A FACE RECOGNITION AND GRAPHICAL PASSWORD BASED HYBRID TECHNIQUE OF INFORMATION SECURITY

A. Wajid, T. Ahmad and M. Rafique

Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan
Corresponding author's E-mail: amna-wajid@hotmail.co.uk

ABSTRACT: The information and computer security is mainly dependent on the use of conventional textual passwords nowadays. But due to the difficulty of remembering random and long passwords, users create simple and short passwords which do not provide enough security and are vulnerable to attacks. Graphical passwords have been designed to make passwords more secure, memorable, easier to create and usable. The current graphical password based techniques do not provide security, memorization and usability features all at the same time. In this paper, we propose and evaluate a hybrid technique of security, based on face recognition and graphical password. The technique has been evaluated by comparing it with the existing techniques and it has also been evaluated by a survey. The results indicated that the proposed system is more secure, usable, efficient and reliable than the existing techniques.

Keywords: Biometric Security, Graphical Passwords, Principal Component Analysis, Local Binary Pattern Histogram

(Received 08/02/2016 Accepted 28-08-2018)

INTRODUCTION

Authentication of user is one of the most important aspects in information security paradigm. Information and computer security have much dependence on passwords in order to authenticate the users and are commonly used in practice (Khandelwal *et al.*, 2010). Passwords play a significant role in various computing applications in daily life like authentication in mobiles, ATM machines, windows login, internet services etc. The main objective of using passwords is to control the unauthorized access to the system (Raza*et et al.*, 2012). The different types of methods used for security include text based password schemes, biometric based security schemes, token based security schemes etc. The most commonly used are the conventional text based passwords. But the text based passwords suffers from security and usability features.

The security provided by text based passwords is not enough for various applications. People use passwords during a login process that controls access to computer operating systems, automated teller machines (ATMs), mobile phones, etc.The degree of security provided by textual passwords can be increased to a certain level by using strong passwords. But due to the fact of difficulty in memorizing strong passwords, the password holders usually write them on a piece of paper or write them in a computer file and save it. Furthermore, text based passwords can be hacked by different methods such as dictionary attack, brute force method, phishing etc. So, usability and security provided by text based passwords is very low (Saharkar and Dhopte, 2014).

Biometric based security techniques involve recognition of people based upon their psychological behaviours or physical characteristics. It consists of fingerprints, hand or palm geometry, iris, facial, signature or voice recognition. Biometric based techniques are much secure than the text based passwords as it is not possible for anyone to steal these. But these techniques cannot be used widely and it is also possible to deceive the biometric device (Kar *et al.*, 2006). For example, In voice recognition, voice of a person can easily be recorded and used for unauthorized access, facial recognition can be affected by changes in lighting, the person's hair, the age, and if the person wear glasses. Similarly other biometric techniques also have limitations.

Graphical passwords based authentication techniques have been proposed as an alternative of the text based passwords. The idea of Graphical passwords was originally presented by Blonder (Sathish *et al.*, 2013). Graphical passwords have been divided into two categories which are recognition based techniques and recall based techniques. In recognition based techniques, a set of images are presented to the user and user chooses images from the given images to register him. For authentication during login process, user selects the same images in the same order as were selected by him during registration for successful authentication. In recall based techniques, a user registers him by creating a drawing on a grid. For login user is asked to reproduce the same drawing in the same coordinates of grid as was produced during registration process. The motivation behind this scheme is the fact that images can easily be remembered as compared to the text strings (Saharkar and Dhopte,

2014). But like all the other security techniques, this technique also has security threats like shoulder surfing, dictionary attack, social engineering etc.

A hybrid user authentication technique was introduced by Walanjkar et *al.* (2014). This technique is based on two parts, one is facial recognition and the other is random question's answer using mobile device. The questions are chosen by user during registration and two random questions are sent to user's mobile before login. User has to send right answers in order to get login (Walanjkar *et al.*, 2014).

One new addition to the biometric based security techniques is keystroke dynamics authentication technology. This technique is based on password typing pattern of user. This technique does not require extra hardware. Only software based technology is used for password security. Keystroke dynamics has two phases of authentication for a successful login, firstly password should be known and secondly, typing rhythm should match. This field is an emerging field. In order to become an effective biometric technique, most of the challenges are needed to overcome. The major challenge in this field is the lack of standard protocol for keystrokes pattern evaluation (Patil and Renke, 2016).

