A Survey on Techniques of Data Hiding using Steganography & Visual Cryptography

Kale Mrunali V.[1] Pardeshi Shreya B.[2] Pardeshi Aniket S.[3]
[1,2,3]Department of Computer Engineering
[1,2,3]JCOE, Kuran

Abstract—In recent time E-Commerce is rapidly growth in E-Market specially for online shopping system. With ever increasing popularity of online shopping, Debit or Credit card wrongful and personal private information security are major concerns for customers, merchants and banks. Personal information and there misuse of that information for making purchase and bank accounts or arranging credit cards. The main motive of the proposed system prescribed in this paper is to handle applications that requires a high level of security, like E-Commerce applications, core banking and internet banking. This can be done by using combination of two methods: Text based Steganography and Visual Cryptography for safe online shopping and consumer satisfaction. This is achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography for this purpose.

Key words: Data Hiding, Visual Cryptography

I. INTRODUCTION

A large number of countries such as India, China and Pakistan that have some problems to become overcome in regard to credit card security such as in 2012 cardholders information was misused for average of 48 days as a result identity theft. In Online shopping the issue of purchase order through with help of electronic purchase request, filling of credit or debit card information. Identity theft or phishing are the dangers in E-Commerce's. Identity theft is the stealing of someone's identity in the form of personal information and misuse.

A new method is proposed, that uses text based steganography and visual cryptography, which limited information sharing between customer and online merchant but enable successful fund transfer and preventing misuse of customer information .Steganography is art of sending hidden or invisible messages. The name is taken "Steganographia" it is Greek world στεγανό-ς,γραφ-ειν meaning "covered writing" .The sending secret messages and attempts to cover the messages by hiding them by making them look like something else have been made .In short Steganographic is information can be hidden in almost anything, While much of modern steganography focuses on images, audio and other digital data, there is also a wealth of text sources in which information can be hidden. That are the various ways to hide information in text, there is a specific set of techniques which are uses. Certification Authority (CA) which has provides Key Infrastructure for secured transactions.

II. STEGANOGRAPHY TECHNIQUES

Over the last few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. Varity of Techniques is used for hiding messages or images information in such a ways that alteration made to the image is perceptually not discernible. Common approaches are includes like LSB, Masking and filtering and Transform techniques are used. The Least significant bit (LSB) algorithm having a simple insertion technique to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant deterministic sequence having bit plane of the cover-image in it.

Because the amplitude of the change is small, So that modulating the least significant bit does not result in human perceptible difference. In this paper, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded messages statistically noticeable increase but also the image fidelity degrades. Therefore a variable size LSB embedding schema is presented, in which the number of LSBs used for message extracting depends on the local characteristics of the pixel. LSB-based method is easy to implement and high message pay-load is the main advantage. LSB hides the message in such way that the humans do not perceive it, is it still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can be easily try to extract the message from the beginning of the image if they are suspicious that there exists only secret information that was embedded in the image. Therefore, a system named Secure Information Hiding System (SIHS) is propose to improve the LSB scheme.

It overcomes the problem of sequencing-mapping by embedding the massage into a set of random pixels, which are scattered on the cover-image. Usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks the Masking and filtering techniques are used. The technique perform analysis of the image, thus embed the data information in significant areas so that the hidden message is more integral to cover image than just hides it in the noise level. Transform techniques embed the message by modulating coefficient in a transform domain, such as the Wavelet Transform or Discrete Fourier Transform. These techniques hide messages in specific areas of the cover images, which all makes them more robust to attacks. Transformations can be applied over the entire image, to block throughout the image, or other variant.

Cryptography is securely related to the disciplines of cryptology and cryptanalysis. Cryptography includes methods such as microdots and merging words with images, and other ways to hidden information in storage or transit. However, in today's computer-centric world and cryptography is most often associated with scrambling plaintext (sometimes it referred to as clear text) into cipher text (that process called encryption), then back again (known as decryption). cryptographers means Individuals who practice this field. the information cannot be understood by anyone for whom it was unintended the information cannot be altered in storage or transit between sender and receiver without the alteration being detected the

creator/sender of the information cannot deny at a remaining stage his or her intentions in the creation or transmission of the information the sender and receiver can confirm each other's identity and the origin/destination of the information.

