Approach for Secure Onlinetransaction using Visual Cryptography & Text Steganography

S. R. Navale[1] , S. S. Khandagale[2], R. A. Malpekar[3], Prof. N. K. Chouhan[4]
Department of Information Technology,
JSPM's Bhivarabai Sawant Institute of Technology & Research,
Pune, India.

***Abstract*— An online payment system permits a consumer to make a payment to an online merchant or a supplier. Payment portal, a channel between consumers and payment processors, use numerous security tools to secure a consumer's payment information, ordinarily card data, during an online transaction. However, the security provided by a payment portal cannot completely protect a consumer's payment information when a merchant is also allowed to obtain the payment information in specific form. Moreover, not all merchants provide a secure payment environment to their consumers and, in spite of having a standard payment plan, adhere to it. Consequently, this exposes a consumer's payment information to risks of being compromised or misused by merchants or stolen by hackers and spammers. In this paper we propose a new approach for online transaction in which a consumer's payment information is minimized to that is only needed for transfer of funds. A consumer sends his payment information directly to a payment portal and a payment portal, upon verifying the consumer, allows the transaction and sends a payment receipt to the appropriate merchant. We use the text steganography and visual cryptography to securely transfer funds to a merchant and protect a consumer's payment data from any Internet susceptibilities.**

Keywords*— *Online Payment Systems, Payment Portals, Steganography, Visual Cryptography.

I. INTRODUCTION

This paper proposes a new approach to electronic payment in which a consumer's payment information cannot be obtained by a merchant. A consumer's payment information is usually a debit or credit card detail, and providing it to a merchant during e-payment exposes this sensitive financial information to several risks. Few of these commonly known risks are data altering, stealing credit card data and credit card fraud. A merchant may or may not exploit consumer data but can definitely store it. In that case, if a merchant's server or system is not secure enough to prevent intrusion of data stealers, spammers, spyware, malware and hackers, consumer data may be stolen and misused. Hence, to avoid the issue of data mishandling or unsecured data on the merchant side, we propose a payment method that does not send consumer payment information to merchants and allows only payment portal to deal with it. Payment portal are secure and reliable, because they comply with the standard data security rules and communicate with banks and credit card companies using the most secure methods and technologies. To strengthen data security, the implemention of a new payment portal scheme is introduced along with visual cryptography & steganography in our proposed online payment system.

The selling and buying of goods and facilities over the Internet is known as electronic commerce (e-commerce). The concept of e-commerce is, however, not just limited to buying and selling of goods. It also includes the entire purchase process of developing, marketing, vending, supplying, servicing and paying for products and services.

With the development of e-commerce, payment systems and protocols have been developed. The current payment system consists of merchants, consumers and transaction portals such that a merchant receives a consumer's payment information and forwards it to a payment portal to process the payment. This, however, exposes a consumer's payment information to risks, because a merchant can save the consumer's payment information in either plain or encrypted form and may misuse it later. It is also possible that a merchant's server, through which a consumer's payment information is forwarded to a payment portal, is compromised and the merchant is unaware of it.

In 2006, five noted payment brands, VISA, MasterCard, Amex, JCB, International and Discover Financial Services, formed a council of security standards called the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an open global forum that works on developing, managing, spreading awareness and educating merchants and consumers about PCI Security Standards. They also work on Payment Application Data Security Standard (PA-DSS) and Pin Transaction Security (PTS) requests. Online merchants who use these five payment brands for payment in their websites are required to follow the PCI DSS policies. Violation of the policies may result in revoking a merchant's right to sell, but an online merchant knowingly or unknowingly may not follow all the PCI DSS policies. Furthermore, violation of a policy is usually tracked when it is reported by someone or a breach is identified with a merchant. Taking all this into consideration, we propose a secure online payment system where a consumer's payment information is directly sent to a payment portal and a merchant do not obtain a consumer's payment information, not even in encrypted/hashed form.

II. STEGANOGRAPHY

With the explosive development of internet in recent years the security and the confidentiality of the sensitive information has become of prime and utmost significance and concern. To protect this information from unauthorized access and tampering various methods for information hiding like , hashing ,cryptography, authentication have been established. In this paper we will discuss one such information hiding technique called Steganography[10]. Steganography is the process of masking sensitive information in any media to transfer it securely over the underlying unreliable and insecure communication network.

