Enhancing Password Immunity Via Mixing Text With Biometric Information

Munthir B. Tuieb

Abstract— The password is a technique uses in authentication which is one of security fields. It provides method to allow authorized users for using a system services and denied the services for others . So it plays an important role in computing security. This paper proposes an approach to enhance password security. The approach minimizes imposing strong policies on the user. It enhances the security of entered text password via mixing it with facial information. It captures an image of user face via live camera and it doesn't deal with other ways that brings user image. Then it removes the noises of image and calculates a center point which serves for extracting binary features of image. This features mixes with text password via exclusive-or operation to enhance the immunity of password. The proposed approach minimizes required storage space and processing overhead, since it uses primitive operations and less amount of extracted information.

1 Introduction

Online roguery is attacking the user of Internet and itself (Internet), this ascending problem may stifle its activity. One of problem features is the criminals can utilize a vitiated account easily, there are explicit sings of fraudster's experience. Sign of them is congregation of schemes used by authors of malware and phishers. For example Trojans use victim target to enhance rates of conversion, relying on lessons utilized by artists of spear phishing. As well, an increasing aspect of malware employs some of deception form to propagate and install. [1]. The speedy growth of E-commerce applications and wireless networks is accompanied with increasing request to shield a privacy of user's credentials and provide diversity of services [2]. An authentication be a trusted part of communication system to protect important information contra malicious antagonist via providing the authentication as well as confidentiality [3]. The authentication via passwords and secrete keys are utilized in schemes of distant user authentication. The password is convenient and easy approach to authenticate the user to fund the computing services for the communications [4]. Password technique can be violated via dictionary attack easily. To solve this problem, passwords and secret keys are utilized in authentication of remote user [5]. Memorizing random and long keys is difficult, therefore they has to store someplace, this is very weak. Biometric based authentication is presented to overcome this problem[6].There are advantages for using biometric authentication compared to password or smartcard authentication technique such as losing resistance occurred via theft of smartcards and password. Also it friendly to the users, biometric technique identifies user identity and forging it is hard[7].

As a literature review for image enhancement and feature extraction [8] uses shock of GSZ filter in order to reduce the noises and enhance contour. They use Gabor filter for feature extraction of the hand. [9] made contrast correction via Gaussian filter to improve the intensity of high pass.[10] the work is based on multi-level of threshold. [11] the work is same as [9] to extract palm and hand vein. while the literature review of authentication [12] introduce graphical approach for authentication depends on visualization of hash technique. Their approach is based on choosing image number from collection of images which generated randomly via a program. Then the user either be authenticated or not based on the choice.

[13] introduce a technique similar to previous one, but it differs in hash function which is SHA. It requires less storage space, its output is 20 byte. They suggest improvement which could be work in PDA's, cell phones and Internet. [14] produce several approach for authentication such as object recognition, image recognition and recognize pseudo word. In image recognition a database contains 20000images is used in the approach and the user must train to recognize 100-200 images. A period (1-3) months are required to user to recognize over 90%.

[15] produce a scheme known as "Draw-a-secret (DAS)". This technique requires drawing any object on grid its size YXY during registration phase via the user. The coordinates must be stored in form of draw.

2 Proposed Method

A proposed method uses biometric authentication via face recognition by camera as live. In addition to text password which provides better security mixing with biometric data. Proposed method divides into three phases as follows:

1- **Registration phase**: it is first phase which requires user data to be entered for storing. It represents input phase, there are an instructions for requiring user information. The proposed method requires an image of user and text password in order to authenticate him. The proposed method depends on live image from camera. The occlusions and objects such as hats and glasses must remove in front of camera to increase the accuracy. The following

• *Munthir B. Tuieb is currently Ass. Lecturer in* ***College of Education-University of Al-Mustansiria, Baghdad****, Iraq, PH-09647704526737.*
E-mail: munthir87@yahoo.com

pseudo-code represents proposed method registration phase :
STEP1: Connect to camera via opening the socket.

STEP2: Configure the camera to take a picture.

STEP3: Take picture (depending on user request).

STEP4: Convert image type into JPEG.

STEP5: Use OpenCV IpIImage to store an image.

STEP6: Request a password from the user.

STEP7: Store the password in buffer (to be used later).

The proposed method requires text password and user image for the authentication process.