Cryptography has changed into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive data or information has proved a critical factors in success in war and business.

Because governments do not wish certain entities in and out of their countries that have access to ways to receive and send hidden data that may be a threat to national interests and cryptography has been subject to various restrictions in many countries and ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that can be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and more importantly and the underlying techniques of cryptography.

III. EXISTING SYSTEM

In online shopping system items selects by customers by using portal and then its directed to the pay on payment page. Online merchant have its own payment system or this can take advantage of third party payment systems such as pay online system, PayPal, Web Money and etc. In payment portal customer submits there credit or debit card details such as credit or debit card number, name on the card and expiry date of the card. Details of information search from shopper vary from one payment gateway to another. For e.g., payment in IRCTC website requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Snap deal or Flipkart requires Visa or Master secure code. In addition to that merchant may required a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is an authorizing code in CNP transactions. According to the PCI Data Security Standard, merchants are prohibited from storing CVV information or PIN data and if it permitted card information such as name, card number and expiration date is stored and certain security standards are required. However recent high profile breaches such as in Epsilon, Heartland Payment Systems and Sony's PlayStation Networks show that card holders' information is at risk both from inside and outside. A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint, is huge and the process is complex and time consuming and it will solve part of the problem. One still has to trust the merchant. And its employees not to use card information for their own purposes.

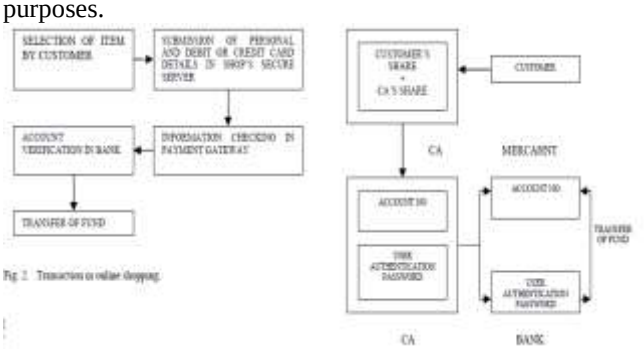

Fig 1: Existing System

IV. PROPOSED SYSTEM

In this paper, after viewing the proposed system will know the flow of work. There is a Customer which will register on the online shopping. Customer will select items on online shopping websites. When shopping is done for doing payment process the option window will be displayed to the customer. There is one extra option which is "Upload the Image". The Image is Steganograph Image which includes in it the Customer's Debit card number, Bank details etc. The customer details will be check by the server side. One Key value is provided to the Bank for the Decryption process. Then the payment process done. Fund will be transfer in the bank by the customer. Those are the working of proposed system which is introduced in this paper.

V. ARCHITECTURE

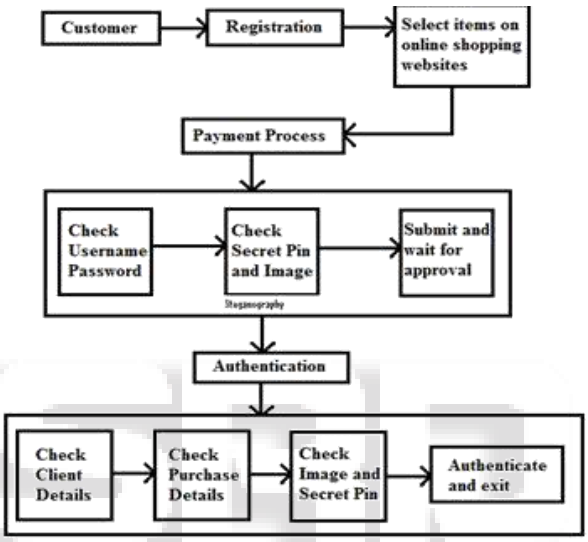

Fig. 2: Architecture of Proposed System

VI. ALGORITHM

In this paper the DES algorithm is used for the hiding the data. In this paper with help of Steganography concept the DES algorithm is work out. In the DES algorithm the key concept was introduced. The key value (KV) is provided for Encryption or Decryption process. The secrete message is converted into Binary format. With the help of key value the XOR operation is perform with the binary data format. Then Encryption process is done.The high security level related to a small key used for encryption and decryption having easily understood.

