International Journal For Technological Research In Engineering
Volume 5, Issue 10, June-2018 *ISSN (Online): 2347 - 4718*

FULLY INCREMENTING VISUAL CRYPTOGRAPHY FROM A SUCCINCT NON-MONOTONIC STRUCTURE

Anjana Jimmington[1], Ambarish A[2]
[1]Department of Computer Science and Engineering, Kerala Technical University, India
[2]Faculty of Computer Science and Engineering, Malabar College of Engineering and Technology, Desamangalam-Kerala

Abstract: Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device. It is the first line of defense against compromising confidentiality and integrity. Though traditional login/password based schemes are easy to implement, they have been subjected to several attacks. The traditional scheme of password authentication involves the transformation of password into hash values. It is comparatively simple and fast. However in this cyber era they can be exposed to cyber-attacks utilizing password by cracking tool or hash-cracking online sites. From hash value that is relatively simple and plain the attackers can thoroughly figure out an original password. Thus a lot of hacking accidents have been reported. As an alternative, an image based authentication systems is introduced. In this work, I suggest an enhanced password processing scheme based on image using visual cryptography (VC). This scheme different from the traditional scheme based on hash and text, transforms a user ID of text type to images which are further encrypted. For each text password the user should make two images consisted of sub pixels. The server only has user's ID and one of the images instead of password. When the user logs in and sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate user by comparing extracted ID with the saved one.
Keywords: authentication, hash, visual cryptography, image based authentication system.

I. INTRODUCTION

With the rapid growth of computer networks and communication technologies, more and more computers are linked together such that facilities can be shared through the networks. Therefore, providers of the facilities have to make resources under appropriate protection. Authentication plays a crucial role in protecting resources against unauthorized and illegal use. Authentication processes may vary from simple password based authentication system to costly and computation intensified authentication systems. Passwords are more than just a key. They serve several purposes. They ensure our privacy, keeping our sensitive information secure. Passwords authenticate us to a machine to prove our identity- a secret key that only we should know. They also enforce non repudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords. Our username identifies us and the password validates us. But passwords have some weaknesses: more than one person can possess its knowledge at one time. Moreover, there is a constant threat of losing your password to someone else with venomous intent. Password thefts can and do happen on a daily basis, so we need to defend them. Passwords are more than just a key. They authenticate us to a machine to prove our identity- a secret key that only we should know. They also enforce non repudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords. Our username identifies us and the password validates us. But passwords have some weaknesses: more than one person can possess its knowledge at one time. Moreover, there is a constant threat of losing your password to someone else with venomous intent. Password thefts can and do happen on a daily basis, so we need to defend them. Traditional password conversion scheme for user authentication is to transform the passwords into hash values. These hash-based password schemes are comparatively simple and fast because those are based on text and famed cryptography. However, those can be exposed to cyber-attacks utilizing password by cracking tool or hash-cracking online sites. Attackers can thoroughly figure out an original password from hash value when that is relatively simple and plain. The most commonly and frequently used include the hash function such as MD5, SHA256. Assume that someone defines password "raymond" in a system. If an attacker is aware of the hash value"F2A414AA78C7621831DA5995E1447242", the value can be sufficiently cracked simply by free crack site like Figure 1. Even though the attacker doesn't know any information about hash function, he or she can easily guess which kind of hash function is adapted in the system. As the result, the attacker can cause secondary damage to the system.

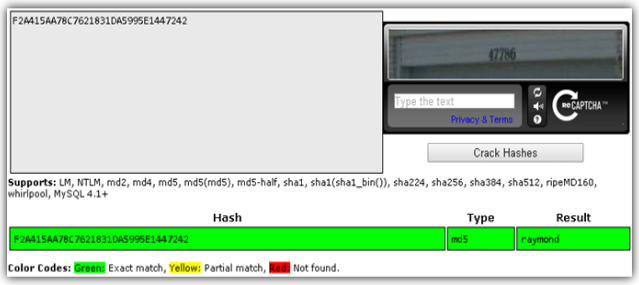

Figure 1 Result of cracked password

Thus to provide a better security to the password a different view text-based scheme is introduced, we suggest enhanced password scheme based on an image created by VC. The image implicitly involves password and ID. In order to verify

password, proposed scheme checks ID through OCR.The goal of our proposal is to prevent cyber-attack and support privacy of personal information with enhanced authentication of password.

