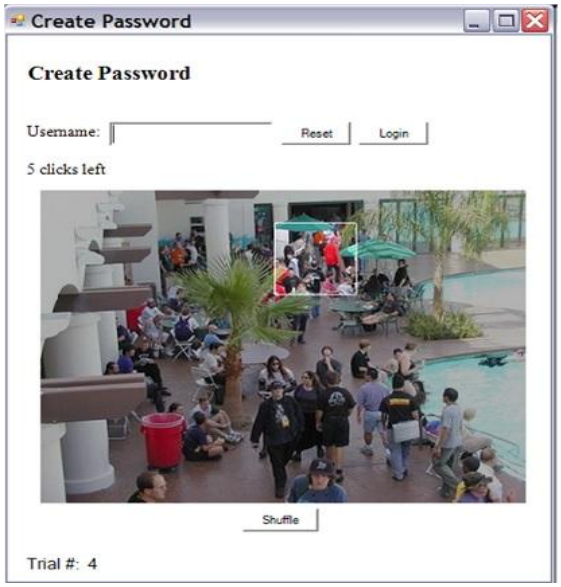

Fig 1: PCCP creates Password.The viewport highlights part of the image

User can choose any area within the highlighted viewport and and cannot click outside the viewport unless they press the shuffle button. PCCP method reduced the HOTSPOT problem, but it is difficult to remember the exact clickable area. PCCP approach proved that remembrance of the graphical password methods is much better than the text based passwords.

4. BIOMETRIC AUTHENTICATION USING FINGER NAIL PLATE

Recently, [1] [9] there are various hand based biometric systems that received considerable attention as they have some various unique features that are highly distinct, unique and informative. In this paper we investigate the true capabilities and performance that can be achieved from finger nail plate surface as a distinctive and unique attribute for personal authentication. In nail plate surface authentication technology the ridge pattern which is present on the nail is very highly unique in case of individual and also in case of twins and also even in different fingers of hand. There has not been any attempt to utilizing texture and appearance based feature of nail plate for personal authentication so it is a new and challenging characteristic of nail plate from hand and is emerging as a promising component of biometric study. This system based on the outer surface of the finger nail. The nail plate is a new and promising biometric device for forensic and civilian and military applications. In this system [9] we propose biometric authentication based on low resolution (1600×1200) finger nail plate images. The cross section of the nail unit consist of nail-plate, nail matrix and the nail-bed that are tightly fused keratinized layers (see Figure 2 (a)). The nail bed consist of two types of tissue such as dermis and epidermis layers which is closest to nail plate surface and this layers are referred to as arched and valley portion of the nail (see Figure 2 (b)) and it forms a unique structure and closely parallel and irregularly spaced. This grooved spatial arrangement of the nail bed is observed on the upper i.e. convex nail plate surface as longitudinal ridges/striations [1].

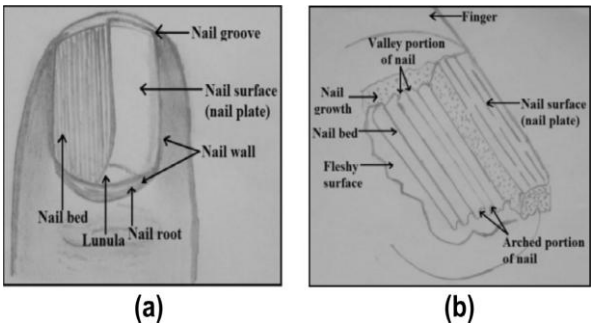

Fig 2: Finger nail surface in (a), magnification of the nail bed structure in (b)

These longitudinal striations which are presented on the nail plate surface are highly unique for every individual and serves as a means of personal authentication. Thus, the individuality in the uniqueness of nail plate surface based biometrics is completely dependent on the intrinsic anatomic characteristics of the nail organ [10].

The block diagram shows (see Figure 3) the main components of biometric authentication using nail plate surface.