By studying and understanding different graphical password based security techniques, we have found that the existing techniques suffer from some major issues which include security threats, usability, reliability and storage space requirement. The current techniques do not provide the mentioned features all at the same time. These methods lack either security, usability, reliability or require too much storage space (Saharkar and Dhopte, 2014, Kar *et al.*, 2006).

Based on the study, we propose a user authentication technique which is hybrid of both biometric and graphical based schemes. The proposed scheme aims to ensure more security and provide protection against shoulder surfing, spyware, brute force and social engineering attacks. Our proposed scheme will be reliable and efficient as it is a combination of two different security techniques. The presented technique will also be usable for the systems requiring improved security. The technique is based on face recognition and graphical passwords. The face recognition has been chosen as it is not very costly because camera is built in most of the systems and it does not require installation of costly hardware.

MATERIALS AND METHODS

The proposed technique is recognition based technique. It is more secure as it used hybrid of biometric and graphical methods. It is easier to use, memorize and learn, and is more reliable and efficient.

Security Feature: In the proposed system, security feature was achieved by firstly using the face recognition. After authentication by face recognition the user was directed to the second phase of system. In second phase the graphical password of the user was registered in the form of images. For registration, the user selected four images from nine images shown to him. To avoid shoulder surfing attack, all nine images were shown to user in random order and a random code was assigned to each image during the login. The user was directed to enter the code associated with those four images which were part of his password. Each time login screen displayed images in random order with random codes. Therefore, it made it difficult for a shoulder surfer or spyware program to get user's password.

Reliability Feature: It is difficult to forge face recognition device and without face recognition, user couldn't enter in second phase of system. Furthermore, the user did not need to memorize the lengthy strings to get login, but only the images.

Usability Feature: This system was easy for users to learn because pictures are easier to remember. Due to the user friendly layout of system, the creation of password using this system was easy.

Efficiency: The system used less memory to store the password. During registration, user selected his graphical password by selecting the images. After that the system assigned a unique secret code to each image and that secret code was stored in database as a password for user, instead of images.

During login, images on login screen were created at run time from the picture of user and a random code was assigned to each image. The user needed to enter that random code associated with those pictures which were parts of his password. This random code was generated for protection from shoulder surfing and spyware programs.

Design of the Proposed System: There were two main modules of the system which are face recognition and generation of graphical password. Module 1 comprised of two parts. One was face detection and the other was face recognition.

Face Detection from Input Image: When an input image was collected by the system then the first task was to extract the face from the input image. For face detection, Viola Jones face detection algorithm (Viola and Jones, 2004) had been used.

Once the face was detected, the next task was to recognize the face. For face recognition, the Principle Component Analysis (PCA) Eigen faces method (Slavković and Jevtić, 2012) and Local Binary Pattern Histogram (LBPH) (Rahim *et et al.*, 2013) methods were used. Figure 1 and Figure 2 are showing the recognition

process of an unknown face by PCA method and LBPH method respectively.

