

Review on Graphical Authentication Technique

Mr. Jitesh S. Zade¹, Ms. Shivani Shukla², Ms. Sonam Raut³, Ms. Anjali Helonde⁴, Ms. Shubhkirti Salode⁵

^{1, 2, 3, 4, 5.} Department of Information Technology, RTMNU Nagpur University

Abstract: *This work, the usability of a randomized numeric keypad was examined and compared to the usability of a conventional numeric keypad. The comparison used completion time measurements and the error rate of short (4-digit) and long (8-digit) PINs to contrast efficiency and accuracy of the keypads. The results showed that the average completion time with a randomized keypad is longer than with a conventional keypad. It also include the other security feature is -Face recognition has been a fast growing, challenging and interesting area in real time applications. A large number of face recognition algorithms have been developed in last decades. In this paper an attempt is made to review a wide range of methods used for face recognition comprehensively.*

Keywords: *Graphical Password, Randomized Keypad, Shoulder Surfing, Numeric, security.*

I. INTRODUCTION

“Shoulder surfing” or “peeping attacks” refers to stealing information (especially authentication information) by looking over the shoulder of an unsuspecting user [1]. In a general sense, shoulder surfing involves the unauthorized observing of an authorized user’s session on an electronic device in order to gain access to information.

Historically, shoulder surfing concerns moved from telephone calling card fraud to automated teller machine (ATM) fraud, and more recently to mobile computer users. Low tech shoulder surfers are reported to sit in a car at a safe distance and use binoculars, telephoto lenses or more recently camera phones to record users entering their personal identification numbers (PINs). Numeric keypads are popular input methods for personal identification numbers (PINs) for many applications, including automated teller machines (ATM), security screening systems within financial organizations, point-of-sale systems, and home/car door locks.

This study evaluated the overall usability of a randomized numeric keypad. The primary goal of this study was to investigate if users were able to complete the task of entering a PIN via a randomized keypad and to compare this activity to the use of a fixed keypad with a conventional layout. This data provided a valuable metric for the efficiency and accuracy of the use of a randomized keypad. A secondary goal of this study was to investigate whether a randomized keypad enhanced the perceived security of the PIN-entry task, particularly for publicly located systems.

Face recognition is an important part of the capability of human perception system and is a routine task for humans, while building a similar computational model of face recognition. The computational model not only contribute to theoretical insights but also to many practical applications like automated crowd surveillance, access control, design of human computer interface (HCI), content based image database management, criminal identification and so on. Many commercial systems for still face recognition are now available. Recently, significant research efforts have been focused on video-based face modeling/tracking, recognition and system integration. New databases have been created and evaluations of recognition techniques using these databases have been carried out. Now, the face recognition has become one of the most active applications of pattern recognition, image analysis and understanding.

II. RELATED WORK

A. Shoulder Surfing and Randomized Keypad

Authentication methods based on physical access cards are vulnerable to theft or loss. Unless the physical card is combined with other authentication means, a person who steals or finds a lost card would have full unrestricted access to the protected information. Using passwords that the user must remember is not perfect either, but is widely used because of the low cost and the relative ease of use [3]. Unlike biometrics or physical keys, passwords do not require special hardware (which reduces costs) and do not require any skills beyond those needed to use the computer itself (typing and mouse handling).

The danger of this information leak is compounded in the case of authentication from crowded public areas, where multiple observers may be watching or even recording several access sessions, then using this information to recover passwords. Shoulder surfing attacks as a security threat to computer users have been discussed in the literature for more than a decade. Many authors mention shoulder surfing as a threat probably the most relevant area of concern for shoulder surfing attacks is that of mobile computing [2]. The combination of public places, mobile computers and wireless networks makes for a fertile ground for shoulder surfers to look for victims

B. Face Recognition Technique

Support Vector Machines (SVM) is one of the most useful techniques in classification problems. One clear example is face recognition. However, SVM cannot be applied when the feature vectors defining samples have missing entries. A classification algorithm that has successfully been used in this framework is the all-known Support Vector Machines (SVM), which can be applied to the original appearance space or a subspace of it obtained after applying a feature extraction method.

The advantage of SVM classifier over traditional neural network is that SVMs can achieve better generalization performance [3]. Modified PCA algorithm for face recognition were proposed in this method was based on the idea of reducing the influence of eigenvectors associated with the large Eigen values by normalizing the feature vector element by its corresponding standard deviation. The simulation results show that the proposed method results in a better performance than conventional PCA and LDA approaches and the computational cost remains the same as that of PCA and much less than that of LDA.

In this context, according to its proponents, the promise of contemporary biometric identification technology is to strengthen the links between attributed and biographical identity and create a stable, accurate, and reliable identity triad [1]. Although it is relatively easy for individuals to falsify.

A novel Haarlet Pyramid based face recognition technique here face recognition is done using the image feature set extracted from Haarlets on gray plane. PCA is usually used but it is very time consuming. In paper authors have shown the comparative study of different face recognition algorithm for plastic surgery Based on the experimentation carried out by authors it has been concluded that face recognition algorithm such as PCA ,FDA ,LLA ,LBP & GNN have shown recognition rate more than 40% for local plastic surgery. A new approach to plastic surgery based face recognition. An approach based on near set theory for comparing pre and postsurgical facial images.

C. Textual password

The same mechanisms can be used for textual passwords and user-chosen PINs. The drawback is, however, that they have much lower entropy per character which increases the number of rounds for a straight-forward implementation and reduces usability.

III. CONCLUSIONS

This paper show the possible ways in which the current implementation of virtual keyboard is vulnerable to attacks. This paper has attempt to review a significant number of papers to cover the recent development in face recognition and random keypad field. The list of references to provide more detail understanding of the approaches describe the enlisted.

REFERENCES

- [1] Nilesh kawale and shubhangi patil International Journal of Current Engineering and Technology in" A Recognition Based Graphical Password System".(April 2014
- [2] Sujata G. Bhele1 and V. H. MankarInternational Journal of Advanced Research in "AReview Paper on Face Recognition Techniques". (October 2012
- [3] Young Sam Ryu, Assistant Proffessor, Ingram School of Engineering Texas State University-San Marcos "Usability Evaluation of Randomized Keypad". (February 201
- [4] Bogdan HoancaComputer Information Systems University of Alaska Anchorage Kenrick Mock Computer Science University of Alaska Anchorage "Screen oriented technique for reducing the incidence of shoulder". (April 2005)
- [5] Önsen TOYGAR Adnan ACAN "Face recognition using PCA,LDA and ICA approaches on colored images". (2003)
- [6] McIntyre, K.E., Sheets, J.F., Gougeon, D.A.J., Watson, C.W., Morlang, K.P., & Faoro,"Method for secure pin entry on touch screen display" United States Patent and Trademark Office. (April 2003
- [7] Samal and Iyengar" Automatic recognition and analysis of human faces and facial expressions". (April 1992)