Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 3, March -2016

New Approach To Online Payment Security

Prof. Dadaram Jadhav[1], Mohit Patil[2], Himanshu Joshi[3], Mohammad Jakir[4], Charushila Talekar[5]

[1]Department of computer Engineering, Trinity college of Engineering and Research
[2]Department of computer Engineering, Trinity college of Engineering and Research
[3]Department of computer Engineering, Trinity college of Engineering and Research
[4]Department of computer Engineering, Trinity college of Engineering and Research
[5]Department of computer Engineering, Trinity college of Engineering and Research

Abstract — *now a days there is huge increase in usage of online shopping. But most of the e-commerce do not provide the best security over the transaction. During the process of transaction all the confidential data like in debit card, credit card, visa card etc. are required for each and every purchase of products. During this process of payment the confidential data is not secure or safe to give towards the third party. To overcome this disadvantage or to protect this data or providing the security to this confidential data, one method is used which is combined use of the steganography and visual cryptography over the payment process.*

Keywords- *Secret key generation, encode, steganography, visual cryptography.*

I. INTRODUCTION

During online shopping there is involvement of debit and credit card which comprises highly confidential data and if this data gets stolen by unauthenticated user there is a chance of invalidated fund transfer by identity theft [1]. This misuse of personal information can lead to suspicion in internet security and it is cause of loss of users in huge numbers. The process of Phishing is an illegitimate action that involves stealing of personal user information to steal personal identity and make invalidated financial frauds [2].

In this paper, a new approach is been proposed, that uses visual cryptography and steganography which unconditionally demolishes any chances of sharing information with the online merchant but it successfully transfers fund from consumer's account to merchant's account and hence it keeping safe the user information and avoid misuse of that information from the merchant side [3][4]. This mechanism could also be extended outside online shopping level as it could be used in physical banking. Steganography is process of hiding textual confidential data in the image which is 24 bit color image and the process involves removing confidential data and the image after removing this complex areas is very large [5][6].

If correct image is used it can be decrypted, this is the technique called visual cryptography [7]. The by Naor and Shamir was proposed this system in1994. Two transparent images used by visual cryptography [8]. This two above mentioned techniques are used in detail for coherent and well-planned functioning of the proposed method

II. EXISTING SYSTEM

Up to now we already researched the number of papers and systems for the online transaction there is unsecure transaction of money over the third party. In the current online payment system, each and every time user need to be submit the all the information regarding account/card. This provides the very poor security towards the user.

III. DISADVANTAGES

The existing system takes the unnecessary information from the user, which provides the poor security in result. The existing system provides the authority to the third party portal to read the all data information regarding user's account.

IV. PROPOSED SYSTEM

In this paper we proposed a technique known as use of steganography and the visual cryptography at the same time to provide the secure transaction. In this propose technique customer only submits the basic information during the registration time.no need to provide the card details to the merchant site.at the time of the transaction the account related information is verify by central certified authority (CA) and the combine use of steganography and visual cryptography method will provide the one share image to the CA for verification. The actual processing steps to understand this technique as follows:

1) Registration process of customer.

2) Online shopping process is done by the customer at merchant site.

3) The actual payment process is start now after the selection of things at the merchant site.

4) Account number and any secret text (random text) is need to enter by the user.

5) Cipher text is generated by encoding and encryption key is sent by the mail to the customer.

6) This cipher text is covered by image using steganography and making two shares of that cover text image.

7) One share is sent to the certified authority (CA) for verification.

8) After verifying or by confirming the user need to enter the encryption key sent by mail.

9) By matching this image and encryption key the payment transaction is successfully completed.

