International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2019.33280

Volume 5, Issue 6
June - 2019

A SECURED WEB-BASED E-PAYMENT SYSTEM INTEGRATING IMAGE-BASED STEGANOGRAPHY ENCRYPTION

ARU OKEREKE EZE[1], UGOJI FRANK-GODRIC CHIDUBEM.[2]

[1]Department of Computer Engineering

[2]Department of Computer Engineering

College of Engineering, Michael Okpara University of Agriculture, Umudike

Umuahia, Abia State

Nigeria

ABSTRACT

Growth in technology has made online shopping such an interesting thing but has introduced fraud, making personal information security a major issue for customers as well as merchants and banks in the case of CNP (Card Not Present). This paper is aim at developing a method for the creation of a Secured web-based e-Payment system that will allow a customer to provide limited information necessary for fund transfer during online/physical shopping and enhance the security of customer data. In this paper, the image-based steganography encryption technique was used to design a web-based e-payment system. The descriptive research methodology was adopted in this research in which questionnaire was used to ascertain how reliable steganography as an encryption mechanism is for better security measure. The result obtained from this research shows that the level of trust on steganography being used to implement the e-payment system is high with a percentage level of 69.2%. This work therefore concludes that image-based steganography encryption technique will enhance the security of information for online payment and prevent misuse of customers information.

Keyword*: Steganography, Encryption, Decryption, E-Payment, Cryptography, Online.*

---

1. INTRODUCTION

The fast growth in technologies have greatly enhanced the way things are done, starting from education, governance, manufacturing, shopping, etc. Purchases and sales of goods and services from any part of the world is now an easy task to accomplish through the use online stores, online payment methods or some others which include; Cash on Delivery (COD), Cheque/Check, Debit card, Direct Debit, Electronic Money, Gifts Card, Postal Money Order, Wireless Transfer/Delivery on Payment (DOP), Invoice, Bitcoins, etc (Lopresti, 2007; Rao, 2010)[1][2]. These concepts are simply referred to as Online Shopping. Customers can access, order and/or make payments for their orders either online or on delivery in online shopping. When making payment online, the customer provides his Bank Card details such as card number, expiry month, expiry year, card holder name, card CVV and card pin to the online merchant, then the merchant uses the payment details to request payment from customer's bank and thereafter, the customer is billed accordingly. Despite the fact that this approach has made shopping easier, faster and better, it has also introduced security challenges such as identity theft, hacking, phishing etc. However, merchant and its employees must be trusted not to use customer information for their own selfish purpose and also not to sell the information to others which is unsecure for customers. In this study, a new method is proposed, that uses image-based steganography encryption which minimizes the sharing of information between consumer and online merchant, enables successful fund transfer from consumer's account to merchant's account, safeguard consumer information and also prevent misuse of consumer's information at the merchant side. Steganography is the art of hiding a file within another so that hidden file is indistinguishable. In steganography, an intruder is unaware of the fact that observed data contains hidden information. The idea behind steganography is that message to be transmitted is not detectable to casual eye. The method proposed is specifically for e-commerce but can easily be extended for manual shopping, online banking and can also be integrated in any commercial site for payment purpose.

2.SURVEY OF RELATED WORK

Steganography is the art and science of invisible communication. It is seen also as the art of concealing a file within another file so that hidden file is indistinguishable. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Some implementations of steganography which include forms of security through obscurity, and key-dependent steganographic schemes that lack a shared secret adhere to Kerckhoffs's principle.
Some research has been carried out in the area of online shopping and payment security which proposes the use of cryptography and/or steganography.

A Critical study of the work of Murugeswari et al (2015) where he employed Bit Plane Complexity Segmentation (BPCS) Steganography Techniques and Visual Cryptography method to implement an e-payment system, reveals that the stego image which contains the payment details is encrypted and sent to the central certified authority (C.A) portal and then to the Bank for payment to be made. The challenge with this method is that there is room to redirect customers to central certified authority (C.A) portal for verification before forwarding payment details to the Bank for payment and through this medium; Fraud Merchant could redirect a customer to its phishing portal, thereby defrauding the customer [3].

