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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

# A Review of an Online Fund Transfer System by Using Steganography and Visual Cryptography

Sonali M. Bhakare, Hirendra R. Hajare, Chhaya C. Prasad

B.E Student, Dept. of CSE, Ballarpur Institute of Technology, Ballarpur, Gondwana University (MS), India

Asst. Professor & HOD, Dept. of CSE, Ballarpur Institute of Technology, Ballarpur, Gondwana University (MS), India

B.E Student, Dept. of CSE, Ballarpur Institute of Technology, Ballarpur, Gondwana University (MS), India

**ABSTRACT**: Non-traditional idea used in days, there is boom of cashless transaction of funds in a market. And major fear for user in online shopping is to provide security to credit or debit card information. Personal identity stealing and phishing are the major issues of online shopping like customer name, password debit or credit card information from victims. There is a techniques used to betray customer. In this paper the idea is to provide to the propose system that uses visual cryptography and text based steganography by using AES algorithm. There is a new approach to provide high level security for fund transfer. And it wills increases user self-assurance and keeps biometric thieving.
.

**KEYWORDS**: Transaction security, Steganography, visual cryptographyand online shopping.

## I. INTRODUCTION

The smart fund transaction security can be known as online fund transfer system by using steganography and visual cryptography, which indicate the automation of fund transfer with internet used in online shopping. This could be control of debit card or credit card information leakage. Online fund transfer system by using steganography and visual cryptography security has changed a lot from the last century and will be changing in coming years. Security is an important aspect or feature in fund transaction applications. The new and emerging concept of fund transfer offers a comfortable, convenient and safe environment for customers. In this paper method proposed is especially for electronic commerce but it can easily be elongated for online as well as physical banking. That system keeps safe intruders by giving image crypting with text that is visual cryptography and text base steganography. However a smart security system offers many more benefits. Mainly focus of this paper on security of fund transfer when the customer is always to be used. Two techniques are proposed. One is visual cryptography and other is steganography to protect from intruders. The first security technique used is steganography which is the art of hiding text with another so that hidden text is identical. The major concept under steganography is that text to be transmitted is not perceptible by casual eye. The ascendency of preferring text base steganography over other steganography technique is its simpler and smaller memory requirement for the transaction.Next visual cryptography which deals with visual secret to share the image between bank and customer. Image encrypted with text and image share with untrusted communication channels for fund transfer from customer account to merchant account by self-grading customer information at merchant side. This project mainly used to decrease the customer information sharing in between the customer and merchant.

### Text based Steganography:

In text Steganography, message can be hidden by shifting word and line, in open spaces, in word succession. Attributes of a conviction such as number of phrases, number of characters, numbers of vowels, location of vowels in a word are also used to hide private message. The advantage of choosing text Steganography over other Steganography techniques is its smaller memory requirement and simpler communication.

DOI: 10.15680/IJIRCCE.2017. 0501004

**Visual Cryptography:**

Visual Cryptography (VC), proposed by Naor, is 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 untrusted communication groove. Only blending the k shares or more give the original secret image.

## II. RELATED WORK

A short measurement of related work in the area of banking security based on online shopping by combine use of Steganography and visual cryptography proposes this methods to eradicate the frauds through text based Steganography hiding data rather than using properties of sentences and each letter is assigned to a num in the range of (0-15) 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.

**Table: Number assignment:**

| Letter | Number assigned | Letter | Number assigned |
|---|---|---|---|
| E | 15 | M | 7 |
| A | 14 | H | 7 |
| R | 13 | G | 6 |
| I | 13 | B | 5 |
| O | 12 | F | 4 |
| T | 11 | Y | 4 |
| N | 11 | W | 3 |
| S | 10 | K | 3 |
| L | 10 | V | 3 |
| C | 9 | X | 2 |
| U | 8 | Z | 2 |
| D | 8 | J | 1 |
| P | 7 | Q | 0 |

The above table 1 shows the number assigned to a letter.

**Encoding**

Steps:

1. Representation of each letter in secret message by its equivalent ASCII code.
2. Conversion of ASCII code to equivalent 8 bit binary number.
3. Division of 8 bit binary number into two 4 bit parts.
4. Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
5. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
6. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
7. Encoding is not case sensitive.

**Decoding**

Steps:

1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.
2. 4 bit binary numbers of combined to obtain 8 bit number.
3. ASCII codes are obtained from 8 bit numbers.