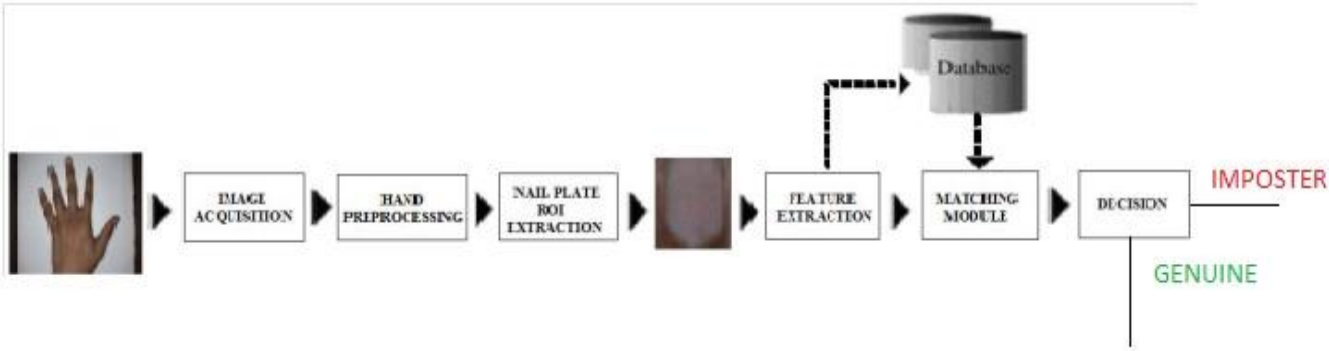

Fig 3: Block diagram of personal identification using nail plate surface

In this step the dorsal part of the hand image acquired from A630 Digital canon camera. The low resolution images acquired using user-friendly, unconstrained and peg free imaging setup [1]. User has the freedom of placing the hand in any orientation. Thus, the acquired hand images present a lot of translational and rotational variations. To extract the exact Region of interest (ROI) of nail plate the pre-processing steps is needed to acquire dorsal hand image. Firstly the each acquired dorsal hand image is subjected to binarization using a fixed threshold value and remove some noise is still present in image which subjected to morphological corrections which fills hole inside the foreground and remove the background debris and resulting the binary mask which is further used for finger localization and alignment. Then to locate the key points in the hand i.e. tips and valley point for eliminate the some rotation and translation variation. Then global hand registration techniques used for normalize the hand and re orientation of the fingers and further used to extract the accurate Region of interest. Then further decompose the finger by drawing the binary line of zeros between two adjacent valley points. Further, the nail plate surface segmentation approach presented to accurately segment the ROI with the grown nail plate or presence of nail polish on the female nail plate surfaces. This approach works at pixel level, and classifying the each pixel into nail plate or non-nail plate region and then Gabor filtering technique is used to extract completely automated and accurate extraction of nail plate ROI .And then matching the extracted feature with database by using score level rules for fusion of matching scores. After matching the decision will be carried out i.e. imposter or genuine [1] [9] [10].

5. EXPECTED RESULTS

In this system first user will enter the username and select 3 images to create password after creating password user will get the message from the system i.e. successfully registered. After the registration user provides the username and verify. If the username is correct then first image will display and it continues till the last image. This process is done in graphical password authentication. After graphical password authentication the verification and identification of the person is done by using finger nail plate. In finger nail plate biometric authentication, the database consists of 2250 nail plate images of 150 users including both male and female. To capture 5 images per user of his/her left hand thus, the database consist of 150×5×3=2250 images of middle, index and ring fingers. For experimentation 3 samples are randomly select for training purpose and 2 samples for testing purpose. Then this training and testing samples are used for generating matching score and performance evaluation. When the test image is matched with the image which belonging to the set of training image of the same user then result will generate genuine otherwise result will generate imposter.

We are expecting the results of biometric authentication using finger nail plate as per [1] shown in figure 4.

All the genuine and the imposter scores are subjected to a threshold for computing the error rates. The ratio of the number of imposters accepted as genuine to the total number of imposters is termed as FAR while the number of rejected genuine users as imposters to the number of all genuine users is termed as FRR. The database performance is evaluated in terms of the error rates. For a biometric authentication, FAR is specified and the corresponding GAR = 100-FRR is computed. We incorporated nail surface of middle, index and ring fingers from hand. The wavelet features are extracted of each of these finger nail plate surface. The genuine and imposter distribution for middle, index and ring finger as shown in Figure 4.

The experiment reports of the performance of wavelet features from individual index, middle, and ring fingers nail-plates.