Souvik and Venkateswaran (2014) proposed an online payment method that applies visual cryptograph and steganography for improved security of payment process. The steganography technique used is based on Vedic Numeric code in which the stego image is encrypted. The method introduced a Central Certified Authority (C.A) through which customer's payment details is verified. The cryptograph method used took an edge of the inflexion, fixed word order and periphrases when encrypting the payment details[4].

A study of the work of More et al (2015) showed that instead of using Steganography method, the merchant just like a customer registers with a bank. Once he logs out at the merchant site, he submits only his account number, thereafter; the merchant uses it to make request for payment from the bank. At the bank, a One-Time password is generated through Steganography technique. Then, visual cryptography splits the One Time Password into two parts. One part is sent to the merchant and the other to the client through E-mail and then, the communication between the merchant and customer leads to the retrieval of the complete One Time Password which the client will then send to the bank for verification and based on the validity of the One Time Password, payment is made. This method offers an enhanced security but using E-mail which is prone to attack makes the system inefficient [5].

Khonde et al (2014) used visual cryptography and Bit- plane complexity segmentation steganography technique to encrypt and embed customer's payment card details in the online shopping system. They also introduce Central Certified Authority portal. The cryptography technique creates two shares of the stego file, one of the stego file is sent to the C.A and the other to the customer. The C.A browses the customers share and retrieves the payment details which are then forwarded to the bank for payment to be made. This does not offer security against the Merchants. Also, Murugeswari et al (2015) in their work, they used the same method but instead of image steganography, text based steganography was used. This provided security of payment details against eavesdroppers but not against online Merchant [6].

Deepti Chaudhary and Rashmi Welekar (2015) proposed a method in whichVisual Cryptography Technique is applied on colour images and Steganography technique used to enhance the security of the system[7].

In the work of Priyanka et al (2017), a new method was proposed. Here, he proposes a technique of processing a secret key of a customer and then dividing it into two different shares. When two shares are created, one is stored in the Bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original secret key. The Correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer [8].

After reviewing some systems, it is clear that there are a lot of loopholes especially, on the part of security of data on the side of the online merchant. A critical study of the security challenges present in the existing system reveals that there is need for a more secure approach to online shopping and payment not only that the system should enhance the security of the process but also create room for customers direct involvement in payment to increase their confidence in the process.

3. RESEARCH METHODOLOGY

The research Design is an exploratory study to investigate the challenges facing information hiding which are encountered by customers and end users during financial transaction. Data was collected from the targeted population so as to ascertain the

DOI: 10.31695/IJASRE.2019.33280

effectiveness, reliability and authenticity of steganography as an encryption mechanism for better security measure and also to know the current ICT security related challenges faced by that population using a questionnaire. It was, therefore, descriptive survey research which brings out quantifiable information from the sample.

3.I System Payment Method

Here, a new method is introduced that used image-based steganography encryption technique to develop a secured web-based e-payment system. The customer after shopping proceeds to the e-payment portal. There, he registers so as to be able to login in other to access the payment portal. On login, he is presented with options to enter his card details and thereafter, generates a token before making payment. Here, once the customers payment details is entered, it is encrypted and forwarded to the server side which also houses the Central Certified Authority (CA) that allows customers information to be verified before proceeding for payment. At the server side, the payment details is verified and then decrypted with the help of the decryption key that is stored there and thereafter, forwarded to the bank for payment to be made. There is no room for redirection in this system as the C.A is contained in the sever side.

