International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

A Combinational Technique in Security System using Cryptography and Steganography

G. Naveen Samuel
Joe Suresh College of Engineering, Tirunelveli

Immanuel Ganadurai
Karpagam University, Coimbatore

Abstract

A new technique proposed with the combination of cryptography and steganography enhanced with powerful algorithms for generating a new security system can be called as Crypto/Stegano System. It consists of both cryptographic functions and steganographic functions. Here in this paper a security system is enhanced by ensuring data hiding operation using steganographic function. The message to be transferred is encrypted using an AES algorithm which is modified for steganography to occur. Encrypted message is encouraged with a text and a key. Now to make the transfer to be more secured we introduce another two keys with the encrypted message where the message is made to be hidden in an image. Image bears the message in which it needs both keys for viewing the text message behind it. A Steganographic function makes the message detection process much harder for the hackers who interrupt between the sender and receiver. This kind of system is to be introduced in applications such as transferring secret data that can be authentication of various fields. This system ensures a secure data transferring option between the source and destination stations.

1. Introduction

a) Cryptography:

In the Presence of third party members in network, a secure communication is practised and studied which is called as cryptography. In networking for data and telecommunications, cryptography is always necessary while making a secure communication over any entrusted medium. Cryptography can be specified as the security service over any network, particularly Internet [4]. Security services are organised over a communication process that are categorised into several services which includes:

i) Authentication: Process of assuring one's identity. Make an authorised transmission between two parties.

ii) Privacy: Data are kept confidential. Here no one can read the message except the indexed receiver.

iii) Data Integrity: Identifying the data received is exactly as sent by the authorized clients in network and ensures an assurance for the data.

iv) Non Repudiation: Provides a proof that the sender really sent this message and the receiver has received the message.

Most efficient usage of cryptography is in user authentication modes. Authentication needs encryption and decryption techniques [2, 7]. These techniques are organised in three different procedures such as Symmetric ciphers, Public key encryption and hash functions.

Symmetric ciphers ensure a classical and modern algorithm of symmetric encryption. Here these processes are engaged in the account of message authentication and key management. This technique consists of five intergradients such as plain text, encryption algorithm, secret key, cipher text and decryption algorithm [20, 23]. Plain text which is the inputted message is enrolled into the encryption

algorithm such as AES or DES algorithm and then brought as cipher text as output. Encryption process can be made with algorithms based on two cipher techniques such as stream ciphers and block ciphers. Stream ciphers are engaged by encrypting a data stream one bit or one byte at a time [12]. Block ciphers are engaged by encrypting a block consisting of the whole plain text to produce a block of cipher text with the equal length. Block cipher techniques are widely used in several standards of algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES). AES encryption and decryption schemes are mostly used in much applications as it works commercially with a large size of input (plain text) and key while comparing to the DES encryption and decryption schemes [9]. AES uses a 128-bit of input block size and a key of 128-256 bits of size. DES uses a block of 64-bit of size and a key holding 56-bit of data. Thus comparing both the standards AES can be used in many applications whereas it also ensures a powerful scheme of encryption and decryption.

Public key Encryption includes two algorithms such as RSA and Elliptic curve algorithms for providing confidentiality. This encryption can be asymmetric as it uses two different keys for performing encryption and decryption standards [11, 17]. Plain text is encrypted into cipher text by using one of two keys (public or private key) with an encryption algorithm. Here the encryption algorithm may be RSA (Rivert, Shamir and Adlemen) algorithm or the elliptic curve algorithm whereas block ciphers are used as the encryption and decryption standards [6].

