International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Pixel Value Graphical Password: A PassPix Clustering Technique For Password Fault Tolerance

Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Muhammad Naim Abdullah Mohd Nazri Ismail, Mohd Rizal Mohd Isa

Abstract*: The pixel value graphical password scheme was introduced to reduce the burden on memorizing a hard textual password and to hide the password information. It gives freedom for the user to utilizing their personal image their password, called PassPix, that makes it is more memorable and hidden in the same time. However, when the PassPix is travelled on a compressed media, the safety information that resides in the PassPix is transformed and demolishing its function as password. This study is aimed to propose the image clustering technique to solve the issues. This paper is organized into 4 sections where an explanation on graphical password scheme as the introduction in section 1, the problem of this study is stated in section 2, the idea of clustering technique is discussed in section 3, and section 4 as the conclusion of this article.

***Index Terms*: Graphical Password, PassPix, Pixel Value, Clustering Technique.**

I. INTRODUCTION

Pixel value graphical password scheme was introduced in 2012 [1] that granted user access using user personal image which is personally picked from user's image storage library. This graphical password scheme is benefiting users by giving the freedom to pick and select an image that they can be easily memorized without exposing the image to the others [2]. Illegal log-in attempt is hard to perform since the information of the password is hidden and the password object is exclusively kept by the legitimate users.

The idea of this invention was users are free to pick their most memorable image to load to the access control system and become their password that called as *PassPix* (Password Pixel). The loaded image is being extracted for its pixel value and the acquired textual pixel value is stored into users' database that respectively associates with a username. For log-in procedure, users are required to reload their image on the log-in interface for the access control system extracting the pixel value. The extracted pixel value is being query to the database with matching username in order to grant a user further access.

II. PROBLEM STATEMENT

As there are no specific features and requirements of digital image that could be utilize as the *PassPix* for pixel value password access control. Users are free to pick any image they desired as their *PassPix* regardless the content of the image itself and it should let it be that way. Also, it require the original image file to be load as *PassPix* on every log-in moment that led the user might store it on cloud storage, mailbox, or in removable disk. This would affect the digital image pixel structure and respectively the pixel value which cause it unusable for log-in. For example, one of the trending way to make a file is available anywhere is sharing a file to another self-owned account through chatting application such as *WhatsApp* [3] application. Such this chatting application is convenience to store a file since both application and uploaded files can be access on the smartphones or desktop computers with faster file loading and download than email or cloud storage. However, every digital media file that sent through that application is compressed in order to make it work well in slow connection.

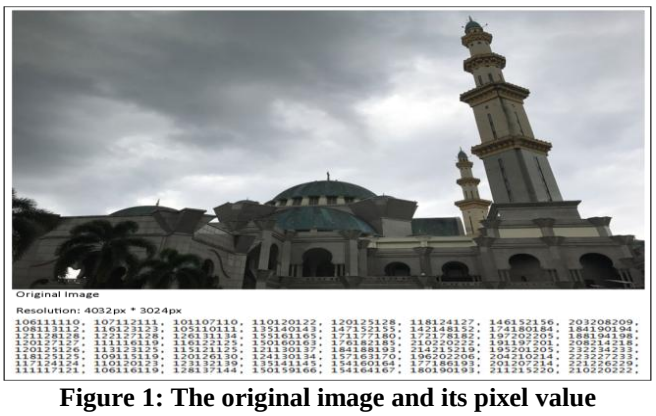

Figure 1: The original image and its pixel value

Manuscript published on 30 September 2019
* Correspondence Author
Mohd Afizi Mohd Shukran*, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia..
Mohd Sidek Fadhil Mohd Yunus, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia.
Muhammad Naim Abdullah, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia.
Mohd Nazri Ismail, Faculty of Defence Science and Technology, Universiti Pertahanan Nasional Malaysia, Kuala Lumpur, Malaysia.
Mohd Rizal Mohd Isa, Faculty of Defence Science and Technology, Universiti Pertahanan Nasional Malaysia, Kuala Lumpur, Malaysia.