3.2 The System Flow Chart

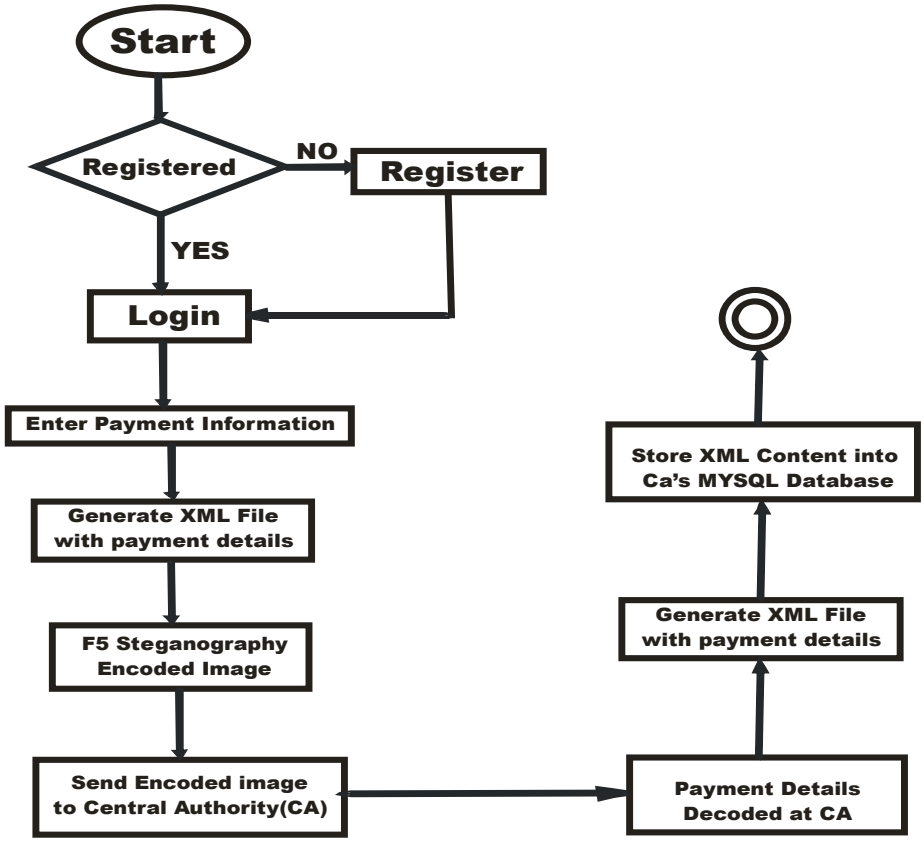


Fig. 1: The system flow chart

4.0 ANALYSIS

The average analysis of the Respondents response on the level of trust in using steganography encryption to implement e-payment system for better security as compared to other encryption mechanism based on their deep knowledge about these encryption mechanisms is shown in the table and depicted by the graph below.

Table 4.1: The respondents level of trust in using steganography to implement e-payment system.

OPTIONS	Not Trusted	Partially	Trusted	Total
RESPONSES	2	41	77	120
PERCENTAGES%	1.7	34.2	64.1	100

