International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Online Payment System using BPCS Steganography and Visual Cryptography

S. R. Khonde[1], Dheeraj Agarwal[2], Shrinivas Deshmukh[3]

[1, 2, 3]Modern Education Society's College of Engineering, Pune, 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 burden 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 shielding customer data and increasing customer confidence and preventing identity theft. The approach uses combined application of BPCS Steganography and visual cryptography for this purpose.***

Keywords: E-Commerce, identity theft, phishing, steganography, visual cryptography.

1. Introduction

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. 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 misusing 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 an illegitimate mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference 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 encompasses both steganography and visual cryptography, which minimizes detailed 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's side. The method proposed is applied to E-Commerce but can be easily extensible for other applications like online banking.

2. Existing System

The traditional method of online shopping involves customer or end-user selecting items online shopping portal and directing it to the payment gateway. Different payment gateways have different mechanism of storing detailed information of consumer. There have been recent high profile breaches such as in Epsilon, Sony's PlayStation Network and Heartland Payment Systems show that card holders' information is at risk both from outside and inside. The traditional system can be diagrammatically expressed in Figure 1:

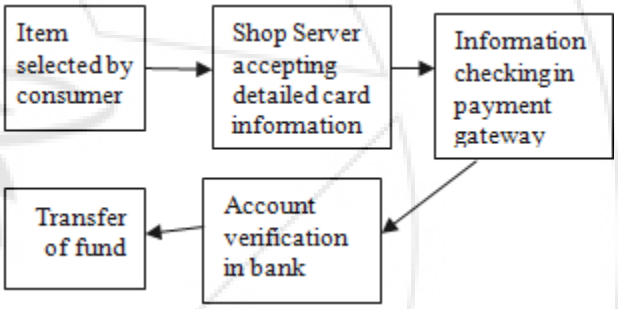

Figure 1: Existing Traditional System

2.1 Drawback

In the traditional system mentioned above, customer is not sure whether his PIN No and CVV No is sent to the merchant. One still has to trust the merchant and its employees to use card information for their own motives. This representation doesn't show 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 these traditional systems, there is no additional non-functional requirement of phishing mechanism which can be harmful and might lead to employment of social engineering and technical subterfuge. Thus, in the proposed system mentioned later in this paper would ensure better security and satisfaction of consumer or other transaction stakeholders.

3. Problem Definition

The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: BPCS Steganography and Visual Cryptography for safe online shopping and consumer satisfaction. Online shopping is generally considered as 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. 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.

4. Proposed System

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing least information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of BPCS Steganography and Visual Cryptography. The information received 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.

4.1 Features

a) Proposed method minimizes customer's detailed information sent to the online merchant. So even if a breach takes place in merchant's database, customer doesn't get affected.
b) Certified Authority acts as a fourth party thereby enhancing customer's satisfaction and security further.
c) Usage of BPCS Steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy. It provides a higher level of security and a high information hiding capacity.
d) Since customer data is distributed over 3 parties, a breach in single database can easily be contented.
e) The 2-out-2 feature of visual cryptography provides effective collaboration of images at the Certified Authority's side.

5. Literature Survey

5.1 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 blacklist, which is maintained 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 color and text changes in the button.
d) Linkguard Algorithm is efficient for phishing prevention. This algorithm is described in detail later.

5.2 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 [1].
b) BPCS Steganography: The information hiding capacity of a true color image is around 50% [2]. 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.

5.3 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 [4].

6. Algorithms

6.1 BPCS (Bit-Plane Complexity Segmentation) Steganography algorithm

The algorithm can be described in concise steps as follows [2].
a) Convert the carrier image (of any file-format) from PBC (Pure Binary Code) to CGC (Canonical Grey Code) system and in png format.
b) Perform the histogram analysis.
c) After that bit-plane analysis is performed.
d) Perform size-estimation i.e. calculate the places where we can store the secrete image.
e) Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.
f) After embedding mail that image to another user.
g) For extracting the embedded image performs de-steganography which is exactly opposite to steganography.

6.2 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 [4].

6.3 LinkGuard Algorithm

LinkGuard works by analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted site [3].

The following terminologies are used in the algorithm.

v_link: visual link;
a_link: actual_link;
v_dns: visual DNS name;
a_dns: actual DNS name;
sender_dns: sender'sDNS name.

```
 int LinkGuard (v_link, a_link}
{
 v_dns = GetDNSName (v_link);
 a_dns = GetDNSName (a_link);
 if ((v_dns and a_dns are not empty) and (v_dns! = a_dns))
 return PHISHING;
 if (a_dns is dotted decimal)
 return POSSIBLE_PHISHING;
 if (a_link or v_link is encoded)
{
 v_link2 = decode (v_link);
 a_link2 = decode (a_link);
 return LinkGuard (v_link2, a_link2);
}
 /* analyze the domain name for
 possible phishing */
 if (v_dns is NULL)
 return AnalyzeDNS (a_link);
}

int AnalyzeDNS (actual link)
{
/* Analyze the actual DNS name according
to the blacklist and whitelist*/
 if (actual dns in blacklist)
 return PHISHING;
 if (actual dns in whitelist)
 return NOTPHISHING;
 return PatternMatching (actual_link);
}

int PatternMatching(actual link){
if (sender_dns and actual_dns are different
return POSSIBLE PHISHING;
for (each item prev_dns in seed-set)
{
bv = Similarity(prev_dns,actual-link);
if (bv == true)
return POSSIBLE_PHISHING;
}
return NO_PHISHING;
}

float Similarity (str, actual link){
if (str is part of actual-link)
return true;
int maxlen = the maximum string lengths of str and actual
dns;
int minchange = the minimum number of changes needed to
transform str to actual dns (or vice verse);
 if (thresh < (maxlen-minchange)/maxlen<l)
 return true
 return false
}
```

