E-Commerce with the Security Techniques of Visual Cryptography and Text Based Steganography

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : September

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Sangeetha, V. (2018). E-Commerce with the Security Techniques of Visual Cryptography and Text Based Steganography. *Shanlax International Journal of Arts, Science and Humanities*, 6(1), pp.129–134.

DOI:
https://doi.org/10.5281/zenodo.1411013

Prof. V.Sangeetha, M.Sc., M.Phil., SET., B.Ed.,
Head, PG and Research Department of Computer Science
Sri Bharathi Women's Arts and Science College
Kunnathur, Arni, T V Malai Dt

Abstract

E-Commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking. Online Shopping, Online Bill Payment, Online Recharge and Online Ticket Booking are necessary for today's life, to achieve those things we should go for online transaction. Debit or Credit card fraud and personal information stealing are major security threats for customers, specifically in the case of CNP that is Card Not Present. In this paper a new method is proposed for providing limited information that is necessary and hiding other secret information from the third party during the online transaction, that secret information only is visible to the bank. In this way, we can safeguard customer data, increase customer confidence, prevent misuse of information at the merchant side and nobody can hack or view the secret information on the network. Text-based steganography and visual cryptography techniques are used in this paper, which minimizes information sharing between consumer and online merchant but enables successful fund transfer from consumer's account to merchant's account, thereby safeguarding consumer information. Here secure online transaction using text-based steganography and visual cryptography is used for E-Commerce but we can also use it for online and physical baking system with enhanced techniques. In text-based steganography, the message can be hidden by shifting word, line and word sequence. Properties of a sentence like number of words, number of characters, number of vowels, the position of vowels in a word are also used to hide the secret message. Visual Cryptography is a cryptographic technique based on visual secret sharing, secret image or text is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only by combining the shares, the secret information can be obtained.

Keywords: Steganography, Encryption, Visual Cryptography, MATLAB

Introduction

Online shopping is a process, which is used by consumers to directly buy goods or services from sellers in real time over the Internet. It is a form of Electronic Commerce. The process referred as retrieval of product information via the Internet and issue of the 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. There are many security threats for online

transaction. Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumer personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer that is SSL encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust the merchant and its employees not to use consumer information for their purchases and not to sell the information to others. Identity theft is another common danger for 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.

Steganography

Steganography is the art and science of hiding messages. Steganography and cryptology are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information, so it appears that no information is hidden at all. If a person views the digital object that the information is hidden inside, he or she will have no idea that there is any hidden information. Therefore the person will not attempt to decrypt the information; this is the main objective behind steganography.

Classification of Steganography Techniques

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible.
Common approaches are including:

- Least significant bit insertion (LSB).
- Masking and filtering.
- Transform techniques

Text Steganography

The Steganography method uses the text media to hide the data known as text Steganography. There are different techniques to embed the secret data in text files.
Format Based Method
Random and Statistical Method
Linguistics Method

Visual Cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.
Working Principle:

- The principle of the onetime pad was developed during World War One, though it was 25 years before a mathematician proved it was perfectly secure, as opposed to merely prohibitously difficult to break. It is a very simple substitution, but with the twist that the key is the same length as the message.
- Each letter has its own unique and random rotation, making the encoded message proof against any sort of analysis without the key as a result. The final result is a pair of random

looking message one the encrypted message of the same length, either of which cannot be broken or analyzed in any way on its own, but which can easily be decoded once the two are brought together. One Time Image extends the principle of those images. First, the source image is converted to black and white, not gray scale, true black and white with pixels of only these two different colors.

Figure Sample Image for VC

A key image is generated as a second step of the same dimensions, where each pixel is randomly set to white or black. Third, the original image is encrypted using this key, if the pixel in the key is white then the corresponding pixel in the original image is used in the encrypted image, whereas if the key pixel is black then the corresponding pixel in the original image is flipped like black to white, white to black for the encrypted image. The result is two images of apparently random black and white pixels but also have the backward compatibility with the previous results in black and white visual cryptography, such as the t out of n threshold scheme, and can be applied to gray level and color images easily.

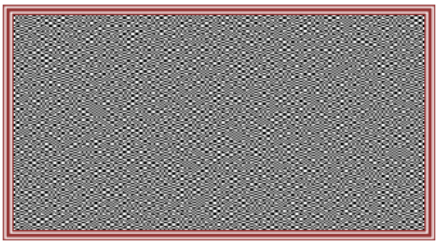

Figure Share Image

Finally, each image is then doubled in size each pixel becomes a 2x2 square of pixels. Black pixels have black pixels in the top left and bottom right corners while the other two pixels are while a white pixel in the original image produces the opposite 2x2 square. These enlarged images are the final, encrypted ones they have the appearance of random static, or snow, and neither one can be decrypted on its own.

Figure Original Visual Cryptography Image

Objectives

Cryptography and Steganography have been for a long time. Earlier a message was cipher using cryptography and sent to the recipient, although it was secure approach yet it was the visible message during. To make it invisible message next they applied steganographic method. In fact, steganography can be useful when the use of cryptography is forbidden where cryptography and

strong encryption are outlawed. Steganography can avoid such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: Steganography fails when the enemy can access the content of the cipher messages, while cryptography fails when the enemy detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The actual process is a method for integrating together cryptography and steganography on image processing. Online shopping provides an easy way to shop for products without taking as many efforts like go for market or anywhere and view different collections with the comparison of the products value. Online shopping also gives us the benefit of offers on rates. We can get the product to our place with the discount so that electronic banking continues to grow but the security and the privacy aspects need to be improved. We have given our secret information such as Password or CVV or PIN directly on the payment portal; this is not a secure approach, merchant or payment gateway authority can view that information and possibly misuse.

