Client-Merchant Online Payment System Exploiting Visual Cryptography

Ganji Sekhar¹, Ch.Kodandaramu²

¹#1 Student of M.Tech (CSE) and Department of Computer Science Engineering, Avanthi Institute of Engineering & Technology
²#2 Asst.Prof, Department of Computer Science and Engineering, Avanthi Institute of Engineering & Technology Visakhapatnam.

Abstract

This paper exhibits another methodology for giving restricted data just that is important for asset exchange amid web shopping along these lines defending client information and expanding client certainty and avoiding wholesale fraud. These days rapid thriving in E-Commerce business sector has been seen in late time all through the world. With continually expanding notoriety of internet shopping, Debit or Credit card extortion and individual data security are real attentiveness toward clients, shippers and banks and the principle rationale of this undertaking is to give abnormal state security in E-Commerce applications and web shopping. This task minimizes point by point data sharing in the middle of buyer and online dealer yet empower effective asset exchange subsequently defending shopper data and anticipating abuse of data next to merchant. This is accomplished by the presentation of Central Certified Authority (CA) and consolidated utilization of Steganography, Visual Cryptography and Digital Signature for this reason. A fast flourishing in E-Commerce business sector has been seen in late time all through the world. With constantly expanding prominence of web shopping, Debit or Credit card extortion and individual data security are real attentiveness toward clients, shippers and banks. The primary thought process of this undertaking is to give abnormal state security in E-Commerce applications and web shopping. This task minimizes definite data sharing in the middle of purchaser and online vendor yet empower effective asset exchange consequently protecting customer data and counteracting abuse of data next to merchant. This is accomplished by the presentation of Central Certified Authority (CA) and joined use of Steganography, Visual Cryptography and Digital Signature for this reason.

Keywords: Steganography, Online shopping, E-Commerce, Encryption, Decryption.

I. Introduction

In to a great degree expanding E-Commerce business sector setting, internet looking has experienced childhood in quality throughout the years, essentially as a consequence of people notification it helpful and easy to rebate, seek from the solace of their home or working environment. Amid this paper, we tend to range unit having some expertise in security of client's close to home information all through on-line seeking. On-line seeking may be a style of electronic business that allows clients to straightforwardly get stock or administrations from a merchant over the net utilizing a program. Steganography is the craft of disguising a record, message, picture, or video inside another document, message, picture, or video [4]. The fortunate thing about Steganography over cryptography is that the assumed mystery message doesn't draw in regard for itself as an object of Examination. Doubtlessly noticeable encoded messages—regardless of how much unbreakable—stimulate intrigue, and ought to in themselves be incriminatory in nations wherever cryptography is precluded. Accordingly, while cryptography is the specialty of ensuring the substance of a message alone, Steganography is disturbed with hiding the very actuality that a mystery message is being sent, besides as hiding the substance of the message. Encryption is that the strategy for cryptography messages or information in such the way that exclusively endorsed gatherings will skim it. The assumed correspondence, information or message, commented as plaintext, is scrambled abuse partner degree mystery composing recipe, creating figure content which will exclusively be skim if decoded. Partner degree mystery composing subject at times utilizes pseudo-irregular mystery composing key created by partner degree equation [2]. Electronic trade is business in stock or administrations abuse portable PC systems, similar to the net. Electronic business pulls in on advances like portable E-trade, electronic assets exchange, give chain administration;
Related Work

