International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Steganography with Cryptography Technique For Data Hiding

Geeta D. Rote[1], Dr. A. M. Patil[2]

[1]Second Year M.E. E/Tc Student, J.T.M College of Engineering, Faizpur, India

[2]HOD of Electronics and Telecommunication, J.T.M College of Engineering, Faizpur, India

Abstract: ***Now a day's sharing the information over internet is becoming a critical issue due to security problems. Hence more techniques are needed to protect the shared data in an unsecured channel. In steganography nothing but the concealed communication which is prefers for secure our data from unauthorized person. In this technique secret information can be replaced or conceal behind the cover information unsuspicious. Cryptography is the technique, where secret information is replaced in unreadable format. The present work is focus on combination of cryptography and steganography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encrypted algorithm in cryptography. Secondly the encrypted data must be hidden in an image or video or an audio file with help of steganographic algorithm. Thirdly by using decryption technique the receiver can view the original data from the hidden image or video or audio file. Transmitting data or document can be done through these ways will be secured. In this paper we implemented three encrypt techniques like RSA algorithm along with steganographic algorithm like LSB substitution technique.***

Keywords: Steganography, Cryptography, Least Significant Bit substitution method, RSA algorithm

1. Introduction

Stenography is the ability of passing information through original files in which existence of message is unknown. It is arrived from Greek word meaning "covered writing"[1]. After conceal data resultant is stego object. Stego key is shared by transmitter and receiver both users for security purpose. Without stego key external user cannot detect or access or recover secret data. Stenography refers as a information or file that has been concealed inside a picture, video or audio file [2]. It is quite similar technique as a cryptography as per appearance and convention [3].

Cryptography is an effective way for protecting sensitive information it is a method for storing and transmitting data in form that only those it is intended for read and process. Cryptography is the technique where original data is converted into meaningless content. It is arrived from Greek word "secret writing". [4]

2. Literature Survey

Difference between steganography and cryptography depends on their objectives. Cryptography process focus on secure the content of secrete message. And steganography process focuses on existence of message secret. For this reason we cannot say which one is more advantageous. If we combine these two methods, we can implement more secure system.

A. **Existing Techniques Used**

2.1 Cryptography

Cryptography is the secret communication technique for data secure from third party. It is used to secure military information as well as sensitive communication with protect national security. Its play important role in secure our information of technology purpose. It consist lots of field like e-mails, e-banking, e-commerce etc, where personal information shared over insecure channel. So cryptography is playing vital role for securing our data by convert original information in unreadable format with secure key [5]. Cryptography techniques are used for data secure from intruder or from unauthorized person, where confidentiality is important as configure by figure 1.

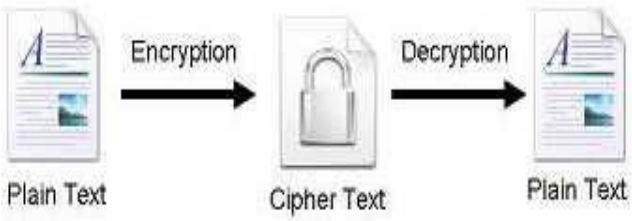

Figure 1: Encryption – Decryption flow of cryptography

a. Concept used in Cryptography [6]

1. **Plain Text**: It is the information present in its original format.
2 **Cipher Text**: When convert plain text to non- readable format it termed as ciphertext.
3. **Encryption**: Transformation from plain text to cipher text is referred as encryption. Encryption algorithm and a key are important in encryption.
4. **Decryption**: Transform cipher text to plain text is termed as decryption. This may also need two requirements Decryption algorithm and key. Figure 1 shows the simple flow of commonly used encryption algorithms.
5. **Key**: Combination of numeric or alpha numeric text or special symbol is referred as key. This is increase security of hide data.

There are two types of encryption methods in cryptography as follows:
1. Symmetric Encryption
2. Asymmetric Encryption.

