© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and
g Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering,
Ahmedabad, Gujarat, India In association with
International Journal of Scientific Research in Science, Engineering and Technology

Critical Analysis of Cryptography and Steganography

Alpa Agath*, Chintan Sidpara, Darshan Upadhyay
*I.T. Department, V.V.P. Engineering College, Rajkot, Gujarat, India

ABSTRACT

Digital communication has become an essential part of infrastructure in the present world and it has witnessed a noticeable and continuous development in a lot of applications during last few decades. Nowadays, almost all applications are Internet-based and it is important that communication be made confidential and secure. Cryptography and steganography are the two important and widely used techniques that are used to provide information security over the open and insecure networks such as Internet. Cryptography distorts the original message itself whereas steganography hides the existence of the message. This paper gives an overview about the concepts of cryptography and steganography. Moreover, it presents a fair comparative analysis between various selected encryption algorithms on various parameters such as key size, block size, speed of encryption, level of security provided by algorithm, and memory usage. It also carries out comparison between traditional steganography methods and Hex Symbol Steganography method on basis of basic parameters such as capacity of carrier file to hide information, robustness and amount of security provided. The comprehensive analysis shows that AES and Hex Symbol Steganography provides more level of security and are robust in nature as compared to other competitors, hence providing more confidentiality.

Keywords: Information Hiding, Cryptography, Steganography, Advanced Encryption Standard (AES), Hex Symbol Steganography.

I. INTRODUCTION

In today's era, due to tremendous growth of networking technologies an enormous amount of data is being exchanged over the Internet as a result of which security of information being conveyed over the Internet is becoming more significant as sensitive data needs to be transferred securely over the internet while maintaining its confidentiality, integrity and availability [1].

To maintain the privacy and security of confidential and sensitive information there is a need of approaches which enhances the level of information security. Information hiding is one of the many available approaches which increase the level of information security. The most powerful and widely used approaches of information hiding used to contravene the threats to information security are Cryptography and Steganography [1]. Cryptography provides security by manipulating the original confidential information so that it becomes unintelligible for the intruders. Steganography conceals the existence of communication by embedding the confidential information in some other cover medium (e.g. image, audio, video, etc.).

Cryptography is used nowadays in almost all applications that use Internet as means of communication. Real time applications of cryptography include ATM machines; password protection of email passwords, social account (Facebook, twitter, etc.) passwords; E-commerce; Defence forces; intelligent agencies.

Steganography is used to overcome the shortcomings of cryptography and support the cryptography techniques to provide better and more efficient information security. Areas where steganography is used include bank and commercial organizations, digital watermarking, E-commerce, military, and the areas where cryptography is used.

The remainder of the paper is organized as follows: Section II introduces a brief note on cryptography and steganography. Classification of cryptography and a detailed comparative analysis of selected encryption algorithms are given in section III. Classification of steganography and a comprehensive comparative analysis of traditional steganography methods and hex symbol steganography are given in section IV. Finally, a brief conclusion with future work is given in Section V.

II. STATE OF ART: CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography and steganography are the two most widely and commonly used approaches to secure information being transmitted over the Internet either by encoding the information or by hiding the information [4].

A. Cryptography

Cryptography is the art and science of fabricating methods or algorithms that allow transmission of data in a secure manner by transforming the readable and understand-able data into irrational and unfathomable data in such a way that only the intended person is able to retrieve the exact original data from the data being transmitted [2][3].

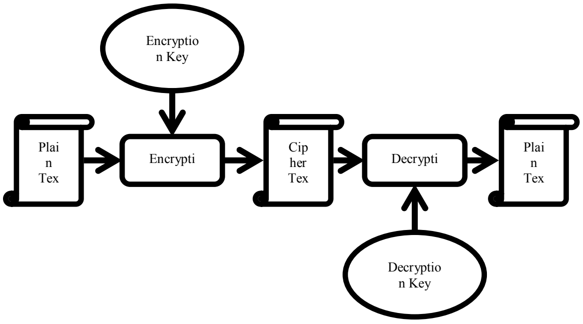

Figure 1. Process of Cryptography [2]

B. Steganography

Steganography is the art and science of camouflaging information into covert channels, hence preventing the detection of the camouflaged information from the eaves-droppers [5].

