Third International Conference on "Materials, Computing and Communication Technologies"
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Detecting Phishing Website Using Cryptography Halftone Technique

Mary Nisha D[1], Evelyn Tabitha E[1]

[1]Assistant Professor, Computer Science and Engineering, Pet Engineering College, Tamilnadu, India

Article Info
Volume 8, Issue 7
Page Number : 01-08

Publication Issue :
May-June-2022

Article History
Accepted: 01 June 2022
Published: 20 June 2022

ABSTRACT

A new scheme for user authentication is proposed using visual cryptography. Visual cryptography which allows visual information to be encrypted in such a way that decryption becomes the job of the person to decrypt via a sight reading. The existing technique uses Collaborative Visual Cryptography Schemes provides high contrast shares which provides quality images and deals with only text codes to hide information. The main disadvantage of the existing system will be, there was only 2 share technique followed, so that it may sometime fall backs to major security issue. The proposed technique uses Binary Halftone algorithm that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. Using proposed methodology we can create the shares using visual images instead of text codes. Also we provides n number of shares (ex. k1, k2, ... kn) that also enhance the security features. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

Keywords —Binary Halftone; n Shares Secret Image; Colloborative Visual Cryptography

I. INTRODUCTION

Online transactions are becoming very popular nowadays and this is behind numerous attacks. Phishing is known as a major security threat in these types of different attacks, and new , revolutionary ideas emerge with this in every second, so preventive mechanism should be so successful as well. Thus the protection is very strong in such cases and should not be easily tractable with ease of implementation. Many systems today are

just as reliable as the underlying device. Given that middleware design and technology has steadily improved, their detection is a difficult issue.

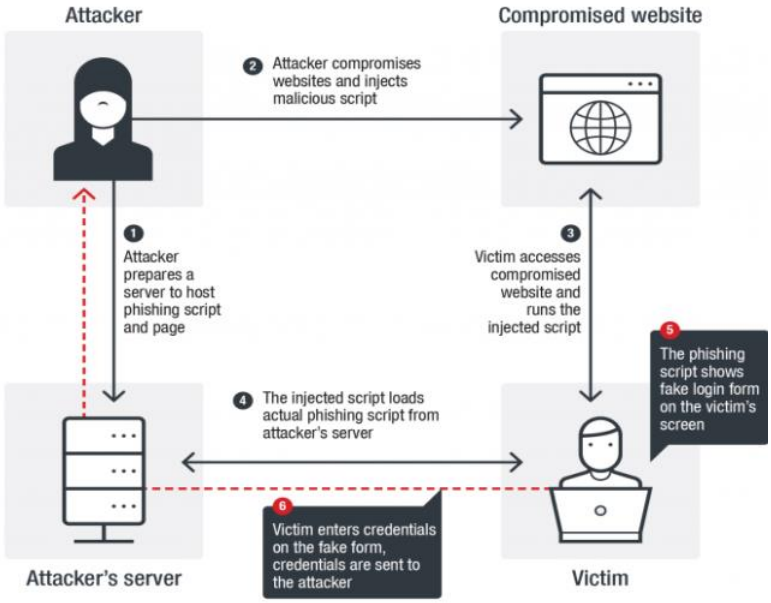

Fig 1.1: Anatomy of Phishing Attack

As a result, it is almost impossible to be sure whether or not a computer that is connected to the internet can be considered confidential and secure. Phishing scams also become an issue for e-commerce and online banking users as explained in Fig 1.1 Anatomy of Phishing Attack. The problem is how to manage applications where a high degree of security is needed. Phishing is a form of online identity theft aiming at stealing sensitive information from users such as online banking passwords and credit card information. Phishing scams have received extensive coverage in the press because the number and sophistication of such attacks has escalated.
One concept of phishing is given, as it is a criminal activity using techniques of social engineering. Phishers attempt to obtain confidential information fraudulently, such as passwords and credit card numbers, by masquerading an electronic message as a trusted individual or company. Another detailed phishing concept notes that it is "the act of sending an email to a user falsely pretending to be an established legitimate business in an attempt to trick the user into surrendering private information that will be used to steal identity." The conduct of identity theft with this obtained sensitive information has also become simpler with the use of technology and identity theft can be defined as "a crime in which the impostor obtains and uses key pieces of information such as social security and driver's license numbers for his or her own benefit."