In symmetric Encryption one key is shared between transmitter and receiver. For convert plaintext into cipher text at sender or transmitter used to improve security level to protect the secure information use one key that same key is used at receiver side to convert cipher text to plaintext. In asymmetric encryption system was developed by Diffie and Helman in 1976 it's also called as Public Key Cryptography. It's the process where converts plaintext to cipher text at the sender with different key will be used to retrieve our secure data from cipher text to plaintext. Public key is used at sender for encryption and at receiver side used different key for decryption process [7].

2.1.1 RSA Algorithm For Cryptography:

As per [8] in 1978, Ron Rivest, Adi Shamir, and Leonard Adleman implemented a cryptographic algorithm, Rivest, Shamir, and Adelman were assistant professors at MIT at the time, Rivest in computer science, Shamir and Adelman in mathematics. RSA is the public key cryptosystem. This is useful for security in electronic mails as well as electronic transmission and transactions for example fund transfer.

There are some advantages of RSA Algorithm: [9, 10].

1. Primary advantage of Public key Cryptography is increased security and convinces.
2. Second, it provides digital signature that can't be repudiated. For example, Kerberos secret-key authentication system involves central database that keeps copies of secret key.
3. Public key authentication prevents the type of rejection and each user has its own responsibility for protecting his private key.
4. We can select large prime numbers for enhancement of security of keys.
5. Public key cryptography may be used with secret key cryptography.
6. Public key cryptography need not to share private keys but in secret key cryptography same key is used at sender as well as receiver, it should transmitted over unsecure channel.

However the RSA Algorithm having some disadvantages also, which are given below: [11]

1. The main demerit of Public key cryptography is its speed during encryption of its given plaintext. In modern cryptosystem there are several secret key encryption algorithm that having faster speed in comparison to public key encryption methods.

2.2 Steganography

In data hiding, three famous techniques are there: Watermarking, Cryptography and Steganography [12]. In steganography we can hide information like text, image, audio and video. In steganography technique for hiding information can be used many formats such as .bmp, .doc, .gif, .jpeg, .mp3, .txt .au and .wav. Information concealing is not capable in text as well as audio as compare to images [13].

2.2.1 Concept Of LSB Steganography

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message [14]. Digital images are mainly of two types:

(i) 24 bit images
(ii) 8 bit images.

In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below-

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0
S(i.j) = C(i,j), if LSB(C(i,j)) = m
S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

Where,
LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded. S(i,j) is the stego image [15].

As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.

For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:

(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.

(11101010 1110100**1** 1100101**0**)
(01100110 1100101**1** 11101000)
(11001001 0010010**0** 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency [16].

Consider 8 bit grayscale images, each byte of cover grayscale image can store 1 bit of secret message. For example, first eight bits of cover grayscale image and if we want to hide character C whose binary value is 10000011, just replace Least Significant Bits of these pixels will be as follows:

11101010	→	11101011
11101000	→	11101000
11001011	→	11001010
01100110	→	01100110
11001010	→	11001010
11101000	→	11101000
11001001	→	11001001
00100101	→	00100101

Very small amount of data is changed after replacing cover image bits with secret data bits. As per [17] if we compare modified data or embedded data with previous cover data, very less amount of data is changed. Embedded image is too much similar with the original cover image. Because of that it cannot easily predict to the Human Vision System (HVS).

