International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Secured Transaction Using Steganography and Visual Cryptography

Vishal Yadav, Dr. J. N.Shinde
Department of Computer Engineering, Al-Ameen College of Engineering, Koregaon Bhima, Savitribai Phule Pune University, Pune, India

ABSTRACT

The utilization of Internet saving money has developed by a wide margin in light of its machine. The security and Information secrecy is one of the wealthiest attacks to the clients of Online Banking Systems. The issue with Online saving money applications is that they have to send the secret substance, for example, Personal Identification Number (PIN), One Time Password (OTP) to the focusing on clients as plaintext, which is shaky. The dissolvable to the above results requires a product application that holds capable encryption methods. To improve the security of the substance that is transmitted over the web, the proposed method present a Dual Enciphering Instrument (DEM) which in clues more than one cryptographic scheme for figure content creation, which guarantees the secured transmission over the system condition and the application is created in Java dialect as a secured double enciphering intrigue (SDEI). In this designated overture e the private managing an account substance, for example, individual recognizable proof number (PIN) is enciphered utilizing Huffmann pressure system, which thusly subjected to symmetric encryption system and the key for the pressure conspire is taken as image, which is at that point transmitted as picture shares utilizing the thought of visual cryptography. The substance at the collector end is submitted to unravelling process, which the symmetric crypto needs conspire key to get the middle code, which thus requires the image, offers to recover the first plain content. Henceforth through the proposed conspire the security issues, for example, 'compromise assaults' and 'mysterious hacking' would be lessened and from the trial comes about it is distinguished that the proposed is known as enciphering or encryption and the disjointed configuration is said to be as figure content or figures.

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

I. INTRODUCTION

A high-speed success in E Business advertises has been seen in late time all through the world. With regularly expanding prevalence of web based shopping, Debitor Credit card extortion and individual data security are real worries for clients, vendors furthermore, banks. The principle intention of this undertaking is to give abnormal state security in E Business applications and web based shopping. This task limits nitty gritty data sharing amongst shopper and on the web dealer yet empower fruitful store exchange there by protecting purchaser data and anticipating abuse of data at shippers side. This is accomplished by the presentation of Central Certied Specialist (CA) and joined utilization of Steganography, Visual Cryptography and Digital Mark for this reason Internet shopping is the recovery of item data by means of the Internet andissue of procurement arrange through electronic buy ask for, _lling of credit or check card data and delivery of item via mail arrange or home conveyance by couri er.Identity robbery and phishing are the regular perils of web based shopping.

Wholesale fraud is the taking of someones character as individual data and abusing that data for making buy and opening of financial balances or orchestrating cralter cards. In 2012 buyer data was abused for a normal of 48 days because of data fraud. Phishing is an ill-conceived system that utilizes both social building and specialized subterfuge to take shoppers individual character information and nancial account accreditations. Installment Service, Financial and Retail Administration are the most centered modern divisions of phishing assaults. Secure Socket Layer (SSL) encryption represses the impedance of purchaser data in travel between the buyer and the online dealer. In any case, one should at present put stock in dealer and its representatives not to utilize customer data for their claim buys and not to offer the informat particle to others.

In this paper, another strategy is proposed, that utilizations content based steganography and visual cryptography, which limits data sharing amongst customer and online trader yet empower fruitful reserve exchange from shoppers record to merchandise ants account along these lines defending buyer data and counteracting abuse of data at dealer side. The technique proposed is specially for E Business in any case, can without much of a stretch be reached out for online and physical managing an account. Steganography is the craft of covering up of a message inside another so that covered up message is undefined. The key idea behind steganography is that message to be transmitted isn't noticeable to easy-going eye. Content, picture, video , sound are utilized as a cover media for concealing information In steganography. In content steganography, message can be covered up by moving word and line, in open spaces , in word arrangement . Properties of a sentence, for example, number of words, number of characters, number of vowels, position of vowels in a word are additionally used to shroud mystery message.

