ISSN : 2231-0711

S.Nagendrudu et al | IJCSET(www.ijcset.net) | June 2015 | Vol 5, Issue 6,162-165

Integration of BPCS Steganography and Visual Cryptography for Secure e-Pay

S.Nagendrudu, V.Ramakrishna Reddy

Computer Science Department,
Santhiram Engineering College,
JNTUA, A.P.,India

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 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, Phishing

I. INTRODUCTION

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. If the user forget the secure ID and account ID, it can be easily retrieved with the protection. So, automatically privacy is enhanced here. 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 methods 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.

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. Today, the online project is becoming more popular. 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. Phishing is also 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. 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.

II. BPCS STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

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 [4], image [5], video [6],

Audio [7] are used as a cover media for hiding data in steganography.

Types of 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 color image is around 50% . A sharpening operation 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.

BPCS (Bit-Plane Complexity Segmentation) STEGANOGRAPHY ALGORITHM

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.

III. Related Work

A. Basic Overview on Cryptography

Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers. The two types of algorithms that will be discussed are

- Joint Key Cryptography (Symmetric Key Cryptography): Uses a single key for both encryption and decryption
- Public Key Cryptography (Asymmetric Key Cryptography): Uses one key for encryption and another for decryption

1. The joint key Cryptography: (Symmetric key cipher)

It uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key.A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world. In other words it serves the purpose of hiding a smaller key instead of the huge chunk of message data.

2. The Public Key Cryptography (asymmetric key cipher)

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. It is a technique that uses a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique. The public key cryptography is a fundamental and most widely used technique, and is the approach which underlies Internet standards such as Transport Layer Security (TLS). The most common algorithm used for secret key systems is the Data Encryption Algorithm (DEA) defined by the Data Encryption Standard (DES)

3. A Hybrid Cryptosystem

A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. It can be constructed by using any two separate

Cryptosystems. It is a more complex cryptography system that combines the features of both joint and public key cryptography techniques. We shall use traditional public key cryptography techniques to covert the message into a cipher. For embedding the cipher into images, a modified joint key technique will be used.

IV. Proposed Bpcs Based Steganography Method

4.1. Introduction

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason, to overcome the short comings of traditional steganographic techniques such as Least Significant Bit (LSB) technique, Transform

Embedding technique, Perceptual masking technique. This traditional technique has limited data hiding capacity and they can hide up to 10 – 15% of the vessel data amount. BPCS steganography makes use of

Important characteristic that of human vision. In BPCS, the vessel image is divided into "informative region" and "noise-like region" and the secret data is hidden in noise blocks of vessel image without degrading image quality. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits . But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region .

4.2. Basic Principle of BPCS Steganography

In BPCS, a multi-valued image (P) consisting of n-bit pixels can be decomposed into set of n – binary pictures. Ordinary image data is represented by a pure binary code system which is commonly used in image processing. However CGC is preferred over PBC in BPCS steganography. Example: P is an n-bit gray image say n=8. Therefore P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each bit plane can be segmented into "informative" and "noise" region. An informative region consists of simple pattern while noise-like region consists of complex pattern. In BPCS, we replace each noise-looking region with another noise-looking pattern without changing the overall image quality. Thus, BPCS steganography makes use of this nature of human vision system

4.3. Bit Plane Slicing Concept in BPCS

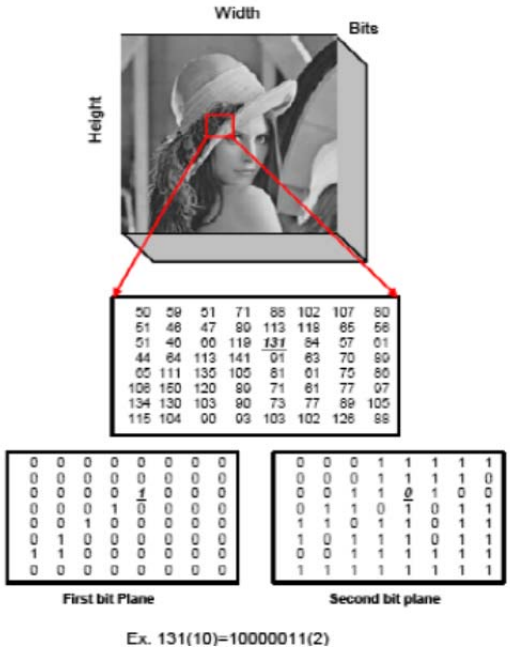

Figure 1: Bit Plane Slicing concept considering pixel having value 131.

