ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

# An Anti-Phishing Framework Based On Visual Cryptography

Razeem Musthafa V[1], Subarna Panda[2]

MCA Student, Department of Computer Science & Information Technology, Jain University, Bangalore, India[1]

M.Tech, Assistant Professor, Department of Computer Science & Information Technology, Jain University, Bangalore, India[2]

**ABSTRACT:** Voting system using Visual Cryptography (VC) aims to provide a facility to cast vote for corporate company elections. It will allow to cast vote from any from any part of the world. A fully confidential election is held applying appropriate security measures to allow the voter to vote. A voter is able to vote for any particular candidate only if he sign in to the system by entering the correct password which will be an image captcha which will be generated by merging the two shares of images using VC scheme. Election master will send share 1 to voter e-mail id before election and share 2 will be available in the voting system for his sign in during election. Voter will get his password to cast his vote by combining share 1 and share 2 using VC. Phishing is an attempt by an individual or a group of individual to get confidential personal information by acting as valid entity. Attackers will create fake websites which appears to be very similar to the original site are being hosted to achieve this. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges such as stakeholder involvement and observation of the process. A new approach is proposed for voting system to prevent such attacks.

**KEYWORDS**: Authentication, visual cryptography, image captcha, phishing, online voting

## I. INTRODUCTION

phishing is identified as a major security threat in internet and lot innovative phishing ideas are rising with this in every seconds. So the preventive mechanisms have to be so effective. Thus the security in these cases should be very high and should not be easily tractable.

Today, most of applications are only secure in their underlying system. Since the steadily improvement in the design and technology of middleware, their detection is also a problem. As a result, the computer that is connected to internet is nearly impossible to predict that whether a computer is considered trustworthy and secure or not. online banking and e-commerce users are mostly targeted by the phishing attackers. How to handle applications that require a high level of security is the major question.

Phishing is a form of online identity theft that aims to steal sensitive confidential information such as username, applications passwords and sensitive information from users.

One of the best the way to protect data is cryptography. It is the way of sending and receiving messages in encrypted format. that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

## II. RELATED WORKS

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, and installation of key loggers and screen captures.Emails are one of the most common techniques for phishing, due to its simplicity, ease of use and wide reach.
One of the best techniques to protect data is cryptography (data encryption/decryption). It is the art of sending and receiving encrypted messages which can be decrypted only by the end user. Encryption and decryption are computed by using mathematical algorithms in such a way that only intended recipient can decrypt and read the message Visual cryptography schemes were separately proposed by Shamir [1] and Blakley [2], their original intention was to safeguard cryptographic keys from loss. These schemes also have been widely used in the construction of several types of cryptographic protocols [3]. They have used these techniques many applications in different areas such as opening a bank vault, access control, opening a safety deposit box or even launching of missiles. Visual cryptography which is based on segment is suggested by Borchert [4] can be used only to encrypt the messages which are containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al., [5] can be applicable only for printed images or text. An iterative VC method proposed by Monoth et al., [6] is computationally complex as the encoded shares are further encoded into number of sub-shares iteratively. Likewise, a technique proposed by Kim et al., [7] also draw backs due to computational complexity, though it avoids dithering of the pixels. Most of the previous research work on Visual Cryptography focused on improving two parameters: pixel contrast and expansion [8]. In these cases, all participants who hold shares are assumed to be trusted user, that is, they will not present false or fake shares during the phase of the secret image recovering. Thus, the image shown on the arranging the shares is considered as the real secrete image. But, this may not be true always. Visual Cryptography Scheme is a cryptographic technique/methodology that allows for the encryption of visual information in which decryption can be performed using only the human visual system.
Ren-junn Hwang has proposed a technique which makes use of watermark method [9] to save digital image copyright ownership using visual cryptography. But here, there is the difficulty of finding the pixels having the watermark pattern.Divya James and Mintu Philip [10] have given an anti-phishing framework which uses visual cryptography for detecting the phishing websites. In this, Image captcha validation scheme is used. There are two phases in this paper. One is for registration while other is for login.

## III. CURRENT METHODOLOGY

In the current methodolody, as shown in the Figure 1, when the user wants to access his confidential information in online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters his information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques. There is no such information that cannot be directly obtained from the user at the time of his login input.

