International Journal of Hybrid Information Technology
Vol.8, No.8 (2015), pp.271-278
http://dx.doi.org/10.14257/ijhit.2015.8.8.28

A Hybrid Technique to Secure E commerce Transaction with the Help of AES Encryption and Stenography in Image

Ekta Chauhan and Unmukh Datta

Dept of Computer Science Engg.
Maharana Pratap College Of Technology, Gwalior, India
ekta.techies@gmail.com, unmukh62@hotmail.com

Abstract

Electronic commerce, commonly known as eCommerce is trade in products using the internet. Security at the e-commerce becomes more and more important. Electronic transaction security is a challenging task because of the insecure communication channel. In this paper, we proposed a new algorithm to make an e commerce transaction more secure. In this work we are using AES to encrypt data and this data is embedded to image edges to perform Stenography in this paper target on compress the time of encryption and decryption adopting parallel processing on which AES will be applied freely. In the results show the comparison between our work and previous work and we found that parallel processing and multi threading on the AES algorithm our results are quite improved, our proposed algorithm is taking much less time in encrypt and embedding or decrypt and extraction.

Keywords*: Electronic commerce, AES, SSL, Stenography etc*

1. Introduction

E-commerce stands for electronic marketing. E-commerce is a methodology of modern business. Through e-commerce we can buy, sell, business of goods and service over the internet. E-commerce is a new way of business over traditional business system. Payment is an important component in e commerce. In day to day commercial dealing, there are various payments, each with its own advantages and disadvantages. To make a secure money transaction on the internet for the user it is the most important feature of e-commerce. An e commerce user should make sure no one can't break or known their personal data or secure password even merchant also. For security purpose, we are using biometric identification. Here we can use fingerprint image, iris, voice, etc. the biometric identification is a human unique identity. No one can't steal it. And user can use unique identity place of a password. Because of e commerce security at the time of money transaction through the internet make secure of all transaction process by the various algorithms. The purpose of the e commerce security means protection of data, network, computer program, computer and other element of computerized information system.

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES has been just different from DES in a number of ways. The algorithm Rijndael allows for a different block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be selected independently from 128, 160, 192, 224, 256 bits and demand not is the same. However, the AES standard states that the algorithm can only obtain a block size of 128 bits and a preferred of three keys - 128, 192, 256 bits. As well as these differences AES differs from DES in that it is not a feistel organization. Memorial that in the feistel organization, partial of a document block is the used to change the other parts of a document block and then the halves are interchanged. In this case the total data block was processed in parallel at the time each round accepting substitutions and permutations. Stenography is the craft

ISSN: 1738-9968 IJHIT

and science of covering communication; a stenographic system, thus embeds covering content in unexceptional hiding place media so as not to the provoke an observer's improbability. In the past, people used unseen tattoos or the unseen liquid ink to convey Stenography element. Today, computer and the network methodologies offered to the easy-to-use communication channels for Stenography. Principally, the knowledge-unseeing procedure in the stenographic system starts with a unique identifying a cover medium's unnecessary bit (those that can be changed without spoiling that medium's integrity). 1 The embedding method design a steno medium by removing these unnecessary bits with the document from unseen information. Current Stenography's aim is to then put its mere presence undetectable, but stenographic systems— due to their offensive behavior—leave behind noticeable touches in the shelter medium.

2. Type of E Commerce

Business to business – B2B: - in business to business, there is an intermediate in between business. Like a business organization sell its product to whole sell through direct order or through the website. To now whole seller sales his product to the final customer.

Business to consumer – B2C: - in business to consumer, there is no intermediate step. Here consumer can directly connect to business like to connect to the website. In b2c, consumer can directly order the product to the organization at the same time. The organization receives an email of the product and dispatches the goods to consumers

Consumer to consumer – C2C: - in consumer to consumer the interaction of consumer on both sides. C2c where consumer post their ad on internet like property, product which they want to sell. On the other side a consumer can purchase goods through the website. C2c it depends on the website to take for advertisement or not.

