Testing Design for Pixel Value Graphical Password Scheme on Image Specimens

Mohd Fahmi Mohamad Amran, Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Omar Zakaria, Nurhafizah Moziyana Mohd Yusop, Mohd Nazri Ismail, Mohd Rizal Mohd Isa, Mohammad Adib Khairuddin, Kamaruzaman Maskat, Yamunah Kathiravan

Abstract*: *In decades, authentication system is relying on username and password as pass-phrase object for authentication process. The longer, wider the variety of symbol choices, and randomly arranged phrase considered as a strong password. A strong password is hard to memorize and make it less preferred by most of the users in most of the cases. To make pixel value graphical password scheme a test-able subject, a coded prototype was developed and deployed. The coded prototype was called as Pixel Value Access Control (PVAC). The study is focused on the testing design and result of experimental testing on different scenario using 24 specimens are used to test the functionality of PVAC pixel value extraction process to produce an accurate pixel value.

Index Terms*: *Testing Design; Pixel Value; Authentication

I. INTRODUCTION

An authentication system comprises an authentication enforcement engine adapted to interface with an authentication provider for performing an authentication process for a user requesting access to a computer resource [1]. Authentication factors can be placed into three categories, namely what you know, (password, secret, personal identification number); what you have, (token and smart card) and what you are (bio-metrics and behavioral) [2]. A blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program while as web trust, authentication is a way to ensure users are who they say they are which the user who attempts to perform functions in a system is in fact the user who is authorized to do so [3].

Passwords and PINs are susceptible to cracking attacks which an automated process of systematically trying all combinations until a match is found, pushed toward two differing authentication techniques namely smartcards which is the notion of 'what you have' and biometric authentication which is the notion of 'what you are'. Most users are more familiar with smartcards than they realize. Electronic Funds Transfer (EFT) cards that require PINs fit the profile of the smartcard architecture that uses in computing authentication but are more commonly implemented for access control and for physical security [4,5]. Biometrics authentication that measures a physical or behavioral attribute of humans to uniquely identify them could relieve users from carrying smartcards and forgetting passwords as it measures physical and they cannot forget. Physical biometrics include: fingerprint, iris, retina, face, voice, and deoxyribose nucleic acid (DNA) while behavioral biometrics includes: handwriting (graphology) and keystroke analysis. Biometric-based authentication required specific input device or tools to enable computer to read and translate into computer signal make it less popular to implement on computer system by most of developers and less prefer by user. The degree to which people's privacy is invaded depends on the type of biometric used, the sensitivity of the information, and the possibility for combining data with other databases [4,5].

This study will describe the testing design and result of the proposed software program for pixel value graphical password scheme. Our previous studies [6-8] have reviewed some of the pixel value method and we managed to propose the design features and requirement of the software program [6].

II. SYSTEM IMPLEMENTATION

As an authentication mechanism, pixel value graphical password scheme could be compatible to implement on any login mechanism on any computer system. In development stage of a computer system, pixel value graphical password scheme was developed as system login and ready to be used with the developed system. As a prototype for pixel value graphical password scheme, Pixel Value Access Control

Revised Manuscript Received on August 19, 2019.

Mohd Fahmi Mohamad Amran, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Mohd Afizi Mohd Shukran, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Mohd Sidek Fadhil Mohd Yunus, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Omar Zakaria, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Nurhafizah Moziyana Mohd Yusop, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Mohd Nazri Ismail, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Mohammad Adib Khairuddin, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Mohd Rizal Mohd Isa, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Kamaruzaman Maskat, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia
Yamunah Kathiravan, Computer Science Dept, Faculty of Defense Science and Technology, UPNM, Kuala Lumpur, Malaysia

(PVAC) is developed as a login mechanism for a mock online database system. In other words, pixel value graphical password scheme can be implementing on any computer system and can be used on any computer platform as long as the device could read or equipped with storage media.

As a login mechanism for any computer system, pixel value graphical password scheme could be implemented on any user interaction environment either client-server environment or system built-in environment. As a prototype, PVAC is developed in web-based environment where it is a client-server environment and can be access by using any web browser.