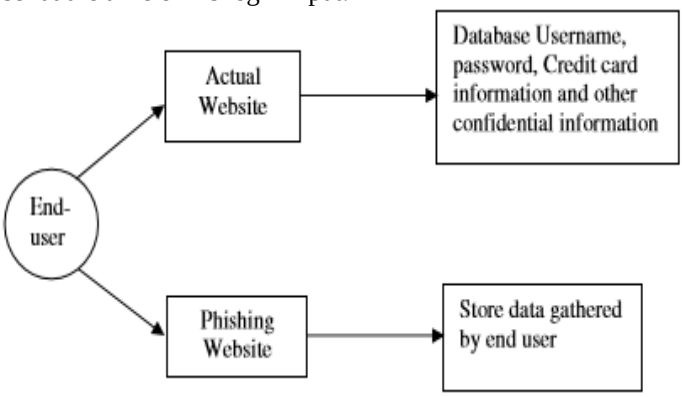


Fig.1 current scenario

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

## IV. PROPOSED METHODOLOGY

In order to prevent from phishing attack, we are proposing a new methodology to detect the phishing website. The proposed methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography It will allow only authenticated users to cast vote.

**Advantages of the Proposed System**

Since Visual Cryptography Technique is used, user can able to find out whether he is in phishing site or original site easily.

- Password Image is divided into two shares and one share is send to votes authorized email id and another share is kept in server for safety.
- Proposed online voting system is very effective and it will useful for voters and organization in many ways and it will reduce the cost and time.

**System Functional Diagram**

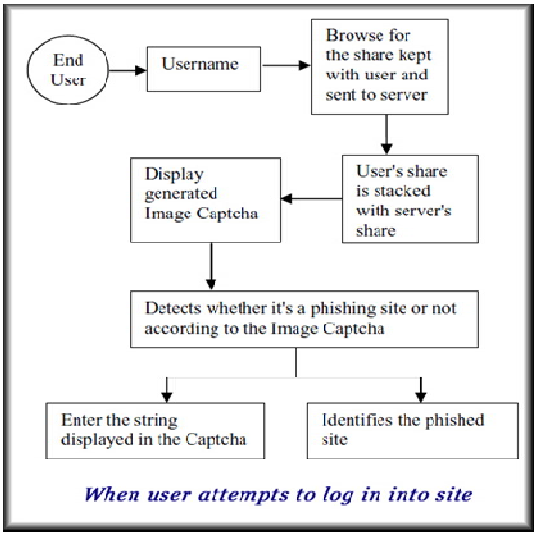


Fig 2.System Functional Diagram

## V. WORKING METHODOLOGY

**VISUAL CRYPTOGRAPHY:**

Visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images and data without any cryptographic computations as shown in Figure 3.


Fig.3 visual cryptography

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

**International Journal of Innovative Research in Computer and Communication Engineering**

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 6, Issue 4, April 2018**

The system is web based application so that it can be accessed by any authorized person anywhere in the world through internet. Firstly, the textual password image is converted into black and white images based on RGB (red, green, blue) values.

For Each pixel in the monochrome image, the pixel will be divided into 4 sub pixels depending on the colour of the pixel and thus, increasing the size of whole image. There are 6 possible permutations to divide a pixel into 4 sub pixels (2 black and 2 white) as shown in the Figure 4.

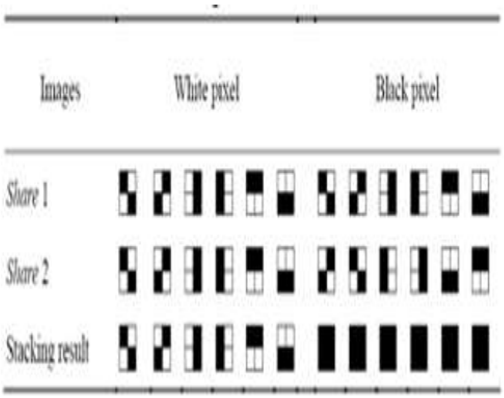


Fig 4. possible combinations of sub pixels

If the colour of the pixel is white, then one of the possible sub-pixels is as shown in the Figure 5.

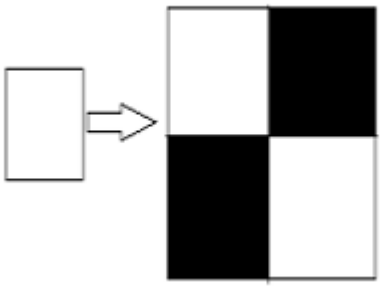

Fig 5. white pixel

If the colour of the pixel is black, the sub pixel is as shown in the Fig 6.

