ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Online Secure E-Pay Fraud Detection in E-Commerce System Using Visual Cryptographic Methods

M. Suresh, Bullarao Domathoti, Nageswara Rao Putta

Pursuing M. Tech, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India

Assistant Professor, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India

Associate Professor, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India

ABSTRACT: A rapid growth in E-Commerce market is seen 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 specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of Steganography and visual cryptography for this purpose.

KEYWORDS: Information security; Steganography; Visual Cryptography; Online shopping; debitcard;

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue of 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 [1]. Identity theft and phishing are the common dangers of 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. In 2012 consumer information was misused for an average of 48 days as a result of identity theft [2]. Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks [3]. Secure Socket Layer (SSL) encryption prevents the interception 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 consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.

The rest of the paper is organized as follows: Section II gives brief description of text based steganography and visual cryptography. Section III contains related works. Section IV presents the proposed steganography method. Section V provides method of transaction in online shopping. Section VI presents proposed payment method. Section VII concludes the paper

A. *Objective:*

The main aim of the project is to design a feasible RS resistance secure algorithm which combines the use of both steganography and cryptography with the goals of improving security, reliability, and efficiency for secret message. DES encryption algorithm is used for encrypting the data into cipher text. Apart from that, LSB steganography is combined with the Genetic Algorithm making it more secure from RS steg analysis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

B. *Brief Overview:*

Image steganography is an emerging field of research for secure data hiding and transmission over networks. The proposed system provides the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA). Original message is converted into cipher text by using secret key using a sophis- ticated encryption algorithm. Then cipher text is hidden into the LSB of original image by manipulating the bit array of the original image. The resultant image file is called the stego image. The stego image contains the actual data encoded

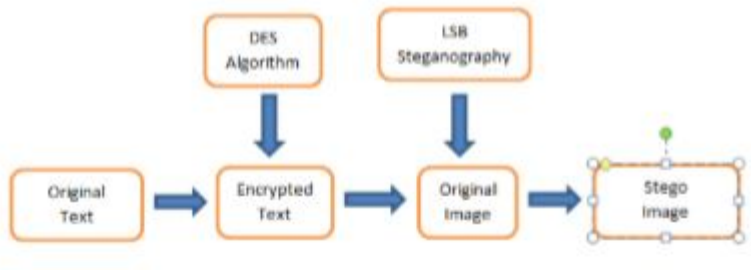

Fig:1. Steganographic Technique

II. RELATED WORK

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

a. Wireless Communication:

Wireless telecommunications, is the transfer of information between two or more points that are physically not connected. Distances can be short, as a few meters as in television remote control; or long ranging from thousands to millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of *wireless technology* include GPS units, garage door openers and or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones. Wireless networking (i.e. the various types of unlicensed 2.4 GHz WiFi devices) is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

b. *Benefits of Wireless Communication*:

Wireless LANs offer the following productivity, convenience, and cost advantages over wired networks:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

- Mobility: Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
  There are now thousands of universities, hotels and public places with public wireless connection. These free you from having to be at home or at work to access the Internet.
- Installation Speed and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Reduced Cost-of-Ownership: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- Scalability: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

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.

- ✓ Proposed method minimizes customer information sent TRANSFER OF FUND to the online merchant.
- ✓ So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side.
- ✓ Presence of a fourth party, CA, enhances customer's satisfaction and security further as 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.

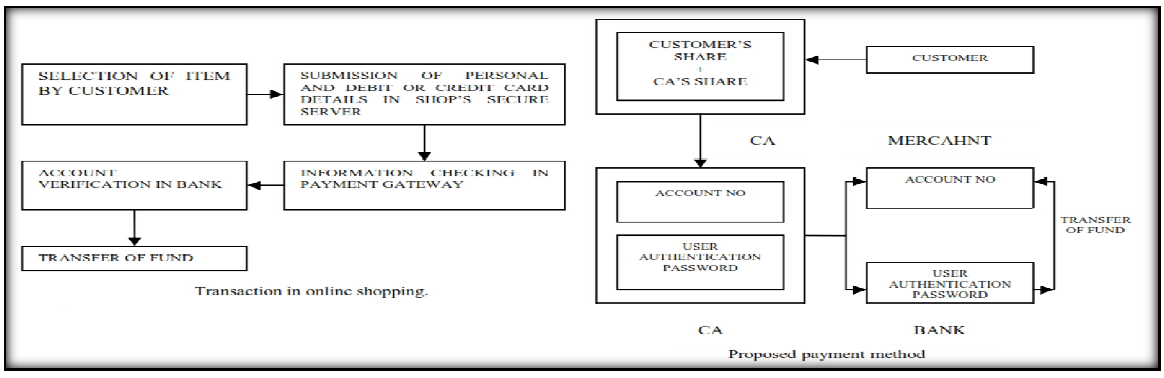

Fig:2.system architecture

EncodingPhase:

In the encoding phase, the cipher data obtained is written into an appropriate im- age. After getting the result of the previous phase in the text area, the software would ask to encode the data. When the encode but

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

tonispressed, the file chooser would open up to select the appropriate image file where the data is to encoded. When image file is selected, it is first loaded. It is better if the image used for encoding the cipher data is .png or .jpg. The image is first converted into a byte representation. The byte representation is important to modify the image. The cipher data is also converted into the byte format. The Bit-wise operations are used to add the cipher data into the image byte array bit by bit at the least significant bit.

