Pixel Value Graphical Password Scheme: An Alternative Hash Password Using Hexadecimal Colour Codes

Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Fatimah Ahmad, Mohd Fahmi Mohd Amran

ABSTRACT--- Pixel value graphical password scheme was designed in 2012 to simplify the user authentication process and reducing the implementation setup resource of graphical password authentication system. It was developed and tested in laboratory control environment using a camera captured photo. Through a dynamic analysis on password strength, accuracies output and usability study, pixel value graphical password scheme shows a promising result with huge potential to put into practice. In some cases, there are few limitations which need to be solved in order to implement the pixel value graphical authentication system and this study is aimed to find an alternative for password text length and size on storage disk. This paper is organised into five sections where the background of the pixel value graphical password scheme is described in the introduction section, followed by a discussion on the password style, brief description of hexadecimal code on following section, then the comparative discussion between eight bits code and hexadecimal code, and the conclusion section. The references are listed at the end of this paper.

Index Terms — graphical password, hexadecimal colour code, Passpix, pixel-value.

I. INTRODUCTION

The researches on graphical password domain are aimed to reduce the burden for memorising a strong alphanumeric password, where users utilising graphical material such as photos and image collection in order to be authenticated during the log-in account creation and authentication process. The Blonder's Method [2] was the earliest graphical password scheme introduced in 1996. It requires users to click on several predestined click points on an image that appears on interface which indisputably has smaller password space than the alphanumeric password. To increase the complexity of the graphical password, in [4] proposed a graphical password design by adopting multiple image clip on authentication interface that involved moving and rotating the image clip into a correct alignment. However, the password complexity caused the authentication process to take a longer time to produce even for a legit user. Opposing the predetermined click location or region, the PassPoint method [5] was introduced that allows user to click anywhere on an image. Unfortunately, this method showed that users tend to pick an obvious password point on an image that created a click hotspot where it would be a useful information to attempt the password.

To reduce the deficiencies on the earlier graphical password scheme, the pixel value graphical password scheme [3] was introduced that eliminated the capability to produce the password illegally and reduced the complexity of authentication process. It was developed and prototyped in 2012 where it required users to load an image file as their password, called as passpix (password pixel), during enrollment (sign-up) stage and authentication (sign-in) stage. The pixel values that resided in a digital image were extracted and delivered the hash pixel array to the system server as a password for a username.

II. PASSWORD STYLE ON PIXEL VALUE GRAPHICAL PASSWORD SCHEME

Pixel value is a key to validate a username during the authentication process that resides in every digital image file. A single pixel value is one of an image file attributes where a grayscale image holds 0 to 255 pixel value and a RGB mode image holds 0 to 255 pixel value for each color (Red: 255, Green: 255, Blue: 255). Pixel value in the form of 255255255 represent the RGB value, is being extracted and being used to validate a username. However, through basic extraction process, the produced pixel value is just a single eight bit colour resulting a small password space stored into the database for each username. The possibility of having the same pixel value for different username is 1:16,777,216.

To increase the password space on the pixel value authentication system, a logical two dimension grid is adopted where the loaded image is divided into a number of dimensional grids set. The password space is resulted differently depending on the grid dimension used (example: 8 by 8, 4 by 4, and 32 by 32). Pixel value on each image grid is being extracted by RGB value to form the eight bits binary number and combination of all grids will create a longer pixel value and password space that can be calculated as follows.

For Gas grid dimension and V as colour scheme combination:

Revised Manuscript Received on February 11 , 2019.

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.

Fatimah Ahmad, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Mohd Fahmi Mohd Amran, Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia.

Password space = G x V

As an example on password space for two dimensional 8 by 8 extractions can be calculated as follows:

Grid dimension = 8 x 8 = 64 grids
For each grid = 16,777,216
For 64 grids = 16,777,216 x 64 = 1,073,741,824

III. COLOUR HEXADECIMAL CODE & ANALYTICAL RESULTS

The RGB value in digital image is also stored in three bits Hexadecimal Code form where each byte represents the intensity level of red, green and blue in the form of hexadecimal, 000000 to FFFFFF [1]. Same as the eight bits colour code, this kind of colour code produces 16,777,216 combinations. Unlike the eight bits colour codes that only utilise one octet, there is no exclusion on grayscale value in hexadecimal colour code where it utilised all the three color octets. Fig. 1 illustrated an example of hexadecimal colour code as follows.

