International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 8 Ver III || Aug 2018 || PP 72-75

Collaboration of Cryptography and Steganography for Enhanced Security: A Review

Swati Nagpal[1], RituNagpal[2]
[1]*Department of Computer Science and EngineeringGuru Jambheshwar University of Science & Technology,Hisar, Haryana, India*
[2]*Department of Computer Science and Engineering Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India*
Corresponding Author: Swati Nagpal

Abstract - *Today most of the communication takes place through web and people are using internet for every day communication. Because of the large advancements in Internet Technology the indispensable need of security for protection of data from the assorted hackers also rises. Cryptography and Steganography both are widely used techniques for secured data transmission. Where Cryptography is a technique which distorts a message and Steganography hides the message/data. For Encryption of secret message we will use AES and then image will be embedded using LSB algorithm which carries our confidential data. The amalgamation of both AES and LSB algorithms will take place to grant Security with confidentiality during communication of the secret data. The main objective of the paper is to assign security levels in the secret data which needs to be converse through the cover image. From the review of literature it is found that there is need to offer confidentiality to the secret message/data by merging the Cryptographic Techniques in Steganography.*

Keywords: *Cryptography, Steganography, LSB, AES.*

Date of Submission: 09-08-2018 Date of acceptance: 23-08-2018

I. Introduction

For communication most of the people are connected through the internet and world-wide web to convey messages or any private data. While internet is an open source of communication so there is indispensable need to provide security in the data as confidentiality & security is the key issue. The two well-known and widely used techniques for security of information are Cryptography and Steganography whereby Cryptography manipulates the information by distortion of the text/data and second approachpelts the actuality of communication. Steganography is the technique that was used earlier for secret transmission of any message or data through a cover object [1]. A cover object or carrier can be an image, audio or video file through which the information or message which a sender wants to convey to a receiver by using the Steganography techniques [2].For long-distance communication it is required to provide safety and security can be done by using the Steganography technique[11]. Both of the methods will be used to provide security, but for better confidentiality and security it is required to combine the techniques of Cryptography and Steganography. Even the terms Cryptography and Steganography can be used straightforwardly but then there is a case when intruder can detect the original message so it is required to correlate both of the techniques together to achieve high-security levels for data hiding [11]. The major focus is to silt a system using additional safetystructures in which the real part of data can be distorted with the help of Cryptography and can be hidden by steganographic techniques. Steganography is a technology that conceals confidential facts. Thisterm is a combination of steganos + graphein in which *steganos* means "covered, concealed, or protected," and the word *graphein* meaning "writing" i.e. concealed writing [3].Earlier used schemes like F5,SSIS i.e. spread-spectrum image steganography, LSB were even Qualitative and quantitative to some extent but attacks are even possible on it [3]. Sometimes the term steganography is confused with cryptography in the terms of usage. But there is a way to differentiate in between both of the terms. The purpose of cryptography is to secure communication from the hackers by converting confidential message into non-understandable form that can be done by encryption of the message but in case of steganography it not only conceals the contents of the message but mere actuality of the communication from an observer is hidden so there is no chance of doubt of the existence of the message. As the cryptographic approach was used in past it is seen that if the encrypted information is sent it creates suspicion but it is not so in case of invisible information.

1.1 CRYPTOGRAPHY

Cryptography is a technique which is used to convert a plaintext into coded or non-understandable form. It is a method of converting information from its plaintext into non-understandable form.The process of protecting plain text, data or information which is to be transformed is done throughaltering it by scrambling into an illegible form known as secret message. The one who are authorized can decode the communication. Cryptography encrypts actual message that is being sent from the sender end to receiver end. Some basic terms which will be used in Cryptography are described as follows:-

Plaintext - The original form of text that is to be transferred from the sender's end.

Cipher text - It is the coded form of the plaintext that is encoded with the key.

Encryption- Encryption is a process of alteringrecords to incomprehensiblemanner.