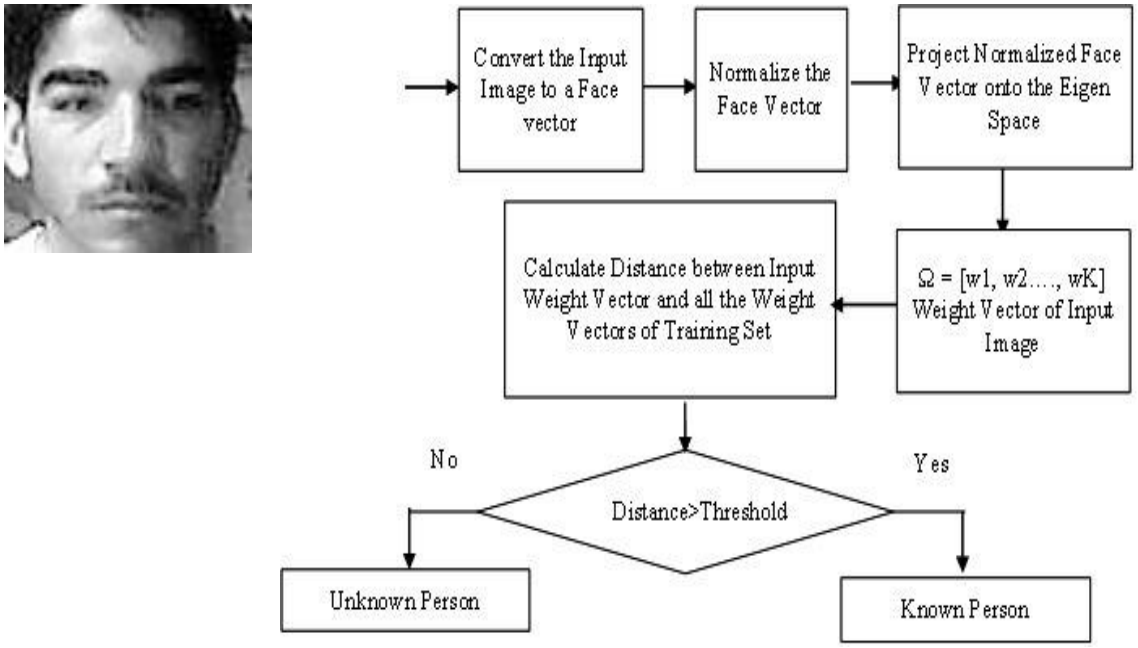

Fig-1. Recognizing an Unknown Face using PCA Eigen Faces Method

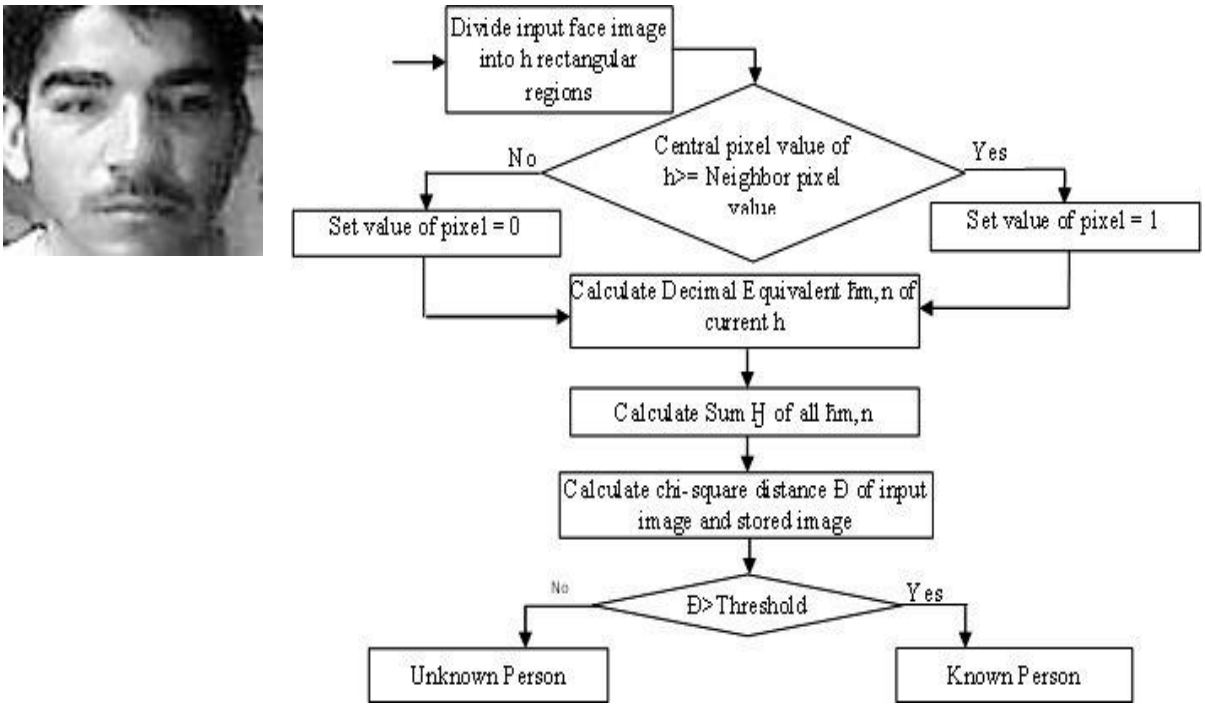

Fig-2. Recognizing an Unknown Face using LBPH Method

Design of Face Recognition System: Face recognition system had two modules which are face recognizer and training set manager. When an input image was fed into the system then firstly face was detected and extracted from image. In order to add new faces into the database and to modify existing images training set manager was used. For recognition of the faces, face recognition module was used. Figure 3 shows the design of face recognition system.