Before adding to the instrument it is important to decide the time variable, economy and organization quality. Once these things are fulfilled, then next steps is to figure out which working framework and dialect can be utilized for adding to the apparatus. Once the software engineers begin fabricating the instrument the developers need part of outside backing. This backing can be acquired from senior software engineers, from book or from sites. Before building the framework the above thought are considered for adding to the proposed framework. Also, the brief review of related work in the range of saving money security in view of steganography and visual cryptography is displayed in this segment. A client verification framework utilizing visual cryptography is exhibited as a part of [4] however it is particularly intended for physical saving money. A mark based confirmation framework for center keeping money is proposed in [5] however it additionally requires physical vicinity of the client showing the offer. [6] Proposes a consolidated picture based steganography and visual cryptography verification framework for client confirmation in center managing an account. A message verification picture calculation is proposed in [7] to secure against ebanking misrepresentation. A biometrics in conjunction with visual cryptography is utilized as verification framework [8]. A brief investigation of related work in the range of managing an account security in light of steganography and visual cryptography is exhibited in this division. A customer verification framework utilizing visual cryptography and steganography is exhibited in [5] however it is decisively intended for physical saving money. A mark based confirmation framework for center managing an account is proposed in [6] yet it likewise requires physical vicinity of the customer introducing the offer. [7] Proposes a joined picture based steganography and visual cryptography validation framework for customer verification in center saving money. A message verification picture calculation is proposed in [8] to ensure against e-keeping money misrepresentation. A biometrics in conjunction with visual cryptography is utilized as confirmation framework [9]. Ghascmict al. [12] proposed a novel steganography plan taking into account whole number wavelet change and Genetic calculation. Umamaheswari [13] pack the mystery message and encode it by the beneficiary's open key alongside the stego scratch and implant both messages in a transporter utilizing an installing calculation. ShyamalenduKandar [14] proposed a system of understood k-n mystery sharing on shading pictures utilizing a variable length key with offer division utilizing irregular number. Anupam [15] portrays how such an even-odd encryption in light of ASCII quality is connected and how encoded message using so as to change over Gray code and inserting with picture can secured the message and in this manner makes cryptanalyst's occupation troubles.
III. System Architecture
In this system there will be two servers, bank server (admin) and merchant server (product admin). Product admin will add the products and product related information in its database. Admin i.e. bank server will add users and merchant servers. User specific data includes user name, user id, transaction password and user password. While merchant server specific data includes server id, password and URL in the Admin's database. Client will select the product and log in to respective site. Then verification request is sent to merchant server. Merchant server will verify the user name, user id and along with that it will add server id, server key and send it to the bank server for the verification. Bank server will verify the server id, server key of merchant server. If it is ok then bank server will generate one OTP through steganography. If the merchant server is fake then it will not generate OTP. After OTP generation it will form two shares using visual cryptography. One will be sent to the client via email and other will be sent to the merchant server. Merchant server will send the second share to the client. After having two shares, at client side these two shares are combined and original OTP gets generate.

III. Encryption and decryption process

Visual Cryptography

The visual cryptographic method is applied here. At first, the original image is binarised to keep the pixel values as either 0 or 1, this is considered for simplicity of LSB bit encryption [3][2][8]. Next the secret message image is scrambled where share 1 is created by taking the odd positioned bits of the secret image and the share 2 is generated using the even positioned bits of the secret image.
Figure 3: LSB bit replacement

Decryption Process

**LSB Extraction**

The LSB bits of the steganographed image is extracted at first. Then the last pixel value LSB number is identified to the share positions. The LSB bits of other pixels are arranged according the number identified. The share 1 and share 2 are generated using this LSB extraction.

**Decryption of visual cryptography**

The obtained shares from the LSB extraction is fed as input to the visual decryption process [4]. Here the shares are combined by alternating the pixels from each share to generate the secret message image.

### III. Technologies Used

#### A. Least Significant Bit

Least significant bit (LSB) insertion could be a common, straightforward approach to embedding data in an exceedingly cowl image. The smallest amount vital bit (in alternative words, the eighth bit) of some or all of the bytes in a picture is modified to slightly of the key message. Once employing a 24-bit image, slightly of every of the red, green and blue color elements will be used, since they're every described by a computer memory unit. In alternative words, one will store three bits in every element. Associate 800 × 600 element image, will so store a complete quantity of 1,440,000 bits or 180,000 bytes of embedded information. As an example a grid of three pixels of a 24-bit image will be as follows: For Example:

(00101101 00011100 11011100)  
(10100110 11000100 00001100)  
(11010010 10101101 01100011)  

When the amount 200, that binary illustration is 11001000, is embedded into the smallest amount significant bits, this a part of the image, the ensuing grid is as follows:

(00101101 00011101 11011100)  
(10100110 11000101 00001100)  
(11010010 10101100 01100011)  

Although the amount was embedded into the primary eight bytes of the grid, solely the three underlined bits required to be modified in step with the embedded message.

#### B. RC6

RC6 (Rivest Cipher 6) could be a symmetric key block cipher derived from RC5. RC6 correct encompasses a block size of 128 bits and supports key sizes of 128, then 192, and 256 bits, but, like RC5, it should be parameterized to support a good sort of word-lengths, key sizes, and variety of rounds. RC6 is extremely almost like RC5 in structure, victimization data-dependent rotations, standard addition, and XOR operations; indeed, RC6 can be viewed as interleaving 2 parallel RC5 encoding processes, however, RC6 will use an additional multiplication operation not gift in RC5 so as to form the rotation depends on equally in an exceedingly word, and not simply the smallest amount important few bits.