Hash Functions serves a variable length message into a fixed length hash value. Hash functions are always combined with secret key to provide a secure message authentication. A secure authentication is made only when a secret key is shared which ensures a symmetric encryption [19]. Message authentication verifies the integrity of the message. Most commonly used cryptographic techniques for message authentication are Message Authentication Code (MAC) and a secure hash function. MAC is an algorithm that requires a secret key usage. MAC algorithms are organised with a variable length message and a secret key as input and introduces a message authentication is published along the usage of hash functions [21]. It is engaged with a hash value of fixed length. Authentication of message by the receiver is by re computing the hash value.

b) Steganography:

A mechanism of hiding the original messages from the hackers and by making a suspect of the existence of the message only to the intended receiver is called steganography. Here the real message is sent as image or text in which a specific hiding operation is done through the encryption of the message in which special keys are arranged for those intended receivers to capture the original message [15, 22]. Thus keys cannot be organised by the hackers or intermediate agents. The receiver alone makes consumption procedure of the real message sent by the sender. Real message can be letters or digits or image which can be encrypted as hidden message in any form as text or image [3]. Here only the intended parties could make their sending and receiving operations and no other parties could be engaged in this process.

2. Proposed Methodology

A secure data transfer can be made using two ways such as Cryptography and steganography in networks. Combination of both these security structures results in achieving a highly secured method for data communication. Encryption and decryption of messages are made under the technique of cryptography [13]. Hiding of data that are to be communicated can be made using steganography. This paper is devised by developing a new security system with additional features in securing data where the data to be transferred are hidden by combining steganographic security technique with cryptography to ensure a confidential structure in transferring options. A modified approach on symmetric encryption algorithm is encouraged along this paper for encryption of messages and a part of message is made to be hidden in an image. The other part of the message that is unhidden can be organised into two secret keys for making a highly secured system. Original message that is to be communicated between the source and destination can be retrieved using the keys that are organised in the encryption state of cryptography and also by using those extra keys mentioned in the process of steganography [24]. Goal of this paper is to develop a new security system that can be highly secured as messages cannot be retrieved easily from the image by the interacting hackers in the communication process. Several modules are proposed in this new security system as formulated below:

a) A modified approach on symmetric key algorithm:

Encryption process made in this module is a common approach of converting a plain text (real message) into a cipher text whereas it ensures a key representation of encouraging AES approach. Here encryption of plain text is organised using a standard symmetric encryption algorithm. A key is byte wise XOR ed can be an external key approach is used in this modified algorithm for the encryption of plain text. Here the standard encryption process includes these modifications as a part of its mechanism. An external key which is used in this approach is defined only by the user or the sender of this encryption process and not generated by the system [18]. System can also generate keys by its own for encryption. Cipher text is obtained as a result of encryption status. As a new approach of key structure is introduced in this key algorithm, it is referred as the modified symmetric key algorithm. This algorithm plays a main role in this paper to facilitate a security in data transferring structure.

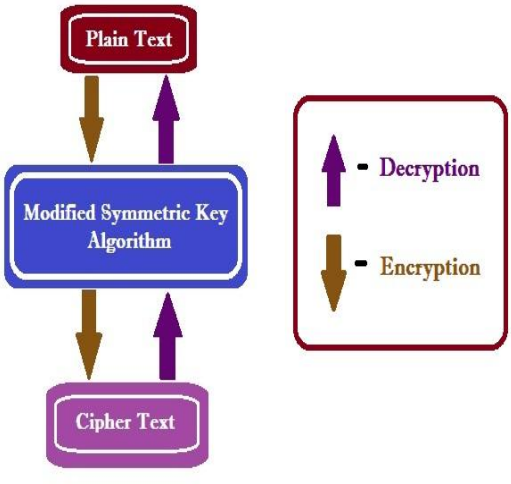

Figure1. Modified Symmetric Key Algorithm

Every encryption technique should be introduced with its reverse process of action. Decryption technique can be the possible reverse action of the encryption whereas the converted cipher text is again reversed by converting it again to the real message. Figure1 enhances the systematic procedure of the modified symmetric key algorithm. This action is encouraged only by the receiver or the destination station [16]. Here the modified symmetric key algorithm plays a role in this module by again making the XOR operation of the round key which is the external key that is XOR ed in the encryption process. This round key is XOR ed with its known pattern for ensuring a symmetric decryption technique. Decryption can be evolved by making the conversion process using a modified approach of key algorithm to show an outcome of the plain text which is the real or actual message to be communicated with the destination.