KEY BASED VISUAL CRYPTOGRAPHY

It is based on the concept of keyless visual cryptography where keys are not involved, it is advantageous in term that Key generation and management is not required, it is simple, complexity of key based approaches is not involved. Based on this approach, a scheme was presented in aiming to achieve key safeguarding and secret image sharing. Mathematical calculations were used to generate an image acting as Key Image. The Key is generated from the secret image and some chosen securing images . To reconstruct the secret color image, the Key image and q securing images are used where q shown in the fig 2.

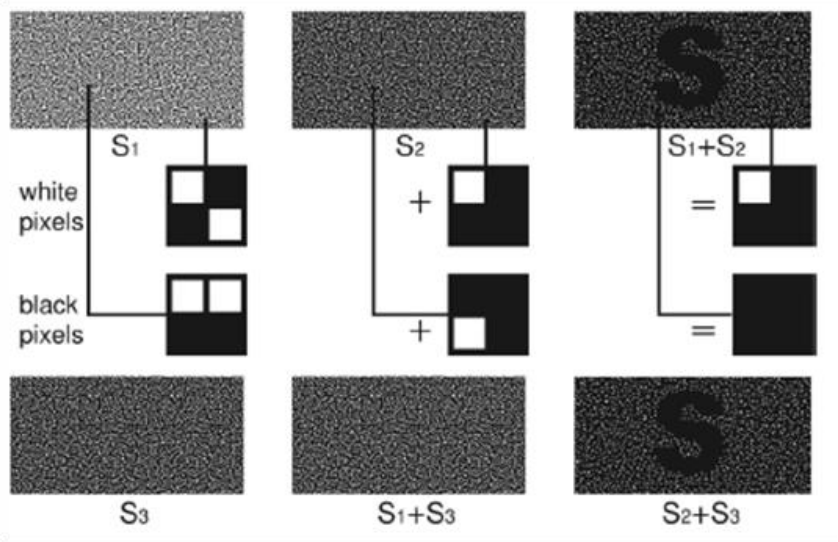

Fig 1.2: Visual Cryptography Scheme

ANTI PHISHING DETECTION

Anti phishing program may be one of the Visual Cryptography applications. Phishing websites seek to steal personal and confidential details including passwords , credit card numbers, pins, etc. By making identical websites to a real one where the customer submits his details, they trick customers. The work of solving this problem, using the technique of visual cryptography. By typing his user name, the customer can verify that this is the real website or not. The server sends out a copy from their database. In order to ensure that this is not phishing web page, the client will superimpose his own share with the one sent by the site and then the user may type the information.

II. LITERATURE SURVEY

In [1], For a group of n participants, a visual cryptography scheme is a method of encoding a hidden SI image into n shadow images called shares, where each participant in p receives one share. Some trained subsets of participants can recover the hidden image "visually," but other, prohibited, sets of participants have no knowledge (in a knowledge-theoretical sense) about SI. A "visual" recovery for an X⊆p set consists of xeroxing on transparencies and then stacking the shares given to the participants in X.

Without any knowledge of cryptography and without any cryptographic computation, participants in a qualified set X will be able to see the secret image. In this paper the authors proposed two techniques for generalized access structures to construct visual cryptography schemes. Also evaluated the visual cryptography schemes structure and prove boundaries on the scale of the shares allocated to the scheme participants.

Advantages

- Provides less processor usage in generating the shares

Drawbacks

- Loss in contrast of the reconstructed image
- All shares are inherently random patterns

In [2], Visual cryptography is a cryptographic technique that allows for the encryption of visual information (photos, text, etc.) in such a way that decryption is a mechanical process that does not require a machine. Moni Naor and Adi Shamir have been credited with one of the best-known methods, which they developed in 1994. We showed a visual secret sharing scheme where an image was broken up into n shares so that the image could only be decrypted by those with all n shares, while any n – 1 shares revealed no information about the original image. Every share was printed on a separate transparency, and the shares were overlaid for decryption. The original picture will show up when all n shares were overlaid. There are several generalizations of the basic scheme including visual cryptography with k-out-of-n. Using a similar concept, it is possible to use transparencies to enforce a one-time pad encryption, where one transparency is a shared random pad and another transparency serves as the cipher.