II. RELATED WORK

Visual Cryptography

Visual cryptography [VC] is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

One of the best-known techniques has been credited to MoniNaorand Adi Shamir, who developed it in 1994.They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

In order to build the shared images, firstly you should prepare an original image including secret message "SASTRA" such as picture (a) of Figure2. It must be exactly composed of white background and black letter. In fact, the research about VC has been extended to half-tone picture moreover color picture. But we are supposed to explain basic VC referred to this paper.

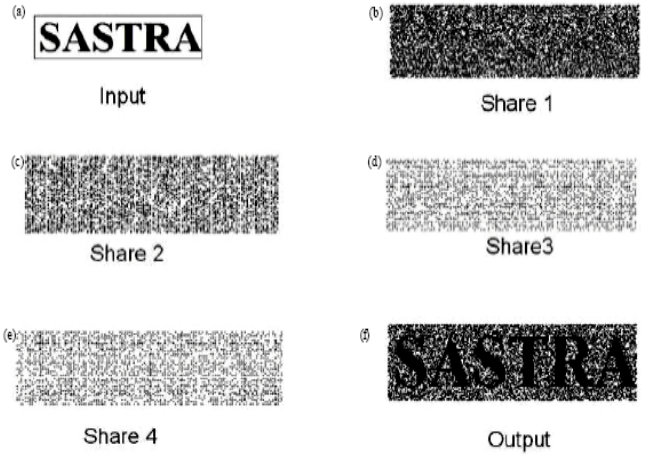

Figure 2. Pictures related with VC

For encryption, you should prepare some patterns consisted of 4 sub pixels arranged in a 2 x 2 array. The half of 4 sub pixels is filled with black and the rest becomes transparent. It can make 6 pattern which is horizontal, vertical and diagonal. VC transforms per a pixel of original image to one of those. After VC-based image is made in full, the sub pixels become as noise because shared image is combination of randomly collected patterns. The way to construct pixels of background and message in shared image should be different from each other. If what you want to convert to a pattern is a pixel of background in original image, it should be following to background pixel matrix in Figures 3. The pattern is randomly determined by one of the forms according to pattern no.

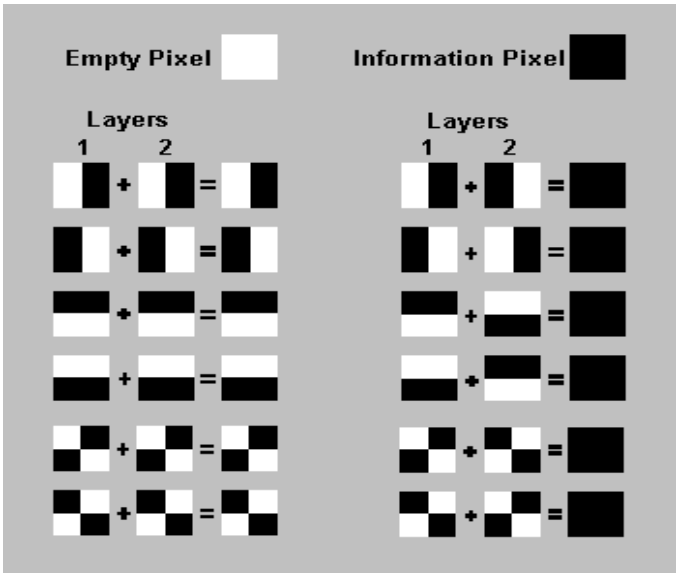

Figure 3. How to make pixel pattern in shared image

In conclusion, first shared image as picture (b) in Figure 2 seems gray. Presented on picture (c) in Figure 2, second shared image also appears similar with first shared image because the own pattern is defined by a pattern of first shared image.Simla-

rly all the other copies of the shared image. However the all the four shared images never reveal secret message "SASTRA" and any rule to build the shared image because black and transparent pixels are mixed in randomly. Exclusively when all four shared images are stacked up, the view of human can confirm the message like picture (f) in Figure 2. If all images are not matched from start point to end point, or one of four image is distorted, you cannot view the message at all. The principle is to utilize higher contrast of character than background. Therefore VC has lower computation for encryption and needs not any computation for decryption.

