Review Paper: Multi-Factor Authentication Scheme

Vasundhara Bhele
Computer Science & Engineering
NUVA College of Engg. & Tech
Nagpur, India

Shyam Dubey
Asst. Professor Computer Science & Engineering NUVA College of Engg. & Tech, Nagpur, India

Nilesh Chaubey
Asst. Professor, Electronics & Communication Engineering
Manoharbhai Patel Institute of Engg. & Tech, Gondia, India

ABSTRACT

Alpha-Numeric passwords, Textual passwords and Graphical passwords are the technique utilized for authentication reason. At the same time these validation techniques are defenseless against eves dropping, dictionary attacks and shoulder surfing. Graphical passwords are presented set up of textual passwords methods, yet it is tricky to recall graphical passwords. The greater part of the graphical plans are defenseless against shoulder surfing. To remove this issue present new technique for authentication, picture can be joined with water marking methods and make Walsh code pin to produce password for authentication reason. In this paper, two techniques are proposed to create password utilizing watermark picture and Walsh code.

Keywords: Image Processing, Watermarking Techniques, Walsh code, DCT (Discrete Cosine Transform).

1. INTRODUCTION

Password-based authentication is generally utilized in computer networks for remote access control. Customary password word based authentication protocols are focused around password kept up by the server. The security of these methodologies depend vigorously on the protection of the password and are powerless against password attacks, for example, such as offline password dictionary attacks, shoulder surfing, brute force attack and corruption attacks, etc.

In the proposed plan, introducing new techniques of password authentication using image water mark technique and Walsh code. Image processing is any form of signal processing for which the input is an image, the output of image processing can be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it.

Watermark Adding an visible watermark it is a typical method for recognizing pictures and shielding them from unauthorized use online. Watermarking technology plays an imperative part in preventing (copyright) as it permits to place a distinguishable. Watermark contingent upon the necessity in the multimedia data to distinguish the honest owner or identify malignant altering of the document.

A watermark is an undetectable mark place on a picture that is intended to distinguish both the source of a picture and its proposed recipient. Watermark methods are utilized for Proof of Ownership (copyrights and IP assurance), Copying Prevention, Broadcast Monitoring and Authentication. The noteworthy parts of the host picture, e.g. the low frequency components have to be modified in order to encode the information in reliable and robust way.

A discrete cosine change (DCT) expressed a grouping of limitedly numerous data points in terms of as sum of cosine functions oscillating at different frequencies. DCTs are vital to various applications in science and engineering from loss compression of audio and picture to spectral methods for the numerical solution of partial differential equations on, it turns out that (cosine) functions are substantially more efficient. Numerous image transforms have been considered like DCT (Discrete Cosine Transform). DCTs are also generally utilized in solving partial differential equations by spectral methods.

2. RELATED WORK

The paper review, most of the paper searched are used passwords for authentication by using textual password, alpha-numeric password and graphical password this authentication techniques are used but having drawback like shoulder surfing brute force attack. Two authentication methods are based on text and colors in this they generate the session passwords and resistant to dictionary attack.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle.

Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences.

To evacuate the drawback of textual password removed by graphical password plans which give a method for making more easy to understand passwords, while expanding the level of security, they are vulnerable to shoulder surfing .Here text was combine with image and color to generate the session password and every time user wants to enter new password as session ends. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Same issue is here as well as previously comes. Drawbacks associated with the textual passwords such as brute-force attacks same this problem held with graphical passwords which includes shoulder-surfing and are very expensive to implement.

3. AUTHENTICATION SCHEMES

The proposed plan illustrated in this paper is entirely based on the idea of Watermark image passwords with Walsh pin code. Here, the main objective of this project is to provide security to the confidential files, folders in computing devices through Watermark image passwords. Using following techniques

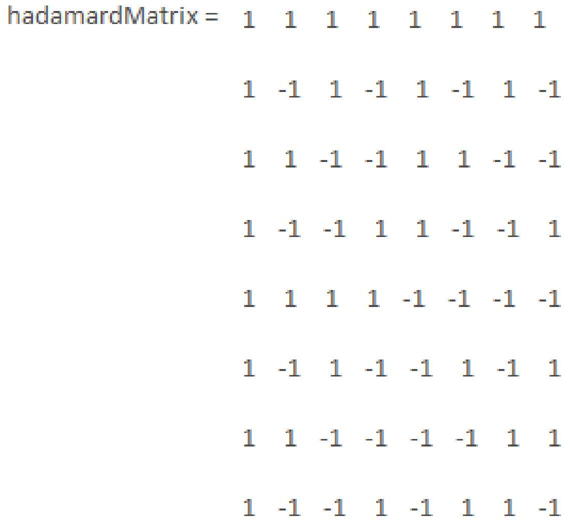
3.1 Walsh Code Algorithm

Walsh codes are fixed length orthogonal codes possessing high auto correlation and low cross correlation properties. Walsh codes are linear phase and zero mean with unique number of zero crossings for each sequence within the set.The Walsh-Hadamard transform (WHT) is a suboptimal, not-sinusoidal, orthogonal transformation that disintegrate a signal into a set of orthogonal, rectangular waveforms called Walsh functions. The transformation is real because the amplitude of Walsh (or Hadamard) functions has only two values, +1 or -1.