Consumer to business – C2B: - in consumer to a business model multiple website showing different results. Different bank website showing car loan interest rate. It depends on the consumer to take what suitable for them in their budget.

Business to government – B2G: - in b2g, various business organizations can trade and exchange information to business can connect to government by the website.

Government to business – G2B: - in government to business search website that show auction or tender of government and also fill application form.

Government to citizen's – G2C:- in government to citizen's the policy of government to citizen's are provided by such website.

3. Basic E Commerce Security Issue

Some of the major technology defenses to address these security issues that can occur in e commerce:

Authentication: - verifies authenticate person. It enforces that person is the only one permitted to log on to his account

Authorization: - allows to person manipulate his resources in specific ways. This prevents person from increasing the balance of person account or deleting a bill.

Auditing: - deals with information hiding. It ensured person cannot spy on another person at the time of internet banking transactions.

Confidentiality (privacy) and integrity (trust):- protection against unauthorized data modification

Availability: - protection against data delays or removal.

No repudiation: - security against any people from reneging on the agreement after the fact.

4. Literature View

Suhad Latef (2011) *et al.*, present that the very fast development of the electronic document interchange, the knowledge safety was becoming more and more important in the document storing and communication. And then as a result of broader use of the images of the manufacturing procedure, it is the important to defend the trusted image document from illegal access. In this paper, a suggested kernel was produced as the key to a LFBSR (Linear Feed Back Shift Register) which is applied to the RGB Bmp image (color image) with the arbitrary keys=2100. The presentation of this procedure has been executed on the two ways of color, image the 8-bit color image (palletized image) and 24-bit color image. [1]

Ravi Subban (2013) *et al.*, present that the FP (Fingerprint) helps to the recognizing that a person verifying is who he/she rights to be. Fingerprint documentation is the most common biometric method because of easiness in the obtaining, obtainability of the plenty sources (*i.e.*, Ten fingers) for the gathering document and their recognized us. In this paper précises the examination effort approved out in the Fingerprint matching methods, recognition techniques and also their presentation examination. This paper presented the related works and performance analysis for fingerprint biometric. The performance evaluation is done on surveys works with different parameters and existing methods. Biometrics presents obvious advantages over password and token-based security [2].

A. Jaya Lakshmi (2012) *et al.*, present that this paper presents ways for generating the strong bio-crypt key based mostly on fingerprint. Fingerprint biometric modality is predominantly thought of due to its two vital characteristics uniqueness and permanence that's able to stay unchanged over the lifetime. In this paper, we presented the basics of fingerprint biometric modality, its applications. Various methods for extracting minutiae points from the input fingerprint images are presented in detail. Fingerprint based key generation algorithm was presented by extracting the minutiae points from three different scenarios. The final cryptographic key generated is complex and stable throughout a person’s lifetime [3].

E. Thambiraja (2012) *et al.*, present that the viewpoint on the existing state of the production in the area of the encryption procedures, in the most specific on the private key block ciphers which are extensively used for the bulk document and connection encryption. He has originally reviewed few of the most general and stimulating procedures presently in use. These paper attentions mostly on the various kinds of encryption techniques that are existing and comparative study every method composed as a literature survey. Goal and wide experimental learning of implementations of several presented encryption techniques. Also focuses on image encryption techniques, information encryption techniques. This study extends the performance parameters applying in the encryption procedures and examining on their secure matters [4].

Sourabh Singh (2013) *et al.*, present that a technique which at major converts the text into the image applying an RGB (Red Green Blue) substitution, and then resulting image is encrypted by the applying Algorithm of AES, under this method, the secure key is rapidly sent along with in a single transmission cipher text, thus it also resolves the key conversation difficulty that commonly arises in the greatest of encryption modes. [5]

Ishaan Agarwal (2014) *et al.*, present that the aim of this scheme was in the progress of a password-based image encryption method that would be essentially secure from brute-force attacks, resulting in the image that would have not recognizable pattern contain. These techniques planned were applied in a Java program. For the purpose of the growth of the securities of the procedure, double encryption keys are generated which is based on user's key are used and have an upgraded no. of issues which is hooked on upon the password. The encryption algorithm can be used for a wide variety of purposes ranging from being commercially used by the consumer to encrypt data for communication or storage to corporate houses handling business secrets to militaries dealing with classified information [6].

