ISSN 2395-1621

Robust and Secure Online Payment System Using Steganography

[#1]Rhutuja Jain, [#2]Namrata Jagtap, [#3]Surabhi Bhagat, [#4]Sonal Angre

[1]rhutujajain30896@gmail.com,
[2]namratajagtap941@gmail.com,
[3]surabhibhagat95@gmail.com,
[4]sonalangre1597@gmail.com

[#1234]Department of Computer Engineering

TSSM's, BSCOER, Narhe, Pune

ABSTRACT

The rapid growing development of data transfer through internet has made it easier to improve the data accuracy and speed to the destination. There are many transmission media to transfer the data to destination like e-mails, social sites etc. At the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography. Online payment systems allow fund transfer with the help of internet. Nowadays, credit cards are used commonly for payment on e-commerce. There has been a tremendous growth and attraction towards the online shopping in recent time throughout the world. But on the other side we have a major task in hand to protect personal as well as banking information. After the rapid use of online transactions the rise in debit & credit card fraud and steeling the personal information is the real worry for the end users and online retailers. This paper provides new approach for providing limited information which is necessary for fund transfer thereby safeguarding customer data and preventing identity theft.

Keywords— E-Commerce, Information Security, OTP, Identity Theft, Steganography, Visual Cryptography.

ARTICLE INFO

Article History

Received: 15th April 2018

Received in revised form :

15th April 2018

Accepted: 19th April 2018

Published online :

21st April 2018

I. INTRODUCTION

Online shopping also called as e-tail is a way of purchasing products over internet. [1]It allows customers to buy goods or services using web browsers and by filling credit or debit card information. In online shopping the common threats are phishing and identity theft. Identity theft is a form of stealing someone's identity i.e. personal information in which someone pretends to be someone else. The person misuses personal information for purchasing or for opening bank accounts and arranging credit cards. As a result of identity theft, the customer's information was misused for an average of 48 days in 2012. Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a criminal mechanism that uses social engineering. Phishing email directs the users to visit website where they take users personal information such as bank account number, password. It is email fraud conducted for identity theft. In 2013, Financial and Retail Service, Payment service are the targeted industrial sectors of phishing attacks. In 2017, news was published which told that OTP was hacked by the white-hat hacker.

Online shopping uses internet, network and web -based technologies in creating interactive medium between sellers and customers. In addition, the existing system of online shopping yield benefits such as easy to business transaction network; saves times and reduces search costs compared to standard shopping process. Because of these benefits, businesses and companies are increasing their use to business transaction through fetching method of delivery using online shopping. With the recent growth of online shopping, it has become an attractive option for expanding the business opportunity available for sellers .Steganography is a technique or a method of hiding the information into the image. It is the practice of concealing a file, message or image into another file, message or image. Steganography combines the word steganos and graphein. The meaning of steganos is covered or protected, the meaning of graphein is writing. The message which is hidden may be in invisible link between the visible lines of personal letter.The advantage of this

technique is that the hidden message does not pay attention to itself as an object scrutiny. It includes hiding of information within computer files. For the transmission purpose media files are considered as ideal because of their large size. Electronic communication involves steganography coding within transport layer.

Cryptography is the practice and the study of techniques for secure communication in the presence of arbitrator. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer. The method proposed in the system uses both steganography and visual cryptography. It reduces information sharing between customer and merchant server and safeguards customers information. It enables successful fund transfer to merchant's account from customer's account and prevents misuse of information at merchant side. In this system there are two shares of image which are combined to get original image. In this way the system provides secure transaction.

II. PROBLEM STATEMENT

Online shopping is generally considered as consulting product information using the internet and issuing the purchased 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 thefts of online shopping. Identity theft is the stealing of someone's personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards.

Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a criminal mechanism that uses social engineering. Phishing email directs the users to visit website where they take users personal information such as bank account number, password. It is email fraud conducted for identity theft. In 2013, Financial and Retail Service, Payment service are the targeted industrial sectors of phishing attacks. In 2017, news was published which told that OTP was hacked by the white-hat hacker.