b) Separation Strategies:

Providing an extra security feature to the system is the main operation of this module. This module entails an intermediate operation in engaging with the separation computation. Here the cipher text is engaged in computation of separation. Cipher text is separated into three parts such as a message or text which is to be hidden and two keys [14]. Here the key separation or distribution strategy is based on the symmetric key algorithm evolved in this module along with the cipher text. The message to be hidden is organised with its character set length ‘n’ for ensuring another process of hiding. A standard procedure is encouraged along this module for generating two other keys from the initial cipher text.

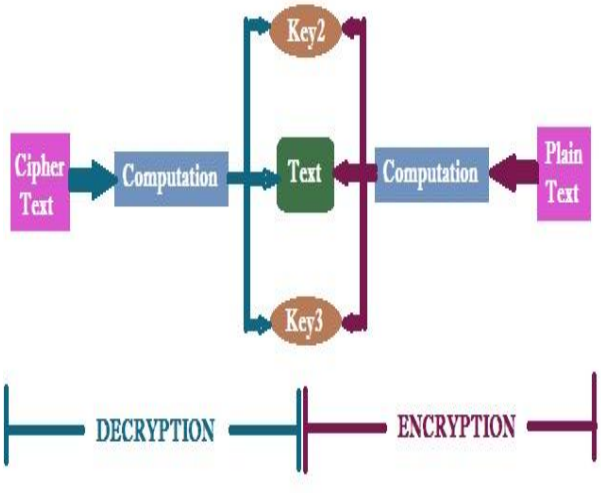

Figure2. Separation Strategies

Figure2 shows the strategic separation technique enrolled in this system. While receiving operation is initiated, then there is a reverse process evolved in this module for regenerating the original cipher text for the decryption module explained before. Receiver needs both the keys generated with the hidden message to generate the original cipher text [10]. After obtaining the cipher text, it is sent to the symmetric key algorithm operation to enrol a decryption procedure on the regenerated cipher text by the receiver statics.

c) Steganographic Procedure:

Data hiding operation is carried out in this module. Here steganography is evolved by hiding the message to perform a high security service in data transmission. Here the part of message which is separated in the separation module is made to be hidden along the steganographic function in which the hidden message can be a secret image [1, 5]. The image enrolled in the message can be a gray scaled image or a colored image. Secret image can be obtained using the RGB components of pixels dropped along the input key image for hiding operation to succeed. This hiding operation of data can be called as steganographic cipher operation. Here this hidden image is accompanied with the two keys as involved in the separation module [8]. Only by using those three options a decipher operation can be made. Original data from the secret image can be transformed in the decipher operation.

3. Implementation Details

Encryption procedure which is based on the *modified symmetric key algorithm* acts as the first module of this new security system. This module is enhanced with the AES (Advanced Encryption Standard) algorithm. AES algorithm plays a role of standard symmetric key encryption. AES can be identified as the symmetric block cipher which is used as a standard algorithm for a wide range of applications than DES algorithm. The drawback of DES is that it uses only a 64-bit block size whereas the present security system needs a large size of block for a fast and secure data transmission. Thus AES algorithm is almost used in wide range of applications as it uses a larger block size than DES. This module generates a cipher text using a modified symmetric key algorithm such as a modified AES algorithm from the plain text or the original message. Encryption procedure needs a plain text with an external key that is byte wise XOR ed with known pattern.

Key = (256-bit key) XOR (0x55)

AES algorithm works in several rounds in which each round is devised with the key that is used in the previous round as input which can be called as round key. Round key can also be XOR ed with 0x55. Here the external keys are organised only by the user or the sender and not defined by the system. Here a modified AES algorithm is referred as the round key evolved in this algorithm are byte wise XOR ed with known pattern. Encryption is made with the plain text along with a 256 bit key.

