Online Payment System using Steganography and Visual Cryptography

ASHOK SINGH, DHONGADE KRUSHNANATH RAGHUNATH, AVINASH GIRI

ABSTRACT

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 onlinemerchant but enable successful fund transfer from consumer‟saccount to merchant‟s account thereby safeguarding consumerinformation and preventing misuse of information at merchant side.

I. INTRODUCTION

A cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an entrusted communication channel. The algorithm mainly deals with Steganography and Visual Cryptograph. A rapid growth in E-Commerce market is seen in Recent time throughout the world.

II. LITERATURE SURVEY

Cryptography is the practice and study of hiding the information into a particular form so that it cannot be read by casual eye.

Encryption

The process of encoding messages or information in such a way that onl;y authorized parties can access it.In an encryption scheme the intended communication information or message refered to as plain text is encrypted using an encryption algorithm,generating cipher text that can only be read if decrypted.

Symmetric key/private key

In encryption key schemes the encryption and decryption nkeys are the same.

Communicating parties must have the same key before they can achieve secure communication.

Asymmetric key/Public key

In public key encryption schemes the encryption key is published for anyone to use and encrypt messages.However only the receiving party has accessed to the decryption key that enables messages to be read.

Cipher text

In cryptograpy ciphertext is the result of encryption performed on plaintext using an algorithm is called as cipher.It contains a form of original plain text that is unreadable by human or computer without a proper cipher to decrypt it.

Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

AES Algorithm

AES is a block cipher. This means that the number of bytes that it encrypts is fixed. AES can currently encrypt blocks of 16 bytes at a time; no other block sizes are presently a part of the AES standard. If the bytes being encrypted are larger than the specified block then AES is executed concurrently. This also means that AES has to encrypt a minimum of 16 bytes. If the plain text is smaller

than 16 bytes then it must be padded.Simply said the block is a reference to the bytes that are processed by the algorithm.

III.PROBLEM STATEMENT

3.1 Problem Definition

This system 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.

3.2 Goals and objectives

The primary reason for selecting steganography among the list of possible project topics was due to the unfamiliarity of the word that twigged an interest in the subject.

Another reason is the data that it provides. Even if the hacker(or intruder) gets access to our multimedia data, then also he can‟t access the information, that is, the hacker has done the difficult part of hacking and getting access to the data but the actual data is still under his nose. This aspect makes it more interesting.

3.3 Outcomes

The system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.

The system does not provide a friendly environment to encrypt or decrypt the data (images).

The visual cryptography schemes that are used for data hiding have a security hole in the encrypted Share file.

Here an image based authentication using Visual Cryptography is implemented

IV.ALGORITHM

AES

AES is a symmetric block cipher. This means that it uses the same key

for both encryption and decryption.The algorithm begins with an Add round key stage followed by 9 rounds of four stagesand a tenth round of three stages. This applies for both encryption and decryption withthe exception that each stage of a round the decryption algorithm is the inverse of it‟scounterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

Enhanced Online Payment System

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage. Each of these stages will now be considered in more detail.

V. CONCLUSION

A payment system for online shopping is proposed by combining steganography and visual cryptography that provides customer data privacy and prevents misuse of data at erchant‟s side. The method is concerned only with prevention of identify theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography.

Phishing has becoming a serious network security problem, causing finical lose of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractiveto normal consumers. In this paper, we have studied the characteristics of the hyperlinks that were embedded in phishinge-mails. We then designed an anti-phishing algorithm, Link-Guard, based on the derived characteristics.

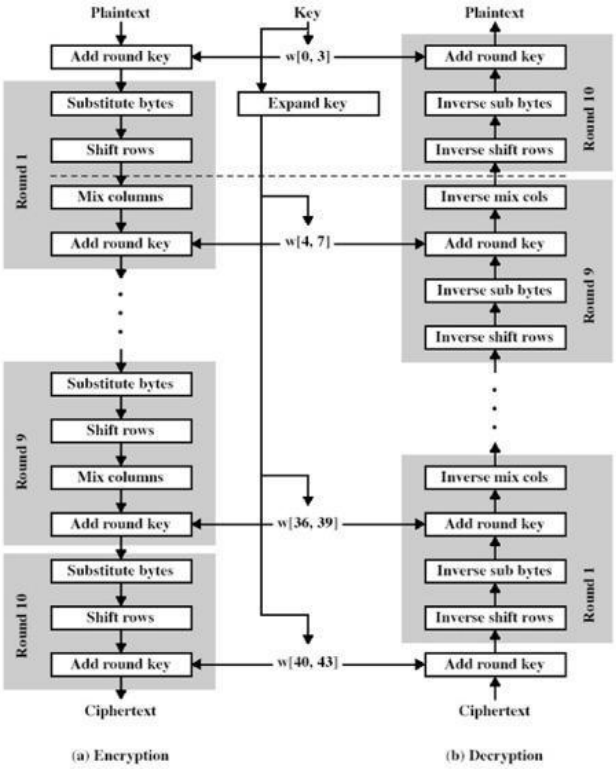

FIG: ARCHITECTURE DIAGRAM

VI. REFERENCES

1] Online Detection and Prevention of Phishing Attacks (Invited Paper)Juan Chen Institute of Communications EngineeringNanjing 210007, P.R. Chinaicechj@msn.com Chuanxiong Guo Institute of Communications Engineering Nanjing 210007, P.R. Chinaxguogieee.org 2006.

2] Secured Bank Authentication using Image Processing and Visual Cryptography B.Srikanth1, G.Padmaja2, Dr. Syed Khasim3, Dr. P.V.S.Lakshmi4, A.Haritha5 1Assistant Professor, Department of CSE, PSCMRCET, Vijayawada 2Associate Professor, Department of IT, PSCMRCET, Vijayawada. 3Associate Professor, Department of ECM, KL University,Guntur .4Professor, Department of IT, PVPSIT, Kanuru. 5Assistant Professor, Department of IT, PVPSIT, Kanuru.2008.

3] New Visual Steganography Scheme for Secure Banking Application S.Premkumar1,A.E.Narayanan2 Dept of Information Technology Periyar Maniammai University Thanjavur- 613 403, Tamil Nadu, Indiamailtosprem@gmail.com1, aenan jack@rediffinail.com2 International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

4] International Conference on Emerging Trends in Engineering, Science and Technolog (ICETEST - 2015) E –PAYMENT SYSTEM USING VISUAL AND QUANTUM CRYPTOGRAPHY Shemin P A a* ,Prof. Vipinkumar K S b Available online at www.sciencedirect.com

5] Design and Implementation of a Novel Authentication Algorithmfor Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme Harinandan Tunga1 and Soume Mukherjee2 1 Department of Computer Sc. & Engineering RCC Institute of Information technology Kolkata, West Bengal, India 2 Department of Computer Application RCC Institute of Information technology Kolkata, West Bengal, India IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012 ISSN (Online): 1694-0814 www.IJCSI.org