© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Review - Transaction Security Using Steganography and Visual Cryptography

Choudhari Amar, Shaikh Sultanhusen, Ghadge Vashista, Prof. Sonawane V. D, Prof. Naved Raza

Al-Ameen College of Engineering, Koregaon Bhima, Savitribai Phule Pune University, Pune, India

ABSTRACT

The usage of Internet banking has grown in leaps and bounds because of its appliance. The privacy and Information confidentiality is one of the richest invades to the users of OnlineBanking Systems. The issue with Online banking applications is that they need to send the confidential contents such as Personal Identification Number (PIN), One Time Password (OTP) to the targeting customers in the form of plaintext, which is insecure. The solvent to the above consequences requires a software application that holds proficient encryption procedures. Toimprove the security of the content that is transmitted over the internet, the proposed technique introduce a Dual Enciphering Mechanism (DEM) which includes more than one cryptographicscheme for cipher text creation, which assures the secured transmission over the network environment and the application is developed in Java language as a secured dual encipheringintrigue (SDEI). In this nominated overture the confidential banking content such as personal identification number (PIN) is enciphered using Huffmann compression technique, which inturn subjected to symmetric encryption procedure and the key for the compression scheme is taken in the form of image, which is then transmitted in the form of image shares using the idea ofvisual cryptography. The content at the receiver end is submitted to deciphering process, which needs the symmetric crypto scheme key to get the intermediate code which in turn needs theimage shares to regenerate the original plain text. Hence through the proposed scheme the security issues such as 'meet in the middle attacks' and 'anonymous hacking' would be reduced and from the experimental results it is identified that the proposed is known as enciphering or encryption and the unreadable format is said to be as cipher text or ciphers.

Keywords: Internet Banking, Huffmann Coding, Decryption, Double Encryption, Visual Cryptography

I. INTRODUCTION

A high-speed prosperity in E-Commerce market has been witnessed in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks. The main motive of this project is to provide high level security in E-Commerce applications and online shopping. This project minimizes detailed information sharing between consumer and online merchant but enable successful fund transfer thereby safeguarding consumer information and preventing misuse of information at merchants side. This is achieved by the introduction of Central Certi_ed Authority (CA) and combined application of Steganography, Visual Cryptography and Digital Signature for this purpose Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, _lling 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 someones identity in the form of personal information and misusing 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 an illegitimate mechanism that employs both social

engineering and technical subterfuge to steal consumers personal identity data and _nancial account credentials. Payment Service, Financial and Retail Service are the most focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference 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 consumers account to merchants account thereby safeguarding consumer information and preventing misuse of information at merchant side.

The method proposed is speci_cally for E-Commerce but can easily be extended for online as well as physical banking. Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text , image , video , audio are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line , in open spaces , in word sequence . Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication .Visual Cryptography (VC), is a cryptographic technique based on visual secret sharing used for image encryption. The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: BPCS Steganography and Visual Cryptography for safe online shopping and consumer satisfaction.

II. METHODS AND MATERIAL

A. Literature Survey

In [1] Chaum D. and Antwerpen van H., "Undeniable signature," Advances in Cryptology – CRYPTO'90, Springer-Verlag, 1990, pp. 2 12-2 16.Digital signatures [DH]-unlike handwritten signatures and banknote printing-are easily copied exactly. This property can be advantageous for some uses, such as dissemination of announcements and public keys, where the more copies distributed the better. But it is unsuitable for many other applications. Consider electronic replacements for all the written or oral commitments that are to some extent personally or commercially sensitive. In such cases the proliferation of certified copies could facilitate improper uses like blackmail or industrial espionage. The recipient of such a commitment should of course be able to ensure that the issuer cannot later disavow it-but the recipient should also be unable to show the commitment to anyone else without the issuer'sconsent.Undeniable signatures are well suited to such applications. An undeniable signature, like a digital signature, is a number issued by a signer that depends on the signer's public key and the message signed. Unlike a digital signature, however, an undeniable signature cannot be verified without the signer's cooperation.

In [2] Delfs H. and Knebl H., Introduction to Cryptography: Principles and Applications, Springer, 2002.This paper attempt has been made to explain a fuzzy commitment scheme. In the conventional Commitment schemes, both committed string m and valid opening key are required to enable the sender to prove the commitment. However there could be many instances where the transmission involves noise or minor errors arising purely because of the factors over which neither the sender nor the receiver have any control. The fuzzy commitment scheme presented in this paper is to accept the opening key that is close to the original one in suitable distance metric, but not necessarily identical. The concept itself is illustrated with the help of simple situation.