For an example, an image (figure 1) is extracted for its pixel value and the same image file is transferred using the *WhatsApp* application. The acquired image from that application shows that the resolution is reduced in an aspect ratios and it is producing a different pixel value than the original pixel value as shown in following figure 2.

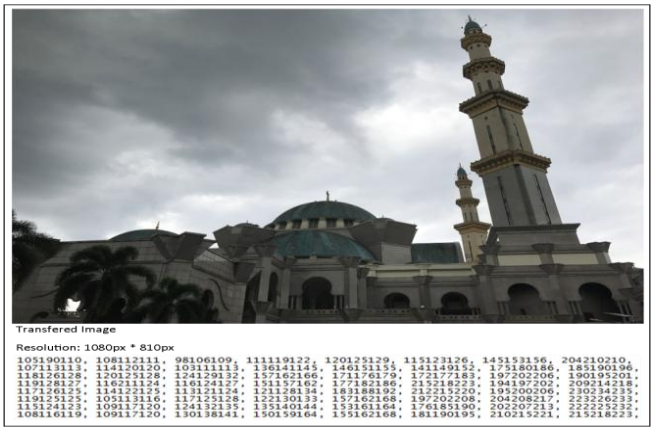

Figure 2: The transferred image with its pixel value

This scenario is proving that some storage media, especially the server based file storage, will alter the pixel structure of a digital image file and as a result, the pixel value become different. Noticed that, the resolution of the image is shrink a lot and that would become the major cause of this matter. When a digital image resolution is being altered, the pixel densities also change where the pixel is denser on a high resolution image than the low resolution image [4]. Unlike the image used in the comparative scenario, in the case of less contrast or blurry image, the pixel value of both images might shows a little similarity to each other where some pixel did not show a clear boundary from each other, but the possibility is still uncertain [5]. Besides the *WhatsApp* chatting application, there are lots more file sharing technique that would altering the pixel structure of a digital image and that was not a good cause for pixel value graphical password scheme.

III. IDEA OF ADAPTING CLUSTERING TECHNIQUE

In the comparative pixel value extraction scenario in section 2, even though both image shows identical features and appearance, both pixel values are totally different from each other. Interesting part is, pixel values in each identical grids shows that the pixel value for each octet is closed (but not similar) that created a pixel value range as shown in figure 3.

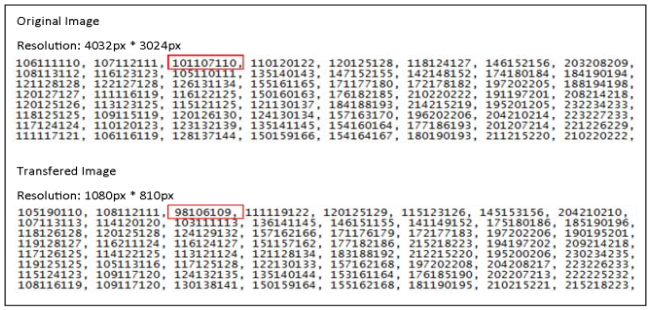

Figure 3: The different on both grids

For an example, the third column of the first row:

Original pixel value: 101 107 110

Altered pixel value: 98 106 109

The pixel value different for each octet is:

R octet; 101 – 98 = 3

G octet; 107 – 106 = 1

B octet; 110 – 109 = 1

Each octet shows small different color strength for both image specimens but the color appearance and shape feature of the image shows similarity. The finding on both image specimens was created a pixel value range where each range would create an image category. This outcome is the great benefit on the adaption of clustering technique to categorizing the *PassPix* for pixel value graphical password scheme. Image clustering is a technique for a self-learn machine to perform the unsupervised image segmentation based on image content features.

There are three type of image segmentation method which are edge-based, region-based, and pixel-based [6]. However, the edge-based and region-based method are consuming a lot of processing resource and time that makes the pixel-based method become more reliable to be implemented on pixel value graphical password scheme. Pixel-Based Segmentation is almost simplest ones defined as Point-based or pixel-based segmentation approach where it is capable to identify the color density and separating an object from the background [7].