2- **Manipulating phase:** the image is passing through several levels in order to optimize authentication process. These levels are describing as following:

- Filtering Level: a digital image may has several noises which effect information extraction from the image. A spatial filters are used here for this purpose. The proposed approach uses mean filter in order to remove image noise. Mean filter makes the image softer, it operates via convolution mask. The result of convolution operation depends on sum of pixel neighbors, so it is a linear filter. It is averaging filter its operation take group if neighbors and calculating their average which is replaced with the center pixel. It is implemented in better way with conjoined noise and Gaussian. For pepper or salt noises the proposed approach uses contra-harmonic mean filter, it is implemented relaying on order of the filter. It is implemented as in the figure 1 which represents the flowchart of implementation the filter depending on noise type :

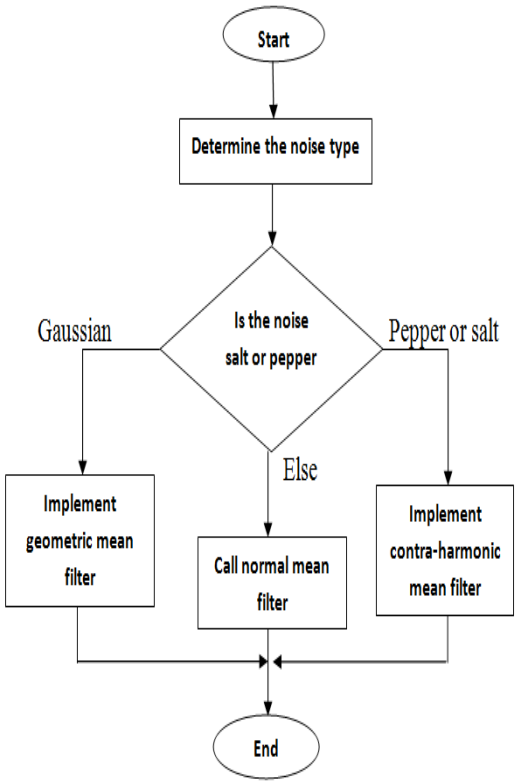

Figure 1 : Flowchart of implemented mean filter depending on noise

Contra-harmonic mean filter is implemented as same as normal mean filter with the difference of contra harmonic execution which is follow the following equation:

$$CHMF = \frac{\sum_{(i,j)\in sw} I(i,j)x-1}{\sum_{(i,j)\in sw} I(i,j)x}$$

CHMF character is abbreviation for Contra-Harmonic Mean Filter, SW is sliding window. The abovementioned equation is depending on x value if it is negative then the algorithm will remove salt noise, while positive value guides the algorithm to process the pepper noise.
Geometric mean filter (GMF) is used in the proposed approach in order to remove Gaussian noise and preserve image technicalities and its information. It differs from the previous filters by using product for values of pixel inside sliding window. The following equation is acted geometric mean filter:

$$GMF = \prod_{(i,j)\in sw} [I(i,j)]1/s*s$$

Where S*S (S2) is sliding window size.

- Calculating Center Point level: The proposed method concern with calculating a center point of the image face, by determine a rectangle which surround the face. The center point is represented via cross point of rectangle diagonals, it is calculated via coordinates as the following equations :

$$R = \frac{x1+x2}{2}, \qquad Z = \frac{y1+y2}{2}$$

The edge detection and center point determination is helped operations to focus the work on the face only. It occurs by obsolete the edge when detect it, also the center point is used to calculate face boundary. The proposed method calculates an angle on boundary as 2π/ no.of samples. The samples are predefined experimentally. These processes utilizes space storage amount because it extracts face information only, the background information are subtracted.

- Extracting Binary Features level: the image of the face is labeled via doing a threshold between the center value which is pre-calculated with 4*4 pixel neighbor. The result will be binary value, binary patterns is produced via multiplying weights of the pixel with threshold value. After that,256 labels histogram of binary pattern labels is calculated and serialized into unique histogram.
- Concatenating image patterns with password level : in order to give more security to image data which is extracted as binary patterns in above step. This patterns is concatenated with password, the password is entered via the user. The proposed method uses exclusive-or to implement the concatenation process. Since exclusive-or require binary modules, therefore the password text must be converted into binary. The proposed method uses ASCII code in order to represent the password as binary value. After that, exclusive-or operation implements between binary patterns of image and binary ASCII code of password. The result will store to be depended in checking phase.