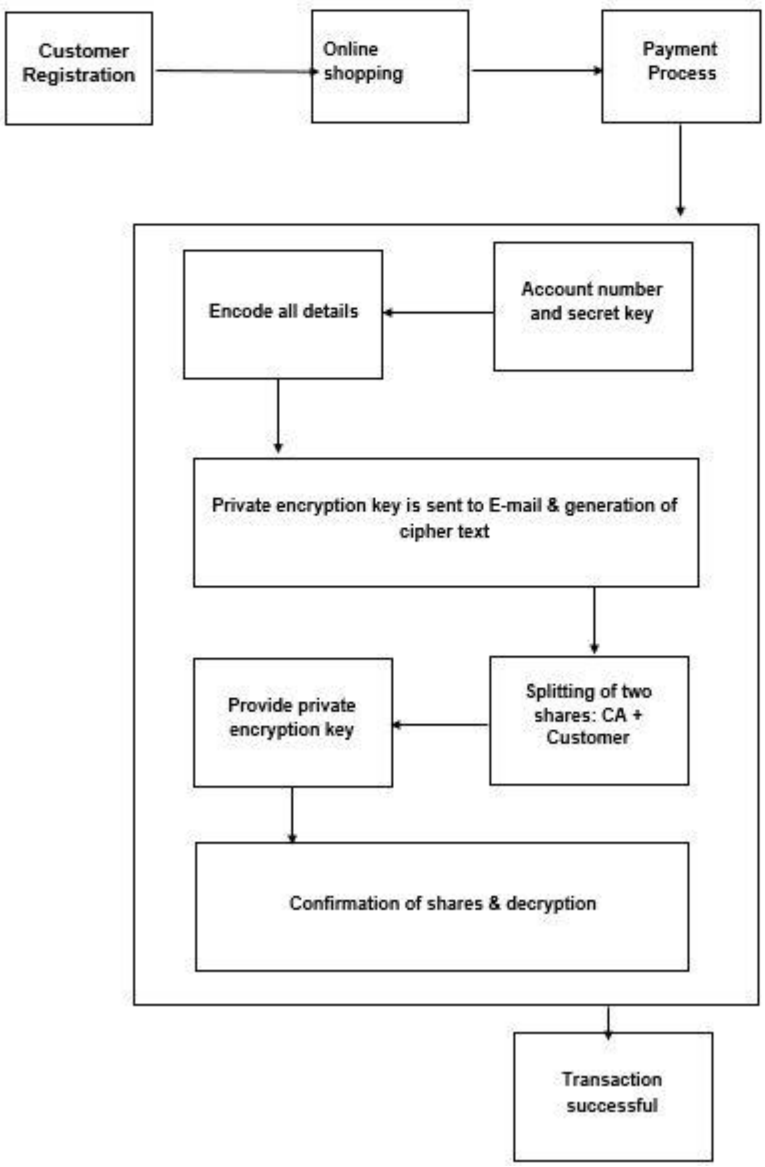

Customer Registration
Online shopping
Payment Process
Encode all details
Account number and secret key
Private encryption key is sent to E-mail & generation of cipher text
Provide private encryption key
Splitting of two shares: CA + Customer
Confirmation of shares & decryption
Transaction successful

Figure 1. System architecture

V. ALGORITHS

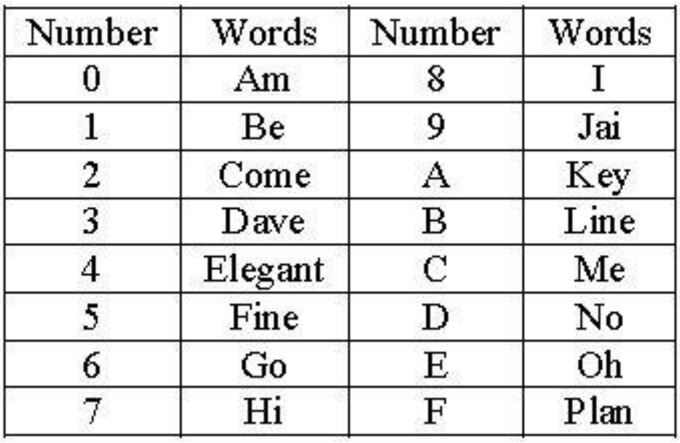
5.1 Steganography algorithm using ASCII code

5.1.1 Encoding steps

1. Take input in the text form. Each letter in it is represented by its ASCII code.

2. Obtained ASCII code which is expressed in 8 bit binary number. The 8 bit binary number is now divided into two 4 bits parts.

3. Each four bit part representing a number in the range 0 to F hex representations is then used to choose corresponding suitable words from the table below:



Number	Words	Number	Words
0	Am	8	I
1	Be	9	Jai
2	Come	A	Key
3	Dave	B	Line
4	Elegant	C	Me
5	Fine	D	No
6	Go	E	Oh
7	Hi	F	Plan

Table 1. Bit part numbers

5.1.2 Decoding steps

1. Word of cover message is now taken and represented by equivalent number from the table.

2. Each number is represented by its four bit binary.

3.4 bit binary numbers are combined to obtain 8 bit number.