Module 2 had two parts. One is registration and the other is login.

Registration: In this module, first step was to register the image of a user. This was done by the admin. After registration of image, user could register password later at any time.

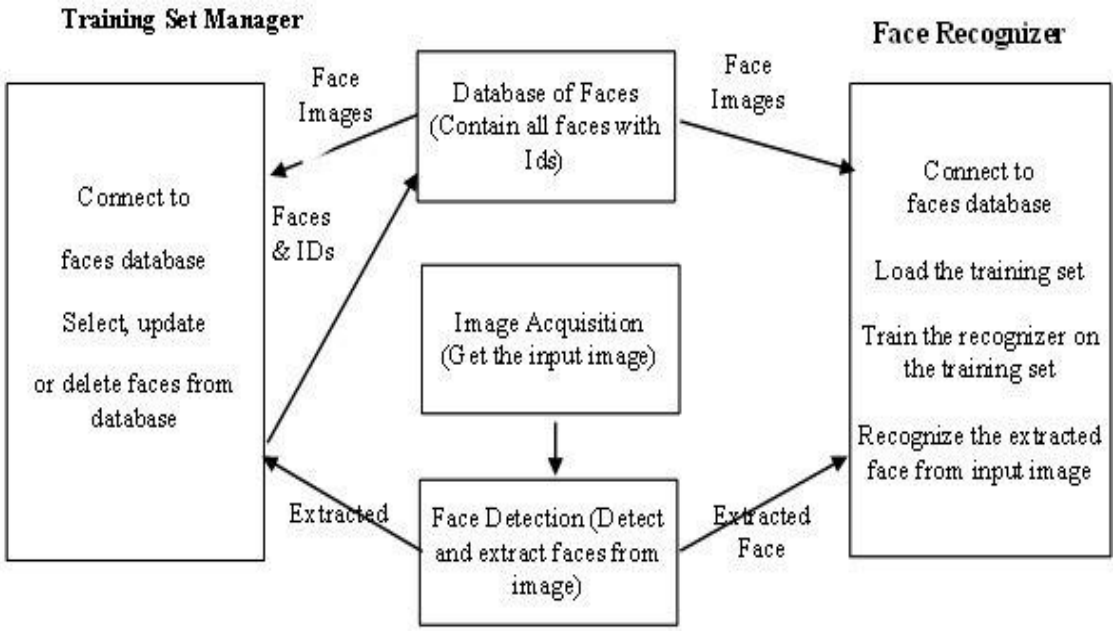

Fig-3. Design of Face Recognition System

For registration of password, firstly the image of user was taken and if user was recognized as a registered user then he was directed to register his password. For registration of password, the face image of the user was split into nine parts which are denoted by **(I_0, I_1, I_2, I_3, I_4, I_5, I_6, I_7, I_8)** and a unique code ρ_j is assigned to each part of image. The j^{th} secret code is denoted by ρ_j and is formed as follows;

$$\rho_j = \# \,||\, I_i \,||\$ \qquad (1)$$

where I_i is the i^{th} image selected by user and || is concatenation operator. The user was asked to select any four image parts as his password. Instead of saving images into the database, the secret code associated with each image was stored in database to save memory. The secret code to save into database was generated by combining all four secret codes associated with each image selected by user as follows;

$$\rho = \sum_{k=0}^{n} \rho^k \qquad (2)$$

After this step registration process got complete. Figure 4 shows the graphical user interface of registration of password.