Optical Character Recognition

OCR is the mechanical and electrical transformation of images of typed, handwritten or printed text into machine-encoded text, whether from a scanned document, a photo of a document, a scene-photo (for example the text on signs and billboards in a landscape photo) or from subtitle text superimposed on an image (for example from a television broadcast).It is widely used as a form of information entry from printed paper data records, whether passport documents, invoices, bank statements, computerized receipts, business cards, mail, printouts of static-data, or any suitable documentation. It is a common method of digitizing printed texts so that they can be electronically edited, searched, stored more compactly, displayed on-line, and used in machine processes such as cognitive computing, machine translation, (extracted) text-to-speech, key data and text mining. OCR is a field of research in pattern recognition, artificial intelligence and computer vision.

The basic OCR algorithm is template-matching method to add algebraically value to acquire a letter is corresponded within the segments of input characters:


```
// Get pixels by R, G, B
alpha = new Color(original.getRGB(i, j)).getAlpha();
red = new Color(original.getRGB(i, j)).getRed();
green = new Color(original.getRGB(i, j)).getGreen();
blue = new Color(original.getRGB(i, j)).getBlue();

red = (int) (0.21 * red + 0.71 * green + 0.07 * blue);
// Return back to original format
newPixel = colorToRGB(alpha, red, red, red);

// Write pixels into image
lum.setRGB(i, j, newPixel);
```

Figure 4.OCR Algorithm

Figure 4 shows the OCR algorithm implementation. But during development of OCR method, several problems can be occurred as follows:

- Rarely distinguish some characters for computers to understand. (Example. Number one "1" and lower case L "l")
- Be more dark background or printed whole image than words for the reason, it has been researched more to recognize the letters.

This paper is adapting one of various OCR algorithms to suggested mechanism.

III. IMAGE BASED PASSWORD AUTHENTICATION SYSTEM

In this system we suppose that a server in general system identifies a user for user authentication. This section explains specifically the procedures between the user and the server though the image based password scheme based on VC and OCR. Simulation result is also provided.

Architecture

The following system shows the architecture of the proposed scheme. The architecture has two sessions the admin session and the user session.

Admin Session

The admin session deals with the creation of the user. The user gives the input image to the admin which in turn via the visual cryptography produces the two shared images and send on copy to the user registered email and the next to the server storage.

User Session

In the user session the OCR is performed by comparing the different shared images generated.

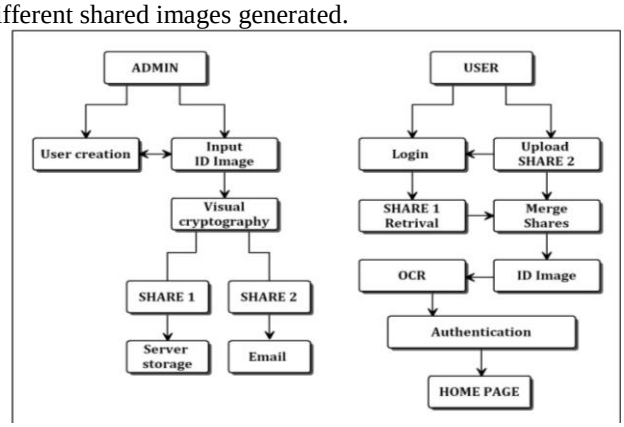

Figure 5. System Architecture

Proposed Scheme

Before user authentication, the user has to register himself or herself to server system. Figure 5 presents the registration process.

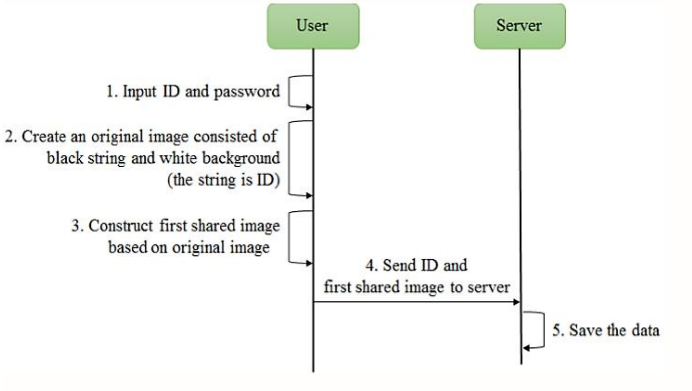

Figure 5. Initial registration process

First, user inputs the ID and password on device. The device starts to create an original image consisted of black letters implying ID and white background. The user may save the image in the device. The device constructs first shared image adapting VC.