P. Muthu Kannan (2012) *et al.*, present that Wireless networks are increasingly used in various applications. Implementing security aspects of those networks are very critical as the communication is done in free space. The biometric is an emerging technology which provides an effective solution to the Security problems of the wireless communication. Two factor biometric keys can also be used to provide enhanced security level. In this work, Cryptographic keys which are generated from face and fingerprint are combined using an effective algorithm. This algorithm can provide better security for wireless communication. In this paper, an algorithm is proposed and implemented for the generation of two factor biometric keys in order to provide more secure accessing of wireless networks. This algorithm combines the two biometric features. The objective of privacy concern is addressed by biometric encryption technique [7].

5. Proposed Work

In e commerce money transaction must be sure to secure our payment information like our password which may be biometric identified like fingerprint, iris, voice, *etc.*, in this paper, we focus on AES encryption algorithm and Stenography with applying pixel swapping to encrypt the input image for the secure transaction purpose. This paper has a target on compress the time of encryption and decryption adopting multithreading. Consider following conspiracy to explain the proposed work.

At sender side-

1. To convert the original image into binary code.

2. Divide binary code into blocks, all blocks contain 16 characters (128bits).

3. Apply AES encryption process to convert plaintext blocks into cipher text blocks.

4. AES Algorithm has the following steps.
   The first step is taking input plain text than apply Key Expansion-Round keys are derivational from the cipher key applying Rijndael's key schedule. Initial Round (Add Round Key- individual byte of the state is joined with the round key using bitwise XOR) Rounds (Sub Bytes-individual byte is replaced with another from lookup table. Shift Rows-individual row of the state is cycle shifting. Mixing Columns- a mixing process which operates on the columns of the state, merge the 4 bytes. Add Round Key) Final Round (Sub Bytes, Shift Rows, then Add Round Key)
5. Transfer these cipher text into binary form.

6. Encrypt image is embedded into cover image by using an LSB technique by applying stego key and finding an image is called stego image and apply the Algorithm of Pixel Swap using a pseudo–random sequence than send to the receiver.

At receiver side-

1. Change the received image into binary.

2. Embedded stego binary image into cipher text bit and decoding, select the pixels using the same
Pseudo-random sequence.
3. Convert the text and divided into block, all 16 characters.

4. Apply decryption process to cipher text block for finding secret image purpose.

Base paper screenshot

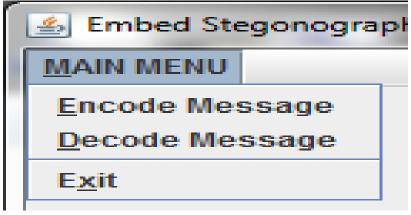
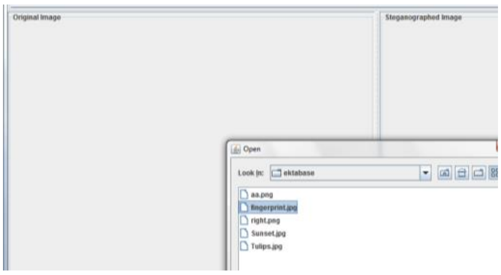


Figure 1

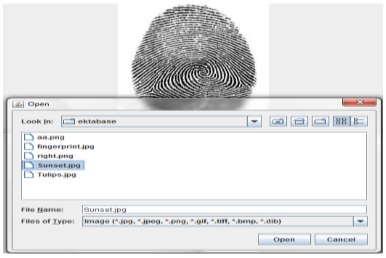
In a Figure 1 shows the main screen which contains main menu file contain encoded message, decoded message and exit.



Look In: ektabase

Figure 2

Then in the Figure 2, screen is divided into two parts, first is the original image and second is the Stenography image and select any fingerprint image.



