A System for Providing Highly Secured Authentication

Kishori N. Ushir[1], **R. B. Joshi**[2]

[1]Computer Department of Engineering, MMCOE Pune, Savitribai Phule Pune University, Maharashtra, India
[2]Computer Department of Engineering, MMCOE Pune, Savitribai Phule Pune University, Maharashtra, India

Abstract: ***In today's environment the increased level of effective and high 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 inspire to user in selecting better password for high security. The proposed system presents an integrated evaluation of the graphical password authentication by using persuasive cued click points, including usability and security evaluations, and implementation considerations along with the biometric authentication using finger nail plate surface to provide high security in various application. It implements the graphical passwords system to increase the difficulty level of guessing it and enables to select more random password with system influence along with the biometric authentication which is very efficient and convenient method by acquiring low resolution images of nail plate surface which is the outermost part of the nail unit using peg free, unconstraint and contactless imaging setup. The contour and texture characteristics of nail plates from fingers which are highly unique in individuals and also in case of different fingers nail plate are represented by the appearance and texture based feature descriptors. This system is provide three high level of security by using user name with graphical password using persuasive cued click points along with biometric authentication using finger nail plate. The scope of the proposed system is for high level of security purpose where it is very important to keep tight security like forensic labs, military application, banking applications, civilian, etc. The objective of this system is to introduce the new system by combining two different authentications and also investigates new biometric modality which helps identification and verification of a person.***

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

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 token based authentication, biometric authentication and knowledge based authentication. But these entire authentications cannot provide high security alone where required high security like in military, banking, forensic lab etc. applications. Because in textual password generally users create most memorable passwords which are easy to guess for attackers and also difficult to remember and there is possibility to forget textual password that's why information can easily stolen by attacker. And in biometric authentication there are various limitation in existing biometric devices for example in fingerprints and palm prints people unconsciously leave their fingerprint and palm prints wherever they touch an object and thus increasing the possibilities of imposter and spoof attacks and impersonation and also face characteristics changes with the age of an individuals in face authentication. So that integration of two types of authentication system is needed to increase the high security level. So we provide the high security level by integrating the graphical password using persuasive cued click points along with biometric authentication based on nail plate surface to reach higher security level than each of the both methods can provide alone.

A. Motivation and Challenges

Graphical based password with Biometric authentication using finger nail plate surface motivates us to work on this because, There are various application which required system to provide high level of security for this purpose different types of authentication available to provide the security but out of them like textual password which can easily guessed by attacker and hard to remember and also in biometric authentication there are some limitation in palm, fingerprint and face, etc. So proposed system motivates us to increase the security level of fooling the access control system by using two different authentication methods in combination like graphical password using PCCP with biometric authentication using finger nail plate. It combines the two different authentication methods to reach a higher level of security than each of the both methods can provide alone. PCCP is an effective method with system influence which reduce the hotspots and pattern formation attack which enables to user in selecting more random and difficult to guess click point on image. In addition this system 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/striations pattern which is present on the outer part of the nail plate surface is highly unique and also stability. And the structure or shape of nail plate surface is highly unique of the individual and also in case of different finger nails of the hand and also in twins. 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 appearance and texture based information and features 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. The main challenge is that to extract the nail plate features with presence of nail polishes over a finger nail plate surface in case of female.

2. Literature Survey

In Biometric authentication there are various biometric modalities in the literature such as retina, face, Iris, finger-print/palm print, etc. but in hand based biometric scheme like in finger print [6] and palm print [5] 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 so gaining popularity and in face recognition the face features changes with the age of an individual and also the face characteristics are same in identical twins. And also in Graphical based password authentication Pass Point, Cued Click Points techniques are in literature. In Pass-Point [3] graphical password 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 drawback of this method is pattern formation in this password can easily guess by attackers because user forms certain pattern to remember the secret code so that pattern formation attacks are easily possible and HOTSPOTS. In Cued Click Point [4] in that CCP scheme uses one click-point on five different images in sequence instead of five click points on one image. The next image displayed based on the location of previously entered the click point on the image. Drawback 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 formation attack but HOTSPOT problem is still present.