Advantages

- Output image is more contrast

Drawbacks

- Larger transparencies size
- Hard to align

In [3], It analyzes visual cryptography schemes in which black pixel reconstruction is perfect, that is, all the subpixels associated with a black pixel are black. For any value of k and n, where 2 = k = n, we provide a construction for (k, n)-threshold VCS that improves with respect to pixel expansion on the best known constructions. We also provide a VCS colored (2,n) threshold construction and a VCS colored (n, n) threshold construction. Both constructions improve with respect to the pixel expansion on the best known buildings. A variant form of secret sharing is visual cryptography (VC).

Advantages

- Enhanced RGB based Visual Cryptography

Drawbacks

- Decryption process is lossy
- Uses Error Prediction

III. SYSTEM MODEL

By adding the Digital Halftoning techniques, Halftone Visual Cryptography improves the Visual Cryptography. Digital halftoning means using computer algorithms to decide how to place the dots. A hidden picture can be encoded into halftone shares taking meaningful visual information in the visual secret sharing scheme by generating complete allocation of random pixels. HVC construction methods in this proposed system improved by generating n number of shares. If all the secret shares are to be overlaid, they will impose the one secret image.

Phishing is an attempt by an individual or a group to thieve personal confidential information from unsuspecting victims for identity theft, financial gain and other fraudulent activities, such as passwords , credit card details etc. The proposed new solution to solving the phishing problem is called "Visual Cryptography on the Anti Phishing System" Here an authentication based on the picture is used using Visual Cryptography (VC). The use of visual cryptography is explored to protect image captcha privacy by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can

only be exposed when both are accessible simultaneously; the individual sheet images do not disclose the original image captcha identity. When the actual captcha image is disclosed to the user it will be used as the password.

Objective

- Main scope of this project is to protect the online users from phishing sites using visual cryptography.
- Anti phishing framework based on visual cryptography to solve the problem of phishing.
- Visual Cryptography is used to decompose an image into N number of shares.
- Secret Image is revealed by combining the appropriate image shares.
- Finally it helps in preventing the password and other confidential information from the phishing websites.

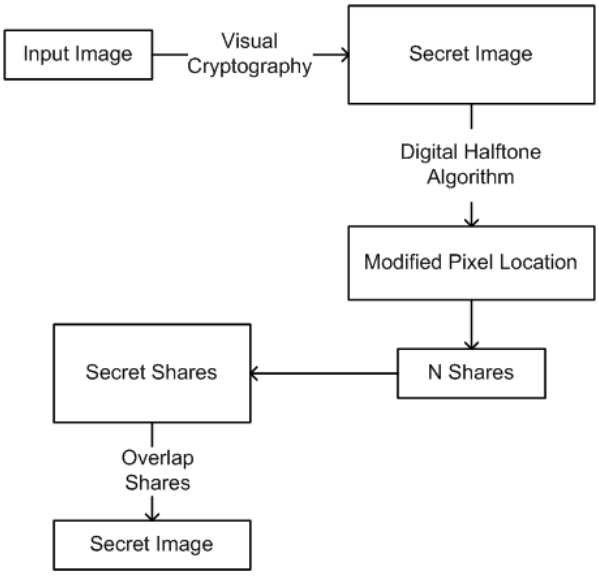

Fig 3.1: Secret Image Generation

Modules

A secret image can be encoded into halftone shares taking meaningful visual information in the visual secret sharing scheme by producing complete allocation of random pixels. HVC construction methods in this proposed system improved by producing n number of shares. If all the secret shares are to be overlaid, they will impose the one secret image.

- Visual Cryptography Share Generation
- Share Overlay
- Halftoning Technique
- Antiphishing Detection

1. Visual Cryptograph Share Generation

In this module the user is asked for an image for the secure website at the time of registration. The image is split into two shares, thus holding one of the shares with the user, and holding the other share in the file.

2. Share Overlay

In this phase the user will be prompted for the username (Login ID) first. The user is then asked to enter his share that is kept with him. This share is sent to the server where the share and share of the user that is stored

in the website's database is stacked together for each user to generate the captcha image. The captcha picture reveals to the recipient.