The benefit of inclining toward content steganography over other steganography systems is its littler memory necessity and less complex correspondence. Visual Cryptography (VC), is a cryptographic method based on visual mystery sharing utilized for picture encryption. The primary thought process of the proposed framework endorsed in this paper is to deal with applications that require an abnormal state of security, for example, E - Trade applications, centre saving money and web managing an account.

This should be possible by utilizing combination of two applications: BPCS Steganography also, Visual Cryptography for safe web based shopping and purchaser fulfilment.

II. METHODS AND MATERIAL

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.

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 tradition all systems, there is no additionalnon 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

RRE'sHIGH-Level Architecture

In the proposed solution, information submitted by thecustomer 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 canbe in the form of account number related to the card used for shopping. The information will only validate receipt ofpayment from authentic customer. The process is shown in Fig.3.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.

Methodologies/Algorithm Details Algorithm:

Visual Cryptography is a special encryption technique to hide information in images, which divide secret image into multiple layers. Each layer holds some information. The receiver aligns the layers and the secret information is revealed by human vision without any complex computation. The proposed algorithm is for color image, that presents a system which takes four pictures as an input and generates three images which correspond to three of the four input pictures. The decoding requires only selecting some subset of these 3 images, making transparencies of them, and stacking them on top of each other, so the forth picture is reconstructed by printing the three output images onto transparencies and stacking them together. The reconstructed image achieved in same size with original secret image

Description

Every single pixel in secret image is splited into subpixels, that can still perceivethem as one pixel by Human vision system. The security of each share depends crucially on the color composition of the original secret image. To recovering a secret image, it is required that the cover image should at least be able to determine the shape or pattern of the original secret image, which is able to determine the boundary between two distinct color regions in the image. In this paper, for the problem of interest here, assuming an input 24-bit bitmap color image which each 3-byte sequence in thebitmap array represents the relative intensities of red, green, and blue, respectively for image sized 256256 RGB pixel for hiding Baboon image. In the following, the steps of the proposed algorithm and illustrate it using an example where the original secret image is a 24-bit color baboon image The encryption process consists of determining the arrangements of transparent subpixels on each

III. RESULTS AND DISCUSSION

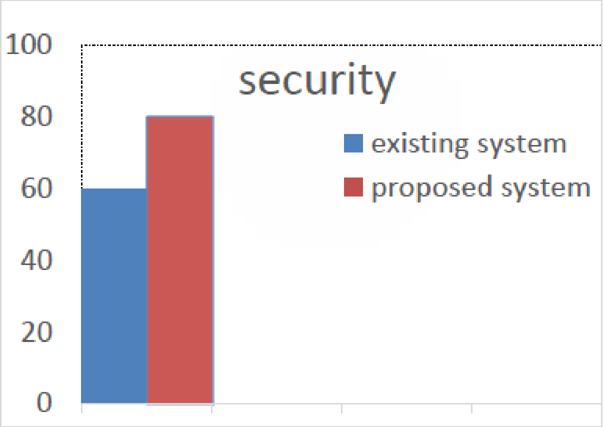

Figure 1. Resultant Proposed Output

In above graph show us that the security levels is increase and we will get much high security compering existing system. System performance as we tested system under diff condition and check for system security is much higher and so login time decreased and we require less login time by using this system.

IV. CONCLUSION

We concoct and attempt a vital issue of an instalment framework for internet shopping is proposed by joining content based steganography and visual cryptography that gives client information protection and counteracts abuse of information at traders side. The strategy is concerned just with anticipation of fraud and client information security. In contrast with other anking application which utilizes steganography and visual cryptography and are essentially connected for physical managing an account, the proposed strategy can be connected for E-Commerce with concentrate territory on instalment amid web based shopping and additionally physical saving money.

V. FUTURE SCOPE

The instalment framework can likewise be stretched out to physical keeping money. Offers may contain client picture or mark notwithstanding client verification secret word. In the bank, client presents its own offer and client physical mark is approved against the mark acquired by joining client's offer and CA's offer alongside approval of client validation secret key.

.

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.