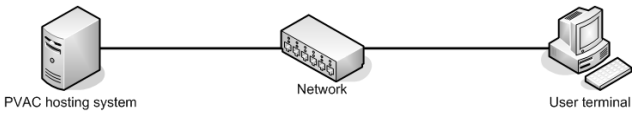

Figure 1. PVAC implementation environments

Fig. 1 illustrates the implementation environment of PVAC where a server role as PVAC hosting system need to be attaches on network. PVAC is hosted as web service through TCP/IP port 80 can be access from user terminal that also attached on net-work. Since PVAC hosted as web service, user could access PVAC by using web browser application (example: Internet Explorer, Google Chrome and Mozilla Fire-fox). PVAC prototype is an example of pixel value graphical password scheme implementation on client-server environment and web-based application. There are many ways of pixel value graphical password scheme could be implemented on computer system and application.

III. TESTING DESIGN

PVAC is tested on coded implementation environment. All of the features are tested to ensure that pixel value graphical password implementation is perform as expected. PVAC was tested with experiment testing to test its efficiency that produced several pixel value patents for each specimen.

In PVAC experimental testing, 24 specimens are used to test the functionality of PVAC pixel value extraction process to produce an accurate pixel value. As shown on Fig. 2, each specimen (specimen n, where n is specimen number) is loaded to PVAC one by one and producing RGB value and DCT value for analysis purpose. The whole testing case is using only one username, which is "pvactester" that registered to first specimen. With the same username, another specimen is being load in each separate test session and the process is repeated until all 24 specimens being load. This means there is 24 image experiment testing session conducted on PVAC. PVAC is extracting pixel value for each specimen in the form of RGB value and DCT value and show the value that is being collected and recorded for further analysis data. The list of specimens is listed in Fig. 3.

Image experimental is a type of functional testing for prototype or system. An experiment is a methodical trial and error procedure carried out with the goal of verifying, falsifying, or establishing the validity of a design theory. Experiments vary greatly in their goal and scale, but always rely on repeatable procedure and logical analysis of the results [9].

There are two types of false specimens (specimen 2 to specimen 24) which are tolerance type and spot type specimen. Tolerance type specimen is a specimen that whole pixel value on that specimen determined the accuracy score such as different pass-pix, color modified passpix, rotated passpix, and resized passpix. Pixel value on every grid must show difference from specimen 1 in order to get full accuracy score. The other type of specimen is spot type specimen where only few predetermined grid or random grid show difference on passpix in order to get accuracy score. Example of spot type specimen is scratch on passpix, grid covered passpix, and watermarked passpix.

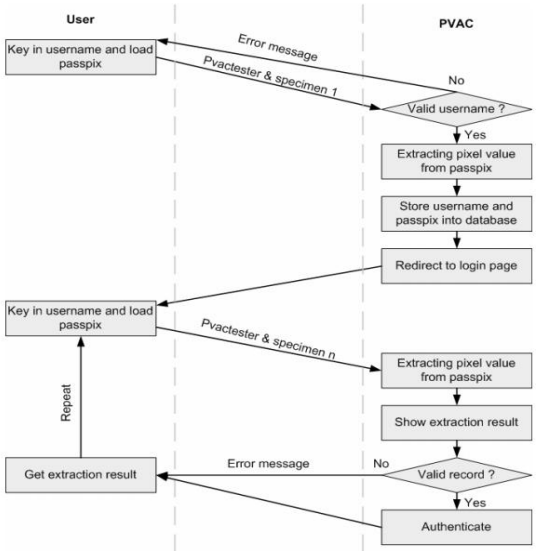

Figure 2. System testing flow

Figure 3. Specimens collection for image experimental testing

IV. RESULTS AND DISCUSSIONS

The Correct passpix

The specimen 1 and username "pvactester" is being registered as a valid user during enrollment stage. PVAC store a record with username as "pvactester" and passpix as shown in left side of Fig. 4. Another enrollment attempt is made with same username and passpix that resulting PVAC is deny

registering the record as username "pvactester" already existed. After record successfully registered, the username and passpix is being used for login that result as getting authentication from PVAC and produce the same pixel value. This process being repeated in 3 time that show PVAC is executing properly without error with the actual account (username and passpix). For the rest of the testing, only this account is being registered on enrollment stage that becomes the only valid account registered on PVAC. RGB value (pixel value) of this account is being used as comparative subject to spot any pixel value differences for others specimen.