When we do Image Encryption this system use two techniques is as

- XOR Operation &
- Bit Rotation Operation.

To perform this operation system must have the input as

- Image
- Image Encryption Key
- Secret Message

then Stego Image will be form.

Take an Example if our Input Key is JAIHIND then from the input key, this system will generate an 8-bit Key Value (KV) by following method.

Bit(ASCII(J) XOR Bit(ASCII(A)) XOR Bit(ASCII(I)) XOR Bit(ASCII(H)) XOR Bit(ASCII(I))XOR Bit(ASCII(N))XOR Bit(ASCII(D))

In Image the color channel R is going to hold the hidden data for that also we are changing only last 4 LSB. Since we are changing the last 4 LSB for only one color channel, there will not be any damage to the real image.

Example: if we are planning to hide a text A
Get the Encrypted value to hide by KV i.e. A (XOR) KV
Let the output Binary value is 0101 1000 Split Binary part into A and B like that A = 0101 and
B = 1000
Let R value in 1, 1 is 120 (R1) and R Value in 1, 2 is 91(R2)
R1 = Binary (120) = 0111 1000
R2 = Binary (91) = 0101 1011
Replace last 4 bit in R1 by A and Replace last 4 bit in R2 by B
After Conversion R1 = 0111 0101 and R2 = 0101 1000
Data Encryption Process:
Let A is a text to be hide, A ASCII Value is 65, Binary is 0100 0001
Let KV value is 1100 1100
Then A (XOR) KV = data to be hided
Example.

A => 0100 0001
KV=> 1100 1100
XOR output => 1000 1101

Data Decryption Process:
Output =1000 1101
KV=1100 1100
XOR output = 0100 0001.

VII. Drawback

In that system hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility sentence construct. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construct. 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 .he traditional system, customer does not know whether her or his PIN No and CVV No is sent to the merchant. They have to trust the merchant and its employees to use card information for that own motives. This representation doesn't show high level security. In traditional systems, that is no additional non-functional requirement of phishing mechanism that can be harmful and might lead to employment of social engineering and technical centrifuge. Thus, in the overcome drawback in our system by mentioned in this paper would ensure better security and satisfaction of customer or other transaction stakeholders.

VIII. Advantages

Proposed method limited customer information sent transfer fund to the online merchant. So in case of a breach in merchant's database, customer doesn't affected. It also prevents illegal. Use of customer information at merchant's side. The present of fourth party, CA, customer's satisfaction and security another part are involved in the process. Usage of Steganography ensures that the Certified Authority does not know customer authentication password thus maintaining customer secure information.

Cover text can be sent in the form of email from Certified Authority to bank to avoid rising suspicion.
Since customer data is distributed over three part, a breach in single database can easily be satisfied.

IX. Conclusion

In our paper, a payment system for online shopping is proposed that combines Steganography and visual cryptography and provides customer data not observed and prevents misuse of data by the merchant's side. Steganography is really effective again staves fall and has a high information hiding capacity as compared to traditional steganography approach. The main objective is customer satisfaction and authorized merchant-bank interaction for fund transaction. This method prevent of identity theft and customer data security. In compare to other banking application that uses steganography and visual cryptography are basically applied for physical banking, the proposed method can be applicable for E-Commerce with interesting areas like payment during online shopping as well as physical banking.

Reference

[1] U.Naresh, U.VidyaSagar, C.V. MadhusudanReddy , " Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36.
[2] 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.
[3] 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.
[4] 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.
[5] ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,",in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008.
[6] Juan Chen, ChuanxiongGuo, "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on Communications and Networking in China (ChinaCom '06), pp. 1 - 7,Beijing, China, 2006. 1143 www.ijergs.orgInternational Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015 ISSN 2091-2730
[7] 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.

