A Survey Paper on Improving Money Transaction Security Using AES and Steganography

Ekta Chauhan
Dept of computer science Engg., Maharana Pratap College Of Technology, Gwalior, India.

Abstract – In the present age technology of communication has been developed, which increase the secure data communication need. The two most important security aspects that deal with the transmitting data or information over some medium like Internet are steganography and encryption method. Steganography deals with the hiding information presence of a message and encryption deals with hiding the information plain text to unread data. Both of them are used to confirm security. AES is a variable bit block cipher and uses 128, 192 and 256 bits length of variable key length. In this paper for high security purpose using both AES and steganography and also for reduce encryption and decryption time using parallel processing also.

Index Terms – AES; steganography; parallel processing,etc.

1. INTRODUCTION

The emerging scenarios of communications system requirement exceptional security means especially in communication and computer network. Security standard assumes a clear separation between users and attackers and network security is gaining significance as the information being exchanged on internet growths. Therefore, the security and privacy are required to safeguard against unauthorized access. This has resulted in an explosive development of the information hiding field, which covers applications for example copyright protection for digital media, Steganography, Cryptography, Digital Watermarking and also fingerprinting. All these data hiding applications are quite diverse. Steganography and Cryptography are commonly used in the data hiding field and has received important attention from both academia and industry in the present. Former conceals the original data while the latter conceals the most fact that data is hidden. Steganography provides a secrecy high level and security through joining with the cryptography. Until quite recent times, the science of Cryptography has been used regularly and exclusively by government and defense sector in order to protect the privacy of classified communication.

As the development of Internet technology increases, the transmission of digital media is now-a-days convenient over the networks Data and information security keeps most importance in today's fast developing era. Various networks are used to exchange the information, which may be secure or sometime not secure. With the rapid growth of computer networks and advancement in technology, a large data amount is being exchanged. Most of the information is confidential or private which increases the demand for stronger encryption techniques. Security has become a capable network critical feature. Communication is not safe due to the presence of some malicious users who wait for a chance to increase access to the confidential information. Cryptography is derived from Greek words "kryptos" (meaning "hidden") and "graphein" (meaning "to write"). Cryptography is the study of shuffling information in such a way that no one can understand the original meaning of messages without knowing the secret key which make it again original text. The converting data (plain text) procedure through transforming it into the format of unreadable (cipher text) is called as encryption. Encryption methods can be sometimes broken through cryptanalysis, also known as code breaking, although modern cryptographic methods are virtually unbreakable. Cryptography encrypts the original information that is being sent. This mechanism employs mathematical method and algorithms to scramble introduction into an unreadable format. It can only be decrypted or decoded through the party that possesses associated key [2]. Steganography is derived from the Greek word "stegnos" (meaning "covered/secret") and "graphein" (meaning "to write/draw") [2]. Steganography is the study of means of hiding the information in order to prevent hackers from detecting the presence of the secret information. The process of hiding the message in a cover without leaving a remarkable trace is known as Steganography. Steganography is the form of convert communication in which a secret message is hidden with a carrier data. Steganography facade the presence of communication, making the true message not easily observable by the observer. Steganography or Cryptography attains the same aim using various means. Encryption data encode so that an unintended recipient cannot define its intended meaning. Steganography in contrast attempts to prevent an unintended recipient from the suspecting that data is there [1].

The authors studied both the algorithms and studied the techniques that use both the algorithm to provide high degree of security and also compare the result on the basis of timing and avalanche effect.

2. AES

Here [3] they realize and design an encryption system based on the algorithm on ARM (S3C6410), which can encrypt data and decrypt in numerous type of memorizers, for example SD card, U Disk and also mobile HDD. In this paper, they implemented and designed an encryption system to encrypt the stored