DOI: 10.31695/IJASRE.2019.33280

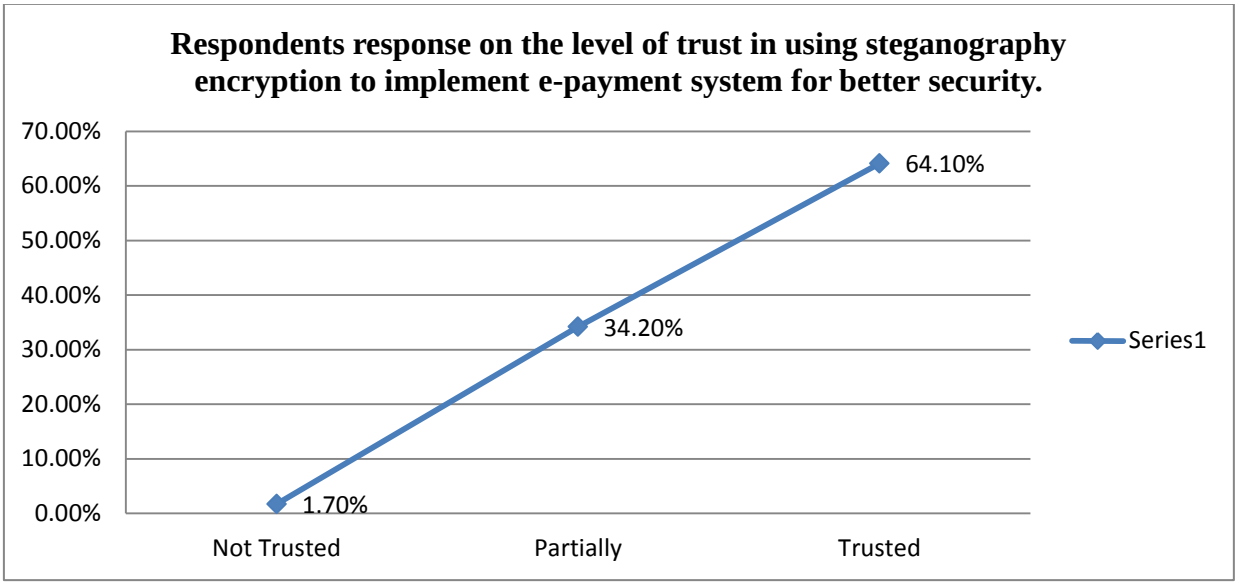


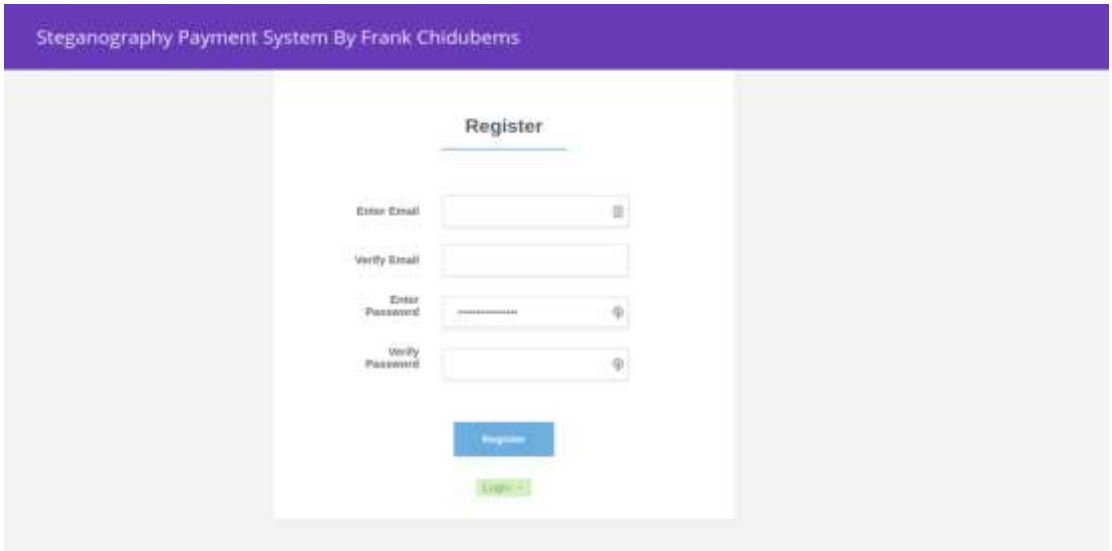
Fig. 2: The respondents level of trust in using steganography to implement e-payment system.

The average result obtained in this research shows that about 1.7% of the respondents do not trust the implementation of an e-payment system with steganography encryption, 34.2% partially believed that it will offer some high sense of security as compared to other encryption mechanism while 64.1% totally agreed to the fact that it is quiet reliable implementing an e-payment system with steganography encryption rather than using other encryption mechanism.