The method which is proposed in this project uses both steganography and visual cryptography. It reduces information sharing between customer and merchant server and safeguards customers information. It enables successful fund transfer to merchant's account from customer's account and prevents misuse of information at merchant side. The proposed system is applied to online shopping otherwise Ecommerce but can be easily extensible for other applications like online banking.

III. LITERATURE REVIEW

In [2] Sneha M. Shelke, Prof. Prachi A. Joshi ,A Study of Prevention of Phishing Threats using Visual Cryptography,2016,proposed method preserves personal information of users. In this paper, anti phishing solution based on visual cryptography has been presented. Using proposed method, end user can easily identify the website is real or fake based on validation of image captcha. Additional security is provided by using OTP. This method provides additional security in terms of not letting the invader log-in into the account even when he knows the mail or id of a particular user.

In [4] N. Shrivastava1, T. Verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", International Journal of Advanced Research in Computer Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015, in proposed method the sender is hiding the information which is to send to the beneficiary as pictures. The picture is a blend of the content which is gotten from the two procedures of the content steganography which has been inferred before. The two procedures utilized are Reflection Symmetry and the Vedic Numeric technique. The sender sends the information into apportioned shape or we can say that the information which is sent by the sender is divided into 2 sections and separate-isolate part is sent to the two procedures. We are doing this as though the Vedic strategy it,which requires more memory. In this way, the content in the wake of being prepared by the two procedures is combined to shape an entire content and after that the content is changed over into picture by the different techniques or calculations ex. LSB, network augmentation. In this way, the content is changed over into picture that is sent to the recipient.

In [5] S. Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", IEEE Conference on Electrical, Electronics and Computer Science, vol. 6, no. 2, pp. 88-93, 2014, new strategy is proposed, based steganography and visual cryptography, which minimizes data sharing to the merchant however empower effective store exchange from customer's record to vendor's record subsequently shielding purchaser data and avoiding abuse of data at dealer side. The strategy implemented specially for Ecommerce.

In [6] Rahna E, V. Govindan, "A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegnoimage", International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013, proposes a novel procedure which tries to understand all the above issues in steganography. In the proposed strategy, rather than substitutions we are utilizing the idea of matches between personal information and cover picture. What's more, we additionally utilize the idea of altered recurrence for every character in English. The proposed technique is lossless, has limitless payload limit, has key size which is just around 10 to 20 rate of the message estimate and has more security.

In [7]P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography and Visual Cryptography for Authenticity", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013, proposes a procedure using picture utilizing Steganography and visual cryptography, and afterward partitioning it into shares. The picture extensions can be .jpg or .png. The message process is computed utilizing the MD5 calculation and this is affixed with the message. The annexed message is then encoded utilizing the AES calculation. The mystery enters utilized as a part of the AES calculation is scrambled utilizing the RSA calculation.

The affixed scrambled message is inserted in the picture utilizing the minimum huge piece calculation. The encoded picture is transmitted. The secret word must be given before transmitting the picture document. At the beneficiaries side the watermarked picture record is taken as the information. The message in the picture record is removed utilizing the LSB calculation. The removed message is separated into the process and the message part. The message process is figured for the message and is contrasted and the got one. In the event that they are similar then message is said to be verified.

IV. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the art of hiding of a message within another message. [9]It is a technique of hiding the information into the image. . Steganography made of the two words steganos and graphein. Steganos means covered or protected and the meaning of graphein is writing. The basic concept behind steganography is that message to be transmitted is not detectable to casual eye. Steganography technique uses text, image,and video, audio as a cover media for hiding data. The hidden message may be in invisible link between the visible lines of personal letter. Number of words, number of characters, number of vowels, and position of vowels in a word are also used to hide the message. A text steganography technique requires small memory and simpler communication. At transport layer, electronic communication involves steganography coding.

Cryptography is the study of techniques for secure communication in the presence of third party. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer. Moni Naor and Adi Shamir developed this technique. It was developed in year 1994. Visual cryptography contains two transparent images. One image contains random pixels and another image contains secret information. It is impossible to retrieve secret information from one of the images. The two images are required to retrieve the correct information.