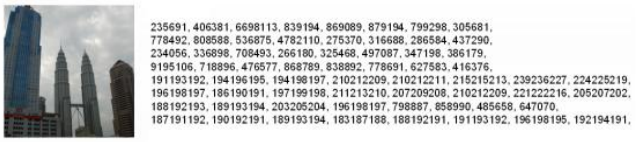

Figure 4. The correct passpix

The Wrong passpix

In this second test scenario, a completely different image file (specimen 2) is choosing to be the passpix as shown on left side Fig. 5. Enrollment stage is not being per-formed in this test session which means there is only one valid user remaining registered on PVAC. The authentication stage is being performed using same username as case 1 ("pvactester"), but using specimen 2 as the passpix to log in. PVAC simply deny the access and fail to authenticate the user as passpix record for "pvactester" is not matching with the stored record in PVAC. As shown in Fig. 5, the whole pixel value is totally different from the pixel value produced from the actual passpix. This case is a false authentication attempt that proves PVAC is working as it should be where PVAC is able to differentiate pixel value between the actual passpix and the wrong passpix.

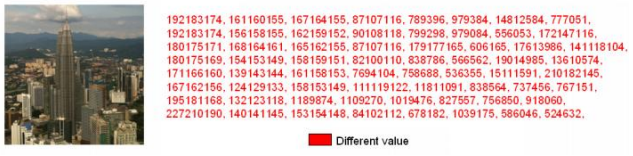

Figure 5. The wrong passpix

The passpix Looks a Like

In this third test scenario, another different image (specimen 3) was picked as registered passpix but it looks almost same with the valid passpix on human eyesight as shown on left side of Fig. 6. As in subsection B, enrollment stage is not being performed in this test session which means there is still one valid user remaining registered on PVAC. With the username "pvactester" and the specimen 3 as passpix, PVAC also denying the access and authentication is

fail where the provided passpix record for "pvactester" is not matched with actual record in database. The produced pixel value is never show similarity at any even though the picture is looking almost the same structure on human bare eye. The chosen image shows almost 70% similarity, but the produced pixel value shows 0% of similarity. This case proves that, PVAC is working perfectly to detecting difference on different image even though the image shows some similarity through human eye.

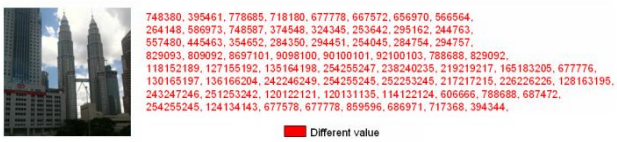

Figure 6. The passpix looks a like

Grayscale Mode passpix

In this test scenario, PVAC is challenge with the same passpix image but in the grayscale mode (4th specimen) as shown on left side of Fig. 7. As in previous test scenario, enrollment stage is not being performed in this test session which means there is still one valid user remaining registered on PVAC The "pvactester" username is being used again with the grayscale passpix and again, PVAC is not authenticating the username and denying the access. Grayscale mode produced a different kind of pixel value where it is shorter than RGB pixel value and result a small password space for grayscale image. This false authentication attempt case proves that beside PVAC is able to deny different color mode passpix.

Figure 7. Grayscale mode passpix

Artistic passpix

Test scenario 5 of experimental testing challenge PVAC with art effect passpix (5th specimen) where the chosen specimen was an edited passpix image with an artistic effect using photo editing software. Again, as in previous test scenario, enrollment stage is not being performed in this test session which means there is still one valid user remaining registered on PVAC. With this passpix and "pvactester" username, PVAC also denying the username and authentication is failed as actual record that stored in database is different from pro-vided image. Produced pixel value is completely different from the actual passpix pixel value even though it is just a simple artistic (water color stroke) effect applying on passpix as shown on Fig. 8. Another false authentication attempt case has failed but successfully prove that the extraction technique apply on PVAC is effectively detecting a small change on passpix.

Figure 8. Art effect on passpix

Re-resolution passpix

Test scenario 6 challenge PVAC with different resolution of passpix as shown on Fig. 9. From the original passpix (600px by 600px), the resolution is changes into 4 type which is enlarge (900px by 900px - specimen 11), shrink (300px by 300px – specimen 12), wide (400px by 600px – specimen 14), and tall (600px by 400px – specimen 13). There is no enrollment stage is being performed in this test session which means there is still one valid user remaining registered on PVAC. Login attempt has made as previous cases and each type of loaded passpix is denied by PVAC and produce almost different RGB value where some grids produce the actual pixel value.