Decryption- Inverse of encryption process is known as decryption.The keys used are public key and private key [6].

In the figure represented below can be seen that plain text is converted into the cipher text with the help of the key and the message can be decrypted in its original plain text form with the help of key. Cryptography approach will be used for distortion of the message or data so that if an attacker tries to attack or any eavesdropper listens to the message they could not predict or understand the real secret data being shared.

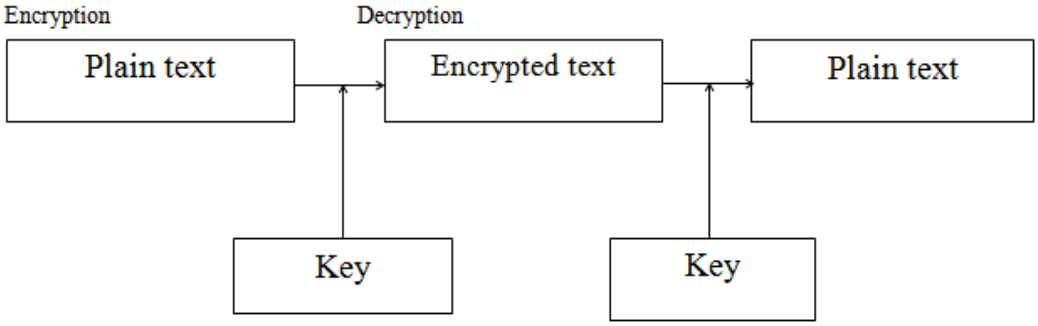

Fig 1.1 General form of cryptographic technique- Encryption and decryption

1.2 STEGANOGRAPHY

Steganography is a technique which is used to hide the existence of the message. Possible carriers which are mostly used are images, audio-visual, manuscript, or some other digital illustrativeprogram .Steganography can be done by using an audio carrier file by hiding the secret data in the echo variations[7], e.g.while a top-secretmemo is concealedinside a media, resultant creation is a stegano-image. Benefit of approach is that the attacker does not even get any idea that the message is being transferred. For example, the picture of an animal or a baby could conceal the plans for our company's latest and confidential technical innovation. The important aspects affecting steganography and its usefulness are Capacity and security [11].

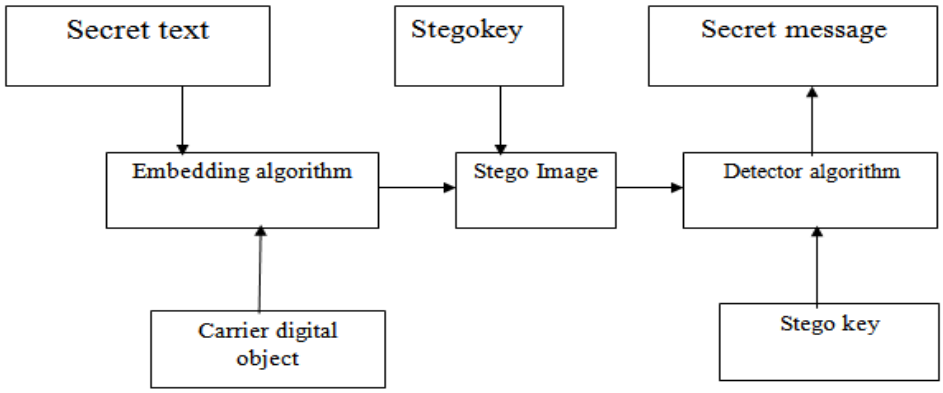

Fig 1.2 Steganography model

STEGANOGRAPHY IN IMAGE

The steganography can be applied on image, audio or on a video file but we will focus on the image file. Todaydigital pictures are used widely as a cover objects. As different file formats are available for

severalpresentations andfor that different kind of algorithms are used consequently. As we know that an image is a collection of bits (which is known as pixel for image) holdingdiversebright intensity in different extents of picture. 24-bit images offer much more flexibility and hugeextent of files can be encoded in place of lesser bit images [1]. But there is a problem with 24-bit pictures i.e. size is quitehuge which makes it doubtful too. Different algorithms are used according to the type of message &image e.g. least significant bit(LSB) and most significant bit (MSB). If we insert some changes in least significant bits then human eyes are not able to detect them easily.