For pixel value graphical password scheme, categorizing *PassPix* content would assist the pixel value access control to identify the content of the *PassPix* similarity when the image's pixel value is unintentionally altered as in scenario in section 2. The *PassPix* content category will the another authentication value query for a username which is unable to authenticate. The fault tolerance plan is illustrate in figure 4.

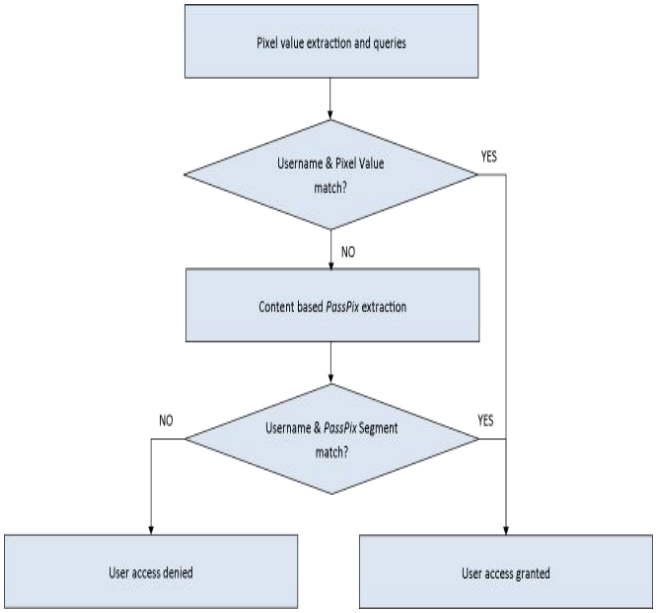

Figure 4: *PassPix* content clustering plan

When a pixel value failed to find its match in the database, the pixel value access control will execute the content segmentation process. The username and *PassPix* content segment need to be similar in order for pixel value access control to grant an access for the respective username.

The *PassPix* content clustering plan will be succeed with an appropriate clustering technique.

There are few features need to be concern on choosing the correct clustering technique which are listed in the following table 1.

Table 1: Clustering features and its issues

Clustering features	***PassPix* issues**
Cluster areas are not fixed	The *PassPix* content segment might be change and mismatch.
	The users account database need to update on every new *PassPix* content registration would cause computational resource consumption.
Predetermined maximum cluster size	If the cluster size is limited to a very small size, too many segment is created and the segment query would take longer time, vice versa, the *PassPix* segment accuracies is reduced.

A clustering algorithm such as K-Means [8], the cluster border is change on every new object input as elaborate in figure 5

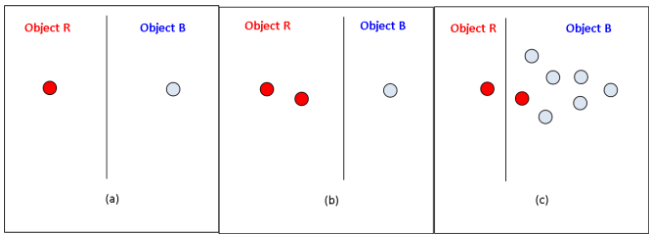

Figure 5: The example of K-Means algorithm

There is a feature of K-Means that will recalculate the segment on every new object input called as iteration. Every cluster must have an object in order to form a cluster as shown in (a). When a new object is inserted, the cluster border is move that give a cluster that have more object a bigger area as shown in (b). The more objects member inserted in a cluster, the more bigger area it gets and even, it absorb some of the object of the other cluster as shown in (c).

For pixel value graphical password scheme, if the *PassPix* matrix is absorb to another cluster, the segmentation query is identify as invalid. The K-Means algorithm is only one of the thousands clustering algorithm available. There must be another algorithm that would suit to be implemented for pixel value access control. Continuous effort for the quest of clustering algorithm for *PassPix* content would solved the pixel value alteration problem.

