Secured Online Payment System

[1]Swapna B Sasi, [2]Aaditya Anil, [3]Arjun T A, [4]Harry John

[1]AP, CSE Department, Jyothi Engineering College, Kerala, India

[2 3 4] Students, CSE Department, Jyothi Engineering College, Kerala, India

---***---

Abstract - *Online payment system allows money transfers to be made only through internet instead of using cash or a check, in person or by mail. Nowadays there is a tremendous growth in online payment throughout the world, so the E-shopping users are facing more problems. The main problem is security. We provide secured online payment system through various techniques. The main techniques used are Steganography, Visual Cryptography and OCR. This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping.*

Key Words: *Information security; Steganography; Visual Cryptography; Online shopping*

1. INTRODUCTION

In this busy world most of us prefer doing online shopping and online payment. Since there is no waste of time in this process a tremendous growth in online payment has been seen throughout the world. Online shopping security is a concern for everyone who makes purchases on the Internet, but it is also an important issue for business leaders — and not just those in the retail sector. Firms go for online shopping, and their employees frequently make business purchases on the company credit card. So, the attackers mainly focus on this process and e-shopping users are facing more problem. Security is the main problem behind this system. Online payment is an electronic payment for goods or services electronically without using cash or check in person or by mail. It could be achieved through different modes. Different modes are Debit card, Credit card, E-money and Electronic fund transfer. Since there is less security by using this type of payment, we provide a secure payment by using different technologies [4].

This paper consist of a new proposed system, that uses text based steganography [2] and visual cryptography [1]. It provides only limited information that is necessary for fund transfer during online shopping and thereby protecting customer data and increasing customer confidence and preventing identity theft [4]. Optical character recognition also known as OCR [7] is used to convert the typed, printed or handwritten text into encoded machine text. It can be used in machine translation, text-to-speech and text mining. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.

2. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is a practice of hiding a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding an encrypted message such that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data. The messages could be hidden under image, audio, video, text.

The text based steganography [2] technique is based on Vedic Numeric Code. Frequency of letters in English alphabet in conjunction with Vedic Numeric Code is used for the steganography technique. No separate importance is given for vowels and consonants. Text steganography [2] uses text as a cover media for hiding message. Message can be hidden by shifting word and line in the open spaces and in word sequence. Sentence properties such as number of words, number of characters and number of vowels and position of a vowel in a word are also used to hide secret message. The advantage of choosing text steganography over other steganographic technique [12] is its smaller memory requirement and simpler communication.

Visual cryptography (VC)[5][10] was brought out by Moni Naor and Adi Shamir at *EUROCRYPT 1994*. It is used to encrypt written material (printed text, handwritten notes, pictures, etc) in a perfectly secure way. The decoding part is done by the human visual system directly, without any computation cost. Using k out of n (k,n) visual secret sharing scheme [11], a secret image is encoded into n shadow images called shares [8][9], in which each participant in P receives one share. The original message is visible if any k or more of them are stacked together, but totally invisible if fewer than k transparencies are stacked together.

3. PROPOSED TEXT BASED STEGANOGRAPHY METHOD

In this paper, 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 more flexibility and freedom from the point view of sentence construction but it increases computational complexity.

3.1 ENCODING

Encoding involves the use of a code to change original data into a form that can be used by an external process. The type of code used for converting characters is known as American Standard Code for Information Interchange (ASCII), the most commonly used encoding scheme for files that contain text. ASCII contains printable and nonprintable characters that represent uppercase and lowercase letters, symbols, punctuation marks and numbers. A unique number is assigned to some characters.

- Each letter is represented in secret message by its equivalent ASCII code.
- ASCII code is converted to equivalent 8 bit binary number.
- 8 bit binary number is divided into two 4 bit parts.
- Suitable letters are chosen from Table 1 corresponding to the 4 bit parts [1].
- Meaningful sentence is constructed by using letters obtained as the first letters of suitable words.
- Encoding is not case sensitive.

3.2 DECODING

Decoding is the opposite process -- the conversion of an encoded format back into the original sequence of characters.

- Representation of corresponding 4 bit number by taking the first letter in each word of cover message.
- 4 bit binary numbers are combined to obtain 8 bit number.
- ASCII codes are acquired from 8 bit numbers.