3. Proposed System

The proposed system integrate graphical password with Persuasive cued click point along with Biometric authentication using finger nail plate surface. This system provides highly secure authentication in three level i.e. username then graphical password and third level is biometric authentication. This system provides three level i.e. high level security. In biometric authentication we extract the nail surface features from the middle finger because middle finger gives best results

3.1 Persuasive Cued Click Points

Persuasive Cued Click Points [2] adding CCP features into it to create the graphical password. In previous pass point and CCP password system attackers can easily guess or stolen the password and also most of user set the click points on the hotspots in each selected image without the system guidance. The system influence in PCCP method is that system randomly shows the viewport to the user to select more random clicks points to set a more random password and difficult to guess, and also it maintains the users memorability. For password generation this method uses two requisites like viewport and shuffle. In this method during registration time only the view port i.e. randomly selected block of the image 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. To create graphical password system is randomly selecting the view port of the image for each image. (In fig 1). The users can select click point anywhere in the view port of the image and also they can change the position of viewport by using Shuffle and 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 shuffle button and viewport appear. Without shading or the view port, images are displayed normally during login process, and the users can click anywhere on the images. User can choose any area within the highlighted viewport and unless they press the shuffle button they cannot click outside the viewport. PCCP method reduced the HOTSPOT problem pattern formation attack, 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.

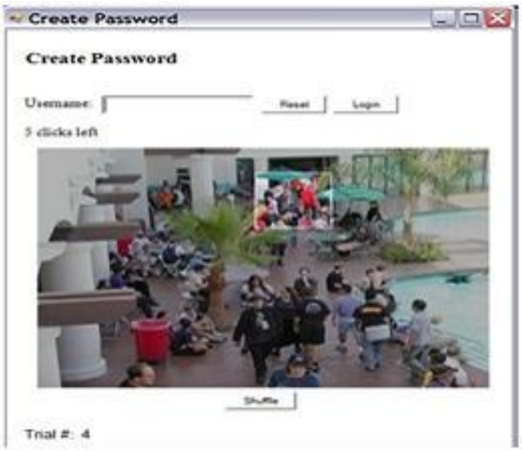


Figure 1: PCCP creates Password. The viewport highlights part of the image

3.2 Biometric Authentication using Finger Nail plate

Recently, there are various hand based biometric systems has received considerable attention as they have various unique anatomical features that are highly unique, distinct and informative. In this paper we investigate the performance and true capabilities that can be achieved from finger nail plates as a distinctive attribute for personal authentication. In the nail plate surface authentication technology the ridge/striations is very unique which is present on the outer part of the nail and also distinct in case of individual and in case of twins and also even in different fingers of hand. There has not been any attempt to utilizing texture and appearance i.e. local shape based feature of nail plate for personal authentication so it is a new and challenging and promising 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 plate. The nail plate is a new and promising biometric modality for civilian and forensic applications. In this system we propose nail plate biometric authentication based on low resolution images. The cross section of the nail unit as in Fig. 2(a) [1] is made of 3 tightly fused keratinized layers that are nail-plate, nail matrix and the nail-bed. The tongue-in-groove arrangement of the dermis and epidermis Layers of the nail bed are referred to as arched and valley portion in Fig. 1(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. These longitudinal striations imitated 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 based biometrics is completely dependent on the intrinsic anatomic characteristics of the nail organ.

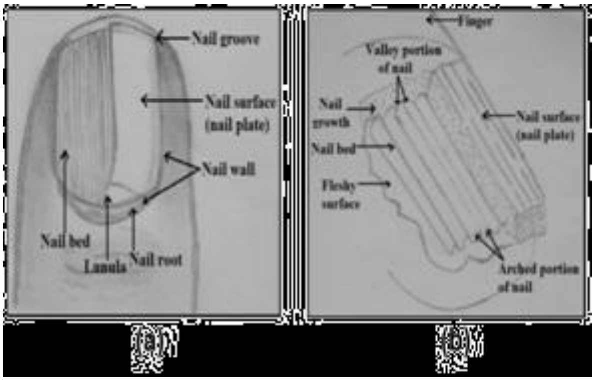


Figure 2: Finger nail surface in (a), Magnification of the nail bed structure in (b)

3.2.1 System Architecture of Authentication using nail plate surface

The system architecture shows the main component of biometric authentication using nail plate surface (in Fig 3). First step is a to acquired the low resolution of dorsal part of the hand images from A630 Digital canon camera by using peg free, user friendly, contactless and unconstrained imaging setup[1].