The pattern to make up the first shared image is determined by pseudorandom generator with SEED which has password and ID as salts. After completing building the first shared image, the user sends ID of text type and the image instead of password to the server via security channel and destroys the image. If the server saves the data about user information, the initial registration process is finished. The server does not know the password at all because it is impossible for server to retrieve the password of the user from just one shared image.

Proposed password processing scheme is as follows:

1. The user inputs the ID and password.
2. The device of user creates an original image composed of black characters and white background. If the saved original image exists on user's device, it does not have to create the original image again.
3. Although the device does not possess the first shared image, it can thoroughly construct second shared image referred to the original image and first shared image because the device already knows the SEED to make up the first shared image.
4. The user sends the second shared image only to the server.
5. The server overlaps the first shared image saved and the second shared image received.
6. The server should remove the background of the overlapped image as in Figure 2 (d), to gain original image.
7. ID is retrieved from the background-removed image by OCR.
8. The server confirms whether the extracted ID corresponds with saved ID, and determines success or fail.
9. The result is sent to the user.

Process of enhanced scheme

The enhanced image based password authentication system process takes place in the following steps:

According to the Figure 6 there are nine steps. There is user and a server.

1. Initially the user has to enter ID and password to the system.
2. Create an original image of the password consisting of back strings and white background.
3. Construct second shared image based on original image and first share image.
4. Send the second shared image to the server.
5. Overlap the first and the second shared images.
6. Remove background patterns of the overlapped images.
7. Extract using OCR ID from the overlapped images.
8. Verify user by comparison with extracted and original ID
9. Send the result(success or failure)

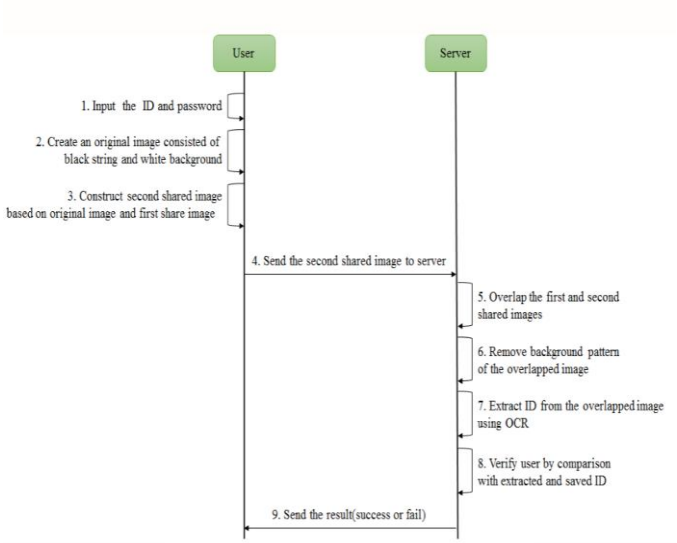

Figure 6.Process of enhanced password authentication

System Implementation

We developed proposal scheme-based application for communication between user and server on internet. It is installed in the devices of user and server as in TALBE I. Suppose that user run on android such as Nexus 7, because this paper wants to show that proposed scheme can be adapted on a machine even with lower spec than general desktop. Operating system is installed on each machine. The device of user part uses Android 4.0. The server with Window7 has static IP (last number is 75) and 9002 port. We import basic java library as well as "java.io and java.net" for networking programming, "java.awt" to manage sockets for networking and "javax.imageio" to conduct images on VC. Especially the server has to import Tesseract API downloaded from Git in order to derive user's ID from stacked images after removing background pattern.

TABLE I. SYSTEM ENVIRONMENT

Part	*User*	*Server*
Development Type	Application	application
Device	Nexus 7	General desktop
OS	Android 4.0	Window 7
IP	~	xxx.xxx.xxx.75
Port	~	9002
Java version	JDK 7	JDK 7
Main Library	java.io.* java.net.* java.awt.* javax.imageio.* java.util.*	java.io.* java.net.* java.awt.* javax.imageio.* java.util.* Tesseract API

Advantages of Proposed Scheme

- A image based password authentication system is relatively inexpensive to implement.
- Image based Graphical passwords provide a way of making user-friendly passwords.
- Image based passwords are not vulnerable to dictionary attacks.
- It is less convenient for a user to give away image based passwords to another person.