information based on ARM (S3C6410). The system that uses Visualization Technology and Human-Computer Interaction provides numerous key generators and encryption algorithms. In this paper, designed and implemented a system of encryption to encrypt the stored information based on the ARM (S3C6410). PN sequences with good properties are produced from chaotic map and system provides two several encryption algorithm kinds, one is a stream cipher with operation of X OR, the other different is a hybrid algorithm of chaos and AES. The AES is a specification for encryption of electronic data which is established by the U.S. NIST. In order to security improve of the private information in memorizer, this inherits the advantages in this paper. "Design of a secure chat application based on the AES cryptographic algorithm and key management" this paper presents the design and implementation of a software application for the provision of secure real time communication services between workstations, based on AES prototype cryptographic algorithms and an advanced secret key management system[5]. The application has been designed based on the military unit requirements, so as to allow groups of authenticated users to communicate and read transmitted information. This application can be used as the basis for the integrated communication system design for the military organization. The present design confines its operation within the local area network limits. "FPGA implementations of advanced Encryption standard: a survey" presents AES based on Rijndael Algorithm which is an effective cryptographic method that conclude ciphers generation for encryption and also inverse ciphers for decryption [6]. AES is the most secure symmetric encryption method that has gained worldwide acceptance. Higher security and encryption/decryption speed is ensured through operations like Sub Bytes (S-box)/Inv. Sub Bytes (Inv. S-box), Mix Columns/Inv. Mix Columns and Key Scheduling. Extensive research has been conducted into S-box /Inv development. S-Box and Mix Columns/Inv. Mix Columns on dedicated FPGA and ASIC to speed up AES algorithm and to decrease circuit area. Fault attacks are efficient and powerful cryptanalysis approaches to find the AES algorithm secret key.[7] "A Robust Fault Detection method for AES," this paper present that these attacks are based on the injecting faults into structure of the AES to obtain the confidential information. The counter measures number have been proposed to protect implementation of AES against these attacks. In this paper, they have proposed a fault detection method for the AES. [8] They present its complete details implementation in each AES transformation. The simulation results present that fault coverage achieves 99.999% for the proposed method. The proposed fault detection method has been implemented on Xilinx Virtex-5 FPGA. Its area overhead and frequency degradation have been compared and it is present that the proposed method achieves a good performance in frequency and area terms. [9] When NN with fast parallel computing and chaotic dynamics complex behavior, it is one of the best choice for designing encryption algorithm. With a chaotic NN through analyzing the complex dynamic behavior and the characteristics of parallel processing, NN-based chaotic encryption algorithm AES is presented, which can help the AES algorithm to overcome the classical key only because of security caused through the characteristics of lower and raise the AES security algorithm. To improve the AES algorithm efficiency on ARM processor, an optimization of AES was introduced and realized on ARM920T processor. [10] One-time key expansion was adopted. In the algorithm, Mix Columns () and Sub Bytes () were defined as T-table to store, which could growth the speed. The proposed algorithm programmed through C language was simulated and debugged on the ARM Develop v1.2 platform. Various implementations were compared to the storage space and speed of processing and a variety of different key length algorithm performances were given. The experimental results present that the execution speed of the presented algorithm improves significantly.

3. STEGANOGRAPHY

Steganography is the craft and science of covering communication; a stenographic system thus embeds covering content in unexceptional cover media so as not to the arouse an eavesdropper's uncertainty. In the past, people used unseen tattoos or invisible ink to convey steganography content. Today, network and computer technologies aprovide easy-to-use communication channels for the steganography. Essentially, the knowledge-hiding procedure in a stenographic system starts by unique cover medium's identifying unnecessary bits (those that can be changing without spoiling that medium's integrity). The embedding method design a steno medium by removing these unnecessary bits with information from the hidden information. Modern steganography's goal is to put its mere presence undetectable, but stenographic systems— because of their invasive nature— leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: changing the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting steno medium's statistical properties. The process of finding these distortions is called statistical steganalysis.[11]

4. LITERATURE SURVEY

The Niranjanamurthy(2013) et al present that an E-commerce Security is a part of the Information Security scheme and is specifically applied to the item that modification e-commerce that consist of Computer protection, Data protection and other wider realms of the Information protection framework e-Commerce provide the banking industry big opportunity, but also describe a set of new risks and vulnerability such as security threats. Information protection, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. In this paper they give an Overview of E-commerce

security, Understand the Online Shopping Steps to place an order, Purpose of Security in Ecommerce, various protection issues in E-commerce, protection online shopping guidelines.[12]

V.SRIKANTH (2012) with the fast development of E-commerce, protection subject is growth of person mind. The protection of the transaction is the core and key issues of the buildup of e-commerce. This paper about the protection subject of Ecommerce action put forward understand plan from two aspects that are technology and system, so as to rise the environment for the buildup of E-commerce and inspire the further buildup of E-commerce. [13]

ShaziaYasin(2012)Web applications growth, integrate services of third-party. Integration introduces new protection challenges due to the complication for an application to the coordinate its states of internally with those of the component services and the web client across Internet. [14] Ecommerce web site owners on one side are thinking of how to invite higher customers and how to make the visitors feel protect when working on the site, on the other side how the end users should rate an ecommerce website and what they should do to secure themselves as one among the internet community. Some objective of writing this research analysis journal is to prepare the readers to have clarity of thoughts on the technology which helps all of us to do secure transactions along with safety tips. And how ecommerce site owners, have to make their internet visitors to be of more comfort or Trust an ecommerce site via Trust marks, and by their security strategies. [15].