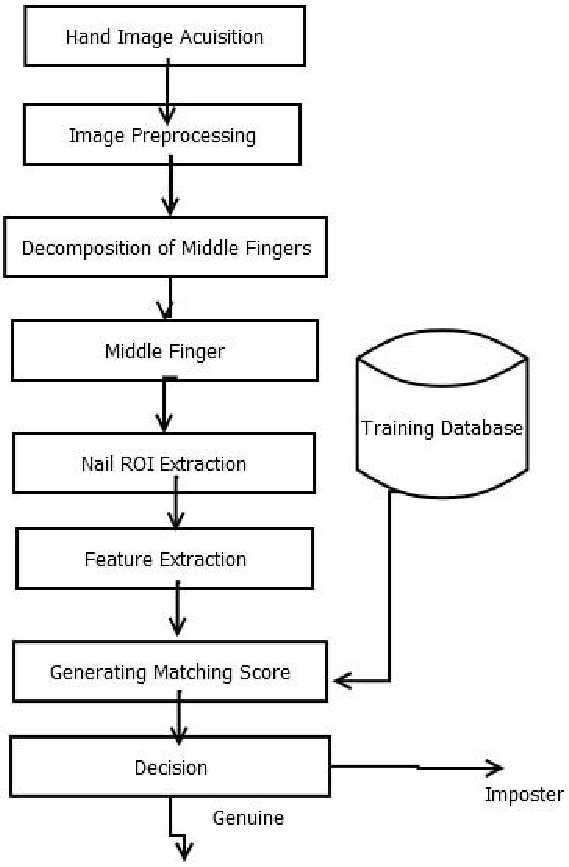


Figure 3: System architecture of authentication using nail plate surface

With this setup user can place the hand in any orientation. Thus, the acquired hand images present a lot of inter and intra class variation i.e. Rotational and translational variations. Hand normalization pre-processing steps are needed to remove the noise and some kind of variation and to extract the exact Region of interest (ROI) of nail plate and to acquire dorsal hand image. Firstly the each acquired dorsal hand image is first subjected to binarization using a fixed threshold value and remove some noise which is still present in image due to variation and then binarized image further subjected to morphological corrections which remove the background debris and fills hole inside the background and resulting the binary mask which is further used for finger alignment and localization. Then to locate hand extremities i.e. tips and valley point in the hand for eliminate the some rotation and translation variation. Once the key points of the hand are located then further these point used to extract the accurate Region of interest. Then further segment or decompose the middle finger from hand by drawing the binary line of zeros between two adjacent valley points. Then 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 based on intensity value of the pixel and classifying the each pixel into nail plate or non-nail plate region and then Gabor filtering technique used to remove the grown nail plate and some skin portion present on finger and extract completely automated and accurate extraction of nail plate ROI .And then texture and appearance based Independent Component Analysis (ICA) techniques used to extract the texture and shape based features and then used to matching the extracted feature with database by using score level rules for fusion of matching scores. After matching imposter or genuine decision will be carried out.

4. Mathematical Model

Mathematical Model of biometric authentication using finger nail plate.