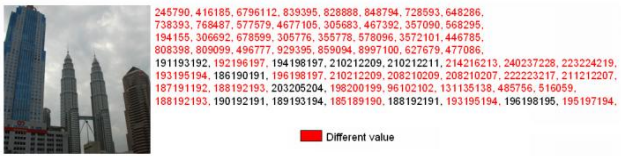

Figure 9. Enlarge passpix

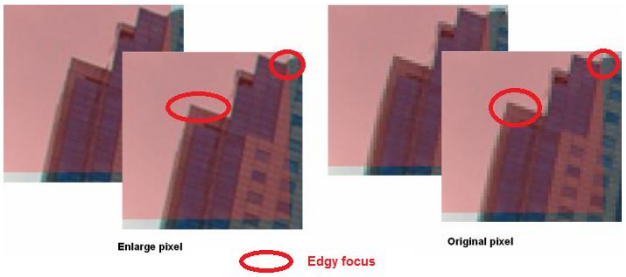

Figure 10. Pixel composition differences

The difference on RGB value is caused by the pixel quality on the passpix. When the image is being stretch or compressed into different resolution, it is also affected the pixel itself. The pixel quality is different on different resolution either it become smaller or larger as shown in Fig. 10. Through 250% zoom in view on two different image resolution shows that the large resolution image is far sharper and more accurate than small resolution image. Small resolution image shows that the pixel is look like scattered into larger blocks. During pixel value extraction process, the loaded image is dividing into 64 grids. For small resolution image, the pixel blocks contain in a grid is lesser than high resolution image file where more numerous is reside in a grid and result different color composition for each resolution image. However not all grids produced a different RGB value de-pending on image contrast. In Fig. 9 shows there is some value are not differentiating from the actual RGB value containing the obvious contrast and the pixels are not scattered into larger block. In this third test scenario, another different image (specimen 3) was picked as registered passpix but it looks almost same with the valid passpix on human eyesight as shown on left side of Fig. 6. As in subsection B, enrollment stage is not being performed in this test session which means there is still one valid user remaining registered on PVAC. With the username "pvactester" and the specimen 3 as passpix, PVAC also denying the access and authentication is fail where the provided passpix record for "pvactester" is not matched with actual record in database. The produced pixel value is never show similarity at any even though the picture is looking almost the same structure on human bare eye. The chosen image shows almost 70% similarity, but the produced pixel value shows 0% of similarity. This case proves that, PVAC is working perfectly to detecting difference on different image even though the image shows some similarity through human eye.

V. CONCLUSION

This paper describes the testing design for image experimental testing and 6 tests were conducted on difference scenarios. The testing design need to carefully developed as it is very important phase before actual testing will take place. 24 specimens are chosen to test the functionality of system as the specimens is loaded to system one by one to produce the RGB and DCT value in order to analyze the data. Findings show that PVAC is able to differentiate pixel value between the actual passpix and the wrong passpix. For future research, different type of scenario will be tested such as opacity value and accuracy score. Besides that, the design on system testing will be conducted.

VI. ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education for providing us grant: NRGS/2013/UPNM/PK/P3 in order to perform this research in Universiti Pertahanan Nasional Malaysia (UPNM). The authors also gratefully acknowledge the editor and anonymous reviewers for their constructive comments on this paper.

REFERENCES

1. Ali, V., & Novoa, M. (2005). U.S. Patent Application 11/036,288.
2. Mohammed, Musa, M., & Elsadig, M.: A multi-layer of multi factors authentication model for online banking services. International Conference on Computing, Electrical and Elecronics Engineering, pp. 220-224 (2013).
3. Zhao, H. & Li, X..: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. International Conference on Advanced Information Networking and Applications Workshops, Vol. 2, pp. 467-472 (2007).
4. Pierce, J. D., Warren, M. J., Mackay, D. R., & Wells, J. G. : Graphical Authentication: Justifications and Objectives. In AISM, pp. 49-63 (2004).
5. Eljetlawi, A. M. :Study and Develop a New Graphical Password System. Faculty of Computer Science and Information System Universiti Teknologi Malaysia (2008).
6. Mohd Shukran, M. A .et. al : Pixel Value Graphical Password Scheme: Identifying Design Features and Requirements, Applied Mechanics and Materials, vol. 548-549, pp. 1561-1565 (2014).
7. Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus & Kamaruzaman Maskat: Access Control Based on Pixel Value Extraction. Australian Journal of Basic and Applied Sciences, 7(4), pp. 415-418 (2013).
8. Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Kamaruzaman Maskat, Wan Sharil Sham Shariff & Mohd Suhaili Ariffin: Pixel Value Graphical Password Scheme-Graphical Password Scheme Literature Review. Australian Journal of Basic & Applied Sciences, 7(4) pp. 688-695 (2013).
9. Arnowitz, J., Arent, M., & Berger, N.: Chapter 7 - Choose a Method. In Effective Prototyping for Software Makers, pages 136-154. Morgan Kaufmann, (2007).