III. VISUAL CRYPTOGRAPHY

Visual cryptography[11] (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual cryptography (VC), proposed by Naor and Shamir, is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption is achieved by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

IV. LITERATURE SURVEY

a. Phishing

a) Microsoft Phishing Filter uses a combination of Microsoft's URL Reputation Service (URS) and local heuristics built into the IE 7 browser.

b) Netscape Browser 9.0 includes a built in phishing filter which relies solely on a prohibition, which is kept by AOL and updated frequently.

c) McAfee's Site Advisor product is a free stand-alone anti phishing product. Suspect or blocked sites are identified by a popup balloon and by colour and text changes in the button.

d) Link guard Algorithm is efficient for phishing prevention. This algorithm is described in detail later.

b. Steganography

a) 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 [13].

b)BPCS Steganography: The information hiding capacity of a true colour image is around 50% [14]. A sharpening operation on the dummy image increases the embedding capability 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.

c. Visual Cryptography

a) Halftone visual cryptography: This novel technique achieves visual cryptography via half toning. Based on the blue-noise dithering principles, this method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.

b) 2-0ut-2 Visual Cryptography: 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 [6].

V. RELATED WORK DONE

A short-lived study of related work in the area of banking security based on steganography and visual cryptography is presented in this division. A consumer authentication system using visual cryptography and steganography is presented in [5] but it is precisely designed for physical banking. A signature based authentication system for core banking is proposed in [6] but it also requires physical presence of the consumer presenting the share. [7] proposes a combined image based steganography and visual cryptography authentication system for consumer authentication in core banking. A message authentication image algorithm is proposed in [8] to protect against e-banking fraud. A biometrics in conjunction with visual cryptography is used as authentication system [9].

VI. EXISTING SYSTEM

Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Facility, Financial and Selling 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 have to trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

A. Sequence of Traditional Payment System:

The standard sequence of steps used in the current payment system is as follows:

a) A consumer visits a merchant's website and selects the items he wants to buy. He adds these items into his online shopping cart.

b) When ready to purchase, a consumer provides his payment information to the merchant. Payment information includes a consumer's debit or credit card information.

c) The merchant redirects the consumer's payment information to a payment portal for authorizing the consumer's payment.

d) The payment portal checks the consumer's payment information, and if correct, authorizes the payment. The payment portal then sends a payment capture token to the merchant. A payment capture token is a message indicating the authorization of a payment to a merchant. The merchant needs to provide the payment capture token information when requesting payment from the payment portal.

e) After receiving the payment capture token from the payment portal, the merchant sends a message to the consumer indicating the authorization of the payment.

f) The merchant sends the consumer's purchased item to the consumer and requests the payment portal for payment of the same. A merchant sends the payment capture information, received from the payment portal, to request payment for a purchase.

g) The payment portal confirms the payment capture information sent by the merchant. If verified, the payment portal sends the payment to the merchant.

B. Drawbacks:

In the existing payment system above, consumer is not certain whether his PIN No and CVV No is sent to the merchant's website. One has to trust the merchant and its employees to use card information for their own motives. This illustration doesn't confirm high level security. Part of the solution can be that the merchant can be forced to be a PCI complaint but it will be time consuming. In this system, there is no additional non-functional requirement of phishing mechanism which can be harmful and might lead to employment of social engineering and technical stratagem. Thus, in the proposed system mentioned later in this paper would ensure better security and satisfaction of consumer or other transaction stakeholders.

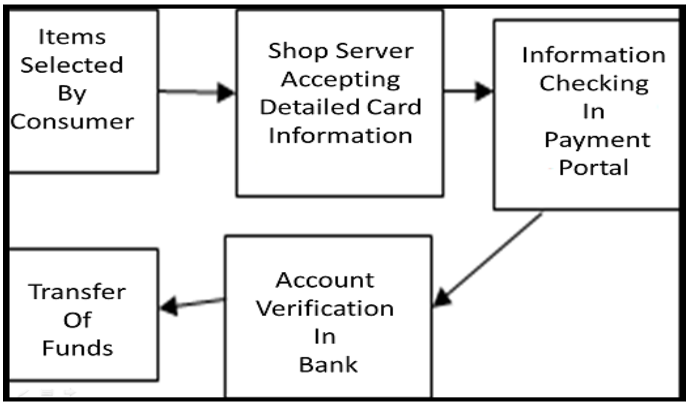
Items Selected By Consumer
Shop Server Accepting Detailed Card Information
Information Checking In Payment Portal
Account Verification In Bank
Transfer Of Funds

Fig. 1. Existing Payment System.