Localization of hand extremities:

```
for(y=0;y<image.getheight();y++)
for(x=0;x<image.getwidth;x++)
int rgb = image.rgb(x,y)
int r = (rgb>>16) and 0xFF;
int g = (rgb>>8)and 0xFF;
int b =(rgb and 0xFF);
int grey =(r+g+b)/3;
if(grey>250)
while(count == 0)
tipy = y;
 tipx = x;
count++;
break;
print tipxX=tipx and
 tipY=tipy
```

Finger Decomposition:

Angle of slope of finger midpoint of finger (X1, Y1)
Tip of it = (X2, Y2)

Nail surface segmentation using Gabor function:
σ= standard deviation of the Gaussian envelope
u=Frequency of the sinusoidal wave
θ=control the orientation of the function.

$$g(x,y,\theta,u,\sigma)=\frac{1}{2\pi\sigma^2}exp\left\{\frac{x^2+y^2}{2\sigma^2}\right\}\times exp\{2\pi(uxcos\theta+uysin\theta)\}$$

Nail surface ROI Extraction:

For ROI Extraction use rectangle of size 80*80;
Height of Rectangle = 80;
Width of Rectangle = 80;
X point of Rectangle = tipx - 40;
Y point of Rectangle = tipy;
ROI has been cropped of size 80 * 80;

Feature Extraction:
Independent component analysis

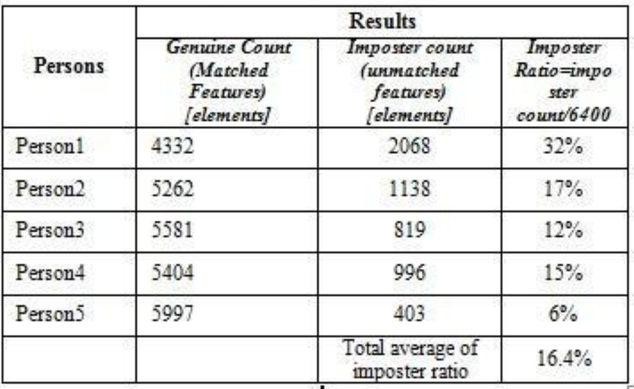
$$D=\sqrt{(r1-r2)^2+(g1-g2)^2+(b1-b2)^2}$$

```
THR=10
if (dist > THR)
resultImage.setRGB(w, h, im2.getRGB(w, h));
imposters++;
else
resultImage.setRGB(w, h, 0);
```

5. Experimental Results

In this system first user will enter the username and select click point on 5 different images sequentially to create graphical 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. If graphical password is correct then the identification and verification of the person is done by using finger nail plate biometric authentication. In finger nail plate biometric authentication, to capture 5 images per user of his/her hand thus, the database consist of images of middle 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. 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 have taken the two different nail plate images of the person to calculate the difference between the images by identifying the matching features and unmatched features. The Matching features are counted and named as genuine elements. The Unmatched features are counted and named as Imposters elements. Total number of elements in image matrix = 6400 elements (As image size is 80* 80 pixels).

5.1 Result 1

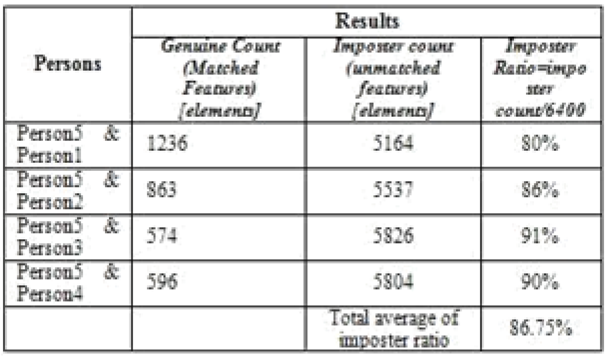


Persons	Results		
	Genuine Count (Matched Features) [elements]	*Imposter count (unmatched features) [elements]*	*Imposter Ratio=imposter count/6400*
Person1	4332	2068	32%
Person2	5262	1138	17%
Person3	5581	819	12%
Person4	5404	996	15%
Person5	5997	403	6%
		Total average of imposter ratio	16.4%

Figure 4: Result for comparing different nail plate images of same finger of same person

Above diagram (In fig 4) shows the results of different nail plate images of same finger of same person which gives the imposter ratio 16.4 percent and genuine ratio is 100-16.4=83.6%.

