Operative Compensation System using Steganography plus Ocular Cryptography

P.G.K.Shobha
M-Tech Student
Department of CSE,
Bharath Institute of Technology And Science for Woman
Mangalpally Village, Ibrahimpatnam Mandal,
Telangana 501510, India.

NVN Sowjanya, MTech
Guide
Department of CSE,
Bharath Institute of Technology And Science for Woman
Mangalpally Village, Ibrahimpatnam Mandal,
Telangana 501510, India.

Abstract: *This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. A cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an un trusted communication channel. Only combining the k shares or more give the original secret image. 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 The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.*

Keywords—Information security; Steganography; Visual Cryptography; Online shopping

INTRODUCTION : Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant.

However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others. In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.

Existing system:-

➢ The existing system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.

➢ The existing system does not provide a friendly environment to encrypt or decrypt the data (images).

➢ The existing visual cryptography schemes that are used for data hiding have a security hole in the encrypted Share file.

➢ Here an image based authentication using Visual Cryptography is implemented.

Disadvantages:

➢ Does not provide a friendly environment to encrypt or decrypt the data (images).

➢ Supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.

➢ The most critical measurements to evaluate the effectiveness of a VCS.

Proposed System:

➢ Proposed System,Visual Cryptography (VC), technique based on visual secret sharing used for image encryption.

➢ Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant.

➢ In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant.

➢ VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system.

➢ For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

➢ Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

➢ Cryptographic technique:(2, 2)- Threshold VCS scheme,(n, n) -Threshold VCS scheme, (k, n) Threshold VCS scheme are used in this proposed system.

➢ **Advantages:**

➢ Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography.

➢ It prevents password and other confidential information from the phishing websites.

➢ For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

CONCLUSIONS:

In this paper, a payment system for online shopping 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 identify theft and customer data security. In comparison to other banking application which uses steganography 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 shopping as well as physical banking.

REFERENCES

[1] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.

[2] Javelin Strategy & Research, "2013 Identify Fraud Report," ttps://www.javelinstrategy.com/brochure/276.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

[4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.

[5] 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, 2003.

[6] Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.

[7] Sandhya.J & G.Hussainbabu, Secure Data Transmission Using Cryptography and Steganography, IJMETMR, Volume No: 1, Issue No: 11, http://www.ijmetmr.com/olnovember2014/SandhyaJ-GHussainbabu-57.pdf

[8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.

[9] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," PurdueUniversity, Cerias Tech Report 2004—2013.

[10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.