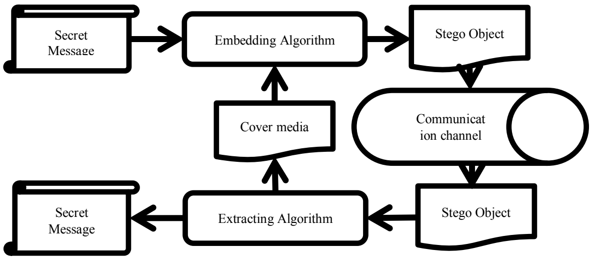

Figure 2. Process of Steganography [5]

Steganography is also known as "Disappearing Cryptography" [6].

III. CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

Encryption algorithms in cryptographic systems can be classified into different categories depending on the number of keys used to encrypt the plain text as shown in Fig. 3.

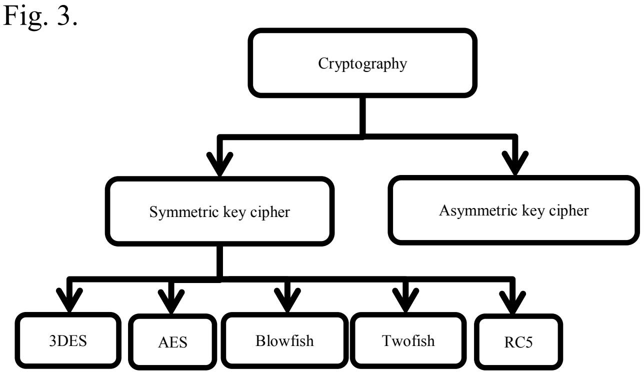

Figure 3. Classification of cryptography [11]

A. Comparison of Symmetric Encryption Algorithms

Comparison of various symmetric encryption algorithms on the basis of some selected parameters is shown in table 1.

Table 1. Comparison of Encryption Algorithms [7] [9] [10] [11]

Encryption Algorithm	**Block Size (in bits)**	**Key Size (in bits)**	**Number of Rounds**	**Encryption Speed**	**Memory Usage**	**Flexibility**	**Level of Security**
3DES	64	112,168	48	Very Slow	Moderate	Yes	Adequate
AES	128	128,192,256	10, 12, 14	Very Fast	Low	Yes	Excellent
Blowfish	64	128-448	16	Fast	High	Yes	Excellent
Twofish	128	128, 192, 256	16	Fast	Low	Yes	Good
RC5	34, 64, 128	128	1-255	Slow	Low	No	Good

The above comparison shows that AES provides higher level of confidentiality to sensitive information.

B. Advanced Encryption Standard (AES)

AES encryption algorithm is a symmetric block cipher that uses a secret encryption key and several numbers of rounds to encrypt the sensitive information (plain text) published by National Institute of Standards and Technology (NIST) in 2001.

1) Encryption Process of AES:

- AES deals with fixed size block of 128 bits or 16 bytes in length which is represented in 4x4 matrixes of bytes known as state array, which is modified at each round of encryption and decryption.
- The key provided as input is depicted as a square matrix of bytes and is then expanded into an array of forty-four 32-bit words, w[i]. Four distinct words (32bits * 4 = 128 bits) serve as round key in each round of the encryption and decryption.
- Based on the length of secret key used (128, 192, 256) for the encryption, the number of rounds i.e., N (10, 12, 14) in the cipher will differ accordingly. The single round of AES encryption process is shown in Fig. 4.
- First N-1 round in the AES cipher structure consists of the four basic transformations that encrypt the plain text of 128 bits in length of which one performs permutation and three perform substitution. The transformations are as follows:
  - o AddRoundKey: It is a simple bitwise XOR operation of the current state array with a portion of the expanded key.
  - o Substitution bytes: It uses an S-box to perform a byte-by-byte substitution of the state array.
  - o ShiftRows: It is a simple permutation.
  - o MixColumns: It consists of substitution operation that makes use of arithmetic over GF (28).
- The final Nth round contains only three transformations, and there is an initial single transformation i.e., AddRoundKey before the first round, which can be considered as round 0.
- The cipher begins and ends with an AddRoundKey transformation because only the AddRoundKey makes use of the key. The other three transformations together provide confusion, diffusion, and nonlinearity, but no security since they don't use the key.
- Each transformation in a round takes one or more 4x4 matrices or state array as an input and produces a 4x4 matrix as output. The output of the final Nth round will produce the cipher text.
- Each transformation is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by performing XOR with the same round key to the block (A XOR A XOR B = B).
- The decryption process in AES will use the expanded keys in the reverse order as used in the encryption. The decryption algorithm is not identical to the encryption algorithm. The order of transformations used in each round of decryption is different from that used in encryption.

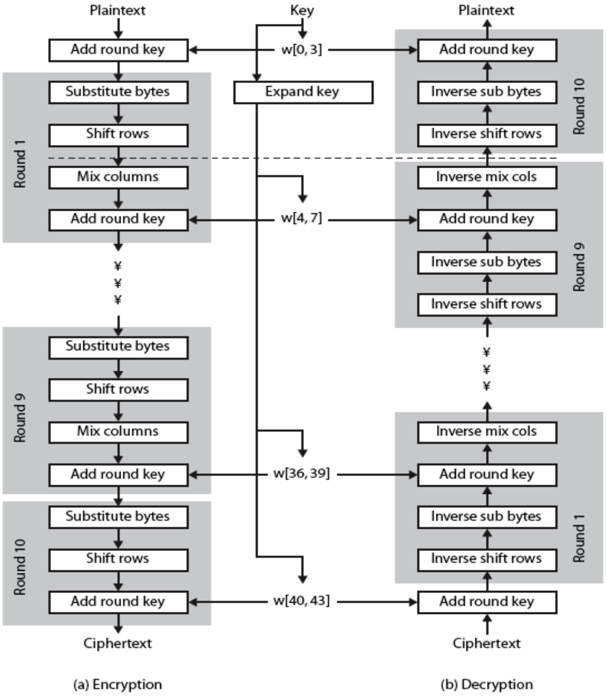

Figure 4. AES Encryption and Decryption Process [8]

IV.CLASSIFICATION OF STEGANOGRAPHY

Steganography can be classified according to type of cover medium used to hide the secret message as shown in Figure 5.

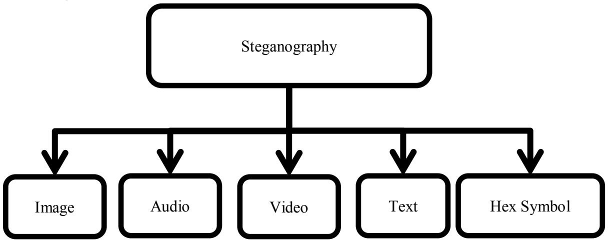

Figure 5. Classification of Steganography [5] [14]

A. Comparison of Traditional Steganography methods and Hex Symbol Steganography

Comparison between traditional steganography methods and hex symbol steganography is shown in table 2 on the basis of primary steganography measures.

Table 2. Traditional Steganography methods vs. Hex Symbol Steganography [14]

Steganography Measures	**Traditional Steganography Methods**	**Hex Symbol Steganography**
Imperceptibility	Concealed data can be recognized in the form of disruption in sound and video files, changes in image frames and colors.	The secret data will be embedded into hex symbols, so it is impossible to recognize by human eyes.
Capacity	Limited capacity to embed secret data.	More capacity to embed secret data as compared to other methods due to the nature of hex symbols.
Robustness	Less robust in nature.	More robust.
Security	Adequate	Excellent
Codes used to conceal secret data	Binary codes	Hex symbol codes

The above comparison shows that Hex Symbol Steganography method is more robust in nature and provides higher level of security (confidentiality) than traditional methods such as image, audio, video steganography.

