

Electronic Payment System Using Visual Cryptographic Scheme

ASAKPA Sunday Ogheneruemu, ADEIFE Oyebola Taiye

Computer Science Department, Federal Polytechnic, Offa
Computer Science Department, Federal Polytechnic, Offa

Date of Submission: 01-02-2023

Date of Acceptance: 10-02-2023

ABSTRACT

The emerging market known as electronic commerce has eased buying and selling of goods and services online however with its attendant challenges usually referred to as cybercrimes. Like the traditional market, money is being exchanged for goods and services being rendered. However, such payments require the use of Internet banking, credit/debit cards or some other means of money exchange, which is susceptible to different forms of attacks such as phishing and Internet frauds. Cryptography is a commonly used means of securing and preventing frauds online. In this paper, we have designed a new approach for securing online payment using visual cryptography. The scheme is based on secret sharing whereby scrambled images (shares) are generated and distributed to the payer and the payee by the issuer. The shares are pulled together before payment can be completed. The designed system is simple, secure and ensures privacy and confidentiality.

Keywords: Internet, Cybercrime, Visual Cryptography, Shares, Payer, Payee

I. INTRODUCTION

Traditional commerce usually involves the exchange of goods and services with an equivalent abstract value usually referred to as money. Advancement in information and communication technology has given birth to electronic commerce (E-commerce) whereby the exchange of goods and services with an equivalent abstract value known as cash is being done over the Internet. This paradigm shift in commerce from traditional method to online technique also requires that new system of payment be put in place, hence the need for electronic payment (E-payment) system. This new method of transacting business via the Internet has some basic challenges, the commonest being identity stealing, financial frauds and phishing. Many have lost their hard earned money to Internet crime commonly referred to as Cybercrime (i.e. Internet crime). Such crimes include identity

stealing, credit / debit card fraud, phishing among others. This has resulted to fear in the minds of many to accept or embrace e-commerce. However, the emergence of technologies such as electronic banking (e-banking), online shopping, cashless society etc is forcing many people with no option than to migrate to e-payment system, a subset of e-commerce in order to settle bills, pay for services and buy goods online. The security of e-payment system is very important in order for people to embrace it on a large scale without the fear of being swindled of their hard earned money. Traditional authentication methods such as password, passphrase, identity documents, etc. are not sufficient to combat this menace [1, 7]. Alternative method such as cryptography has been used largely on most e-payment platforms but it has key management issue. The security of information is fully dependent on the security of the keys used. Most ciphers are public knowledge, what is not known is the key, once the key is revealed, we can easily encrypt and decrypt any message. The most secure key management scheme keeps the key in a single, well-guarded location (a computer, a human brain, or a safe). This approach is highly unreliable since a single misfortune (a computer breakdown, sudden death, or sabotage, misplacement, theft) can make the information inaccessible. An obvious solution is to keep a multiple copies of the key at different locations, but this increases the danger of security breaches. A possible solution is to distribute the key among a group of people so that no single individual has the key. This is known as secret sharing scheme. This is the concept behind visual cryptography (VC), which is the methodology employed in order to combat the challenges bedeviling e-payment in online transaction.

II. LITERATURE REVIEW

E-payment systems have attracted significant attention of recent from the academia and the industries because of the vital role they

play in e-commerce, e-banking and other business related online transactions. Briggs and Brooks [2] describe e-payment as a form of inter-connections between organizations and individuals supported by banks and inter-switch houses such as Paypal that enables monetary exchange electronically. E-payment service is a convenient and efficient way of doing business and financial transactions online. However, the Internet is not a secure medium. Hence, the need for various researchers to design and implement various security measures to ensure e-payment system. Public key cryptosystem such as Rivest Shamir Adleman (RSA), digital signature, secure electronic transmission, blind authentication protocols are among the common security measures for e-payment [3]. However, the basic challenge of this technique is key management issue. Souvik and Venkateswaran [4] proposed an online payment system using steganography and visual cryptography. The work is however vulnerable to phishing attack. The contribution of this work is the use of secret sharing scheme to overcome the problems of key management and phishing in e-payment.

2.1 Secret Sharing

Secret sharing otherwise known as splitting was discovered almost simultaneously and independently by George Blakley and Adi Shamir in 1979 [5]. The general ideas behind “secret sharing scheme” are:

- Distribute a secret to **n** different participants;
- Any group of **t** participants can reconstruct the secret;
- Any **t-1** or fewer participants cannot reveal anything about the secret [5].

Thus, it is a method of distributing a secret among a group of participants, each of whom is allocated a share of the secret. The secret can be revealed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. In a typical secret sharing scheme, there is one dealer and **n** players. The dealer gives a share of the secret to the players, but only when specific conditions are fulfilled will the players be able to reconstruct the secret from their shares.

2.1.1 The Secret Sharing Model

A secret sharing scheme is a means for **n** parties to carry shares or parts s_i of a message s , called the secret, such that the complete set s_1, \dots, s_n of the parts determines the message. The various secret sharing schemes can be generally categorized into either two-party or, multi-party.