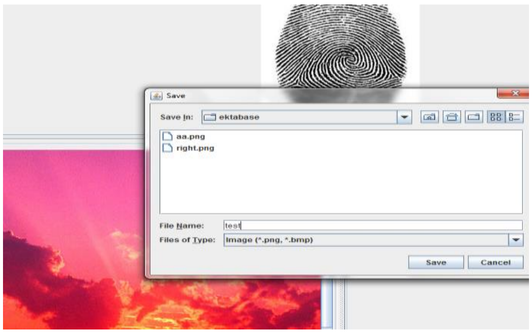
Look In: ektabase

File Name: Sunset.jpg

Files of Type: Image (*.jpg, *.jpeg, *.png, *.gif, *.tiff, *.bmp, *.dib)

Figure 3

Then in Figure 3 select another image.



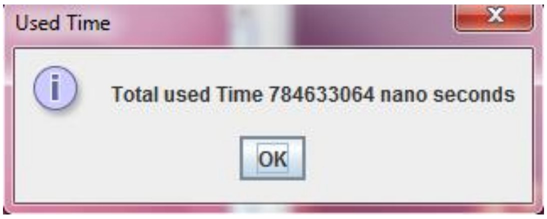
Save In: ektabase

File Name: test

Files of Type: Image (*.png, *.bmp)

Figure 4

In Figure 4 Stenography image is created it means the fingerprint image is embedded into another image.

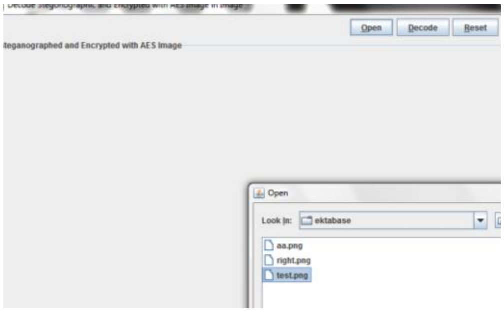


Used Time

Total used Time 784633064 nano seconds

Figure 5

In Figure 5 show the base paper embedded and encryption time in a nanosecond.

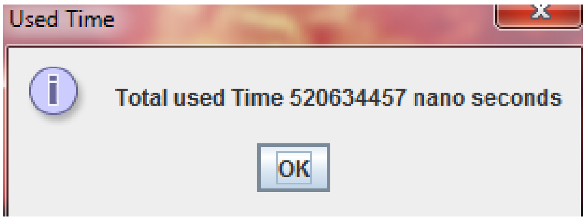


teganographed and Encrypted with AES Image

Look In: ektabase

Figure 6

In Figure 6 shows the decoded message



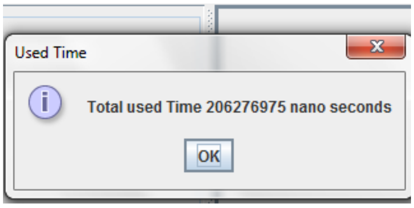
Used Time

Total used Time 520634457 nano seconds

Figure 7

In Figure 7 shows the decoded time in a nanosecond.

Final Paper Implementation

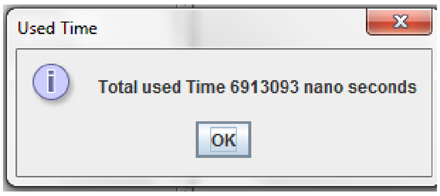


Used Time

Total used Time 206276975 nano seconds

Figure 8

In Figure 8 shows the original image is divided into two different images with the help of AES encryption and Stenography with help of applying multithreading. And show encoded time, which is very less compare to base paper encoded time.



Used Time

Total used Time 6913093 nano seconds

Figure 9

In Figure 9 shows the Decode message time. And show decoded time, which is very less compare to base paper decoded time.