Black	Red	Green	Blue	White
FFFFFF	FF0000	00FF00	0000FF	000000

Fig. 1: Example of hexadecimal colour code

IV. COMPARATIVE PASSWORD STYLE

For an authentication system, the password style is a crucial part of security issue that determines how secure an authentication method can be. Two-dimension RGB extraction will produce 1,073,741,824-pixel value combinations. However, each grid will produce up to 3 octets of pixel value where each octet has a limit value is up to 256. In other words, each logical grid used comes with 3 password spaces when the pixel value stored into database and can be calculated as follow:

Maximum password space, S = 3(X * Y)

where X = Sum of grids on X axis and Y = Sum of grids on Y axis.

For example, for a case of an authentication system set to have length of X axis is eight grids and length of Y axis is eight grids, the maximum password space should be 192. The maximum combination is the key to password strength that affected on how hard the pass-object info can be predicted. Therefore, password strength can be calculated as follows:

Maximum password strength, P = (3(X * Y)) 256 = S x 256

where S = maximum password space.

Example for a case of an authentication system set to have length of X axis is 8 grids and length of Y axis is eight grids the maximum password strength is 49,152. Besides the numeric character limit and password space, grid dimensions set for image extraction is also affecting the password space. Fig. 2 shows how number of grids is affecting the password strength.

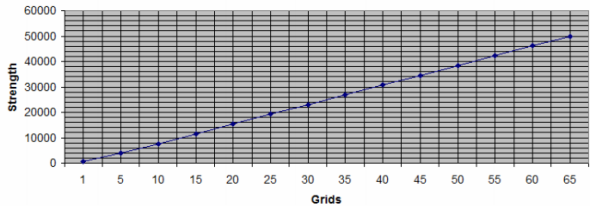

Fig. 2: Password strength against grids

Password strength increase equally with the number of grids which leads to a statement that the more grids set to use on the image extraction will increase the password strength. Logically, since both colour code scheme has 16,777,216 combinations; therefore, both colour codes would have the same password space and password strength. Even though both colour code schemes logically have the same password space and strength, the extracted hash text structure has a significant difference as showed in following Fig. 3 and 4.

Fig. 3: Comparison between 8 bits and hexadecimal hash text for 2 by 2 image grid

In the 2 by 2 image example, Fig. 3 shows an image that uses 4 red colour varieties and the eight bits colour codes will create a 34 characters of hash text while hexadecimal colour code will produce 24 characters. Eight bits colour codes produce a longer password than a hexadecimal colour code for a multi-colour image. However, if a user intentionally uses a simple colour image, there are possibilities where the eight bits colour code produces a shorter password. For example, an image that only contains lime colour (RGB: 02550), the eight bits color code will produce only 20 password characters while the hexadecimal colour code produces 24-character password as shown in following Fig. 4.

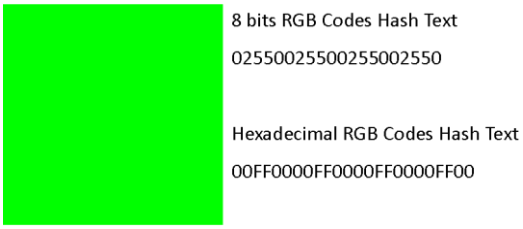

Fig. 4: Simple colour image colour code comparison

The eight bits colour code can be represented as small as three digits (such as Black; 000) up to nine digits (such as white; 255255255) while the hexadecimal code is always represented by six characters code. Thus in some cases of user choice passpix, hexadecimal colour code will produce a longer hash text as a pixel value graphical authentication system.

V. CONCLUSION

Pixel value authentication system utilises the extracted colour pixel value from a loaded passpix. Both colour codes can be used as a hash text producer for the password. Even though the eight bits colour code produces longer hash text password than hexadecimal code, in some cases, the hexadecimal code will be a better choice. It is not just in simple colour image case, there will be a possibility server limitation such as data type limit and database size. Logically, shorter data only need small storage space. In Table 1, the comparison between eight bits colour code and hexadecimal colour code is concluded.

Table 1: Comparison between eight bits RGB codes password and hexadecimal codes password

	8 Bits RGB Codes	Hexadecimal RGB Codes
Text Length	From 3 to 9 digits for each grid	Always 6 characters for each grid
Text Confusion	Hard to identify the colour code	Easy to identify the colour code
Data Type	Numbers	Strings

REFERENCES

1. HTML color codes. Available: https://html-color-codes.info/.
2. G. E. Blonder, Patent No. 5,559,961, Washington D.C., 1996.
3. M. A. M. Shukran, and M. S. F. M. Yunus, Patent No. MY-167835-A, Kuala Lumpur, 2018.
4. L. Sobrado, and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, 4, 2002, pp. 12-18.
5. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 63(1-2), 2005, pp. 102-127.