B. Problem Statement

In the traditional system mentioned above, customer is not sure whether his

PIN No and CVV No is sent to the merchant. One still has to trust the merchant and its employees to use card information for their own motives. This representation doesnt show high level security. In these traditional systems, there is no additional non-functional requirement of phishing mechanism which can be harmful and might lead to employment of social engineering and technical subterfuge. Thus, in the proposed system mentioned later in this paper would ensure better security and satisfaction of consumer or other transaction stakeholders.

III. RESULTS AND DISCUSSION

Systems Architecture

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority(CA) and combined application of steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer. The process is shown in Fig.1.

In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method as mentioned in section IV. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography.

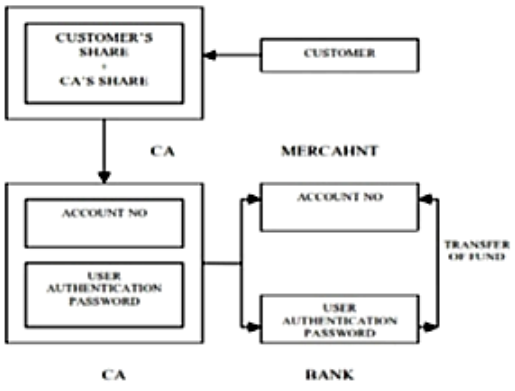

Figure 1: System Architecturen Daigram

Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

The problem is that CA does not know to which bank to forward the cover text obtained from combining two shares. It can be solved by appending 9 digit routing or transit number of bank with customer authentication information. If "text" is customer unique authentication password and account no of customer is 12345678910111, snapshot of cover text and account no is shown in Fig. 4 and resultant shares by the application of visual cryptography on snapshot are Fig. 5 and Fig. 6. Fig. 5 shows share 1 kept by customer and Fig. 6 shows share 2 kept by CA. Fig. 7 shows the result of combing share 1 and share 2.

Advantage:

- Proposed method minimizes customer information sent to the online merchant. So in case of a breach in merchant's database, customer doesn't get affected.
- Presence of a fourth party, CA, enhances customer's satisfaction and security further as more number of parties are involved in the process.
- Usage of steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy.
- Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.

- Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

IV. CONCLUSION

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 identity theft and customer data security. In comparison to other anking application which uses steganography and visual cryptography and 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.

V. FUTURE SCOPE

The payment system can also be extended to physical banking. Shares may contain customer image or signature in addition to customer authentication password. In the bank, customer submits its own share and customer physical signature is validated against the signature obtained by combining customer's share and CA's share along with validation of customer authentication password.

VI. REFERENCES

[1] Chaum D. and Antwerpen van H., "Undeniable signature," Advances in Cryptology- CRYPTO'90, Springer-Verlag, 1990, pp. 2 12-2 16.

[2] Delfs H. and Knebl H., Introduction to Cryptography: Principles and Applications, Springer, 2002.

[3] Diffie W. and Hellman M., "New directions in cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, pp. 644-654.

[4] EsraSatir, HakanIsik "A Huffman compression based text steganography method, " Multimed Tools Appl Springer Science 20 12.

[5] Hongjun Liu, Xingyuan Wang, "Triple-image encryption scheme based on one-time key stream generated by chaos and plain images," The Journal of Systems and Software 86 (2013) pp. 826- 834

[6] "Hybrid Steganography using Visual Cryptography and LSB Encryption Method " Gokul.M Final Year – M.Tech - CVIP Amrita VishwaVidhyapeetham University Coimbatore Umeshbabu R Final Year – M.Tech - CVIP Amrita VishwaVidhyapeetham University Coimbatore, International Journal of Computer Applications (0975 – 8887) Volume 59– No.14, December 2012

[7] Narpat Singh Shekhawat, Durga Prasad Sharma, "Cloud Computing Security through Cryptography for Banking Sector",Proceedings of the 5th National Conference; INDIACom-20 11.

[8] Askari, H.M. Heys, and C.R. Moloney "An Extended Visual Cryptography Scheme Without Pixel Expansion For Halftone Images" 2013 26th IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE).

[9] Schoenmakers B., "A simple publicly verifiable secret sharing scheme and its application to electronic voting," Advances in Cryptology - CRYPTO'99, SpringerVerlag, 1999, pp. 148-164.

[10] Souvik Roy and P. Venkateswaran ,"IEEE Online Payment System using Steganography and Visual Cryptography" 2014 IEEE.