#### C. One Time Password (OTP)

A one-time password (OTP) is a keyword that is effective for only one login session or operation, on a computer system or other numerical device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also include two factor authentication by confirming that the one-time password requires access to somewhat a person has (such as a small keying fob device with the OTP calculator built into it, or a smart card or exact cellophane) as well as somewhat a person knows (such as a PIN). The most important advantage that's self-addressed by OTPs is that, in distinction to static passwords, they're not prone to replay attacks. This implies that a possible interloper who manages to record an OTP that was already wont to log into a service or to conduct a dealing will not be able to abuse it, since it will not be valid. A second major advantage is that a user who uses an equivalent (or similar) positive identification for multiple systems, isn't created prone to all of them, if the positive identification for one amongst these is gained by an offender. Variety of OTP systems additionally aim to substantiate that a session cannot simply be interrupted or derived while not data of random knowledge created throughout the previous session, so reducing the attack surface more. Ways of delivering OTP area unit text electronic messaging, mobile, exclusive token, web based mostly technique, hard copy.

### VII. Proposed Methodology

In the proposed system, information submitted by the consumer to the online website at merchant’s site is minimized by providing only minimum information that will only verify the payment made by the
consumer from its account. This is accomplished by the introduction of a central Certified Authority (CA) and combined application of Steganography and visual cryptographic technique. The information obtained by the merchant will only validate receipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

Sequence of Proposed Payment System
Step 1: Consumer registration process.
Step 2: Share 1 generated using Steganography and Visual Cryptography.
Step 3: Consumer opts for online shopping (Merchant Side).
Step 4: Consumer completes the shopping process and directed to payment process.
Step 5: Consumer submits the share 1 provided while registration and Merchant provides its account details.
Step 6: The Consumer Share and Bank Share are combined and verified by the CA.
Step 7: If the share is valid then the transaction will be synchronized with the bank. If share not valid then error message will be sent.
Step 8: For valid share the Bank will extract the Account number from the original image and perform the transaction.
Step 9: A notification will be sent to the consumer via mail.

Fig. Proposed Payment System.

VIII. Conclusion
In the proposed payment systems, a consumer’s payment information is sent to a payment portal via a merchant. This makes the payment system vulnerable to intrusions and Information leaks, causing consumer data theft, identity theft and fraudulent transactions. To protect a consumer’s financial information from being compromised, we developed an approach for online payment systems in which a consumer’s payment information is directly provided to a payment portal rather than sent through a merchant’s website. This approach, however, introduced by the introduction of a trusted third party called certified authority, CA, and a combination of text steganography and visual cryptography. A CA verifies the identity of a consumer by combining share 1 and share 2 before processing the payment. The combination of text steganography and visual cryptography provides consumer’s information privacy and protects data from misuse. Hence, we show that our proposed payment system is secure and protects a consumer’s payment information and payment against network intruders or attackers.

Future Scope
The payment system can also be extended to internet or physical banking. Shares may contain consumer image or signature in addition to consumer authentication password. In the bank, consumer submits its own share and consumer physical signature is validated against the signature obtained by combining consumer’s share and CA’s share along with validation of consumer authentication password. It prevents misuse of stolen card and stops illegitimate consumer. This can be also applied for standardization of a particular product or an organization by having their personal identification secured.

References


Authors

GANJI SEKHAR holds a B.Tech certificate in Computer Science Engineering from Gayatri Vidya Parishad College of engineering at Visakhapatnam Affiliated to the University of JNTU HYDERABAD. He presently Pursuing M.Tech (CSE) department of computer science engineering from Avanthis college of engineering at Visakhapatnam Affiliated to JNTU KAKINADA. Attended CSI Workshops, student coordinator in National Level technical symposium behalf of college. One of the active member in student committees. Attended several conferences, seminars, summits & presented technical paper presentations. Done some social activities, medical camps behalf of trust. Areas of interests are Online Web Security, Web Portal Developments, Data Communication systems, Computer Networks.

KodandaRamu Chintu working as Asst.Prof in Avanthi Institute of Engineering and Technology at Visakhapatnam. He is an M.Tech post graduate in Computer Science & pursuing Ph.D from ANDHRA UNIVERSITY. Areas of research interest include Data mining in data mining like cluster analysis, outlier analysis, trends and time series data. His hobbies include playing various sports & games like cricket, shuttle etc. and listening to songs, reading books.

He believes in the wordings of Swami Vivekananda: “Truth can be stated in a thousand different ways, yet each one can be true.”