1.3. STEGANOGRAPHY AND CRYPTOGRAPHY

1.3.1Comparison of Steganography and Cryptography

CRYPTOGRAPHY	STEGANOGRAPHY
The message which is to be passed is known.	The message which is to be passed is not known.
Unauthorized party cannot easily discover the actual content of the information because of the encryption.	It prevents the discovery of existence of any communication.
Common technology is being used from past.	Steganography is a little known technology as compared to cryptography.
Structure of the confidential data is altered.	It only hides the confidential data and no alteration is there.
As soon as the intruder is able to recite the real data the system is cracked.	If attacker came to know that data is hidden behind any cover media and he breaks it then he can see the embedded information.

1.3.2 Benefits of collaboration ofSteganography and Cryptography

Steganography is not the same as Cryptography. In cryptography encryption is done in which the plaintext message is encrypted that transforms text into a non–understandable form but in steganography the message is hidden [13]. We can combine both of the methods to produce better protection for the message.

In case if Steganography approach fails& the attacker gets to know the data then even our security does not fail because encryption has been done prior to it. This combination gratifies the necessitiesof capability, confidence&sturdiness for a protectedinformationcommunicationdone on an open network. Earlier works anticipated that cryptography has its own key generation algorithm and even similarstrategies are used for encryption and decryptionprocess [6].The combination can be possible by collaborating LSBtoinsert top-secretrecords in last bit of blue pixel &restricted green works of unplanned pixel localities in edge of image. LSB approach is even applied on the file by taking the most significant bits sometimes RGB modules of arbitrarilydesignated pixelthrough smooth extents. By integrating it withAdvanced Encryption Standard it can be robust [10].

Steganography by using LSB:-

It is a technique in which the last bit of some or all pixels inside an image getsexchanged with the bit of top-secretdispatch. In this technique we use the last bit to hide and transfer the data because least significant bit is the least important bit. If we change the values of last bit then there is no huge change seen in the image and the human eye cannot distinguish between the two images that is original image and the image with hidden text or data in it so least significant bit method is used. The encrypted image data is hidden with the LSB algorithm which offers high security level [14]. By comparing the different Steganography techniques like Transform domain, SpreadSpectrum, LSB and various other techniques on the basis of Imperceptibility, Robustness, Payload Capacity it is observed that LSB is better as compared to other techniques [5]. LSB array based algorithm can be used with the Cryptographic technique like RSA to provide two level security one with Steganography and other level with Cryptography and even if it offers high capacity still attacks are possible on it [9]. According to the length of the data edges 1-2-4 bit substitution can be applied with the Least Significant Bit method which results in indefinite reduced frequent pixels [12]. One can apply steganography by using twin image and the secret information which need to be sent through the image should be converted into the binary form & the results got after the processing are with better MSE and PSNR[8].

Blend of AES&LSB algorithm**:**

Advanced Encryption Standard'sdata is arithmeticallyeffective& haswell-designed procedure as compared to DES(Data Encryption Standard) and it'skeyforte reposes in the selection of varying key sizes of 128, 192 / 256-bit keys, which makes it tougherif compared witha 56-bit key of algorithm DES. A lot of cryptographic symmetric & asymmetric algorithms can be used. AES is analytically stronger than DES. RSA

and Diffie-Hellman algorithms can also be used. Even the combination of the compression, Cryptography &Steganography can be done by using 3 keys with high authentication ,and with good image quality[3] . In terms of structure AES uses permutation - substitution to produce the converted block. The creative DES inventorsinventedinordinatesupport to informationsafety, but somehow all were down to zero because of the combined superiority of AES algorithm over others. As Brute Force Attack possible on DES. So, AES is preferred here.