VII. PROPOSED METHODOLOGY

In the proposed system, information submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information that will only verify the payment made by the consumer from its account. This is accomplished by the introduction of a central Certified Authority (CA) and combined application of Steganography and visual cryptographic technique. The information obtained by the merchant will only validate receipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

1. *Sequence Of Proposed Payment System*

Step 1: Consumer registration process.
Step 2: Share 1 generated using Steganography and Visual Cryptography.
Step 3: Consumer opts for online shopping (Merchant Side).
Step 4: Consumer completes the shopping process and directed to payment process.
Step 5: Consumer submits the share 1 provided while registration and Merchant provides its account details.
Step 6: The Consumer Share and Bank Share are combined and verified by the CA.
Step 7: If the share is valid then the transaction will be Synchronized with the bank. If share not valid then error message will be sent.
Step 8: For valid share the Bank will extract the Account number from the original image and perform the transaction.
Step 9: A notification will be sent to the consumer via mail.

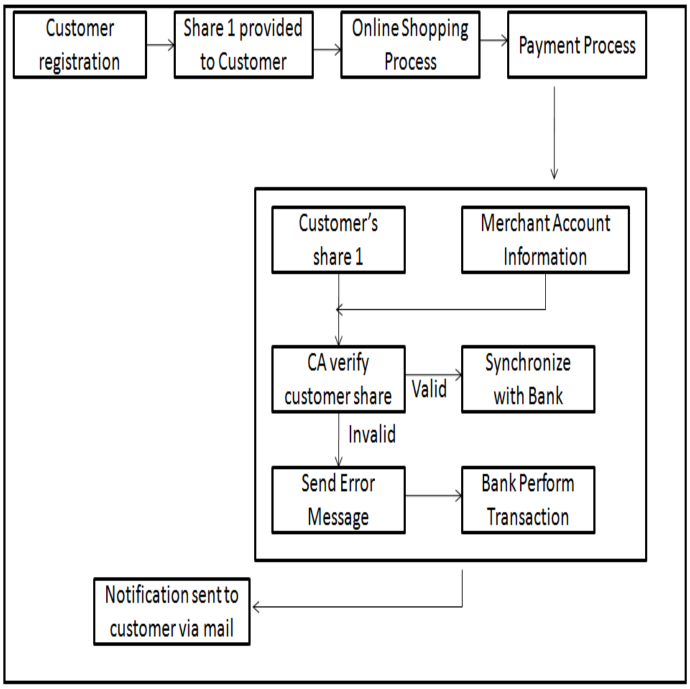

Fig. 2. Proposed Payment System.

2. *Steganograhy algorithm using ASCII Code*

Encoding Steps :

- Take input in the text form.
- Each letter is represented by its ASCII code.
- Obtained ASCII code is expressed in 8 bit binary number.
- The 8 bit binary number is then divided into two 4 bits parts.
- 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 Word Assignment

Decoding Steps:

- Word of cover message is taken and represented by corresponding number from the table.
- Each number is represented by its four bit binary.
- 4 bit binary numbers are combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes

3. *Algorithm for Visual Cryptography*

(k, n) threshold RG-based VC.
Input: A binary secret image S and a cover binary image C, both with M × N pixels, the threshold parameters (k, n), and two light transmission parameters w_0, w_1, where $0 < w_1 \leq w_0 < 1$
Output: n meaningful shares $SC_1, SC_2, \ldots SC_n$.
Step 1: For each position (i, j) € $\{(i, j) \mid 1 \leq i \leq M, 1 \leq j \leq N\}$ in the secret image, repeat Steps 2 to 6.

Step 2: Set $б_1$= S(i, j), Repeat Step 3 for k-2 times, i.e for p = 1, 2,…, k - 2, to generate pixels $b_1, b_2, \ldots b_{k-2}, b_{k-1}$ where b_x and $б_x$ denote the temporary pixels, x =1, 2,…, n-1, n.

Step 3: If $б_p = 0$, $б_{p+1} = b_p$; otherwise, $б_{p+1} = б_p$. Where b_p is generated randomly by flip-coin function.

Step 4: If the corresponding cover image pixel C(i, j) = 0, w = w_0 ; otherwise, w = w_1.

Step 5: Generate a pixel b_{k-1} by $b_{k-1} = g(w)$.
If $б_{k-1} = 0$, $b_q = b_{k-1}$, q = k, k+1,…, n;
otherwise, $b_q = g(w)$, q = k,k+1,…,n.