- i. Two-party secret sharing. Let s be a secret, encoding as an integer in $\mathbb{Z}/m\mathbb{Z}$. Let $s_1 \in \mathbb{Z}/m\mathbb{Z}$ be generated at random by a trusted party. Then the two shares are defined to be s_1 and $s - s_1$. The secret is recovered as $s = s_1 + s_2$.
- ii. Multiple-party secret sharing. Let $s \in \mathbb{Z}/m\mathbb{Z}$ be a secret to be shared among **n** parties. Generate the first **n - 1** shares s_1, \dots, s_{n-1} at random and set as shown in equation 1.

$$s_n = s - \sum_{i=1}^{n-1} s_i \quad 1$$

The secret is recovered as by equation 2.

$$s = \sum_{i=1}^n s_i \quad 2$$

2.2 Visual Cryptography

At the Eurocrypt in 1994, the duo of Moni Naor and Adi Shamir presented a new cryptographic paradigm that is used for encryption and decryption. It is a special kind of secret sharing scheme for hiding a secret image into a set of binary transparencies which seem like random noise, than can be used to encrypt written material such as printed text, handwritten notes, pictures, graphical images, etc. in a perfectly secure way. And the decoding can be done by simply pooling the scrambled random like transparencies together without the use of computer system [6]. This characteristic favours the application of visual cryptography for financial transactions that are carried out online.

2.2.1 The VC Model

Visual cryptography uses a visual secret sharing scheme based on a (t, n) threshold framework, where **n** means a secret image will be hidden in **n** transparencies, and **t** is that we stack **t** or more than **t** transparencies to reconstruct the secret image. Visual cryptography is simply, a secret sharing scheme mainly for images.

For a set **p** of **n** participants, a secret image s is encoded into **n** shadow images called shares, where each participant in **p** receives one share. Certain qualified subset (**t**) of participants can visually recover the secret image, but other forbidden (**t-1**), sets of participants have no information about the secret s [7].

In visual secret sharing, the message bit is a collection of black and white pixels (assuming a binary image) and each pixel is treated individually. Each pixel appears in **n** modified

versions (called shadows or shares) of the image, one for each transparency. Each share consists of m black and white sub-pixels. Each share of the sub-pixels is printed on the transparency in close proximity (to best aid the human perception, they are usually structured together to form a square with m selected as a number). This results in a $[n \times m]$ Boolean matrix S defined as:

$S = (S_{ij})_{n \times m}$ where $S_{ij} = 1$ if and only if the j th sub-pixel in the i th transparency (share) is black, and $S_{ij} = 0$ if and only if the j th sub-pixel in the i th transparency (share) is white.

When these shares $i_1, i_2, i_3, \dots, i_r$ are pooled together in a way which properly aligns the sub-pixels, we will see a stacked share whose black sub-pixels are represented by the Boolean "OR" of rows $i_1, i_2, i_3, \dots, i_r$ in S . The grey level of this combined share is proportional to the Hamming weight $H(V)$ of the "OR"ed m -vector V . This grey level is being interpreted thus:

white if $H(V) < d - \alpha \cdot m$

and

black if $H(V) \geq d$

for some given threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$.

III. METHODOLOGY

3.1 E-Payment Schema

The designed e-payment system is an integration of visual cryptography into e-commerce platform in order to overcome the vulnerability usually associated with e-payment. Figure 1 shows a generic payment system [8].

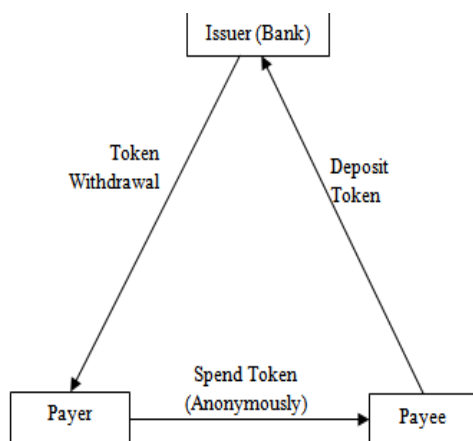


Figure 1: Generic model of a payment system

There are usually two types of parties involved in all payment systems, the issuers and the users. An issuer is an entity that operates the

payment service, such as bank. An issuer holds the items that the payments represent. The users of the payment service perform two main functions, that of making payments (i.e. the payer) and that of receiving payments (i.e. the payee). This relationship between the issuer and the users (payer and payee) is illustrated by figure 1. The above schema is modified to integrate visual cryptography to ensure security [9], as shown in figure 2.