B. Hex Symbol Steganography (HSS):

Hex Symbol steganography uses hex symbol carrier files to conceal the confidential information instead of digital multimedia carrier files such as image, audio, video and text files [14]. It uses the hex symbol codes to embed the secret information unlike the traditional steganography methods Which use binary codes to conceal the secret information [14].The stego object obtained after embedding the secret message in the hex symbol carrier file will be unfathomable (difficult to understand) by the intruders who are trying to gain access of the confidential information stored in the secret message.

1) Hex Symbol Algorithm:

- Prior to communication the authorized parties i.e., both the sender and receiver will decide certain patterns which will act as key to embed the secret information in the carrier file.
- The patterns used to conceal the secret information will be created by converting a chosen carrier file into hexadecimal symbols, segmenting the resulting hexadecimal carrier file with size of each segment being a 16x16 matrix, and then numbering the matrices (segments) sequentially [18] as shown in Figure 6.

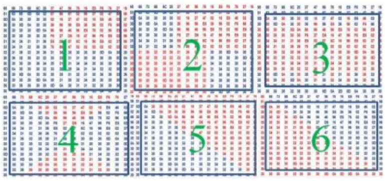

Figure 6. Segmented Hex Symbol Carrier File [14]

- Some of the segments of the hexadecimal carrier files are used to conceal the secret information on the basis of the pattern chosen by the sender and receiver.
- A codebook is prepared which consists of a letter representing the pattern with the sequence of segment numbers that are used to embed the secret message [14]. The letter representing the pattern will act as the stego key in the process of steganography. The example of code book is shown in Table 3.

Table 3. Example of Shared Secret Codebook [14]

Key Symbol	**Selected Random Sequence**

S	524316
O	643125
M	365124
Y	513642

- Once the codebook is prepared, it is shared between the sender and receiver in a secure way and then the secret message containing the confidential information can be embedded in the carrier file.
- The secret message is first converted into its equivalent hexadecimal representation.
- The resulting hexadecimal values for each character are then inverted in order to increase the security. For example if letter ‘n’ is represented as 68 in hexadecimal, then it is inverted as 86. Now 86 will represent the letter ‘n’ in the secret message [14].
- The content of the resulting secret message is concealed into the hex symbol carrier file according to the chosen key symbol and pattern from the codebook shared between the sender and the receiver.
- The contents of the matrix segments used for embedding the secret message are relocated by exchanging the rows with the columns of the matrix in order to increase the complexity of the embedding process [14].
- Once the entire secret message is concealed in the hex symbol carrier file according to chosen pattern, the resultant stego file is concatenated with the key symbol (which represents the pattern of segments used in embedding process) and sent to the authorized receiver.
- The hex symbol steganography with its embedding process and extracting process is shown in Fig. 3.5.1 (ii).
- The receiver will receive the stego file containing the confidential information along with the key symbol which indicates the chosen pattern used for embedding the secret message.
- On receiving the key symbol, the receiver will now be able to recognize the arrangement of the matrix segments by referring to the secret codebook.