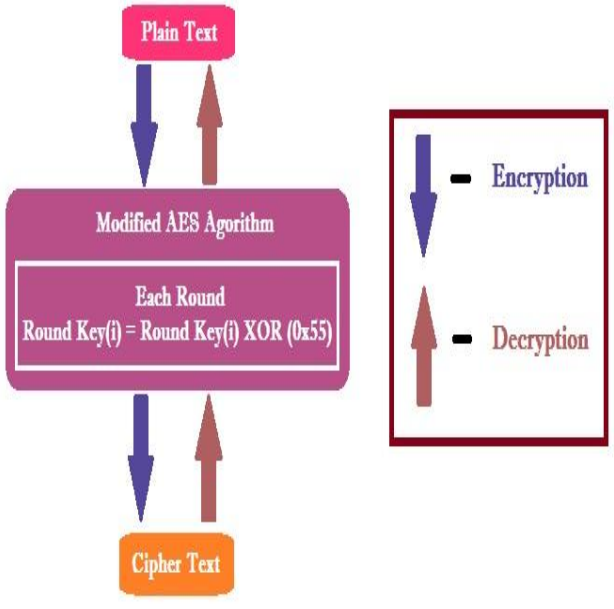

Figure3. Modified Approach on AES

Figure3 shows the approach which is modified in the standard AES algorithm. Decryption procedure of the module is also based on the modified approach of the AES algorithm. Here it is the reverse process of the AES encryption structure. The outcome of the encryption process becomes the input of the decryption process. Same key procedure of encryption is devised also in this decryption process by making the round key to be XOR ed with 0x55. Cipher text and 256-bit key are made as the input of this process and the outcome is the plain text or the original message.

Intermediate *separation strategies* exist as the second module of this proposed security system. Here the cipher text got from the encryption procedure is separated into a message that is to be hidden for the confidentiality and also separated with another two keys. This module makes the data transmission more secure. Here the keys are not organised externally. The system generates these two keys automatically by itself from the cipher text. Here the cipher text which is the input of this module is separated into alphabets and digits. The first ‘n’ bytes of characters can be hidden in

image whereas the remaining part is made to be appended at the end of the digit string which is devised as the key2. Another key1 is devised by tracking the position of all the character every time. The current position on the characters in cipher text is defined as key3. The result of this module is generating a confidential message with two keys (key2 and Key3).

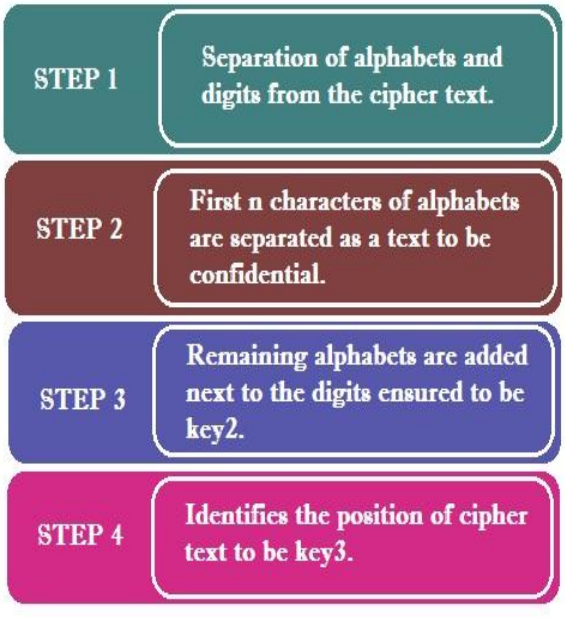

Figure4. Separation Procedure

A reverse process is also studied in this module for the receiving process in the communication. Here key2 which consists of digits and also the remaining alphabets is separated then by combining those alphabets with the confidential text. Figure4 shows the procedure to be maintained in the separation process. Confidential text can be made as the first set of alphabets and continuing it with the remaining alphabets. Next step makes the results of generating cipher text by combining both the digits and the set of alphabets.