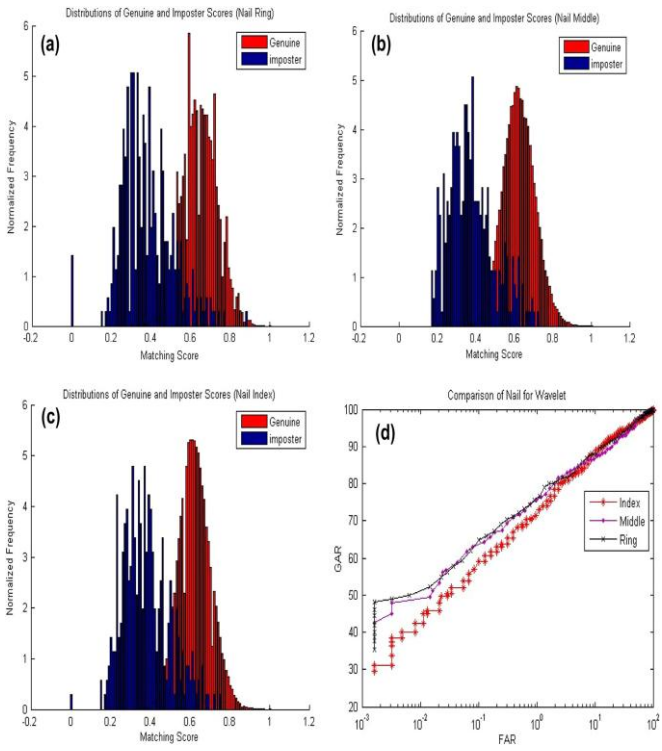

Fig 4: impostor and genuine distribution for nail (a) ring, (b) middle and (c) index (d) their combined ROC.

In this experiment we are extracting wavelet features from ring, middle, and index finger nail-plates. The distribution of genuine and imposter matching scores from these three fingers are shown in Fig. 4(a), Fig. 4(b), and Fig. 4(c). Receiver Operating Characteristics (ROC) curve, this ROC is a plot of GAR vs. FAR for these finger nail-plates corresponding to wavelet feature is shown in Fig. 4(d). It can be observed from Fig. 4(d) that ring nail-plate provides the best performance among the middle and index nail plate surfaces with GAR = 50%, GAR = 40%, and GAR = 32% respectively at the same FAR = 0.001%. However, with increase in FAR = 1%, we find corresponding increase in GAR = 76%, GAR = 75%, and = 72% for ring, middle, and index nail-plate surfaces, respectively.

6. CONCLUSION

There are various applications where they required high security for this purpose this paper combines the biometric and the username, graphical password based authentication methods to reach a higher security level than each of the both methods can provide alone. This presents a high security level to the system by providing the Persuasive Cued Click-Points technology which encourages users to select less predictable, and makes it more difficult to select graphical passwords where all five click-points are hotspots and it is effective at reducing the formation of hotspots and avoiding known hotspots and also provide the biometric authentication using finger nail plate which provides a novel and fully automatic nail-plate identification framework. The ridge pattern on the finger nail plate surface has high stability over entire life and is highly unique. The nail surface structure is considered to be quite unique, even in the case of two identical twins and in different finger nails of an individual. In this we incorporated the three ring, middle and index finger nails from left hand. This highly secure authentication scheme increases the high security level. It is a very promising, encouraging and challenging method to implement the combination of two different type of authentication to reach high security level.The main challenges in biometric authentication using nail plate surface is its weakness involving nail polish on nail surface specially in case of female's nail and other skin attributes. The future work is to address these challenges by using more representative and efficient Independent Component Analysis (ICA) based shape features extraction method which can reduce the effect of nail polish.

7. REFERENCES

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

[2] S Chiasson,, E. Stobert, 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.

[3] Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.

[4] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[5] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online palmprint identification," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 25 (9), pp. 1041-1050, 2003.

[6] N. Ratha, and R. Bolle, Automatic Fingerprint Recognition Systems, Springer, 2004.

[7] A. Kumar and Ch. Ravikanth,"Personal authentication using finger knuckle surface," IEEE Trans. Info. Forensics & Security, vol. 4, no. 1,pp. 98-110, Mar. 2009.

[8] Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. "Face recognition by independent component analysis," Proc in IEEE Transactions on Neural Networks, 13(6), 2002

[9] Shruti Garg, Amioy Kumar, and M. Hanmandlu, "Finger Nail Plate: A New Biometric Identifier,"Proc in International Journal of Computer Information Systems and Industrial Management Applications. Volume 6 (2014) pp. ISSN 2150-7988, 126 – 138.

[10] Shruti Garg, Amioy Kumar, and M. Hanmandlu, "Biometric Authentication Using Finger nail surface,"Proc in IEEE 2012