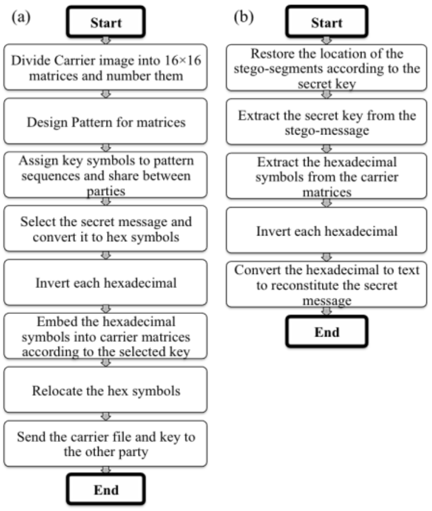
(a)
Start
Divide Carrier image into 16×16 matrices and number them
Design Pattern for matrices
Assign key symbols to pattern sequences and share between parties
Select the secret message and convert it to hex symbols
Invert each hexadecimal
Embed the hexadecimal symbols into carrier matrices according to the selected key
Relocate the hex symbols
Send the carrier file and key to the other party
End
(b)
Start
Restore the location of the stego-segments according to the secret key
Extract the secret key from the stego-message
Extract the hexadecimal symbols from the carrier matrices
Invert each hexadecimal
Convert the hexadecimal to text to reconstitute the secret message
End

Figure 7. (a) Embedding of the secret message in carrier file by the sender (b) Extracting of the secret message from stego file by the receiver [14]

- Once the receiver is able to recognize the pattern, steps of the embedding process can be executing in the reverse order so as to extract the secret message from the stego file.

V. CONCLUSION AND FUTURE WORK

The comprehensive analysis shows that among the symmetric encryption algorithms, Advanced Encryption Standard (AES) and among the steganography methods, Hex Symbol Steganography is more efficient and boosts the level of confidentiality when compared with their respective competitor.

Future contribution will focus on proposition of an approach which consists of merging cryptography and steganography into a single security system and hence enhancing the level of information security by providing high level of confidentiality while maintaining the privacy and secrecy of information stored and transmitted through insecure communication channels.

VI. REFERENCES

[1] S. Almuhammadi and A. Al-Shaaby, “A Survey on Recent Approaches Combining Cryptography and Steganography”, Computer Science & Information Technology (CS & IT), 2017.

[2] S. Mishra, P. Pandey, “A Review on Steganography Techniques Using Cryptography”, International Journal of Advance Research In

Science And Engineering, Volume 4, Special Issue (01), 2015.

[3] M. Pandey and D. Dubey, “Survey Paper: Cryptography The art of hiding Information”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 12, 2013.

[4] K. Rahmani, K. Arora and N. Pal, “A Crypto-Steganography: A Survey”, International Journal of Advanced Computer Science and Applications (IJACSA), Volume 5, No. 7, 2014.

[5] P. Joseph and S. Vishnukumar, “A Study on Steganographic Techniques”, Proceedings of Global Conference on Communication Technologies (GCCT), IEEE, 2015.

[6] http://io.acad.athabascau.ca/~grizzlie/Comp607/menu.htm

[7] M. Kumar, V. Kumar and A. Sharma,” A Survey on Various Cryptography Techniques”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, 2014.

[8] A. Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”, Cryptography and Network Security, 2017.

[9] G. Yadav and A. Majare,” A Comparative Study of Performance Analysis of Various Encryption Algorithms”, International Conference on Emanations in Modern Technology and Engineering (ICEMTE), Volume: 5 Issue: 3, 2017.

[10] D. Talukdar and L. Saikia,” A Review On Different Encryption Techniques: A Comparative Study”, International Journal of Engineering Research and General Science, Volume 3, Issue 3, 2015.

[11] S. Swathi, P. Lahari and B. Thomas,” Encryption Algorithms: A Survey”, International Journal of Advanced Research in Computer Science & Technology (IJARCST), Volume 4, Issue 2, 2016.

[12] N. Singh, ”Survey Paper on Steganography”, International Refereed Journal of Engineering and Science (IRJES), Volume 6, Issue 1, 2017.

[13] A. Rashid and M. Rahim, “Critical Analysis of Steganography “An Art of Hidden Writing””, International Journal of Security and Its Applications, Volume 10, No. 3, 2016.

[14] S. Asbeh, H. Al-Sewadi, S. Hammoudeh and A. Hammoudeh, “Hex Symbols Algorithm for Anti-Forensic Artifacts on Android Devices”, International Journal of Advanced Computer Science and Applications (IJACSA), Volume 7, No. 4, 2016.