Steganography is ensured in the system as the third module in the proposed system which could be a sub module of the above module. Here the text to be made confidential is set as the input of this module. The text is made confidential by hiding the text with a image. This operation could be made using the RGB components of each pixel. By alternating the RGB values of each pixel in an image, the text can be hidden in it. In this module only the needed pixels are chosen for changing its RGB components. Figure5 explains the procedure of steganographic function. A variation in the pixel position depends on the data and size of the image. For altering the RGB components of the pixels a mathematical approach is engaged. The outcome of this module is a secret image where the data is hidden in it.

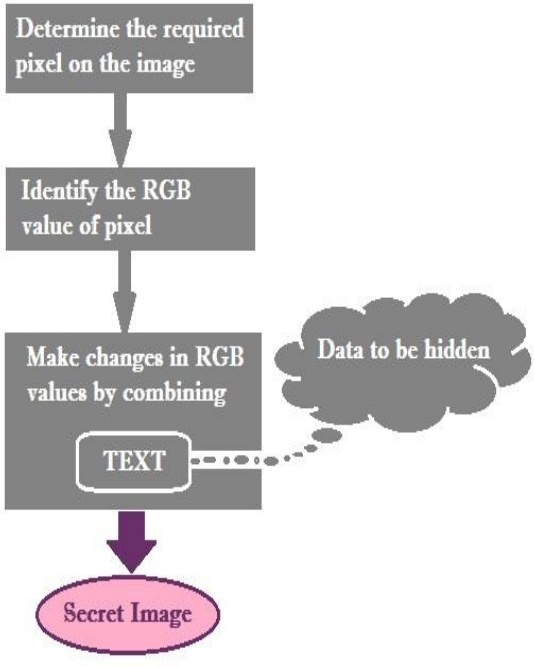

Figure5. Steganographic Procedure

Receiver or the destination station makes a decipher operation by generating the confidential data from the secret image. This module is processed by identifying the RGB value of each pixel of the secret image and also identifies its entire original RGB value of each pixel. While comparing those RGB values of the secret image and from the original image which acts as the key in this module, the data can be found from the difference of the RGB values in the image.

4. Performance Analysis

In present scenarios, Cryptography is accumulated by several networks in presenting a security system. Here in this paper, the proposed security system with the combination of both cryptography and steganography ensures an effective

security than the other security systems used in the network. Hackers are banned in this new combinational security system [4, 17]. Proper encryption and decryption are made along with the steganographic functions. Steganography is a value added function in which by using this function, the data hiding operations are mainly used and directed to propose an effective policy on the field of security. This paper initiates the working of the cryptographic and steganographic functions along with the text separation strategy [11]. Keys which are used in the proposed system are much harder to detect by the hackers interrupting the communication process. Usage of only the steganography functions shows less security to the data but while enhancing cryptographic functions in it gives an effective security policy. Objective of the security system is fully verified and it results good in this present security structures [23]. Proposed technique maintains a prominent relation with the sender and receiver and gives them assurance on the security of their data which are about to be transmitted. Performance of this proposed system satisfies most of the communicators and administrator of the network.

5. Conclusion

A new security system with a combination of cryptography and steganography is devised in this paper. Here four keys are used for securing the data transmission. Cryptography is meant to be a security service, while combining steganography it becomes a powerful security tool. This system enables a secure data communication without the interpretation of hackers in it. Secret image proposed in this system ensures a high security structure in which the image quality with distortion is analysed. A highly secured encryption algorithm (AES) is used along the system with the combination of steganography to make the detection of keys by the hackers to be harder. Several enhancements could be made in the future to speculate a high security structure. Some enhancements such as algorithms for image processing and some more algorithms for encryption and decryption can be made to turn this paper in providing high security into this overall system.