3.2 Walsh (or Hadamard) Functions

Walsh functions are rectangular or square waveforms with values of -1 or +1. An important characteristic of Walsh functions is sequence which is determined from the number of zero-crossings per unit time interval. Every Walsh function has a unique sequence value. Walsh functions can be generated in many ways . Here we use the hadamard function in MATLAB® to generate Walsh functions. Length eight Walsh functions are generated as given below.

```
N = 8;  % Length of Walsh (Hadamard) functions
hadamardMatrix = hadamard(N)
```



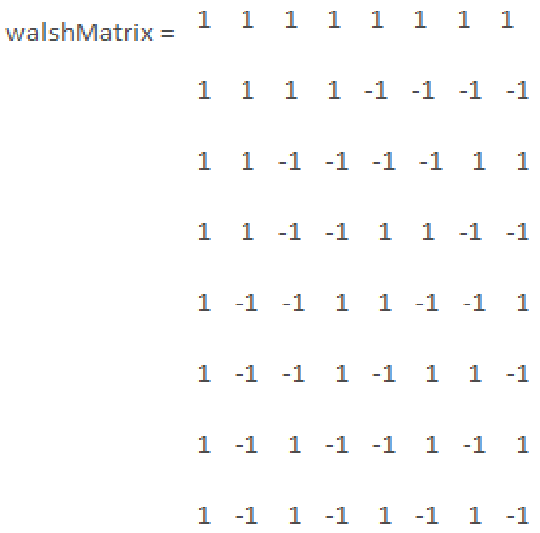
```
hadamardMatrix =  1   1   1   1   1   1   1   1

                  1  -1   1  -1   1  -1   1  -1

                  1   1  -1  -1   1   1  -1  -1

                  1  -1  -1   1   1  -1  -1   1

                  1   1   1   1  -1  -1  -1  -1

                  1  -1   1  -1  -1   1  -1   1

                  1   1  -1  -1  -1  -1   1   1

                  1  -1  -1   1  -1   1   1  -1
```

Fig. 1 : hadamardMatrix

The rows (or columns) of the symmetric hadamardMatrix contain the Walsh functions. In the matrix are not arranged in increasing order of their sequences or number of zero-crossings (i.e. 'sequence order') but are arranged in 'Hadamard order'. That Walsh matrix, which contains the Walsh functions along the rows or columns in the increasing order of their sequences is obtained by changing the index of the hadamardMatrix as follows.

```
HadIdx = 0:N-1;                    % Hadamard index
M = log2(N)+1;                          % Number of bits to
represent the index
```

Each column of the sequence index (in binary format) is given by the modulo-2 addition of columns of the bit-reversed Hadamard index (in binary format).



```
walshMatrix =  1   1   1   1   1   1   1   1

               1   1   1   1  -1  -1  -1  -1

               1   1  -1  -1  -1  -1   1   1

               1   1  -1  -1   1   1  -1  -1

               1  -1  -1   1   1  -1  -1   1

               1  -1  -1   1  -1   1   1  -1

               1  -1   1  -1  -1   1  -1   1

               1  -1   1  -1   1  -1   1  -1
```

Fig 2 : walshMatrix

3.3 Discrete Walsh-Hadamard Transform

The inverse and forword Walsh transform pair for a signal x(t) of length N are

$$y_n = \frac{1}{N}\sum_{i=0}^{N-1} x_i WAL(n,i), n = 1, 2, \ldots, N-1$$

$$x_i = \sum_{n=0}^{N-1} y_n WAL(n,i), i = 1, 2, \ldots, N-1$$

The functions fwht and ifwht implement the forward and the inverse WHT respectively.

3.4 Discrete Cosine Transform

With the character of Discrete Fourier Transform (DFT), discrete cosine transform(DCT) turn over the image edge to make the image transformed into the form of even function. It’s one of the most common linear transformations in digital signal process technology. Two dimensional discrete cosine transform(2D-DCT) is defined as

$$F(jk)=a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

The corresponding inverse transformation is

$$f(mn)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

The 2D-DCT can not only focus the main data of original image into the smallest low-frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the data centralizing and the computing complication. So it obtains the wide spreading application in the compression coding.

4. CONCLUSION

In this proposed arrangement, two authentication methods focused around Watermark image and Walsh code. These methods produce passwords and are impervious to dictionary attack, brute force attack and shoulder-surfing. Both the methods use grid for passwords generation.

These strategies can likewise be produced for window application for registration and login for security reason. It will evacuate the disadvantage of shoulder surfing and it will secure from the hacking passwords, in this we recommended that each time new picture will show with watermark id which gives on picture. However these plans are totally new to the clients and the proposed authentication procedures should be checked broadly for ease of use and effectiveness.

5. REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.

[2] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.

[3] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing

[4] DCT, http:/www.slideshare.com

[5] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of international conference on security and management*. Las Vegas, NV, 2003.