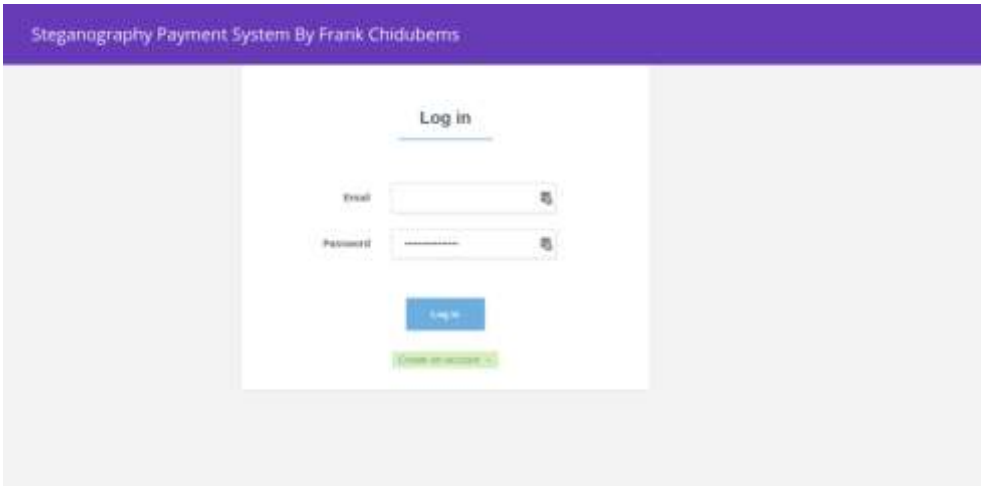
The result obtained therefore shows that steganography encryption will enhance security of information for online payment purposes and also prevent misuse of customer's information.

4. 1 DESIGN VIEW OF THE SYSTEM

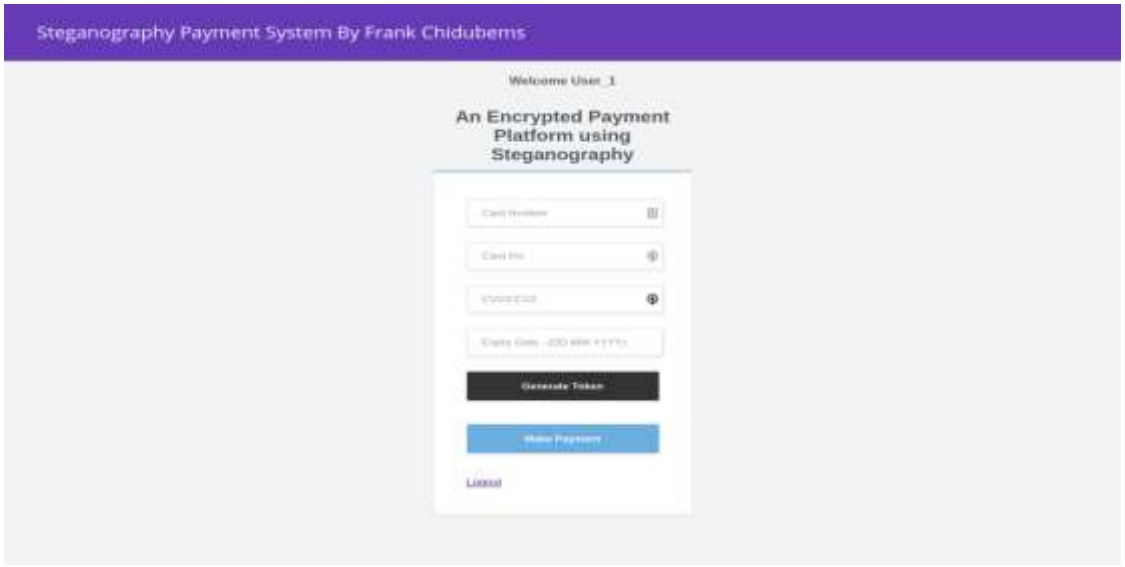
Starting the application for the first time, the user is presented with an authentication interface to simulate User Logging and Registration processes on typical e-commerce platforms after which he can login.