After comparison base paper encode and decode message time and final paper encode and decode message time contain a lot of difference between them. And the final result comparison is

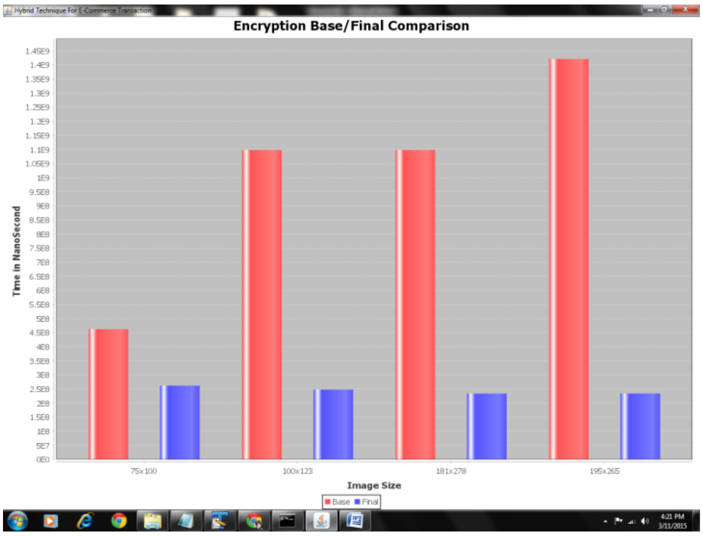


Figure 10

The two bar graphs represent the variance between decoded and encoded image time of previous work and our work. Also show results after applying multithreading result is shown in two chart X coordinate represents the image size and Y coordinate represents the time in nanosecond. Red bar represents the base paper and blue bar represent the proposed paper.

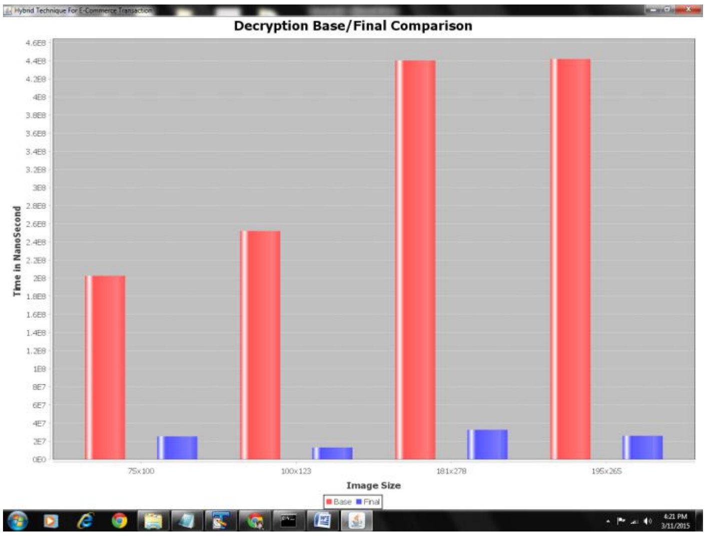


Figure 11

6. Conclusion

Electronic commerce, commonly known as eCommerce is trade in products using the internet. The main concern in online shopping is secure. Security at the e-commerce becomes more and more important. In this proposed paper, improve the Secure electronic transaction by using biometric identification payment system. For security purpose use of AES and Steganography. By using AES encrypt the data and this data are embedded to image edges to perform Stenography. By this encryption and decryption time reduced with the adoption of multithreading. The graph shows the comparison between base paper and proposed paper in terms of time.

References

[1] Suhad Latef," Color Image Encryption using Random Password Seed and Linear Feed Back Shift Register", Journal of Al-Nahrain University, Vol.14 (1), March, 2011, pp.186-192.

[2] Ravi Subban," A Study of Biometric Approach Using Fingerprint Recognition", Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013

[3] A. Jaya Lakshmi," Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality", IOSR Journal of Engineering, Vol. 2 Issue 2, Feb.2012

[4] E. Thambiraja," A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012

[5] Sourabh Singh," An Enhanced Text to Image Encryption Technique using RGB Substitution and AES", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013

[6] [6] Ishaan Agarwal," Password-oriented Image Encryption with multiple dependent factors", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 5, Ver. VI (Sep – Oct. 2014)

[7] [7] P. Muthu Kannan," Secured Encryption Algorithm for Two Factor Biometric Keys", International Journal of Latest Research in Science and Technology Vol.1,Issue 2 :Page No.102-105 ,July .August (2012)