Login: Login phase had two steps. First step was the authentication of user by taking image of user and recognizing it. After recognition, the user was directed to step two, in which user entered the password. At login screen, user was shown the split parts of his face image in random order. The new positions of images are calculated as follows;

$$I'_j = \text{rand}\,(I_{max}) \qquad (3)$$

where I'_j is the new position of j^{th} image and I_{max} is the max no. of images that are generated after splitting the original image I. After calculating new position of image $\mathbf{I'_j}$, the current position of image $\mathbf{I_j}$is replaced with new position $\mathbf{I'_j}(I'_j \leftrightarrow I_j)$.

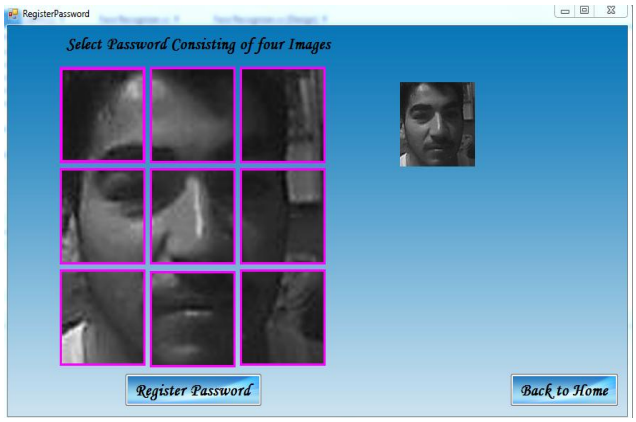

Fig-4. Registration of Password

A random code was associated with each image part. Therefore, instead of selecting the images which were part of password, the user was asked to enter the random code associated with the images which were part of his password. The use of random codes made this technique shoulder surfing and spyware resistant. The random code was different for each login and was calculated at run time for each login. The code is calculated as follows;

$$\partial = N \bmod M \quad (4)$$

Where **N** is any number in the range of **{1, M-1}** and **M** is the range of numbers to be generated.

Once user entered the correct login codes associated with the password images, the user got access to system. Figure 5 shows the graphical user interface of login phase. The complete design of graphical password generation and login is shown in Figure 6.

