ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Steganography and Visual Cryptography Authentication System for Customer Online Payment Transactions

Rabia Basri
M.Tech,CN,
Shadan Women's College of Engineering & Technology, Hyderabad.

Amena Sayeed
Assistant Professor,
Department of CSE,
Shadan Women's College of Engineering & Technology, Hyderabad.

Ms.Saleha Farha
HOD,
Department of CSE,
Shadan Women's College of Engineering & Technology, Hyderabad.

ABSTRACT:

A high-speed prosperity in E-Commerce market has been witnessed 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. The main motive of this project is to provide high level security in E-Commerce applications and online shopping. This project minimizes detailed information sharing between consumer and online merchant but enable successful fund transfer thereby safeguarding consumer information and preventing misuse of information at merchant's side. This is achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography and Digital Signature for this purpose .

KEYWORDS:

E-Commerce, Online Shopping, Identity Theft, Phishing, Steganography, Visual Cryptography, Digital Signature.

INTRODUCTION:

Online shopping is the retrieval of product information[15] 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. 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 misusing 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. Phishing is an illegitimate mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service,[15] Financial and Retail Service are the most focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference of consumer information in transit between the consumer and the online merchant[5]. 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[3], 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. Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text , image , video , audio are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line , in open spaces , in word sequence . Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Visual Cryptography (VC), is a cryptographic[11] technique based on visual secret sharing used for image encryption. The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: BPCS Steganography and Visual Cryptography for safe online shopping and consumer satisfaction.

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing least 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 BPCS [7] 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's detailed information sent to the online merchant. So even if a breach takes place in merchant's database, customer doesn't get affected.

•Certified Authority acts as a fourth party thereby enhancing customer's satisfaction and security further.

•Usage of BPCS Steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy. It provides a higher level of security and a high information hiding capacity.

•Since customer data is distributed over 3 parties, a breach in single database can easily be contented. Link guard Algorithm is efficient for phishing prevention.

•The 2-out-2 feature of visual cryptography provides effective collaboration of images at the Certified .

LITERATURE SURVEY:
STEGANOGRAPHY:

Text-Based Steganography: It makes use of features of English Language like inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a statement .

BPCS Steganography: The information hiding capacity of a true colour image is around 50% . A sharpening operation[11] on the dummy image increases the embedding capacity quite a bit. Randomization of the secret data by a compression operation makes the embedded data more intangible. The steganography program for each user is easy. It further protects against eavesdropping on the embedded information. It is most secured technique and provides high security.

VISUAL CRYPTOGRAPHY :

Halftone visual cryptography:

This novel technique achieves visual cryptography [11] via half toning. Based on the blue-noise dithering principles, this method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.

2-0ut-2 Visual Cryptography:

Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares .

RELATED WORK:

A brief survey of related work in the area of banking security based on steganography and visual cryptography is presented in this section. A customer authentication system using visual cryptography is presented in but it is specifically designed for physical banking. A signature based authentication system for core banking is proposed in but it also requires physical presence of the customer presenting[9] the share. proposes a combined image based steganography and visual cryptography authentication system for customer authentication in core banking. A message authentication image algorithm is proposed in to protect against e-banking fraud[15]. A biometrics in conjunction with visual cryptography is used as authentication system .

ALGORITHMS:
BPCS (Bit-Plane Complexity Segmentation) STEGANOGRAPHY ALGORITHM:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The algorithm can be described in concise steps as follows .

•Convert the carrier image (of any file-format) from PBC (Pure Binary Code) to CGC (Canonical Grey Code) system and in png format.

•Perform the histogram analysis.

•After that bit-plane analysis is performed.

•Perform size-estimation i.e. calculate the places where we can store the secrete image.

•Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.

•After embedding mail that image to another user.

•For extracting the embedded image performs de-steganography which is exactly opposite to steganography.

VISUAL CRYPTOGRAPHY ALGORITHM:

•Visual cryptography is a type of cryptography which allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system.

•Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process.

•This is equivalent to using the logical OR operation between the shares .