Payment Method Using Steganography and Visual Cryptography Techniques

In this method information submitted by the customer to the online merchant is minimized by providing only general information that will be visible to an online merchant to verify the payment made by the said customer from its bank account. This is achieved by the 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 the authentic customer. Customer unique authentication password in connection to the bank is hidden inside a cover text using the text-based steganography method. Customer authentication information that is account number in connection with the merchant is placed in its original form. Now a snapshot of the cover text is taken, from the snapshot image, two shares are generated using visual cryptography.

Sentence Based Encryption and Ecryption Technique

In today's information age, information sharing and transfer have increased exponentially. The threat of an intruder accessing secret information has been an ever concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Cryptography involves converting a message text into an unreadable cipher.

On the other hand, steganography embeds the message into a cover media and hides its existence. Both of these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecured communication channel and are vulnerable to intruder attacks. Although these techniques are often combined to achieve higher levels of security still there is a need for a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

Text-Based Steganography

Sentence Based Encryption and Decryption text-based steganography uses characteristics of English language such as inflection, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from sentence construction but it increases computational complexity. The steganography technique is based on the frequency of letters in English vocabulary. It is used as the basis for assigning numbers to the letters in the English alphabet. Number assignments of letters are shown in the table. No separate importance is given for vowels and consonants.

Principle of Visual Cryptography

Each pixel of the images is divided into smaller blocks. There is always the same number of white transparent and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above use pixels that are divided into four parts.

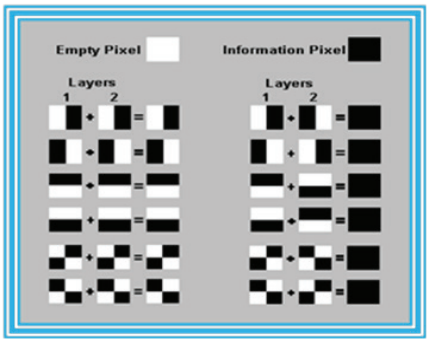

Figure Merging layers to get pixels in Visual Cryptography method

In the table, we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer two may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and two are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

Implementation

MATLAB is used for implement the method of "Secure transaction using Steganography and Visual Cryptography." The payment portal interface will get customer's account, credit or debit card information and E-Mail ID to send Mail to the customer. CONCLUSION

The Random Character Generation of Encryption and Decryption process using text-based steganography and visual cryptography will be used to increase the security of the E-Commerce system. According to this method, the secret information which has been given by customer will be encrypted using text-based steganography and split into two hidden shares using visual cryptography. One share is kept by the merchant; another one will be kept by the customer. Bank will receive both shares and overlap with one another then reveal the content which is hidden after that get the secret key and password using decryption method. Then verify with the account number from its database, then transfer fund to the merchant, if given details are correct.

Thus we can ensure the security of the secret user details from the third party and it can be used as advancement over the Sentence Based Encryption and Decryption option to input the security phrase to hide the secret user details from merchants, gateways and various web-based applications because the Sentence Based method is very critical if the secret message is too long and there are some of the possible ways to decrypt the hidden message but in Random Character Generation of Encryption and Decryption process no more possible ways to hacker or intruders to decrypt the message because of ultimate random generation of characters.In the case of text-based steganography, when a secret message being transferred, the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred. This multimedia data can be transferred in the normal way. Video files and image streams can also be used to

transmit data. In case of image streams, part of the message can be sent in each image. This will increase the security of the system. 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, the customer submits its 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. It prevents misuse of the stolen card and stops illegitimate customer.

References

Books

Bharati Krishna Tirthaji. (1992). "Vedic Mathematics and its Spiritual Dimension," *Motilal Bansari Publishers.*

Daniel Gruhl, Anthony Lu, Walter Bender. (1996). "Echo Hiding," Proceedings of the First International Workshop on Information Hiding, Cambridge, UK.

Judge, J.C.(2001). "Steganography: Past, Present, Future," SANS Institute, 30.

Chen,J., Chen, T. S., & Cheng,M. W. (2003). "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering.

Jack Brassil, Steven Low, Nicholas Maxemchuk & Larry O'Gorman. (1995). "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University

Juan Chen, Chuanxiong Guo, (2006). "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on Communications and Networking in China, Beijing, China, .

Naor, M., & Shamir, A. (1995). "Visual cryptography," Advances in Cryptography: EUROCRYPT'94, LNCS.

Walter Bender, Daniel Gruhl, Norishige Morimoto. (1996). A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35.

Web Sources

https://en.wikipedia.org/wiki/Online_payment
https://nano.mae.cornell.edu/pubs/erickson_JCIS261.pdf
https://www.irjet.net/archives/V3/i3/IRJET-V3I3219.pdf
http://www.datagenetics.com/blog/march12012/index.html
http://balagharhackers.blogspot.com/2011/05/how-to-hide-data-in-image-audio-video.html
https://nyuscholars.nyu.edu/en/publications/analysis-of-lsb-based-image-steganography-techniques
http://www.ijmra.us/project%20doc/IJMIE_JUNE2012/IJMRA-MIE1320.pdf
http://manualzz.com/doc/11035860/computerised-one-time-pads
https://www.slideshare.net/saurabhnambiar1/steganography-using-visual-cryptography
https://www.sciencedirect.com/science/article/pii/S0031320302002583
https://wwjmrd.com/upload/1509039801.pdf
http://www.ijcta.com/documents/volumes/vol2issue3/ijcta2011020338.pdf
https://plus.google.com/communities/101091973299684733701
http://www.ijcscn.com/Documents/Volumes/vol5issue5/ijcscn2015050508.pdf
http://paper.ijcsns.org/07_book/201204/20120417.pdf
https://www.coursehero.com/file/p65e7le/Each-pixel-of-the-images-is-divided-into-smaller-blocks-There-is-always-the/