Step 6: The order of the n pixels $b_1, b_2, \ldots b_{n-1}, b_n$ are rearranged and there arranged n pixels are assigned to $SC_1(i,j), SC_2(i, j), \ldots SC_n(i, j)$.

Step 7: Output the n shadow images $SC_1, SC_2, \ldots SC_n$.

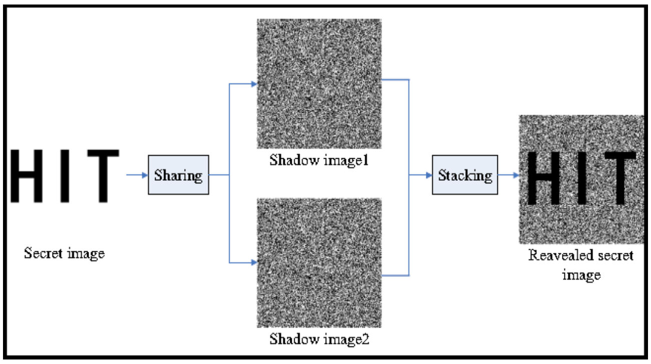

Fig. 3. An application example of RG-based (2,2) VC The secret is encrypted into two random shares which have the same size as the secret image.The revealed image shows the secret image with 50% contrast loss.

4. *Advantages*

- Proposed method minimizes consumer information sent for TRANSACTION OF FUNDS to the online merchant’s website.
- So in case of a breach in merchant’s database, consumer’s information doesn’t get affected. It also prevents illegal use of consumer information at merchant’s website.
- Presence of a fourth party, CA, enhances consumer’s fulfilment and security further as number of parties are involved in the process.
- Usage of Steganography ensures that the CA does not know consumer authentication password thus maintaining consumer’s privacy.
- Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.
- Since consumer data is distributed over different parties, a breach in one database can easily be contented.

VIII. CONCLUSION

In the proposed payment systems, a consumer’s payment information is sent to a payment portal via a merchant. This makes the payment system vulnerable to intrusions and Information leaks, causing consumer data theft, identity theft and fraudulent transactions.To protect a consumer’s financial information from being compromised, we developed an approach for online payment systems in which a consumer’s payment information is directly provided to a payment portal rather than sent through a merchant’s website. This approach, however, introduced by the introduction of a trusted third party called certified authority, CA, and a combination of text steganography and visual cryptography. A CA verifies the identity of a consumer by combining share1 and share2 before processing the payment. The combination of text steganography and visual cryptography provides consumer’s information privacy and protects data from misuse. Hence, we show that our proposed payment system is secure and protects a consumer’s payment information and payment against
network intruders or attackers.

IX. FUTURE SCOPE

The payment system can also be extended to internet or physical banking. Shares may contain consumer image or signature in addition to consumer authentication password. In the bank, consumer submits its own share and consumer physical signature is validated against the signature obtained by combining consumer’s share and CA’s share along with validation of consumer authentication password. It prevents misuse of stolen card and stops illegitimate consumer. This can be also applied for standardization of a particular product or an organization by having their personal identification secured.

REFERENCES

[1] Electronic payment systems [http://www.hit.bme.hu/~buttyan/courses/Revkomarom/e-payments.pdf]

[2] (Stealing credit card) Understanding Credit Card Frauds [http://www.popcenter.org/problems/credit_card_fraud/pdfs/bhatla.pdf]

3] R Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", Proceeding of the 2001 International Conference on Image Processing, vol.3, pp. 1019-1022, 2001.

4] 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.

5] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and CommunicationTechnologies, pp. 1181-1186, Mumbai, India, 2011.

6] 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.

7] 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.

8] 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.

9] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptographyimprovises 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.

10] A Survey on Various Data Hiding Techniques and their ComparativeAnalysis[http://arxiv.org/ftp/arxiv/papers/1206/1206.1957.pdf]

11] Moni Naor, Adi Shamir, "Visual Cryptography", EUROCRPT1994.[http://www.fe.infn.it/u/filimanto/scienza/webkrypto/visualdecryption.pdf]

12] A Text based Steganography Technique with Indian Root [http://ac.elscdn.com/S2212017313005033/1s2.0S2212017313005033main.pdf?_tid=08afb448c75711e499c300000aacb35e&acdnat=1426013915_a5f583feeba0f05c6d58f27b9dc103a7]

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

[14] Pranita P. Khairnar, Prof. V. S. Ubale, " Steganography Using BPCS technology,"in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.