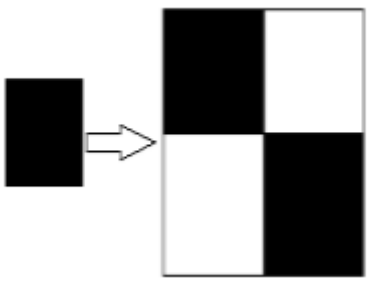

Fig 6. black pixel

White pixel is called as an empty pixel and black pixel is called as the information pixel. If the source pixel in the monochrome image is black, then the sub pixels in share 1 and share2 will be inverted as shown in the Figure 7.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

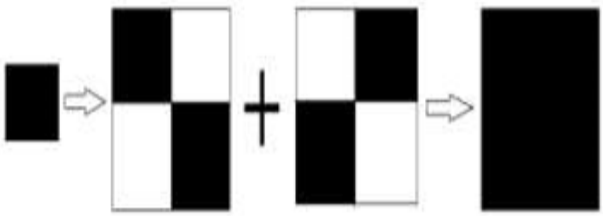

Fig 7. merging of black pixel

If the source pixel in the monochrome image is white, then the sub pixels in the share1 and share 2 will be identical as shown in the Figure 7.

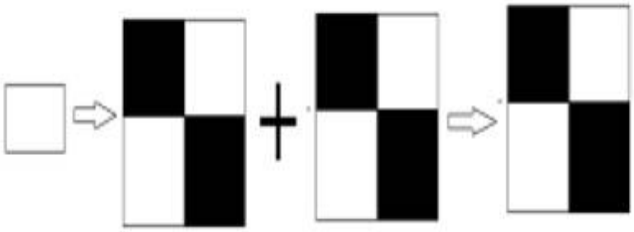

Fig 7. merging of white pixel

## VI. RESULT

The result of the overall process after merging the two shares is an image containing the textual password which will be represented by information pixels (black pixels) as shown in the Figure 8.

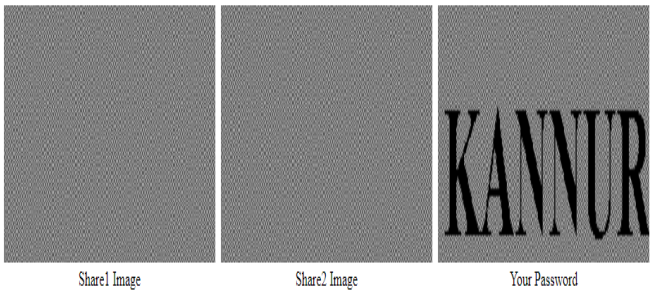


Fig 8. Password

Here “Kannur” is the password that is on written on the image captcha. User will be knowing his/her password only at the time of login that is when user share of image and other share of image are matched. if the two image share are wrongly matched then output image will be a blur image

## VII. FUTURE ENHANCEMENT

There are various problems left unsolved. Some of them like the following, may be the core issues for future work:

- The quality of the recovered secret images is not perfect. In future, the improvement of the image quality without any additional computation can be considered.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

- Visual cryptography scheme can be applied to different digital applications for tamperproof and reliable transmission of information with low computational capable devices like mobile phone, digital camera etc.

## VIII. CONCLUSION

Internet-based voting offers many benefits including low cost and increased voter participation. Voting systems must consider security and human factors carefully, and in particular make sure that they provide voters with reliable and intuitive indications of the validity of the voting process. The system we propose uses visual cryptography to provide mutual authentication for voters and election servers. The user is only able to login if he gets the two correct shares of password.one share of password is sent to users Email id and second share is saved in the server.so to perform a phishing attack the attacker has to attack both user client and server at same time. It is not possible. Thus securing our voting system from phishing attack.

## REFERENCES

[1] A. Shamir," How to Share a Secret?" Communication ACM, vol. 22, 1979, pp. 612-613.
[2] G. R. Blakley," Safeguarding Cryptographic Keys." Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.
[3] A. Menezes, P. Van Oorschot and S. Vanstone, "Handbook of Applied Cryptography". CRC Press, Boca Raton, FL, 1997.
[4] B. Borchert, "Segment Based Visual Cryptography", WSI Press, Germany, 2007.
[5] W-Q Yan, D. Jin and M. S. Kanakanahalli," Visual Cryptography for Print and Scan Applications." IEEE Transactions, ISCAS-2004, pp.572-575.
[6] T. Monoth and A. P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion," in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 4143.
[7] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, "An Innocuous Visual Cryptography Scheme," in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
[8] C. Blundo and A. De Santis." On the contrast in Visual Cryptography Schemes," in Journal on Cryptography, vol. 12, 1999, pp. 261-289.
[9]. Ren-Junn Hwang," A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).
[10]. Divya James, Mintu Philip," A novel Anti-phishing framework based on visual cryptography", IEEE 2012.
[11]http://www.phishing.org
[12] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Anti-Phishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.