6. References

[1] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice‖ ", *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003

[2] Neil.F.Johnson, Zoran Duric, Sushil Jajodia, "*Information Hiding:Stegnography and Watermarking-Attacks and Counter Measures‖ "*, Kluwer Academic Publications,2000

[3] Ingemar J. Cox, *"Digital water marking and Steganography‖ "*, Second Edition 2000.

[4] Bruice Schneier ,"*Applied Crytography:Protocaols and Algorithms",* Second edition 2006.

[5] Wang H & Wang S, *"Cyber warfare: Stegnography Vs Steganalysis*", Communications of the ACM, October 2004

[6] Jithesh .K, Dr. A.V. Senthil Kumar, "Multi Layer Information Hiding -A Blend Of Steganography and Visual Cryptography", *Journal of Theoretical and Applied Information Technology*, Vol-19, No-2.

[7] William Stallings, *" Cryptography and Network Security‖ -Principles and Practices",* Third Edition.

[8] Alaa Taqa, A.A Zaidan, B.B Zaidan, "New Framework for High Secure Data Hidden in The MPEG Using AES Encryption Algorithm", *International Journal of Computer and Electrical Engineering*, Vol. 1, No. 5 December, 2009.

[9] Dunbar, B., *"Steganography techniques and their use in an Open-Systems environment",* SANS Institute, January 2002.

[10] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques., in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[11] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", *IEEE Journal of Selected Areas in Communications*, 16(4): 474-481, May 1998. Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.

[12] Sujay Narayana, Gaurav Prasad, "Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions", *Signal & Image Processing: An International Journal(Sipij)* Vol.1, No.2, December 2010.

[13] C.-C. Chang, T. D. Kieu, and Y.-C. Chou, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," *Proc. of the 2008 International Symposium on Electronic Commerce and Security*, pp.16-21, August 2008.

[14] C. C. Lin, and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," *Journal of Systems and Software*, 73(3):405-414, December 2004.

[15] Mohammad Ahmad Alia, Abdelfatah A. Yahya, "Public–Key Steganography Based on Matching Method", *European Journal of Scientific Research*, ISSN 1450-216X Vol.40 No.2 (2010), pp.223-23.

[16] Al-Husainy, M. A., (2009) "Image Steganography by Mapping Pixels to Letters," *Journal of Computer Science*, 5 (1): 33-38.

[17] Diffie, W. and , Hellman, M. E., (1976) "New Directions in Cryptography," *IEEE Transactions on Information Theory*, IT-22, pp. 644-654.

[18] M Chandra Jyotsna, I V S Venugopal, "Steganography In Tie With Compression And Cryptography", *International Journal Of Communication Engineering Applications-Ijcea*, Vol 02, Issue 03; July 2011.

[19] R.J. Anderson and F. A. P. Petitcolas (2001) "On the limits of the Stegnography", *IEEE Journal Selected Areas in Communications*, 16(4), pp. 474-481.

[20] Dipti Kapoor et al,"A new horizon in data security by Cryptography & Steganography", *International Journal of Computer Science and Information Technologies*, Vol. 1 (4) , 2010, pp.212-220.

[21] Robert L,Nadarajan R,"New Algorithms For Random Access Text Compression",*Proceedings of the Third International Conference on Information Technology:* ITNG 2006,IEEE,pp104-111.

[22] Sarker M.Z.H, Parvez M.S.,"A Cost Effective Symmetric Key Cryptographic Algorithm for small amount of data", *9th International Multitopic Conference*, IEEE INMIC 2005,pp.1-6.

[23] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana. R, "A Novel Security Scheme for Secret Data using Cryptography and Steganography", *I. J. Computer Network and Information Security*, 2012, 2, 36-42.

[24] B.Raja Rao, P.Anil Kumar, K Rama Mohana Rao, M.Nagu, "A Novel Information Security Scheme Using Cryptic Steganography", B. Raja Rao Et. Al. / *Indian Journal Of Computer Science And Engineering*, Vol. 1 No. 4 327-332.