3. Halftoning Technique

Patterning is the simplest of the three digital halftoning image generating techniques. It generates an image of greater spatial resolution than the image source. The output image's number of halftone cells is equal to the source image's number of pixels. If pixels are below the threshold, or one (white) otherwise, they can be converted to zero (black). With the continuous-tone (high-resolution) images taking pixel values from 0 to 1 inclusive, a M pixel mask has thresholds of 0,1 / M, 2 / M, ..., 2 / M, ... ,1, supporting levels of M+1 intensity.

4. Antiphishing Detection

To display the secret image the end user must enter the share. Using the username and image shares created by stacking two shares one can test whether the website is a secure website or a phishing website and also verify whether the user is a human user or not. A phishing hyperlink detection approach is proposed using the rule-based system formed by genetic algorithm, which can be used as part of an anti-phishing enterprise solution. A legitimate webpage owner may use this approach to look for suspicious hyperlinks on the web. Genetic algorithm is used in this approach to create rules that are used to distinguish phishing link from legitimate link.

Algorithm

These four shares are then decoded using Manchester decoding algorithm. after decoding these four shares are again combined into two shares as share1 and 2, share 3 and 4 so that they can be merged to give two shares.

```
        Input: RGB Image
        Output: 2 Binary Secret Image
1:      counter1 ← 1
2:      counter2 ← 1
3:      for i = 1 to 2n do
4:          for j = 1 to n do
5:              w ← wh(i, 1 to j)
6:              if w is an even number then
7:                  Cn0 = Cn (i, 1 to j)
8:                  counter1 = counter1 + 1
9:              else
10                 Cn1 = Cn(i, 1 to j)
11:                counter2 = counter2 + 1
12:             end if
13:         end for
14:     end for
15:     Return Cn0, Cn1
```

IV. RESULT

The image 'tiger.png' which needs to be secretly transmitted has dimensions 600x400. It is shown in figure 4.1. The image is resized to 600x400 so that it has even number of rows.

