Password Processing using Visual Cryptography and Optical Character Reader

Sreelakshmi[1], Sonali S[2], Sowmya G S[3], Sumaiya A[4]
[1234]*Atria Institute Of Technology*

Abstract- Hash-based password schemes aresimple and fast, that can be exposed to digital assaults by cracking tool. Accordingly, numerous hacking incidents have been happened overwhelmingly in systems adopting those hash-based schemes. In this paper, we propose password authentication using Image decipherment (IC) and OCR (Optical Character Recognition). The scheme transforms a user ID of text type to three images encrypted by IC. The client should make three images comprised of sub pixels by random function with SEED which incorporates individual data. The server keeps up client's ID and one of the image. At the point when the client logs in and sends another image, the server can extract ID by using OCR (Optical Character Recognition). As a result, it can verify client by comparing extracted ID with the saved one. The proposed enhances authentication, prevents digital assaults with lower computations.

Keywords- hash; visual cryptography; image-based password scheme;

I. INTRODUCTION

Visual Cryptography is a technique, which is used to conceal the secret image into transparencies (which will vary with the user) and these transparencies are distributed to the intended recipients. In Extended Visual Cryptography Scheme, the transparencies are embedded into the meaningful images so that the intended recipient will have a transparency, which is a meaningful image. User authentication in general systems has proceeded basically through verification of the ID and password. In order to send and verify password, the system uses a hash-based password scheme that transforms original password to hash value by famed function. The advantages are that it can be adapted in system without difficulty, and computational velocity of process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. But it is vulnerable to attacks such as brute-force attack or dictionary-based attack plainly by password cracking tool or hash cracking online sites.

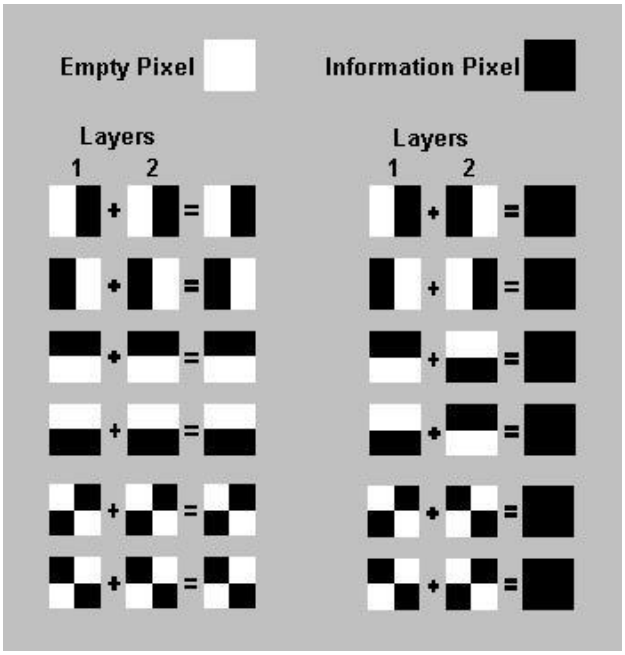
II. RELATED WORK

A. Visual Cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Either transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.

In the table below, we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.



We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed.
These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.
If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result.

B. OCR

Optical character reader,**(OCR**) isthe mechanical or electronic conversion of images of typed, handwritten or printedtext into machine-encoded text, whether from a scanned document, a photo of a document, a scene-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, bankstatements, 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.

1. OCR text works well with printed text only and not with handwritten text. Handwriting needs to be learnt by the computer.
2. OCR systems are expensive
3. Images produced by scanner consume lot of memory space.
4. Images lose some quality during scanning and digitizing process.
5. Quality of the final image depends on the quality of the original image.
6. All the documents need to be checked over carefully and then manually corrected.

Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

Tesseract is anoptical character recognitionengine for various operating systems.[3]It is free software, released under the Apache License, Version 2.0 and development has been sponsored by Google since 2006.
In 2006, Tesseract was considered one of the most accurate open-source OCR engines then available.

II. ENHANCED PASSWORD PROCESSING MECHANISM

Since the server identifies a user for user authentication, it explains the authentication though proposed password scheme based on VC and OCR.

A. Proposed System

Before user authentication, user inputs the ID and password on device where 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. Then the device generates the first shared image based on VC, these images are determined by pseudorandom generator with SEED which has password and ID as salts. After developing the first shared image the device sends the ID and the image to the server instead of password. The user can save or delete the image after sending it to the server. Once the server saves the data that is sent by the user the registration process is completed. This clearly represents that the server does not know aboutthe password until the second shared image is overlapped with the first. Proposed password processing scheme is as follows:

1) The user provides ID and password as input.
2) The device of user creates an original image based on white background and black character. If the original image exists in the device then there is no need to create the original image again.
3) If the device does not possess the first shared image it can possess the second shared image referred to the original 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 3 (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.

B. 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. 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. Enhanced password processing scheme has certain difference when compared to traditional hash based scheme. In this scheme VC is used instead of hash basedtext, even though the input value is password but the output value is user's ID as in traditional scheme. At last for authentication user sends only one image to the server having ID and password.

There are certain advantages based on these features:

1. Prevents cyber-attack using vulnerable points of hash function.
2. Lower computational cost.
3. Supporting privacy of users.

By using VC random pattern number per pixels are generated for encryption. Generation random number has lower computational complexity than hash function because a pseudorandom number is obtained just by repeating exclusive-or (XOR).

This scheme is mostly used to prevent cyber-attack such as brute force attack and dictionary attack as that often occurs in hash based scheme. . Even though the attacker extorts saved image, it is impossible for the attacker to acquire any information about original password or rule to array subpixels. Even if the attackers knew that it is made of certain shapes but hey cannot identify what it is and how the patterns are arranged.

Lastly, this scheme supports the privacy of user. The server saves only one shared image instead of the password and receives another shared image not to expose ID from user. As a result, no information of user such as ID or password is revealed in each shared image.

III. CONCLUSION

Most of the users make use of same and short length passwords for multiple accounts by this password management is affected which leads to cyber-attacks. We suggested a distinctive method different from conventional password scheme. It is based on encoded images by VC with a SEED number and OCR and more strong protection from cyber-attacks. We evaluated security aspect on attacks, computational cost and privacy. Our proposal is light weight and more secure in the aspect that hashed values of important information are not stored in the system. The combination of visual cryptography provides a better security during communication as there is no much difference observed in the image quality the cover image. .Further this can be applied on colour images with the combination of techniques of visual cryptography methods and compared for quality. This method could be converted as application.

IV. REFERENCES

[1]. Ashutosh, & Sen, S. D. (2008). Visual Cryptography. 2008 International Conference on Advanced Computer Theory and Engineering.

[2]. Implementation of Visual Cryptography and OCR Techniques for Processing the Enhanced Password Mechanism Hamsalatha J, Alisha Erum K, Janani G S Dept of CSE Dr.TTIT, KGF

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

[4]. Dana Yang, Inshil Doh, Kijoon Chae, "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.

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

[6]. Holley, Rose, "How good can it get? Analysing and improving OCR accuracy in large scale historic newspaper digitisation programs," D-Lib Magazine

[7]. Nguyen, Thi Thu Trang, and Quang Uy 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.