International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

ONLINE PAYMENT SYSTEM USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

S.Shanmuga Priya,
Department of Computer Science Engineering,
VeltechMultitechDr.RR Dr.SR Engineering College,
Chennai,India.

V.Priyadharshini,
Department of Computer Science Engineering,
VeltechMultitechDr.RR Dr.SR Engineering College,
Chennai,India.

Abstract: With the rapid growth of Online Payment transactions, Debit or Credit card fraud andpersonal information security are major concerns for customers. This paper presents a new approach for providing additional security for fund transfer during online payment thereby safeguarding customer data. A combination of image based steganography and visual cryptography is proposed.

Keywords: Information security; Steganography; Visual Cryptography

I. INTRODUCTION

Online payment is the exchange of information via the Internet to make banking transactions.Identity theft [1] and phishing [2] are the common dangers of online payment. Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc., from unsuspecting victims for identity theft, financial gain and other fraudulent activities.Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information. The main objective of this project is to safeguard customer data and prevent phishing attacks during online payment by using visual cryptography and steganography.A cryptographic technique based on visual secret sharing is used for image encryption. A secret image is encrypted in shares, which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more gives the original secret image. Once the original image is revealed to the user it can be used as a password.The method proposed is specifically for online banking but can easily be extended for E-Commerce.

II. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the art of hiding of a message withinanother so that hidden message is indistinguishable.[3][4] The keyconcept behind steganography is that message to be transmitted is not detectable to casual eye. Digital images are the most popular coverobject for steganography because of their suitable size in comparison to other digital media and of their massive presence on the internet, they can afford to carry large amount of secret data embedded into them. Digital images often have a large amount of redundant data and for this reason it is possible to hide secret message inside image file.

In image steganography, it is necessary to ensure that the changes in the stegano-image due to the embedding of data are visually and statistically negligible for making the steganographic method difficult to detect. The most effective way of hiding data in an image is to change the image content i.e. the colours of the pixels. Such technique, although crude, hides a large volume of information inside the image. The idea is to embed the data into a significantly larger object so that the changes are undetectable.

Visual cryptography 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 MoniNaor and Adi Shamir, who developed it in 1994.[5] 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 but this paper uses (2,2) visual secret sharing case.

III. (2,2) VISUAL SECRET SHARING

In this scheme we have a secret image which is encoded into 2 shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if the 2 shares are stacked on top of one another the secret image becomes decipherable by the human eye.

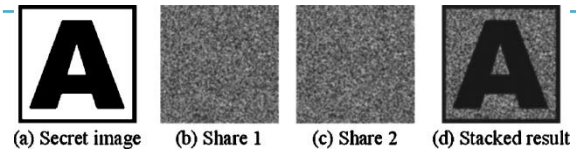
Every pixel from the secret image is encoded into multiple subpixels in each share image using a matrix to determine the color of the pixels. There is a simple algorithm for visual cryptography that creates 2 encrypted images from an original unencrypted image.

The algorithm is as follows:

1. Create an image of random pixels the same size and shape as the original image.
2. Create a second image whose pixels are the exclusive-or (XOR) of the first image and the original image.

This will image will look random.The two apparently random images can now be combined with XOR to re-create the original image.

IJCRCST © 2017 | All Rights Reserved



(a) Secret image (b) Share 1 (c) Share 2 (d) Stacked result

IV. EXISTING SYSTEM

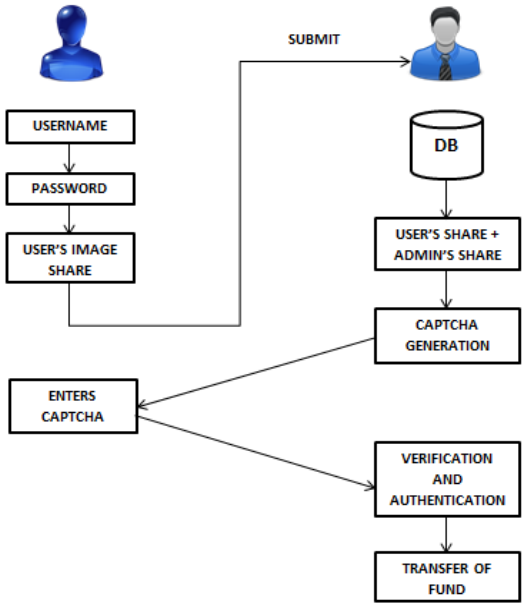
- In existing system, in order to perform user authentication, a basic text type of password is used.
- After being authorized the user will have to enter sensitive information on the bank's website to perform transactions.
- Unsuspecting users may enter these sensitive details on a different hoax website that imitates the looks of the bank's website.

V. DISADVANTAGES

- In the existing system only text information is used as password, which may be vulnerable to attacks.
- The existing system does not provide a friendly environment to encrypt or decrypt the data.
- Existing system is prone to phishing attacks.

VI. PROPOSED SYSTEM

In the proposed system, an additional layer of security is projected. A combined application of image based steganography and visual cryptography (VC) technique is used. At the time of user registration a secret image is taken. This image is divided into two shares using the (2,2) visual cryptography technique. One share is given to the customer and the other share is stored in the bank's database. During authentication, both shares are required to reveal the original image.



The image which is given to the customer may be vulnerable to attack. To prevent this, the image is computed as a stegano-image before being made available for download by the customer. Thus any attempt by hackers to access this image will be nullified. At the time of login, the user is required to upload their share of the image, along with their text password and other details. This share will be decoded at the bank's side and the corresponding second half will be merged with it. This will reveal the original image. Once this is verified the bank authenticates the user and fund transactions can take place.

VII. ADVANTAGES

- Decryption algorithm is not required (since human visual system is used), therefore computational complexity is reduced.
- Since both the shares are required to decrypt the image, hoax websites cannot steal information.

VIII. CONCLUSION

In this project, a payment system for online banking is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identity theft and customer data security. In comparison to other banking applications wheresteganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online transaction as well as physical banking. In the future the proposed system can be extended to E-Commerce with focus area on payment during online shopping, making it an alternative secure payment portal with a trusted third party certificate authority. This will safeguard user data from misuse at the merchant side.

REFERENCES

[1]. Javelin Strategy & Research, "2013 Identify Fraud Report".
[2]. Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013".
[3]. Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489,2011.
[4]. J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2012.
[5]. Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.