Himanshu Gupta (2011) et al present that electronic transaction Security over an insecure communication channel is a issue assignment that conclude numerous critical areas as protect communication channel, strong information encryption mode and trusted third party to the maintain electronic database. Conventional encryption methods in protect e-transaction can only maintain the data protection. The classified data of customer could be accessed through the unauthorized user for malicious plan. Therefore, it is needed to apply active encryption approach to intensify data protect as well as data communication authentication. The multiple encryption method provides acceptable electronic transactions security over wireless network. In this research paper, the needs of multiple encryption method in Secure Electronic Transaction are proposed to enhance the security of private data. This technique development the data security in such a manner that unauthorized user cannot access any information part over wireless network as internet.[16] Multiple encryption is an ambivalent encryption technique for Secure Electronic Transaction and it will play an important and revolutionary role in secure electronic transactions over wireless network. Multiple encryptions in Secure Electronic Transaction describe the enhanced security as well as integrity of confidential data due to multiple encryption operations. The main advantage of multiple encryption is that it gives better security because even if some secret or encryption keys are cracked or some part of cipher texts are broken, the confidentiality and privacy of the original data can still be maintained through multiple encryption. Secure electronic transactions with multiple encryptions will be an important part of electronic commerce in the future. Such level of security is required to earn the interest and trust of customers, merchants and financial organizations for online transaction over a wireless network. The ideal of the secure electronic transactions protocol (SET) with multiple encryption is important for the success of electronic commerce. Lucie Veseláa(2014) et al present depending upon the supplier or buyer location, tax regulations also may need a government- number of issues identification, qualified electronic signatures, particular content fields and also long-term archiving of the invoice(Keifer, 2011).

(Schmandt andEngel-Flechsih, 2013)For invoice must ensure the credibility of its origin, the integrity of its content and its readability. The authenticity of the origin of the tax document in the form of electronic and the integrity of its content can be provided through recognized electronic information or electronic signature exchange (Chamber of Commerce, 2012).

This represents a considerable time and effort waste, especially provide that the reproduction procedure can lead to the inaccuracies and introduction. Automating this function not only eliminates these risks, but enables the digitized content to be re-used in a more effective way (Hayward, 2013).

An effective management of inward cash flows from completed sales is absolutely critical for staying in business (Hanif, 2013).

Sourabh Singh, AnuragJain(2013) et al present that a technique which at first transforms text into an image applying an RGB substitution, and then encrypts the resulting image applying AES Algorithm, under this method, secret key is smartly sent along with the cipher text in a single transmission, thus it also solves the key exchange issue that commonly arises in most of the encryption models. The encryption and decryption procedure create the combination database use for text to image transformation. A method which implemented will lead to a highly secure transmission of text. If a hacker anyhow decrypts the image, then he gets another image, which further confuses him whether the actual information is in text or in image format, the blend of text to image transformation and then AES encryption makes actual information (plain text)highly secure for transmitting it on extremely vulnerable and insecure network environment.

E.Thambiraja (2012) et al present that an aspect on the present state of play in the plot of encryption algorithms, in individual on private key block ciphers which are usually used for bulk information and link encryption. We have initially survey few of the more amusing and famous algorithms at present in use.