V. TYPES OF FRAUDS

Spam and identity fraud:
Identity fraud terms used to refer to all type of crime in which someone unfair obtains and uses someones confidential data in some way that involve fraud , typically for economic gain. In this identity of a person is stealing from social network site and this information is used for the unjustified purpose.

Credit card fraud:
There are various medium of Credit card fraud are as follows: Duplication: Card is with the owner and is a duplicate is made by stealing data of the owner. Skimming: Collection of data from the card's magnet and copy it to a blank card.
Call center leaked:
The card information in sold to Fraudsters.

Bank back office data: By hacking the bank server and getting the personal information.
Data theft: Stealing the information by sending spam E-mails.
Man in middle attack: Gaining the access when the customer is contacting with the vendor for payment and accessing the information.

Investment fraud:
Various investment schemes typically target merchandise investors, trying to steal money and investors' confidential data. Some of these scams will come in the form of an online newsletter. In these newsletters, frauds will offer inside information on stocks, for a fee, and offer false data instead of real information.

Online bulletin boards have also become a breeding ground of illegal activity. Companies often use online bulletin boards to publish information; however, a bogus board will release disinformation. A pump and dump scheme can start with a fraudulent newsletter or bulletin board where secret or private information is offered. The object of this fraud is to alter stock values. After effectively delaying a stock, the schemer will sell his or her own stock in a timely fashion for personal gain.

VI. PROPOSED SYSTEM

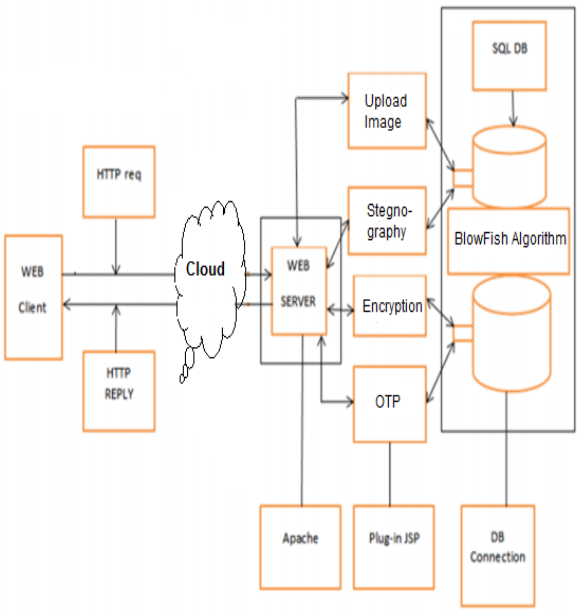

Fig.1. [1]System Architecture

Above fig.1 shows that we are authenticating the client . So the information of customer which is given to the bank side and merchant side is the issue of security. The system helps the clients to prevent phishing by providing secure transaction. This is achieved by the introduction of combined application of steganography and visual cryptography. In the proposed system, client shares the secret image to the merchant side.Then merchant splits the encrypted image into two parts and shares half encrypted image to client and the other half image remains to the merchant itself, after that both the splitted images are combined to verify the authorized user.In this way the

system provides secure transaction during the money transferring one account to another.

VII. BLOWFISH ALGORITHM

Blowfish algorithm is a fast and alternative to existing encryption algorithms. It is called as symmetric block chipper to safeguard the data effectively.[8] It has two modules such as encrypt and decrypt as shown in figure 1. The encrypt module is used to hide visual information. The decrypt module is used to get the hidden visual information as original image. It takes the cipher image file as an input and gives original image asan output. In addition to that, the algorithm generates sub keys as follows: Blow Fish uses a large number of sub keys. These keys must be pre - computed before any data encryption or decryption.

The P-array consistsof1832-bit subkeys:
P1, P2,..., P18.
There are four 32-bit S-boxes with 256 entries each:
S0 , 0, S0,1,..., S0,255;
S1, 0, S1, 1,..,, S1,255;
S2, 0, S2,1,..., S2,255;
S3, 0, S3, 1,..,, S3,255.