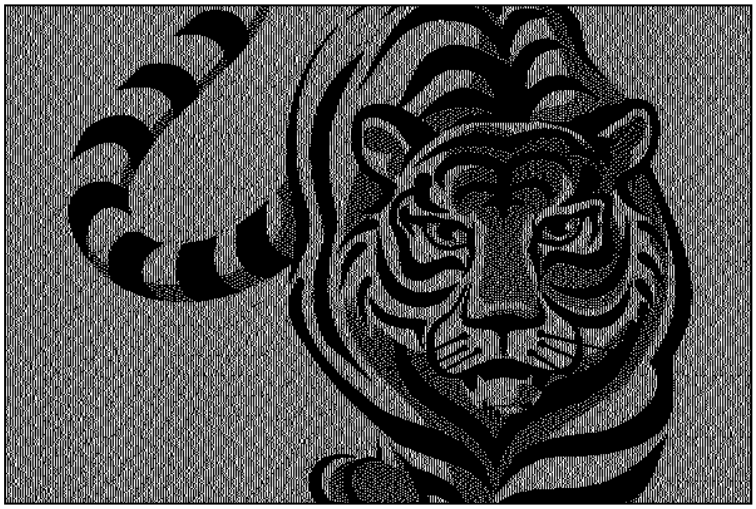

Fig 4.1: Overlayed Secret Shares

i. Comparision of Visual Cryptography Schemes

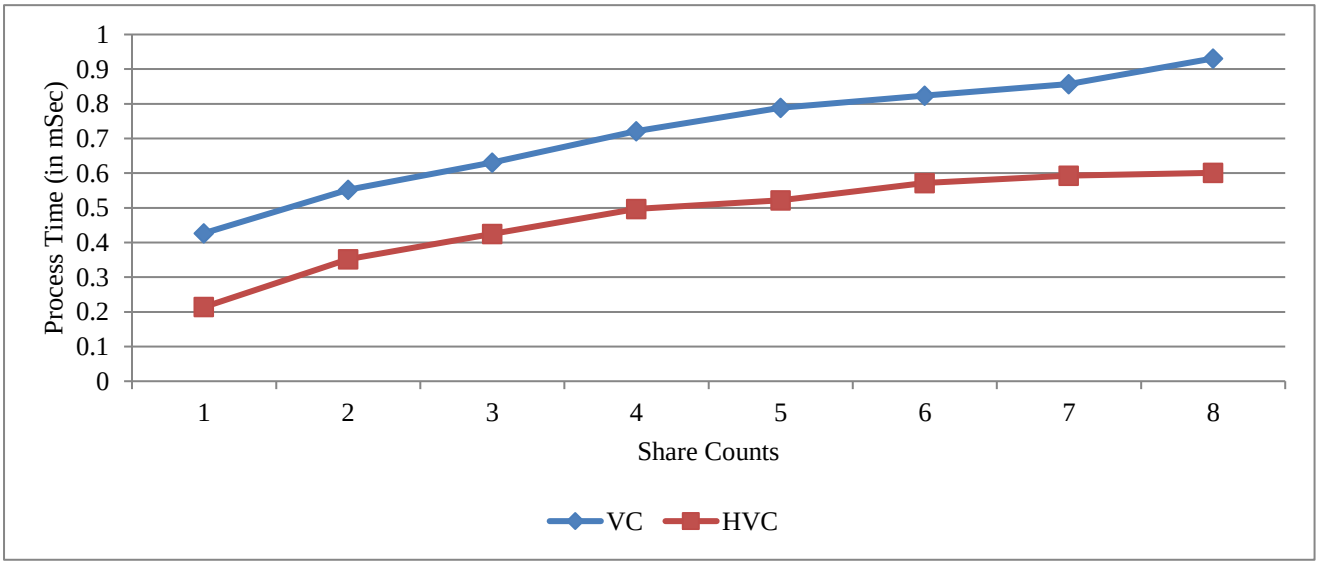

Fig 4.2: Comparison of Visual Cryptography Schemes

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed posuere tellus nunc, et condimentum elit auctor nec.

V. FUTURE SCOPE

Here modular arithmetic can be introduced in the future to make the more effective process. And it can give better quality images It as input to improve its efficiency.

VI. CONCLUSION

Phishing attacks are so common at the moment as it can target internationally, capture and store sensitive information about the user. Many who are indirectly interested in the phishing process use this knowledge for the attackers. Both phishing websites and human users can be easily identified using our proposed "Visual Cryptography based Anti-phishing Framework". The methodology proposed retains confidential user information using 8 layers of security. The first layer tests whether the website is a genuine / secure website, or a website for phishing. If the website is a phishing website, then in that situation the phishing website can not display the captcha image for that particular user due to the fact that the captcha image is generated by the stacking of N shares, all the shares are available with the user as well as the actual website database. However the server will provide N/2 shares and the remaining N/2 shares will be prompted by the user. The secret image will be revealed when all of the N shares are overlayed.

VII. REFERENCES

[1]. Ateniese. G, Blundo. C, De Santis. A, and Stinson. D. R, “Visual Cryptography for general access structures,” Inf. Comput., vol. 129, no.2, pp.86106, 1996.

[2]. Blundo.C, De Bonis.A, and De Santis.A, “Improved schemes for visual cryptography,” Designs, Codes, Cryptogr., vol. 24, no. 3, pp. 255–278, 2001.

[3]. Blundo. C, Cimato. S, and De Santis. A, “Visual cryptography schemes with optimal pixel expansion,” Theoretical Comput. Sci., vol. 369, nos. 1– 3, pp. 169–182, 2006.

[4]. Bose. M and Mukerjee. R, “Optimal (k, n) visual cryptographic schemes for general k,” Designs, Codes, Cryptogr., vol. 55, no. 1, pp. 19–35, 2010.

[5]. Droste. S, “New results on visual cryptography,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 1109. Berlin, Germany: Springer-Verlag, 1996, pp. 401–415.

[6]. Eisen. P. A and Stinson. D.R, “Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels,” Designs, Codes, Cryptography, vol. 25, no. 1, pp. 15–61, 2002.

[7]. Shyu. S. J, “Experimental study of visual cryptographic schemes for General acces structures.” [Online]. Available: http://www.csie.mcu.edu.tw/~sjshyu/public/gvcs_lp/es_gvcs.html, http://dl.dropboxusercontent.com/u/62383867/~sjshyu/public/gvcs_lp/es_gv cs.htm, accessed Oct. 2013.

[8]. Shyu. S. J and Chen. M. C, “Optimum pixel expansions for thresholdvisual secret sharing schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no.3, pp. 960–969, Sep. 2011.

[9]. Tzeng.W.G and Hu.C.M, “A new approach for visual cryptography,” Designs, Codes, Cryptogr., vol. 27, no. 3, pp.207–227, 2002.