IV. ACKNOWLEDGEMENT

We would like to thank to Ministry of Higher Education Malaysia and Universiti Pertahanan Nasional Malaysia for giving us the opportunity to assist us in this research.

V. CONCLUSION

As the *PassPix* travel over the compressed media, the pixel value on it is altered that caused the *PassPix* lost it function. The clustering technique is seems to be the solution to that problem where it will grouped the *PassPix* based on content into a designated cluster. However, the clustering algorithm must be equipped with fixed cluster area and size to prevent the *PassPix* segment mismatch. Plus, the segment size needs to be determined properly to prevent the *PassPix* deficiencies. Further research on the matters of segment area or cluster size would solve the pixel value alteration problem on pixel value graphical password scheme.

REFERENCES

1. M.A.M. Shukran & M.S.F.M. Yunus, Patent No. MY-167835-A, Kuala Lumpur, Malaysia, 2018.
2. M.A.M. Shukran & M.S.F.M. Yunus, Pixel Value Graphical Password Scheme: Fake Passpix Attempt on Hexadecimal Password Style, Red, 25500, 2018, p.02550.
3. WhatsApp Inc., WhatsApp Features, Available: https://www.whatsapp.com/features/, 2019.
4. M.S.F.M. Yunus, Dynamic Analysis of Pixel Value Graphical Password Scheme, Master Thesis, National Defense University of Malaysia, Kuala Lumpur, 2014.
5. A. Singh & K. Gupta, A Contrast Enhancement Technique for Low Light Images. AIP Conference Proceedings. 1715. 10.1063/1.4942739, 2015.
6. M.S. Sonawane & C.A. Dhawale, A brief survey on image segmentation methods, IJCA Proceedings on National conference on Digital Image and Signal Processing, 2015
7. M. Panda, A.E. Hassanien & A. Abraham, Hybrid Data mining approach for image segmentation based Classification, Biometrics: Concepts, Methodologies, Tools, and Applications, 2017, pp. 1543-1561
8. J. Macqueen, Some methods for classification and analysis of multivariate observations, Proceedings of the fifth Berkeley symposium on mathematical statistics and probability, 1, 1967, pp. 281-297

AUTHORS PROFILE

Mohd Afizi Mohd Shukran is currently teaching Computer Science in Universiti Pertahanan Nasional Malaysia (UPNM). He has several research experiences and published more that 100 journals indexed by SCOPUS, IEEE and others. His education background is Bachelor in Information System from Melbourne University. Then he did his Master of IT in Sydney university and PhD in Sydney University, Australia..

Mohd Sidek Fadhil Mohd Yunus is currently pursuing his PhD degree in Universiti Pertahanan Nasional Malaysia. His undergraduate degree is from UniKL an obtained his Master by Research degree from Universiti Pertahanan Nasional Malaysia. He has published 20-30 journals in high impact journals and proceedings.

Muhammad Naim Abdullah is currently pursuing his PhD degree in Universiti Pertahanan Nasional Malaysia. His undergraduate degree is from Universiti Pertahanan Nasional Malaysia specialised in Artificial Intelligence. He had obtained his Master by Research degree from Universiti Pertahanan Nasional Malaysia. He has published 20-30 journals in high impact journals and proceedings.

Mohd Nazri Ismail is currently teaching Computer Science in Universiti Pertahanan Nasional Malaysia (UPNM). He has several research experiences in Computer Network Security. He had published more that 100 journals indexed by SCOPUS, IEEE and others. His education background is he did his undergraduate degree in Universiti Kebangsaan Malaysia.Then he did his Master degree at Multimedia University, Malaysia and PhD in Universiti Kebangsaan Malaysia.

Mohd Rizal Mohd Isa is currently teaching Computer Science in Universiti Pertahanan Nasional Malaysia (UPNM). He has several research experiences in Image Processing and Digital Watermarking. He had published more that 60 journals indexed by SCOPUS, IEEE and others. His education background is he did his undergraduate degree and MAster degree i Universiti Teknologi Mara. Then he did his PhD degree at University of Portsmouth, United Kingdom.