- **Proposed Encryption Algorithm based on Blowfish:**

The Encryption of Blow Fish algorithm precedes the following steps.
Step 1: Initialize S Box and T Box as arrays.
Step 2: Convert the matrix Inverse to Transpose and store in T Box.
Step 3: The input is a 64-bit data element, x.
Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL
XOR Pi xR = F(xL)XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the cipher image.

- **Image Decryption With The Secret Key Decryption**

Decryption process precedes the following steps:

Step 1: Initialize S Box and T Box as arrays.
Step 2: Secret key comparison between original key which is created while encryption.
Step 3: The input is a 64-bit data element, x.
Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL
XOR Pi xR = F(xL)XOR xR
Swap xL and xR
After the sixteenth round, swap xL and xR again to undo the last swap.
Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the original image

VIII. APPLICATIONS

- **Online Banking**

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

The client visits the secure banking website, and enters the online banking facility using confidential data which was previously used. The types of banking transactions which a customer may transact through online banking are determined by the banking institution, but usually includes obtaining account balances, a list of the recent transactions, electronic bill payments and funds transfers between a customer's or another's accounts.

- **E-Commerce**

Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. [10]Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle although it may also use other technologies such as e-mail.

This transaction includes the shopping of online books (Amazon) and music purchases (songs from iTunes Store), and to a less area.

- **Online Shopping**

Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser.[10] Customers find a product of interest by visiting the website of the retailer directly or by searching among alternative sellers using a search engine, which displays the similar product's availability and pricing at different e-vendors. As of 2016, customers can shop online using a range of different computers and devices, including desktop computers, laptops, tablet computers and smartphones.

Online stores typically enable customers to use "search" features to find specific models, brands or items. Online customers must have access to the Internet and a valid method of payment in order to complete a transaction, such as a credit card, an Intera c-enabled debit card, or a service such as PayPal.

IX. RESULT

Sr. No	Parameters	System Using OTP	System using Stegano- image
1	Techniques	Random function used	Blowfish Algorithm
2	Encyption	No	Yes
3	Robustness	Less	More
4	Applicability	Universally	Universally

5	Layers of Security	2-layers	3-layers
6	Confidentiality	Less	More
7	Mechanism	Random OTP is generated	Secret image is used
8	Naked Eye Identification	No message hiding concept	No,as message is hide within cover image

X. CONCLUSION

In this paper, we use visual Cryptography to provide secure transaction in online shopping. It secures the customer's confidential information as well as merchant's credentials and prevents misuse of data at bank side by Admin Application. This method is mainly concerned with preventing identity theft and providing customer data security. It also prevents phishing attacks.

XI. ACKNOWLEDGEMENT

We wish to express our profound thanks to all who helped us directly or indirectly in making this paper. Finally We wish to thank to all our friends and well-wishers who supported us in completing this paper successfully. We are especially grateful to our guide Prof. M.K.Mokashi for his valuable guidance. Without the full support and encouragement of our guide, the paper would not have been completed on time.

REFRENCES

[1] Harshad Talera, Nalini Wagaskar, Shital Kapse, Pooja Deshmikh, Shweta Shanwad, "Implementation of Secure Online payment using Stegano Images",2017.

[2] Sneha M. Shelke, Prof. Prachi A. Joshi ,A Study of Prevention of Phishing Threats using Visual Cryptography,2016.

[3] K. Kanagalakshm ,"Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key", July 2016.

[4] N. Shrivastava1, T. Verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", International Journal of Advanced Research in Computer Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015.

[5] S. Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", IEEE Conference on Electrical, Electronics and Computer Science, vol. 6, no. 2, pp. 88-93, 2014.

[6] Rahna E, V. Govindan, "A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage", International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013.

[7] P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography and Visual Cryptography for Authenticity", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013.

[8] Monika Agrawal and Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877- 882.

[9] S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

[10] Abdulghader.A. Ahmed, Hadya.S.Hawedi Online Shopping and the Transaction Protection in E-Commerce: A case Of Online Purchasing,2012.