This paper focuses mostly on the various encryption methods that are existing, and comparative study every methods together as a literature survey. Aim an extensive experimental study of implementations of numerous presented encryption methods. Also focuses on image encryption methods, data encryption methods. This study extends to the performance parameters used in encryption procedures and analyzing on their security issues.[17]

Swati Paliwal (2013) et al present that concentrates on the various types of encryption methods that are existing. It also frames all the methods together as a literature survey. Goal an extensive experimental study of implementations of numerous presented encryption methods. Also focuses on image encryption methods, knowledge encryption methods, double encryption and Chaos-based encryption methods. This study extends to the performance parameters used in encryption processes and analyzing on their security issues.[18]

5. PROPOSED METHODOLOGY

In e commerce money transaction must be sure to secure our payment information like our password which may be biometric identification like finger print, iris, voice etc. in this paper we focus on AES encryption algorithm and steganography with applying pixel swapping to encrypt the input image for secure transaction purpose. This paper has target on compress the time of encryption and decryption adopting parallel processing. Consider following conspiracy to explain the proposed work. There is a file of 8 megabit (6.4e+7 bits) which use to be sent from sender to receiver. Using a 128bit AES algorithm the number of steps required will be 6.4e+7 /128=500000. This means 500000 data blocks will be created on which AES will be applied independently. But using the parallel access the number of steps required will be 500000/64=7812.5where 64 is number of processors. The entire time required to process the data will be decreased by number of processor time's Uniprocessor time. The proposed access initially breaks the input file into 128 partitions.

At sender side-

1. To convert the original image (carrier image) into binary code.
2. Divide binary code into blocks, all block contains 16 characters (128bits).
3. Apply AES encryption process to convert plaintext blocks into cipher text blocks.
4. AES Algorithm has following steps.

   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 shift cycle. Mix Columns- a mixing operation 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 alteration component technique with apply stego key and finding image is called stego image and apply the Algorithm of Pixel Swap using a pseudo–random sequence than send to 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 division into block, all 16 characters.

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

6. CONCLUSION

AES encryption method and steganography encryption are well known methods for data security. To enhance the security we can use combined AES encryption and steganography instead of using AES encryption or steganography alone. In this paper we have reviewed various combinations of AES encryption and steganography methods. For high security purpose applying combinations of both AES and steganography and also for reduce encryption and decryption time using parallel processing also.

REFERENCES

[1] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998.pp. 32-47.
[2] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.
[3] Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen"ARM Realization of Storage Device Encryption Based on Chaos and AES Algorithm" 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications
[4] Chun Yuan, Yuzhou Zhong, and Yuwen He, "Chaos Based Encryption Algorithm For Compressed Video," Chinese Journal of Computers, Vol.27 No.2, Feb 2004, pp.257- 263.
[5] Nikolaos G. Bardis, Konstantinos Ntaikos, "Design of a secure chat application Based on AES cryptographic algorithm and key management"

[6] Shylashree.N; Nagarjun Bhat; V. Shridhar, "FPGA Implementations of advanced Encryption standard: a survey" Directory of Open Access Journals (Sweden), Jan 2012
[7] Hassen Mestiri; Noura Benhadjyoussef; Mohsen Machhout; Rached Tourki, "A Robust Fault Detection scheme For Advanced Encryption tandarad," Directory of Open Access Journals(Sweden), Jan 2013
[8] Rui Zhao, Qingsheng Wang, and Huiping Wen, "Design of AES algorithm Based On Two Dimensional Logistic and Chebyshev Chaotic Mapping," Microcomputer
[9] Yi Li, and Xingjiang Pan, "AES Based on Neural Network of Chaotic Encryption algorithm," Science Technology and Engineering, Vol.10 No.29, Oct 010, pp.7310- 7313.
[10] Ruxue Bai, Hongyan Liu, and Xinhe Zhang, "AES and its software implementation based on ARM920T," Journal of Computer Applications, Vol.31 No.5, May 2011, pp.1295-1301.
[11] file:///c:/users/techii%20group/downloads/2-14 1372154968
[12] rui wang, shuo chen "how to shop for free online security analysis of cashier-as-a-service based web stores". ieee s&p'11 proceedings
[13] v.srikanth "ecommerce online security and trust marks". ijcet issn 0976 – 6375, volume 3, issue 2, july- september (2012),
[14] shazia yasin1, khalid haseeb, rashid jalal qureshi,'' cryptography based e-commerce security''ijcsi international journal of computer science issues, vol. 9, issue 2, no 1, march 2012.
[15] lucie veseláa,*, miroslav radiměřskýa,'' the development of electronic document exchange, enterprise and the competitive environment 2014 conference, ece 2014, 6–7 march 2014, brno, czech republic
[16] 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*
[17] e. thambiraja," a survey on various most common encryption tecnique", international journal of advanced research in computer science and software engineering, volume 2, issue 7, july 2012
[18] swati paliwal," a review of some popular encryption techniques", international journal of advanced research in computer science and software engineering, volume 3, issue 2, february 2013