3- **Checking phase:** this phase is activated when the user wants to login in the system. The user must enter the password and take a picture in suffixed camera. The proposed method can't go on when the picture of user or password misses. This phase is implemented as an algorithm which is shown in figure 2 acts flowchart of checking algorithm :

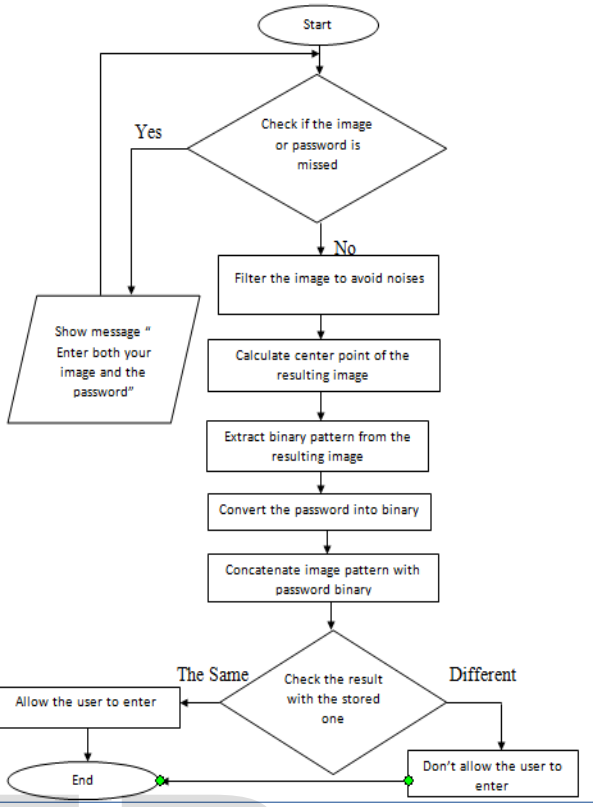

Figure 2 : Flowchart of Checking Algorithm

3 Results

One of the vulnerability which can be exploited via intruder to attack the password is unsupervised events. Malicious application or intruder can have the ability to override or modify unsupervised events within the device. The proposed method has an immunity against such situations as in following states:

1- The malicious application can make an image for intruder and sign in with it, this situation is overcome via proposed method. Because the proposed method deals with real-time image (it is captured in camera at the same time of sign in).
2- The information can be intercepted after processing and go to store them. Also the proposed method overcomes such problem, because the information will be encrypted by exclusive-or operation with the password. So intercepting the information needs decryption process in order to read and understand the target information.

In order to test the robustness of proposed approach security Kame and Tcpdump tools are used.

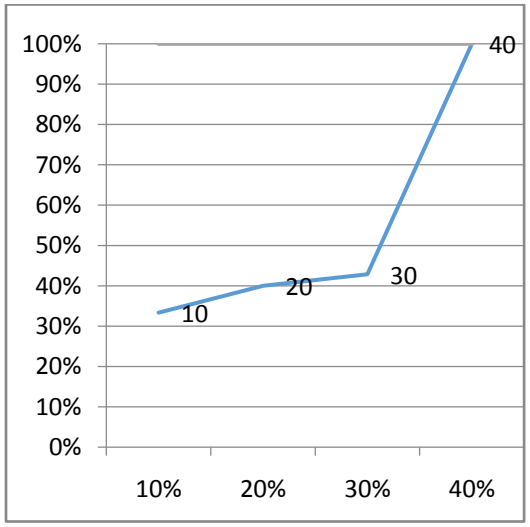

Figure 3 : Chart of the relation between normal password and adopted one

The row of chart represents the ratio of the normal password applications and developed approach. The column of chart represents the immunity of the technique. The range from 10 to 30 is acting the normal password application, while the range from 30 to 40 is acting proposed approach measurement. The chart is built depending on the ratio of password length to no. of attack. The experiments shows the immunity of proposed approach against some trail attacks such as social engineering, eavesdropping, brute force exhaustion and shoulder surfing. Figure 4 shows application of proposed approach which is developed via Java V6.