5.2 Result2



Persons	Results		
	Genuine Count (Matched Features) [elements]	*Imposter count (unmatched features) [elements]*	*Imposter Ratio=imposter count/6400*
Person5 & Person1	1236	5164	80%
Person5 & Person2	863	5537	86%
Person5 & Person3	574	5826	91%
Person5 & Person4	596	5804	90%
		Total average of imposter ratio	86.75%

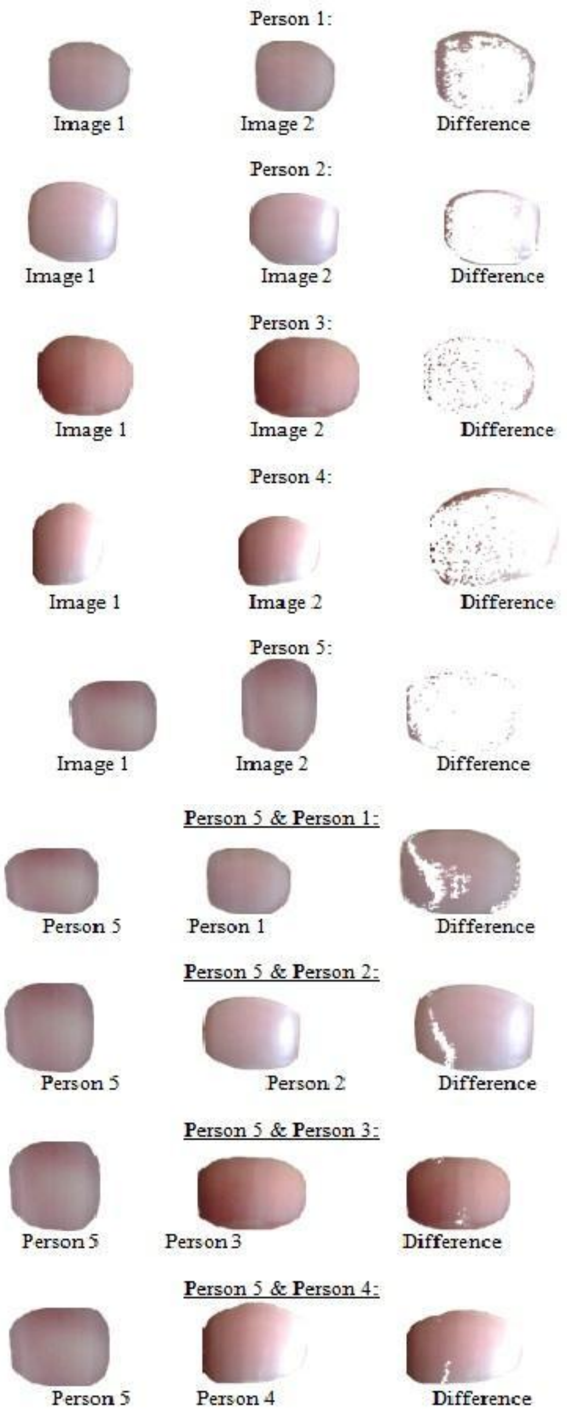


Figure 5: Result for comparing different nail plate images of same finger of different person

Above Diagram (in fig 5) shows the results of different nail plate images of same finger of different person which gives the imposter ratio 86.75 percent and genuine ratio is 100-86.75=13.25 percent.

6. Conclusion

There are various applications where they required high level of security for this purpose this paper integrate the username, graphical password and biometric authentication methods to reach 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, more random password 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 and promising and challenging nail-plate identification framework. The ridge pattern on the finger nail plate surface has high stability over entire life and is highly unique and stable. The nail surface structure is considered to be quite unique, even in the case of identical twins and in different finger nails of an individual. In this we incorporated the middle finger nails from hand. This highly secure authentication scheme increases the high security level.

References

[1] Amioy Kumar, Shruti Garg, M. Hanmandlu, “Biometric authentication using finger nail plates, Proc in Expert Systems with Applications, Elsevier, 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, “Pass-Points: Design and Longitudinal Evaluation of a Graphical Password System, Intl 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 and Security, vol. 4, no. 1,pp. 98-110, Mar. 2009.

[8] Bartlett, M. S., Movellan, J. R., and 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. ISSN 2150-7988 Volume 6 (2014) pp. 126 138

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