DOI: 10.31695/IJASRE.2019.33280



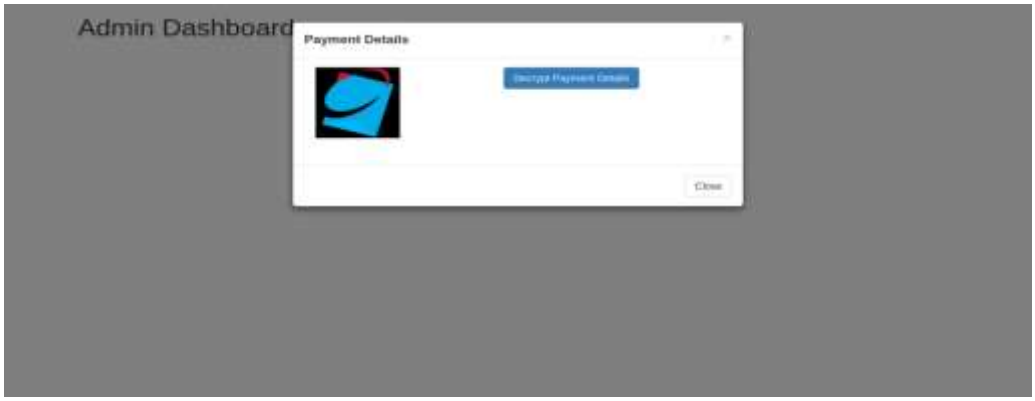
Since this project is primarily concerned with protecting and encrypting User's payment details for payment purpose, on successful completion of the authentication, the User is redirected to a Payment portal.



On the Payment interface, arbitrary card details are entered, these details include a 16-Digits Card Number, 4 digits Card Pin, 3-digits CVV and the Card Expiration date in Date-Month-Year format.
Once the payment details are entered accordingly. The details are passed through the Steganography tool that encrypts the details in a specified image also including additional key information which is stored on the server. This image can be seen only by the Admin personnel on the Admin dashboard.

Clicking on 'View Details' would display the image with the encrypted details.

DOI: 10.31695/IJASRE.2019.33280



The 'Payment Details' maintain the encrypted state until the 'Decrypt Payment Details' button is clicked, a request is triggered to the server to retrieve the payment details for that specific user.

After the payment details has been decrypted, the information is forwarded to the bank for the customer to be billed accordingly.

5. CONCLUSION

In this paper, a web-based secured e-payment system for online shopping has been developed using image-based steganography encryption that provides customer data privacy, prevents misuse of data at merchant's side as well as protect data from middle attackers. The analysis made in this work shows that steganography encryption will enhance security of information greatly for online payment purpose and also prevent misuse of customer's information. The method was applied for E-Commerce with focuses on area of payment during online shopping as well as physical banking.

REFERENCES

1. Lopresti, M., (2007), "Bill-2-Phone Lets Customers Add Online Purchases to Their Phone Bill".pp 2-3.
2. Rao, L., (2010), "Mopay Now Allows You To Bill Mobile Payments To A Landline Account"., pp 2-4.
3. Murugeswari, D. et al, (2015), "Secure e-pay using text based Steganography and visual cryptography". International Journal of Engineering Research andGeneral Science Volume 3, Issue 1, pp. 1133 - 1144.
4. Souvik, R. & Venkateswaran, P., (2014), "Online Payment System using Steganography and Visual Cryptography". s.l., IEEE, pp 2-6.
5. More, P. et al, (2015). Online Payment System using Steganography and Visual Cryptography. International Journal of Latest Technology in Engineering, Volume 4, Issue 10.,pp. 94 - 96.
6. Deepti Chaudhary and Rashmi Welekar (2015), "Secure Authentication Using Visual Cryptography", International Journal Of Computer Science And Applications Vol. 8,No.1.
7. Khonde, S. R. et al, (2014), "Online Payment System using BPCS Steganography and Visual Cryptography". International Journal of Science and Research (IJSR) Volume 3 Issue 11, pp. 2336 - 2339.
8. Priyanka et al, (2017), "Review on Implementation Visual Cryptography & Steganography for Secure Authentication", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 02 | Feb -2017

DOI: 10.31695/IJASRE.2019.33280