Comparison of DES and AES algorithm

		AES
Block Size	Block size is of 64 bits.	In AES it is of 128 bits.
Key Length	There is a single option of 56 bit key length.	In AES there are many variants like 128, 192, or 256 bits.
Cipher Type	Symmetric block cipher	In AES also symmetric block cipher is used.
Security	Proven inadequate and not secure.	Measured secure.

II. Conclusion

From the study of various papers & earlier done works it is concluded that LSB is the widely used technique because its insertion is secure in Steganography and it is a lossless algorithm & with AES the encryption process will be done to provide confidentiality.In this paper, the collaboration of Cryptography has been done with the Steganography by merging the LSB technique with the AES algorithm in which firstly the message will be encrypted with AES algorithm and then the image is used as a cover object and the data will be hidden in the image, so that the eavesdropper if get a chance to go through the hidden details then even because of the encryption the message is secured.

References

[1]. SujayNarayana and Gaurav Prasad, "Two New Approaches for Secured Image Steganography using Cryptographic Techniques and Type Conversions", SuSignal& Image Processing : An International Journal (SIPIJ), Volume1, No.2, December 2010.

[2]. Arvind Kumar, Km. Pooja, "Steganography-A Data Hiding Technique", International Journal of Computer Applications, Volume 9 No.7, November 2010.

[3]. EpuruMadhavarao, ChikkalaJayaRaju, PedasanagantiDivya, A.S.K.Ratnam, "Data Security using Cryptography and Steganography", International Journal of Advanced Research in Computer Engineering & Technology, Volume 1, Issue 5, July 2012.

[4]. SeptimiuFabian Mare, MirceaVladutiu and Lucian Prodan, "Secret data communication system using Steganography, AES and RSA",IEEE17th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2011.

[5]. Sarita Nain, Sunil Kumar, "Steganography and Its Various Techniques", International journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463, Volume 3, Issue 6, pp.(241-245), June-2014.

[6]. DarshanaPatil, Prof. P. M. Chawan, "A Secure Data Communication System Using Enhanced Cryptography and Steganography", International Journal Innovative Research in Computer and Communication Engineering (An ISO 3297:2007 Certified Organization), Volume 5, Issue 6, June 2017.

[7]. SurekhaShrivastava, Mr.Gajendra Singh Chandel, Mr.KailashPatidar, "A Modified Approach Audio Steganography Based on Technique LSB Coding", International Journal of Engineering and Applied Sciences(IJEAS) ISSN:2394-3661, Volume 2,Issue 5, May 2015.

[8]. GiridharMaji, SharmisthaMandal, SoumyaSen, Narayan C. Debnath," Dual Image based LSB Steganography", IEEE 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom) ,2018 .

[9]. Gandharba Swain and Saroj Kumar Lenka," LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits", Springer-Verlag Berlin Heidelberg, pp. 479–488, 2012.

[10]. MamtaJuneja and Parvinder Singh Sandhu," A New Approach for Information security using an Improved Steganography Technique", Journal of Information Processing Systems, Volume 9, No 3, pp. 405-424, 2013.

[11]. Nagham Hamid, AbidYahya, R. Badlishah Ahmad &OsamahM. Al-Qershi, "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume 6, Issue 3, 2012.

[12]. SuchiGoyal, ManojRamaiya, DeepikaDubey,"Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images", IEEE International Conference on Computational Intelligence and Communication Networks, 2015.

[13]. A.Joseph Raphael &Dr. V. Sundaram," Cryptography and Steganography- A Survey", International Journal of Computer Technology and Applications, Volume 2, pp. 626-630,2014.

[14]. Mohammad Ali BaniYounesandAmanJantan , "A New Steganography approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, Volume 8 No.6, June 2008.

Swati Nagpal"Collaboration of Cryptography and Steganography for Enhanced Security: A Review." International Journal of Engineering Science Invention(IJESI), vol. 7, no. 8, 2018, pp. 72-75