IV. EVALUATION

Our scheme has a few differences from traditional password based scheme. The first is the adopting VC instead of text-based hash. The second is that the output value is user's ID even if input value is password and salt as in traditional scheme. The last is that user sends only one image involving the ID and password for authentication.

Based on these features, our proposal has advantages as follows:

- Lower computational cost
- Preventing cyber-attack using vulnerable points of hash functions
- Supporting privacy of users

By applying the peculiarity of VC, suggested scheme also has identical peculiarity. VC requires little computation to create random pattern number per pixel for encryption. Random number generator has lower computation complexity than hash function because a pseudorandom number is obtained just by repeating exclusive-or (XOR) operator with a shifted version. Secondly, this scheme is able to prevent cyber-attack such as dictionary-attack and birthday-attack from the attackers aiming at cracking hash values. Even though the attacker extorts saved image, it is impossible for the attacker to acquire any information about original password or rule to array sub pixels. Even if the attacker knows that the image is built by repeating some shapes with regard to sub pixels, he or she can never understand the rule to match the shapes with pattern number and the rule to generate pseudorandom number. The dictionary for VC is not able to exist because shared image size is very diverse different from static hash size, and it is more difficult to search the information by image than by text.

V. CONCLUSION

Security and computation cost are always the important issues of the password authentication protocol. In this article, we present a new password authentication protocol which is image based. Here the images are encoded by VC with a SEED number and OCR and thereby providing a more strong protection from cyber-attacks. We evaluated security aspect on attacks, computational cost and privacy. Our proposal is light weight and more secure system the provides a high security to the data stored in the system in a distinctive way.

Future Scope

Although the use of image based passwords is not as secure as other forms of authentication like the use of biometric means of authentication (very expensive). Text-based passwords should be replaced with image based passwords because they are more secure.As a future enhancement, the application can be developed for the colored images and supporting more image formats. This application contains various input pages (images) from user. As a future work, the application can be enhanced by making these input parameters automated and also by reducing the number of operations that the user has to perform. This proposal is light weight and more secure system that provides a high security to the data stored in the system in a distinctive way.

REFERENCES

[1] Gaw, Shirley, and Edward W. Felten “Password management strategies for online accounts,” Proceedings of the second symposium on Usable privacy and security. ACM, 2006.

[2] Nguyen, Thi Thu Trang, and QuangUy Nguyen, "An analysis of Persuasive Text Passwords, "Information and Computer Science (NICS), 2015 2nd National Foundation for Science and Technology Development Conference on. IEEE, 2015.

[3] Tam, Leona, Myron Glassman, and Mark Vandenwauver, "The psychology of password management: a tradeoff between security and convenience, "Behavior & Information Technology 29.3 (2010): 233244.

[4] Wang, Luren, Yue Li, and Kun Sun, "Amnesia: A Bilateral Generative Password Manager," 2016 IEEE 36th International Conference on Distributed Computing Systems.

[5] Gauravaram, Praveen, "Security Analysis of salt|| password Hashes," Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on. IEEE, 2012.

[6] Dana Yang, InshilDoh, KijoonChae, “Mutual Authentication based on Visual Cryptography and OCR for Secure IoT Service,” Source of the Document 2016 6th International Workshop on Computer Science and Engineering, WCSE 2016, 2016, Pages 214-219.

[7] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptology EUROCRYPT94 LNCS, Vol. 950, pp. 1-12, 1995.

[8] Mori, Shunji, Ching Y. Suen, and Kazuhiko Yamamoto, "Historical review of OCR research and development," Proceedings of the IEEE 80.7 (1992): 1029-1058.

[9] Patel, Chirag, Atul Patel, and Dharmendra Patel, "Optical character recognition by open source OCR tool tesseract: A case study," International Journal of Computer Applications 55.10 (2012).

[10] Holley, Rose, "How good can it get? Analyzing and improving OCR accuracy in large scale historic newspaper digitization programs," D-Lib Magazine 15.3/4 (2009).

[11] Marsaglia, George, "Xorshiftrngs," Journal of Statistical Software 8.14 (2003): 1-6.