4. Finally secret message is recovered from ASCII codes.

**Result**

To implement the above text based steganography method, a secret message is considered. Suppose it is “text”.
Text = 01110100011001010111100001110100
Result of encoding is shown in Fig

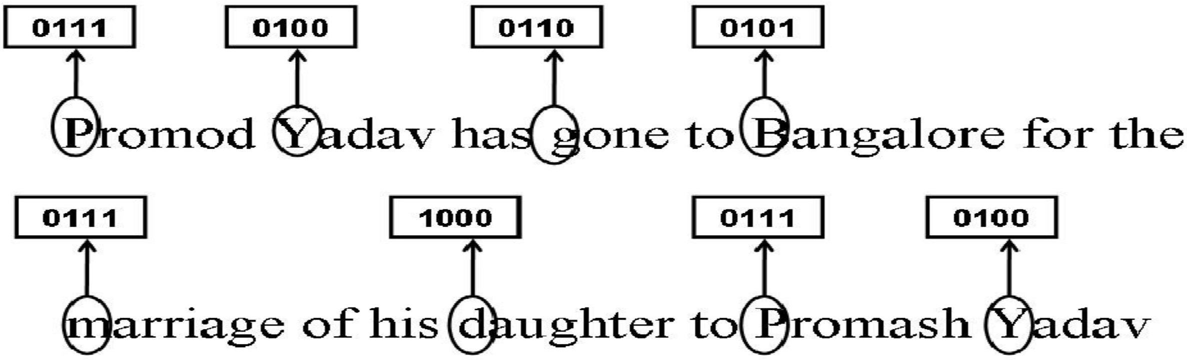
0111
0100
0110
0101
Promod Yadav has gone to Bangalore for the
0111
1000
0111
0100
marriage of his daughter to Promash Yadav

Fig: Cover message.

**Drawback**

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 createspam mail to hide one’s banking information.

## III. PROPOSE SYSTEM

The proposed work is basically a framework designed in C# .Net with two main modules e.g. Steganography using AES Algorithm and Visual Cryptography. An input image is accepted as cover image for the input message in plain text format. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the stegno-image are modified by the visual cryptography to keep their statistic characters. The experimental results should prove the proposed algorithm’s effectiveness in resistance to steganalysis with better visual quality. The user can select their targeted information in terms of plain text for embedding the secret message in LSB of the cover image. The implications of the visual cryptography will enable the pixels value of the stegano-image to keep their statistic character. LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. This is also one of the strong algorithms which keep theinformation proof from any intruder. The applied technique uses allocation of pseudorandom number as well as exchange of pixels. One of the contrast parts of this implementation is that while decrypting, the stegano-image will be morphologically same compared to the cover image with respect to the shape and size thereby preventing pixel expansion effect. The implementation of the algorithm yields in better result with insignificant shares when stegano images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in both grey as well as coloured output.

DOI: 10.15680/IJIRCCE.2017. 0501004

**ADVANTAGES**

1. The proposed system provides two way authentication i.e. authenticating client and merchant server.
2. Proposed method minimizes customer information sent transfer of funds to the online merchant.

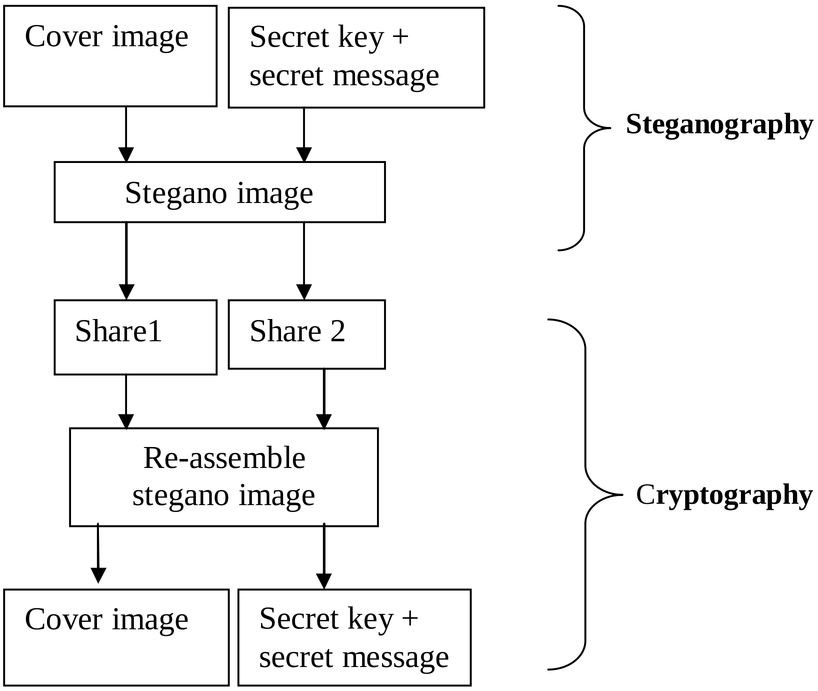
Cover image
Secret key + secret message
Stegano image
Share1
Share 2
Re-assemble stegano image
Cover image
Secret key + secret message
Steganography
Cryptography

Fig: Propose method Architecture

## IV. ALGORITHMS

**Algorithm**: Text base steganography **(Embedding the text inside the image)**
**Input**: secret message and secret Key
**Output**: Stegano image

1. Calculate the Pixels of the image.
2. Make a loop through the pixels.
3. In each pass get the red, green and blue value of pixels.
4. Make the LSB of each RGB pixel to zero.
5. Get the character to be hidden in binary form and hide the 8-bit binary code in the LSB of pixels.
6. Repeat the process until all the characters of the image are hidden inside the image.