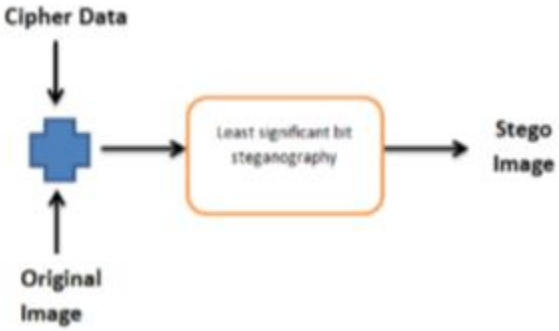

Figure .3: Encoding Phase

Pixel Modification Phase:

After the cipher data has been encoded into the image at the least significant bit. The image byte array has to be manipulated to enhance security and reliability. The LSB approach for data hiding is less secure as could be easily detected by steganalysis process such as RS steganalysis. So it is better to modify the pixel locations where the image has been stored. The RS analysis is considered as one of the most famous steganalysis algorithms which has the potential to detect the hidden message by the statistical analysis of pixel values The process of RS steg analysis uses the regular and singular groups as the considerations in order to estimate the correlation of pixels. The presence of robust correlation has been witness in the adjacent pixels. But unfortunately using traditional LSB replacing steganography, the system renders the alteration in the proportion in singular and regular groups which exposes the presence of the steganography. For pixel modi- fication, genetic algorithms are employed.

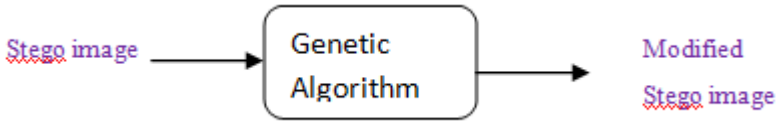

Figure 4: Pixel Modification Phase

of steganography and visual cryptography has been considered as a distinct topic for image security. Although there are extensive researches based on combining these two approaches, but the results are not so satisfactory with respect to RS analysis. Other conventional methods of image security has witnessed the use of digital watermarking extensively, which embeds another image inside an image, and then using it as a secret image. The use of steganography in combination visual cryptography is a sturdy model and adds a lot of challenges to identifying such hidden and encrypted data. Fundamentally, one could have a secret image with confidential data which could be split up into various encrypted shares. Fi- nally when such encrypted shares are re-assembled or decrypted to redesign the genuine image it is possible for one to have an exposed image which yet consists of confidential data.

Thecombinationofgeneticalgorithmalongwithvisualcryptographyhasbeen a powerful tool to enhance security and reliability. There is no steganalysis algorithm that could detect hidden data in such kind of images. Hence we can say that it is complete full proof approach without loopholes at least till date.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

OverlappingPhase:

The two shares of the same image are needed to retrieve the original information. As the cipher data is distributed in both the images, it is impossible for anyone to get the data by obtaining just a single share of the image. Hence both the shares are required to obtain original information. After the both the shares are obtained, the overlaying (overlapping) phase starts. In overlaying phase, one of the shares is overlaid over the other one appropriately. If it is overlaid properly, then we will get the original stego image otherwise a distorted image will be obtained. The in- formation cannot be retrieved from the distorted image. Hence it is very important to overlay the image properly.

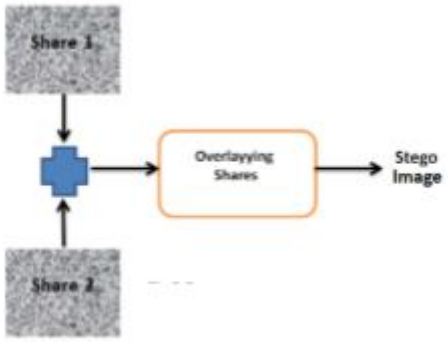

Figure 5. Overlapping Phase

After the overlapping phase, the inverse genetic algorithm is employed on the image to retrieve the original stego image back by re-modifying the pixel locations. The inverse genetic algorithm, as the name suggests, is the inverse process of genetic algorithm employed at sender side.

Decoding Phase:

In the decoding phase, the cipher data is decoded from the stego image. The cipher data can be retrieved by the inverse process of encoding process that was employed at the sender side.

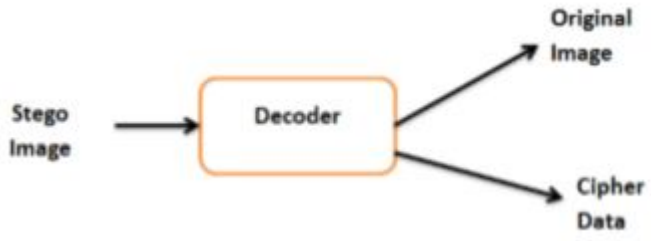

Figure .6: Decoding Phase

Decryption Phase:

In the decryption phase, the cipher data is converted into the original data. The DES algorithm is used in the inverse manner using the same encryption key(secret key) as used during encryption of the original data. Finally, the system will display the original text.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

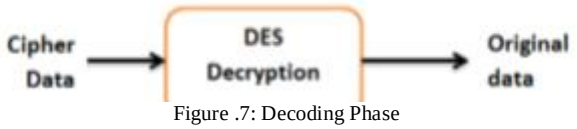

Figure .7: Decoding Phase

Customer Authentication:

Customer unique authentication password in connection to the bank is hidden inside a cover text using the text based Steganography method. 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. Now one share is kept by the customer and the other share is kept in the database of the certified authority.

Certification Authority Access:

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.

Final Authenticated Information Results

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.

IV. CONCLUSION AND FUTURE WORK

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 banking application which uses Steganography and visual cryptography 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.

REFERENCES

1. Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.
2. Javelin Strategy & Research, "2013 Identify Fraud Report," https://www.javelinstrategy.com/brochure/276.
3. Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwgtrendsreport_q2_2013 .pdf .
4. Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.
5. J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
6. Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.
7. Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

8. Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.
9. K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.
10. J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.
11. M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
12. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
13. Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008.
14. 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.
15. K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.
16. S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.