The bit plane slicing can be better understood with the help of figure 1. The operation of splitting the image into its constituent binary planes is called “Bit plane slicing”. Pixels are digital numbers composed of bits. In an 8-bit image, intensity of each pixel is represented by 8-bits. The 8-bit image is composed of eight 1-bit plane regions from bit plane ‘0’ (LSB) to bit-plane ‘7’ (MSB). Plane ‘0’ contains all lowest order bits of all pixels in the image while plane ‘7’ contains all higher order bits. Bit plane Slicing is useful

for image compression. Complexity of each bit–plane pattern increases monotically from MSB to LSB

.

V. Proposed System

- Proposed System Visual Cryptography (VC), technique based on visual secret sharing used for image encryption.
- Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant.
- 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.
- VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system.
- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.
- Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.
- Cryptographic technique :(2, 2) - Threshold VCS scheme, (n, n) -Threshold VCS scheme, (k, n) Threshold VCS scheme are used in this proposed system.
- Cryptographic algorithms generally need a reference table which aids the conversion of a small block of data into another block (may not be a block of data in the original content).
- In order to provide higher security levels the algorithm is designed to use a reference

Database. The reference database will consist of various reference grids. Each of these grids will have a 3-d representation of the encoding schema which will be used to represent the characters in terms of specific numbers. (The same number may or may not represent a different character in a different grid).

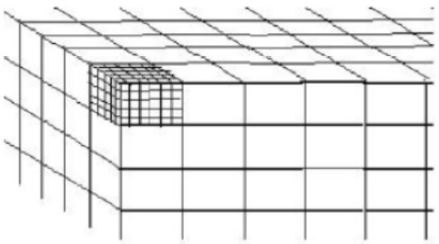

Fig. 2 Matrices in a Grid of the Reference database

A .Encryption Algorithm

- The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm. This cipher will now be hidden into a multimedia file.
- The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit (or a predefined digit) and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. (This change should be less than 5 for each of R,G and B values) This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited. Thus one byte of data will be stored per pixel in the image.
- In this method the cipher sequence can be decoded without the original image and only the edited image will be transmitted to the receiver.
- In the first few lines of image properties, the attributes of the image will be encrypted and saved so as to provide us the information if the image is edited or modified or the image extension has been changed like jpg to gif. These properties can be used in the decoding. So only the correct encrypted image in the correct format will produce the sent message.
- For decryption, the receiver must know which image to decode and in which format as changing the image format changes the colour distribution of the image. Every image gives a random data on decryption that

has no meaning. But only the correct Format decryption gives the original message.

- After hiding the data in the image, the image will be sent to the receiver. The receiver should have the decryption key (private key) which will be used to decode the data.

B. Decryption Algorithm

- The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image.
- The receiver's private key is used to identify the reference grid from the reference database.
- After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component as shown in Fig. 3.

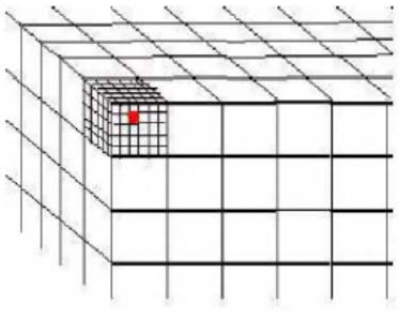

Fig 3: Identification of correct grid in reference database

- The cipher is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). These numbers will now define the saved bit and will form the Cipher text.
- This cipher can now be decrypted using an inverse function of the DEA algorithm to get the message text.

C. Advantages:

- Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography.
- It prevents password and other confidential information from the phishing websites.
- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

VI. CONCLUSIONS

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 identify theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography [12, 13, and 14], 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/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.

[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.

AUTHOR BIBLIOGRAPHY

S.Nagendrudu is working as a Lecturer in CSE Department, Satnhiram Engineering College, nandyal, kurnool District,Andhra Pradesh. he has a total of 8 Years Experience in Teaching. he has six International Journal Publications.

V.Rama Krishna Reddy is working as a Lecturer in CSE Department, Satnhiram Engineering College, nandyal, kurnool District,Andhra Pradesh. he has a total of 5 Years Experience in Teaching.