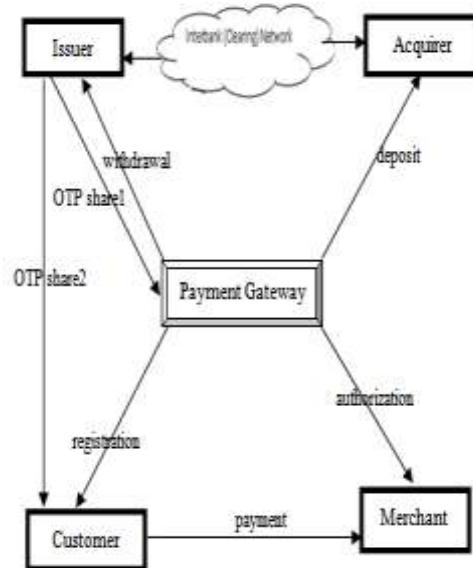


Figure 2: The designed e-payment model

3.2 2-out-of-2 Scheme

This is a simple threshold secret sharing scheme which splits a binary image into two different shadows (shares). Each pixel is divided into a black and white sub-pixel placed next to each other. In the case of white pixel, one of the two combinations of sub-pixels will be chosen with a probability of 0.5 to represent the pixel in each of the shares. When these shares are placed one on top of the other, the pixel are visually ORed and hence a white pixel looks grey (half black and half white) to the human eye. The pixels are chosen in a similar manner for the case of a black pixel. But when the sub-pixels are visually ORed, the two black sub-pixels placed next to each other appear as a single black pixel. This idea is applied to images, pictures and texts to develop a basic 2-out-of-2 scheme by using 2 sub-pixels.

2-out-of-2 visual secret sharing scheme problem is represented by the following collection of $n \times n$ matrices:

$C_0 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \}$

$C_1 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \}$

When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black). Figure 3 shows the partitions for white and black pixels for 2-out-of-2 VC scheme.













Pixel		Share1	Share2	Result
White	$p = 1/2$			
	$p = 1/2$			
Black	$p = 1/2$			
	$p = 1/2$			

Figure 3: Partitions for black and white pixels for 2-out-of-2 scheme (2 sub-pixels)

IV. EXPERIMENT AND RESULT

An application program is developed using MATLAB (R2015) to implement the designed e-payment system. Whenever a transaction is initiated online, the payer will attempt to make withdrawal from the issuer. The issuer in response will generate a pin that is shared in the form of shadows between the payer and the payment gateway. The payer uses this share (i.e. shadow) to initiate payment with the payee. The payee checks for the authorization with the payment gateway. If the pin is revealed, deposit is made unto acquirer and the transaction (i.e. payment) is exchanged for goods / services. Figure 4 shows a sample result.

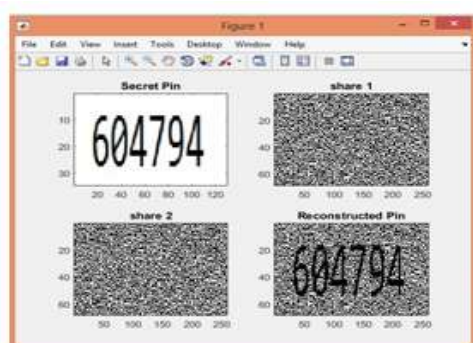


Figure 4: Sample Result

Whenever the shares are combined, the secret pin is revealed and transaction can be authorized. Any form of modification to either

share or both will result in access being denied, as no pin or tangible information will be revealed.

V. CONCLUSION

Security of payment information on the Internet is a major concern that has discouraged the wide acceptability of electronic commerce. In this paper, we have been able to overcome this fear by integrating secret sharing scheme into payment platform, thereby eliminating risks associated with e-commerce while promoting the confidence of the populace in e-commerce. One time pad is created for each transaction, hence, payer's payment information is not exposed to security threats. The system is simple and secure.

REFERENCES

- [1]. S. O. Asakpa, B. K. Alese, O. S. Adewale and A. O. Adetunmbi, Secret Sharing Scheme for Securing Biometric Template. Conference Procedure of the 27th Nigeria Computer Society, Abuja, 2016, 2-9.
- [2]. A. Briggs and L. Brooks, Electronic Payment Systems Development in a Developing Country: The Role of Institutional Arrangements, The Electronic Journal on Information Systems in Developing Countries, 2011, 1-16.
- [3]. M. Manorial, A. K. Shrivastave, S. S. Thakur, and D. Sinha, Secure Biometric. Cryptosystem for Distributed System, International Journal Communication and Network Security, 2011 27-32.
- [4]. R. Souvik, and P. Venkateswaran, Online Payment System using Steganography and Visual Cryptography. IEEE Students' Conference on Electrical, Electronics and Computer Science, 2004, 1-5.
- [5]. D. R. Stinson, Cryptography: Theory and Practice (2nd ed.: CRC Press, 2006).
- [6]. M. Naor and A. Shamir, Visual Cryptography, Proc. the Advances in Cryptology–Eurocrypt, 1995, 1-12.
- [7]. S. Katta, Secret Sharing in Visual Cryptography, (MSc Thesis. US: Oklahoma State University, 2011).
- [8]. B. Mihir, A. Juan, H. Ralf, H. Amir, K. Hugo and S. Michael, Design, Implementation and Deployment of the iKP Secure Electronic Payment System, IEEE Journal of Selected Areas in Communication, 2000.
- [9]. N. Chaudhari, and P. Priya, Secure Online Payment System using Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering, 5(2), 2016, 552-553.