4. ASCII codes are obtained from 8 bit numbers.

5. To end secret message is recovered from ASCII codes

5.2 Visual cryptography

Input: Stego-Image

Output: Two Encrypted Shares

Step 1: Read stego Image which is generated by steganography algorithm.
Step 2: The stego image is break down into two 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 completely.
Step 3: The re-assembled picture and the extracted data will be gained again from shares.

Here are screenshots from web application:

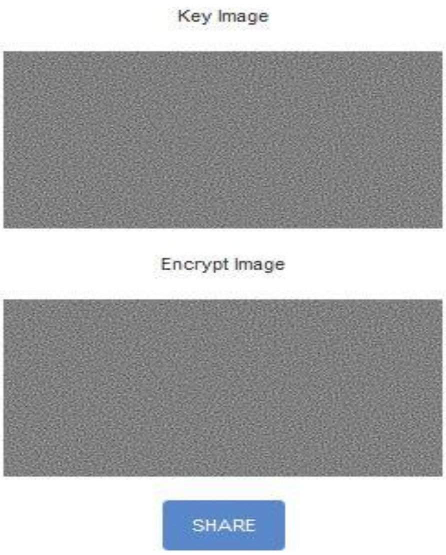
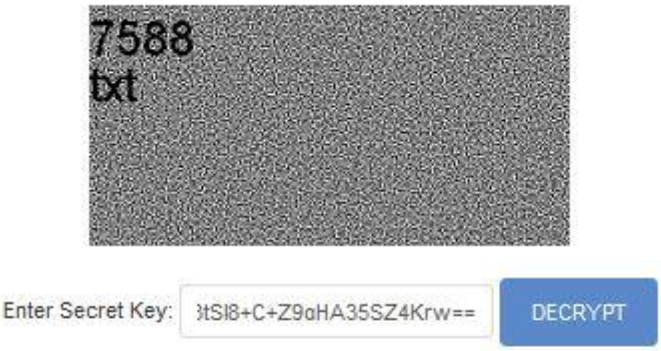


Figure 2. Splitting of shares by visual cryptography



Enter Secret Key: 3tSI8+C+Z9aHA35SZ4Krw==

Figure 3. Decryption

VI. CONCLUSION

We have developed a web-based application "Online payment system" which uses text based steganography and visual cryptography to make the online payment processing more secure and a lot more confidential. The major aim of the developed application is to avoid misuse or inappropriate usage of confidential data at the merchant's side. The current methodology can also be expanded for implementation at physical banking to make it more secure.

VII. FUTURE SCOPE

As this application is designed to protect from identity theft and misuse of confidential user data so it could also be used in small business which has a customer base as purchase in the stores can also be done with the use of credit and debit cards for which the security has to be ensured. It can also be expanded for usage in physical banking to make the physical commercial transfers more secure. This can also be implemented for standardization of a particular product or a community by making their personal identification or confidential identity secured and make it remain confidential.

As this application is designed to protect from identity theft and misuse of confidential user data so it could also be used in small business which has a customer base as purchase in the stores can also be done with the use of credit and debit cards for which the security has to be ensured. It can also be expanded for usage in physical banking to make the physical commercial transfers more secure. This can also be implemented for standardization of a particular product or a community by making their personal identification or confidential identity secured and make it remain confidential.

VIII. REFERENCES

[1] Souvik Roy and P. Venkateswaran "Online Payment System using Steganography and Visual Cryptography" 2014 IEEE Students, Conference on Electrical, Electronics and Computer Science.

[2] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report, 2013".

[3] Applied cryptography by Bruce Schneier.

[4] M. Naor and A.Shamir, "Visual cryptography," Advances in cryptography: EUROCRYPT'94, LNCS, Vol. 950, pp, 1-12,1995.

[5] J. Chen, T.S. Chen, M.W. Cheng, "A new data hiding scheme in binary image," Proceeding of fifth internation symposium on Multimedia Software Engineering, pp. 88-93, 2003.

[6] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding" Proceesings of the first international workshop on information hiding315, cambridge, UK, 1996.

[7] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu,"Techniques of data hiding,"IBM Systems Journal, Vol. 35, Nos.3 and 4 pp.313-336, 1996.

[8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniquesfor Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[9] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating OnlineThreats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.

[10] J.C. Judge "Steganography: Past , Present and Future." SANS Institute November 30, 2001