**Algorithm**: Visual Cryptography
**Input**: Stego-Image
**Output**: Encrypted Shares

1. Read Stegao-Image generated
2. The stegao image is braked into three layers namely split- 1, split-2 these two files are containing the hidden data and to get the hidden data these two files have to be reconstructed perfectly then,
3. The re-assembled picture and the extracted data will be gained again.

## V. FUTURE SCOPE

The proposed work in this paper uses a steganography technique called image steganography. The data is embedded into the steganography image. The main purpose of the project is to provide security. The cover media helps to embed the data. In future we can use different carriers and different keys for encryption and decryption of data which will provide greater security.

## VI. CONCLUSION

In this paper, we proposed a payment system for online shopping by combining text based Steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant side. The computing is implicating only with prevention of identity theft and customer data security. In likening to other banking application which uses Steganography and visual cryptography are basically applied for the physical banking, the proposed method can be applied for the E-Commerce with focus area on payment during online shopping as well as physical banking.

## REFERENCES

1. 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science 978-1-4799-2526-1/14/$31.00 ©2014 IEEE "Online Payment System using Steganography and Visual Cryptography" Souvik Roy1 and P. Venkateswaran2 Department of Electronics & Tele-Communication Engineering Jadavpur University, Kolkata-700032, India(souvikece31@gmail.com1, pvwn@ieee.org2).
2. International Journal of Computer Applications (0975 – 8887) Volume 124 – No.6, August 2015 Combine Use of Steganography and Visual Cryptography for Online Payment System V. Lokeswara Reddy, PhD Associate Professor Department of CSE KSRM College of Engineering Kadapa, YSR District. AP (INDIA).
3. Volume IV, Issue X, October 2015 IJLTEMAS ISSN 2278 - 2540 www.ijltemas.in Page 94 Online Payment System using Steganography and Visual Cryptography Priyanka More, Pooja Tiwari, Leena Waingankar, Vivek Kumar Department of Computer Engineering, Savitribai Phule Pune University, Pune-411041, India.
4. Volume 6, Issue 3, March 2016 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com Steganography Based on AES Algorithm and BPCS Technique for a Securing Image Arjun Kumthe, Kajal Jadhav, Nikita Dhande, Prof. Arati Dandawate Dhole Patil College of Engineering, SPPU, Pune, Maharashtra India.
5. Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedingsof the First International Workshop on Information Hiding, pp. 293-315, Cambridge, UK, 1996.
6. K. Bennet, "Linguistic Steganography: Surevey, Analysis, andRobustness Concerns for Hiding information in Text," PurdueUniversity, Cerias Tech Report 2004—2013.
7. Javelin Strategy & Research, "2013 Identify Fraud Report,"https://www.javelinstrategy.com/brochure/276.
8. Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L MPatnaik, "Secure Authentication using Image Processing and VisualCryptography for Banking Applications," Proceedings of 16thInternational Conference on Advanced Computing andCommunications, pp. 65-72, Chennai, India, 2008.
9. M. Naor and A. Shamir, "Visual cryptography," Advances inCryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
10. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "NovelAuthentication System Using Visual Cryptography," Proceedings of2011 World Congress on Information and CommunicationTechnologies, pp. 1181-1186, Mumbai, India, 2011.
11. Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shoppingonline," Proceedings of 2011 International Conference on Electronic andMechanical Engineering and Information Technology (EMEIT), vol. 9,pp. 4693-4696, 2011
12. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994.

## BIOGRAPHY

**Sonali M. Bhakare**isStudent of Dept. of Computer Science And Engineering, Ballarpur Institute of Technology, Ballarpur, Gondwana University Gadhachiroli,She received diploma in Information Technology from Government Polytechnic, Bramhapuri (MS), India. Her research interest in latest computer technology, Algorithms etc.

**Hirendra R. Hajare**is Assistant Professor and HOD Dept. of Computer Science And Engineering, Ballarpur Institute of Technology, Ballarpur, Gondwana UniversityGadhachiroli, he received master degree form RTM university, Nagpur, his research interest are computer networking and wireless technologies etc.

**Chhaya C. Prasad**Student of Dept. of Computer Science And Engineering, Ballarpur Institute of Technology, Ballarpur, Gondwana University Gadhachiroli (MS), India. Her interest in programming languages.