LINKGUARD ALGORITHM:

•Link Guard works by analyzing the differences between the visual link and the actual link.

•It also calculates the similarities of a URI with a known trusted site.

EXISTING SYSTEM:

Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding[7][8] data rather than using properties of a sentence as in.

This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity. The steganography technique is based on Vedic Numeric Code in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary is used as the basis for assigning numbers to the letters in English alphabet. Number assignments of letters are shown in table 1. No separate importance is given for vowels and consonants as compared. Each letter is assigned a number in the range of 0 to 15. For different frequencies, different numbers are assigned to the letters. Number assigned in range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11. It basically represents frequency of letters in integer form. Above number assignment method is used to maximize no of letters in a particular assigned number group which in turn gives flexibility in word choosing and ultimately results in suitable sentence construction.

DISADVANTAGES OF EXISTING SYSTEM:

•In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction.

•Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

PROPOSED SYSTEM:

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. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 Now one share is kept by the customer and the other share is kept in the database of the certified authority. 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. 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. The problem is that CA does not know to which bank to forward the cover text obtained from combining two shares. It can be solved by appending 9 digit routing or transit number of bank with customer authentication information.

ADVANTAGES OF PROPOSED SYSTEM:

•Proposed method minimizes customer information sent 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 more number of parties are involved in the process. *f*

•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.

IMPLEMENTATION:

Steganography Process:

In this module, Steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity.

Encoding:

•Representation of each letter in secret message by its equivalent ASCII code.

•Conversion of ASCII code to equivalent 8 bit binary number. o Division of 8 bit binary number into two 4 bit parts.

•Choosing of suitable letters from table 1 corresponding to the 4 bit parts.

•Meaningful sentence construction by using letters obtained as the first letters of suitable words. o Encoding is not case sensitive.

Decoding Steps:

•First letter in each word of cover message is taken and represented by corresponding 4 bit number.

•4 bit binary numbers of combined to obtain 8 bit number.

•ASCII codes are obtained from 8 bit numbers.

•Finally secret message is recovered from ASCII codes.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

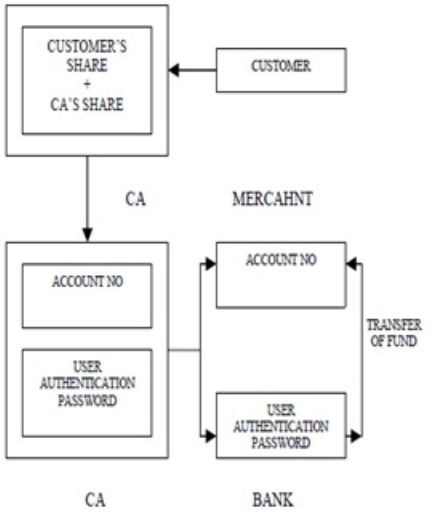

Fig :- Proposed payment method

CONCLUSION:

In our project, a payment system for online shopping is proposed by combining BPCS steganography and 2-out-2 visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. BPCS Steganography is really effective against eavesdropping and has a high information hiding capacity as compared to traditional steganography approach. The method is concerned only with prevention of identity theft and customer data security. The main aim is consumer satisfaction and authorized merchant-bank interaction for fund transaction. 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. 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 share1 and share2 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:

[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/apwg_trends_report_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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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.

[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.

[17] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.

Author's Details:

Ms.Rabia Basri has completed her B.Tech. in Information Technology from Greenfort Engineering College, JNT University, Hyderabad. Presently, she is pursuing her Masters in Computer Networks from Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, T.S, India.

Ms.Amena Sayeed has completed B.Tech (Computer Science Engineering) from JNT University, M.Tech (CSE) from JNT University. Currently, she is working as an Assistant Professor of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India.

Ms. Saleha Farha has completed her B.Ttech (Computer Science & Engineering) and M.Tech (Software Engineering) from JNTUH University, Hyderabad. She has five years of experience in teaching field. Currently, she is working as the Head of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India.