Fig-5. Login Screen

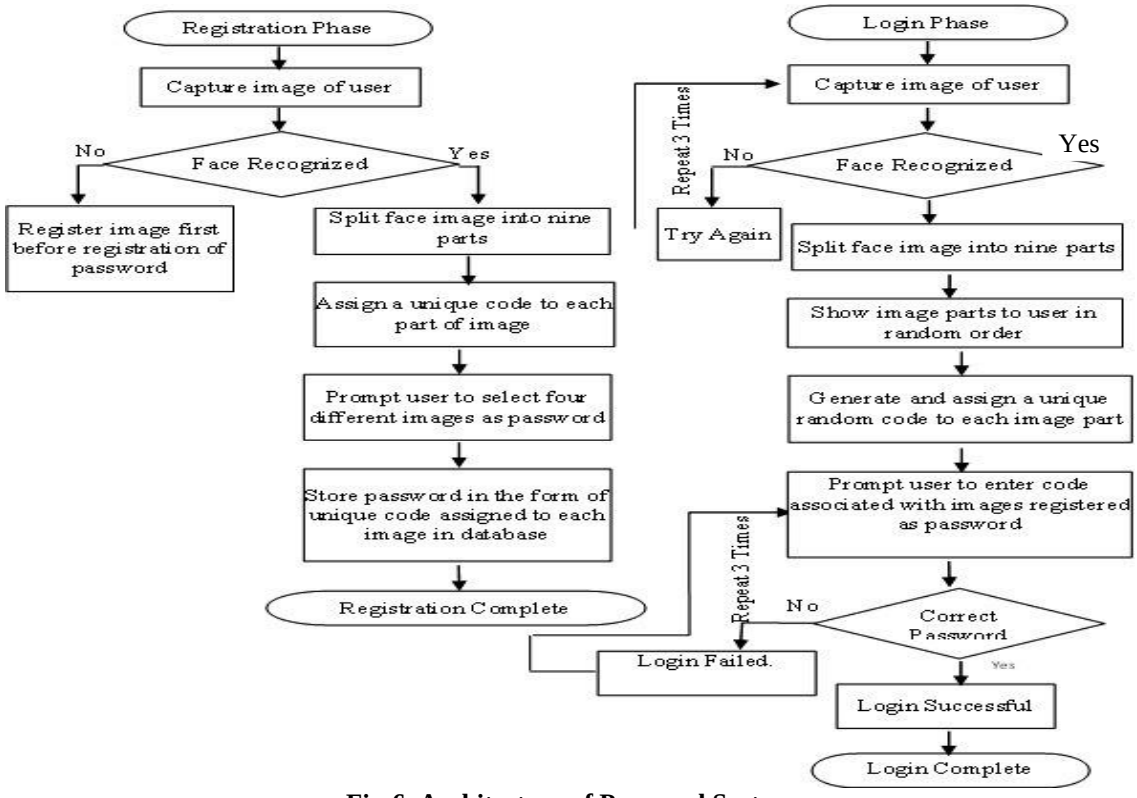

Fig-6. Architecture of Proposed System

Pseudo Code:

Input: Capture Image of user

Output: Password of user associated with registered images of user

Registration Phase Steps:

Step 1: Recognize input image and split it into nine small images and assign a random code to each small image.

Step2: Ask user to select any four images of his choice to be used as his password in future

Step3: Save password of user

Login Phase Steps:

Step 1: After recognition of user's face, split recognized face into nine small images and assign a random code to each image part.

Step 2: User will enter code associated with those images which were part of his password.

***Step 3:** Successful or unsuccessful login depending upon entered password.*

RESULTS AND DISCUSSION

The testing of system was done using 1000 images of 100 persons (10 images per person). For this work frontal faces were used. The images were taken at different face angels. All the images were captured under same lighting conditions. This work was dependent on lighting and it had greater effect on recognition rate. For Recognition purpose, a combination of both PCA and

LBPH algorithm has been uses. According to the results recognition rate of LBPH algorithm was better than the PCA algorithm.

The time take to recognize an unknown face was checked by varying the number of images which were stored in database. The results indicated that the response time of LBPH algorithm was better than the PCA algorithm.

A questionnaire was used to get the users' response. The questionnaire had six questions including the user interface design, ease of use, ease of creation of password, ease to memorize, response time and security provided by system. Table 1 shows the results of survey. The results of survey are graphically shown in Figure 7.

Table1. Results of Survey about System.

Survey Results		
Parameters	**YES**	**NO**
User Friendly GUI	100%	0%
Easier to Use	90%	10%
Easier to Create Password	100%	0%
Easy to Memorize Password	80%	20%
Good Response Time	50%	50%
Security	100%	0%