Finally secret message is restored from ASCII codes

Table -1: 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

4. PROPOSED PAYMENT METHOD

In the proposed payment system solution, information to the online merchant submitted by the customer is minimized by providing only minimum information that verifies only the payment made by the said customer from its bank account. This is attained by the introduction of a central Certified Authority (CA) [3] and combined application of steganography and visual cryptography [1] [10]. The information accepted 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. In the proposed method, the user first need to register by entering his account no and password including other details. By registering he/she will get the certificate. It contains the customer unique authentication password in connection to the bank which is hidden inside a cover text using the text based steganography method by using LSB (Least Significant Bit) algorithm [6]. This process is shown in Figure 1.

The LSB based image steganography embeds the secret message in the least significant bits of pixel values of the cover text. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover text with the bits of the messages to be hidden without destroying the property of the cover text significantly. Customer authentication information that is the account no in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken as shown in Figure 2. From now one share is kept by the customer and the other share is kept in the database of the certified authority as shown in Figure 3 and Figure 4. Figure 5 shows the result of combining share 1 and share 2.

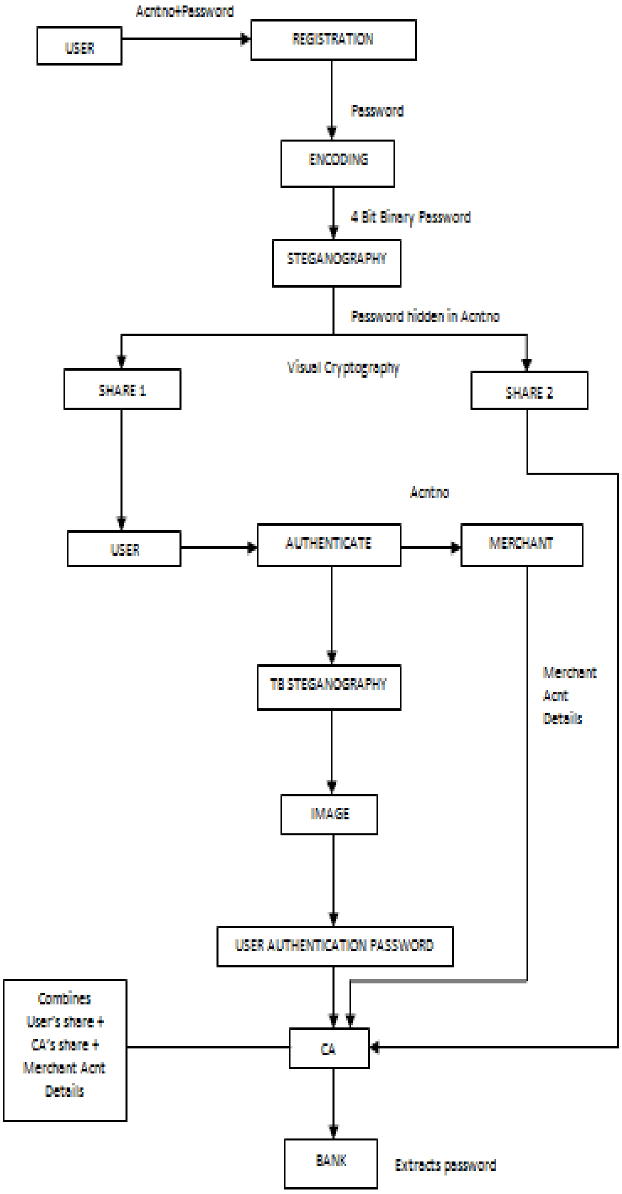

Fig -1: Architectural Diagram

During online shopping, 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 or the customer submits his/her own share and the 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's account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. This is done by OCR technology [7] [15]. OCR (optical character recognition) is the recognition of printed or written text characters by a computer. This involves photo scanning of the text character-by-character, analysis of the scanned-in image, and then translation of the character image into character codes, such as ASCII, commonly used in data processing. Customer authentication information is sent to the merchant by CA. After receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, then the bank transfers fund from the customer account to the submitted merchant account. Finally when the merchant receives the fund, then merchant's payment system authorizes receipt of payment using customer authentication information.

One 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.

5. ADVANTAGES

- Provides high security due to the usage of 2 techniques viz, Steganography and Visual Cryptoraphy [1].
- 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 [3], CA, enhances customer's satisfaction and security further as more number of parties is involved in the process.
- 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.