7. Proposed System Workflow

7.1 Workflow of System

In our proposed system of online shopping, user logs in and enters into the online store to view the products. When he/she adds the item to the cart, he/she will be entering the card no and unique authentication password. This information will be created as a stego or stegno image using BPCS Steganography. 2-out-2 algorithm of visual cryptography will create two shares out of the stegno image. (Customer's share and CA's share). CA browses user's share and generates the card no which is sent to the bank so as to extract the customer's PIN (de-steganography). Finally fund will be transferred from the bank to the merchant. Workflow of our system show in Figure 2:

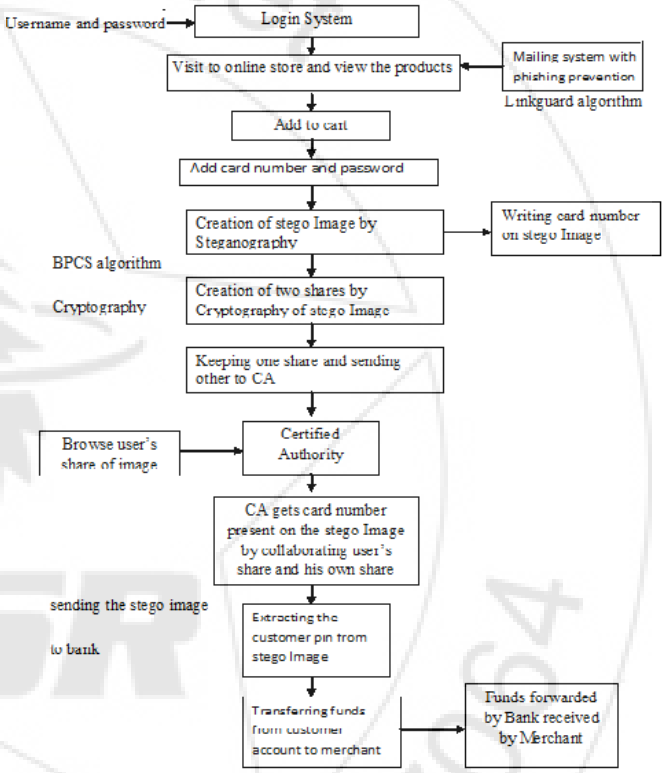

Figure 2: Workflow diagram

7.2 Sequence diagram:

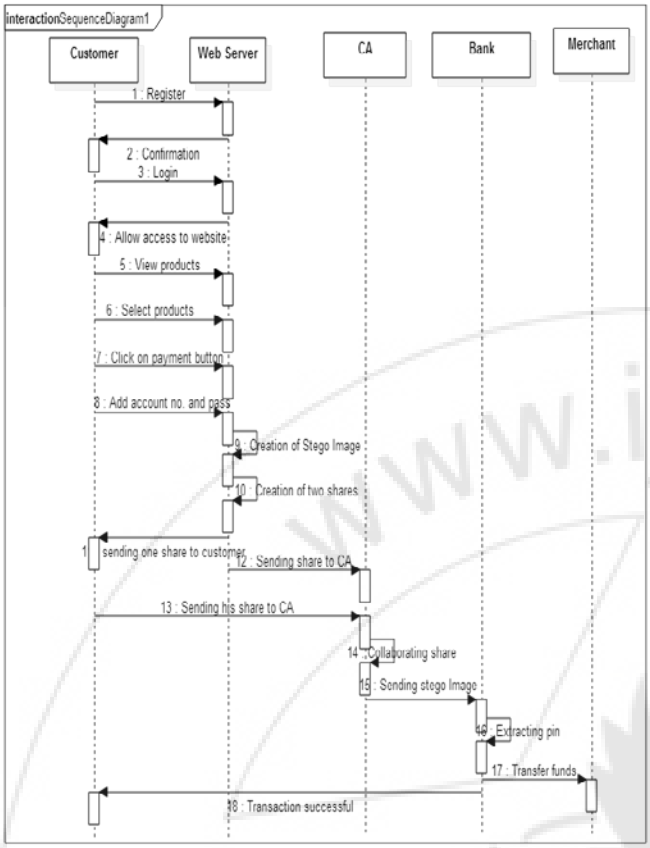

Figure 3: Sequence Diagram

8. Conclusion

In our project, a payment system for online shopping is proposed by combining BPCS steganography and 2-out-2 visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. BPCS Steganography is really effective against eavesdropping and has a high information hiding capacity as compared to traditional steganography approach. The method is concerned only with prevention of identity theft and customer data security. The main aim is consumer satisfaction and authorized merchant-bank interaction for fund transaction. In comparison to other banking application which uses steganography and visual cryptography 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.

9. Future Scope

The payment system can also be extended to internet or physical banking. Shares may contain customer image or signature in addition to customer authentication password. In the bank, customer submits its own share and customer 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. This can be also applied for standardization of a particular product or an organization by having their personal identification secured.

References

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

[2] 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.

[3] U.Naresh, U.Vidya Sagar, C.V. Madhusudan Reddy , " Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36.

[4] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,",in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008.