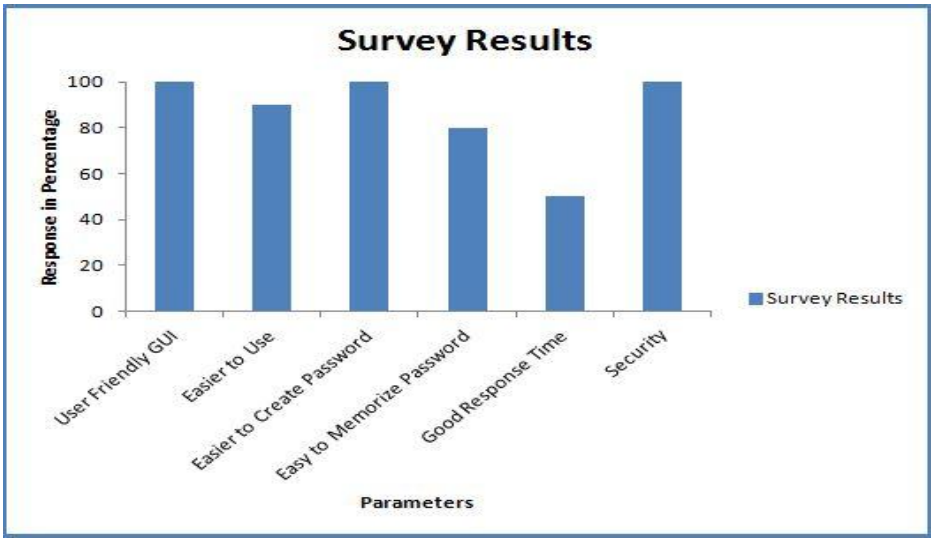

Fig-7: Response of User's about System

Table 2. Comparison of Proposed System with Existing Techniques

Graphical Password Techniques	Security Attacks				Usability				Efficiency	Reliability
	Shoulder Surfing	Spyware	Social Engineering	Brute Force	Easier to Create	Easier to Memorize	Easier to Use	Good Interface		
Déjà vu Technique (Dhamija *et al.*, 2000)	Yes	No	No	Yes	Yes	No	Yes	No	Yes	Average
Triangle Technique (Sobrado and Birget 2002)	No	No	No	Yes	Yes	Yes	Yes	No	No	Average
Hong Technique (Dawei *et al.*, 2004)	Yes	No	Yes	Yes	No	No	No	Yes	No	Poor
Count based Hybrid Technique (Ezhilarasan *et al.*, 2014)	No	No	No	No	No	No	Yes	Yes	Yes	Good
Jetafida Technique (Ali and Norafida, 2008)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Good
Proposed Technique	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Good

Comparison of Proposed System with Existing Techniques: We had compared the proposed technique with the existing graphical password based techniques. The parameters which were used for comparison are security attacks, usability features, efficiency and reliability. The results of the comparison are shown in Table 2 and the results indicated that the proposed technique was better than the other techniques in all the aspects.

REFERENCES

Dhamija, R. and Perrig, A. (2000). Deja Vu-A User Study: Using Images for Authentication. In USENIX Security Symposium, Denver, Colorado, USA, USENIX Association. Pp: 4-4

Eljetlawi, A. M. and Ithnin, N. (2008). Graphical password: Prototype usability survey. In Int. Conf. on Adv. Comp. Th. Engg. IEEE. Pp: 351-355.

Ezhilarasan, M., Dhanabharathi, D., Vasanthakumar, P. and Ayyanar, B. (2014). Count based hybrid graphical password to prevent brute force attack and shoulder surfing attack. Int. J. Res. in Engg. Tech. 3(7): 405-411.

Hong, D., Man, S., Hawes, B., and Matthews, M. M. (2004). A Graphical Password Scheme Strongly Resistant to Spyware. In Proceedings of Int. Conf. on Sec. and Manag. Las Vegas, United States. Pp: 94-100.

Kar, S., Hiremath, S., Joshi, D. G., Chadda, V. K. and Bajpai, A. (2006). A multi-algorithmic face recognition system. In Int. Conf. on Adv. Comp. and Comm. IEEE. Pp: 321-326.

Khandelwal, A., Singh, S. and Satnalika, N. (2010). User authentication by secured graphical password implementation. Int. J. Comp. Appl. 25(1): 100-104.

Patil, R. A. and Renke, A. L. (2016). Keystroke dynamics for user authentication and identification by using typing rhythm. Int. J. Comp. Appl. 144(9): 27-33.

Rahim, M. A., Azam, M. S., Hossain, N. and Islam, M. R. (2013). Face recognition using local binary patterns (LBP). Global J. Comp. Sci. Tech. 13(4): 1-8.

Raza, M., Iqbal, M., Sharif, M. and Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World Appl. Sci. J. 19(4): 439-444.

Saharkar, C. S. and Dhopte, S. V. (2015). Authentication for the System by using Graphical Region and Alphanumeric Password. Int. J. Rec. Innov. Trends in Comp. Comm.. 3(5): 2513-2516.

Sathish, S., Joshi, A. B. and Shidaganti, G. I. (2013). User Authentication Methods and Techniques by Graphical Password: A Survey. Int. J. Comput. Eng. Inf. Technol. 2(3): 1-4.

Slavković, M. and Jevtić, D. (2012). Face recognition using eigenface approach. Serb. J. Electr. Eng. 9(1): 121-130.

Sobrado, L. and Birget, J. C. (2002). Graphical passwords. The Rutgers Scholar, an electronic Bulletin for undergraduate research, 4: 12-18.

Viola, P. and Jones, M. J. (2004). Robust real-time face detection. Int. J. Comp. Vis. 57(2): 137-154.

Walanjkar, D.D. and Nandedkar, V. (2014). User Authentication Using Graphical Password Scheme: A More Secure Approach using mobile interface. Int. J. Innov. Res. Comp. Comm. Engg. 2(12): 7329-7335.