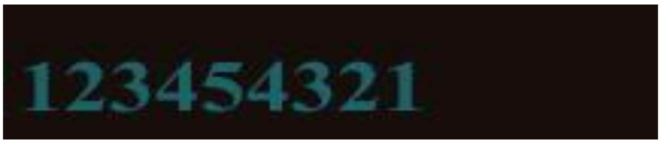
123454321

Fig -2: Snapshot account no and cover text.

Fig -3: Share 1 kept by customer.

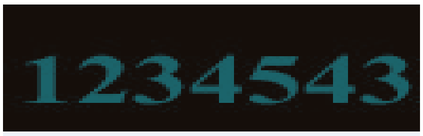

Fig -4: Share 2 kept by CA.

Fig -5: Overlapping of share 1 and share 2.

6. METHOD EXTENSION

The present system is developed in such a way that it can undergo future enhancements in an efficient manner. Now the password is converted using encoding technique whereas in future, encryption techniques can be implemented to make the system more secured. A mobile application can also be build so that users will be more comfortable in using it. The payment system can also be extended to physical banking. In addition to customer authentication password, shares may contain customer image or signature. In the bank, customer submits its own share and customer's physical signature is validated against the signature obtained by combining customer's share and CA's share along with validation of customer authentication password. It prevents misuse of stolen card and stops illegitimate customer.

7. CONCLUSIONS

The traditional approaches in online payment system somehow do not allow necessary secrecy to the users. In this paper online payment system is proposed by combining text based Steganography and visual cryptography [1]. It provides customer data privacy and prevents misuse of data at merchant's side. This paper proposes a steganographic algorithm for hiding text files in images. The visual cryptography is used for secret sharing of images. The CA will control the encoding and decoding processes. OCR technology [13] is used for identifying texts and characters from images and this OCR technology method is concerned only with prevention of identity theft and customer data security. In comparison to the banking application which uses steganography and visual cryptography they are basically applied for physical banking. Not only for physical banking, the proposed method can be applied for e-commerce which focuses on payment during online shopping as well as physical banking.

REFERENCES

[1] Souvik Roy, P. Venkateswaran "Online Payment System Using Steganography and Visual Cryptography," 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Sharma et al., "A New Approach to Hide Text in Images Using Steganography," International Journal of Advanced Research in Computer Science and Software Engineering 3(4), April - 2013, pp. 701-708.

[3] Wang Yang Yu, Chun Gang Yan "Modeling and verification of online shopping business processes by considering malicious behaviour patterns," IEEE Transactions,2014.

[4] K.S.Suganya, K.Manikandan"Enhanced Secure E-Gateway using Hierarchical Visual Cryptography," IJETT vol.3 Jan 2015- ISSN: 2349 – 9303.

[5] Shyam Nandan Kumar "Cryptography during Data Sharing and Accessing Over Cloud," International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 12-18.

[6] Shilpa Gupta1,Geeta Gujral2,Neha Aggarwal3 "Enhanced Least Significant Bit algorithm For Image Steganography," IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

[7] Amarjot Singh, Ketan Bacchuwar, Akshay Bhasin "A Survey of OCR Applications," International Journal of Machine Learning and Computing, Vol. 2, No. 3, June 2012.

[8] Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli "Visual Cryptography for Print and Scan Applications," Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium

[9] Pallavi Vijay Chavan, R.S. Mangrulkar, Third International Conference on Emerging Trends in Engineering and technology, "Encrypting Informative Color Image using Color Visual Cryptography" 2010 IEEEDOI 10.1109/ICETET.2010.94.

[10] Lekhika Chettri, "Visual Cryptography Scheme Based On Pixel Expansion for Black & White Image", International Journal Of Computer Science and Information Technologies, Vol.5 (3),2014,4190-4193.

[11] Mr Rohith S, Mr Vinay G "A Novel Two Stage Binary Image Security using (2,2) Visual Cryptography Scheme," International Journal Computational Engineering Research, ISSN:2250-3005.

[12] Arfan Shaikh1, Kirankumar Solanki2, Vishal Uttekar3, Neeraj Vishwakarma4" "Audio Steganography And Security Using Cryptography" International Journal of Emerging Technology and Advanced Engineering, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.

[13] Ayatullah Faruk Mollah, Nabamita Majumder, Subhadip Basu, Mita Nasipuri,"Design of an Optical Character Recognition System for Camera-based Handheld Devices", International journal of Computer Science Issues, Vol. 8, Issue 4, pp. 283-289, July 2011.