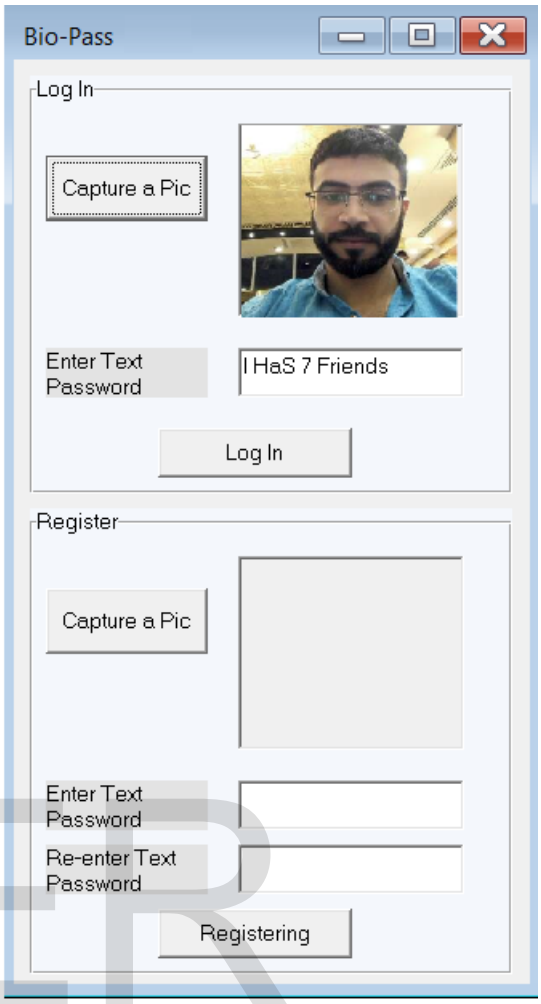

Figure 4 : User Interface for Implementing Adopted Scheme

At the application whose interface is shown above, the user must register at first, else message box will tell the user "You must register at first". This message also appears when the user log in via wrong information. Otherwise message box appears to inform the user " He is allowed to enter the system" which happened at log in state.

4 Conclusion

The following points represent the conclusion of proposed approach :

The proposed approach preserves a shape and location of the facial image, because of these features affects the checking process and produces incorrect results.

The proposed approach is affected by differentiation of image lights, angles and obstacles, since these differentiation will make comparing be different images in checking process.

The proposed approach minimizes the requirements of storage space, because it stores the result of feature extraction and password concatenation.

The approach provides better security for the information stored in the system, since it is producing encrypted

information via exclusive-or concatenation.

The security of the approach is related to the password incrementally. Whenever the password be more secure the entire approach provides more secure environment.

The proposed approach doesn't need more extensive equipments excepts camera to provide real-time facial image of the user. This means the approach isn't wasted more hardware devices.

REFERENCES

[1] M. Jakobsson, S. Taveau, "The Case for Replacing Passwords with Biometrics", FIDO Alliance, 2014.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani and R. Buyya, "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges", IEEE Communications Survey & Tutorial, vol. 16, no. 1, 2014.

[3] V. Odelu , A. K. Das , and A. Goswami, "Cryptanalysis on 'Robust Biometrics-Based Authentication Scheme for Multi-server Environment', Cryptology ePrint Archive , 2014.

[4] C. T. Li, "An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards," in Proceedings of the 5th International IEEE Computer Society Conference on Information Assurance and Security, Xi'an, China, 2009.

[5] J.Nam, K.K.R. Choo, M. Kim, J. Paik and D. Won, "Dictionary Attacks against Password-Based Authenticated Three- Party Key Exchange Protocols", KSII Transactions On Internet And Information Systems, Volume 7, NO. 12, December 2013.

[6] Y. Choi, D. Lee, J. Kim, J. Jung, and D. Won, "Cryptanalysis of Improved Biometric-Based User Authentication Scheme for C/S System", International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.

[7] Y. Sui, X. Zou and Y. Du , "Biometrics-based Authentication: a New Approach", Computer Communications and Networks (ICCCN), 2011.

[8] H. C. LEE, B. J. KANG, E. C. LEE, K. R. PARK, "Finger vein recognition using weighted local binary pattern", Journal of Zhejiang University-SCIENCE C (Computers & Electronics), 2010.

[9] WANG, Yunxin, WANG, Dayong, LIU, Tiegen, et al." Local SIFT analysis for hand vein pattern verification", International Conference on Optical Instrumentation and Technology, International Society for Optics and Photonics, 2009.

[10] D. Saptono, "Conception d'un outil de prototypage rapide sur le FPGA", thèse de doctorat, Universite De Bourgogne, 2011.

[11] K. A. TOH, H. L. ENG, Y. S. CHOO, Y. L. CHA, W. Y. YAU, and K. S. LOW, "Identity verification through palm vein and crease texture", chez Advances in Biometrics, Springer-Verlag, Berlin, Heidelberg, Zhang , D. and A.K. Jain,2005.

[12] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", in Proceedings of 9th USENIX Security Symposium, 2000.

[13] S. Akula and V. Devisetty, "Image Based Registration and Authentication System", in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[14] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004.

[15] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, "The Design and Analysis of Graphical Passwords", In Proceedings of the 8th USENIX Security Symposium, 1999.