3. Proposed Work

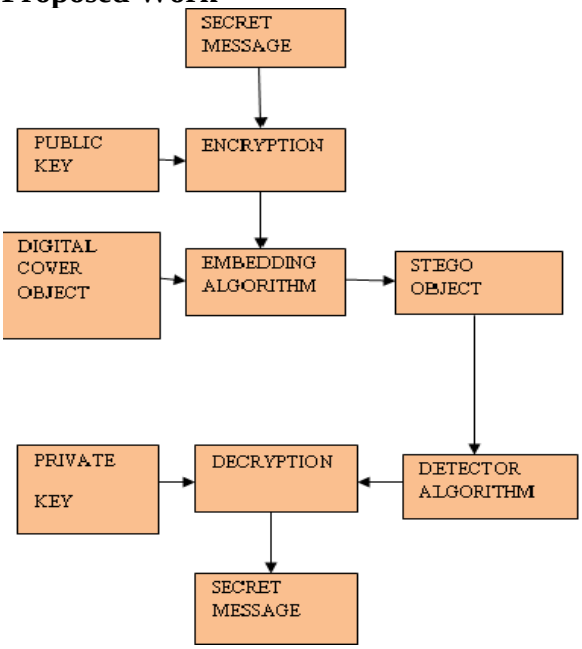

Figure 2: Model of Steganographic Method with Cryptography

A. Text Message Hiding Behind Cover Image

I. Select Image

In this step we can select image as a cover mage. This image is used to hide the secure information. That image may be in 24 bit images or 8 bit images.

II. Enter Secret Message

In this step we can enter the secret message which will hide behind the selected image.

III. Encryption With RSA

In Encryption process entered text or plaintext covert into ciphertext. In this step we have used the RSA algorithm. This is the asymmetric or public key algorithm. At the time of encryption, data is send along with the public key.

IV. LSB Encryption

In this step encrypted text message is converted into binary equivalent. And these bits are replaced with Least Significant bits of cover image to hide secret message.
The embedding procedure is as follows:

Input: Cover Image, Secret message
Output: Stego Image
PROCEDURE:
Step 1: Extract pixels of cover message.
Step 2: Extract the characters of the text file. Convert that ASCII characters into binary string.
Step 3: Insert characters of text file in each least significant bits of cover pixels by replacing it.
Step 4: Repeat step 3 till all the characters has been embedded.

Step 5: Obtained stego image

V. LSB Retrieval

In LSB retrieval embedded data is extract. Here encrypted text message is extracted from Least significant Bits of cover image. The extraction process is as follows:
Inputs: Stego-image file.
Output: Secret text message.
Procedure:
Step 1: Extract the pixels of the stego image.
Step 2: Extract secret message characters from least significant bit component of cover message. Follow Step 2 till up to terminating
Step 3: Extract secret message.

VI. Recover Message

This is the final step and here we get our original secret message or the data which is hidden behind the cover image. For recover the message decryption process is used. At the time of decryption it use private key. At this step we can convert ciphertext message into plaintext or original message.

B. Message Image Is Hiding Behind Cover Image

1. Select one of the cover Image BMP, GIF, PNG, TIFF or JPEG.
2. Read Cover Image.
3. Enter message image.
4. Shift message image bits by n-8.
5. And operation perform between cover image with bitwise complement of cover image by 2^n-1
6. The bitor operation performs between shifted message image and result of step 5. This make changes only in cover image LSB bits, so image is hidden in the cover image.
7. At the time of retrieval this stego image shift by 8-n.
8. Bitand operation perform between 255 i.e. 11111111 which extract message image. It is Anded with 255 because initially all LSB's were made 0. Now it is recover back.

4. Results and Discussions

In LSB steganography text message can hide behind cover image. Here image is boy.bmp with 300 X 300 dimensions with 24 bit depth. When message is hiding behind the cover image is formed stego image. As shown in following Table 3.

Table 3: Text message hide in cover image by using LSB steganography

METHOD	COVER IMAGE	MESSAGE HIDE	STEGO IMAGE
LSB STEGANOGRAPHY		HAVE A NICE DAY!	
	IMAGE: Boy1.bmp SIZE: 264 KB DIMENSIONS: 300 X 300 BIT DEPTH: 24 Bit	CHARACTER: 16	IMAGE: msgimage.bmp SIZE: 264 KB DIMENSION:300 X 300 BIT DEPTH: 24 Bit

But for more security we can embed steganography with cryptography. So Based on proposed algorithm, for text message is hiding in cover image by using LSB steganography with RSA cryptography**.** Here text message is 'HAVE A NICE DAY!' is hiding behind the Least significant bits of cover image Boy1.bmp. It is shown in following Table 4. Here text message is hiding in encrypted form which is non-readable format with public key cryptography, so it is more secured.

Table 4: Text message hide in cover image by using LSB steganography with RSA algorithm

METHOD	COVER IMAGE	MESSAGE HIDE	STEGO IMAGE
LSB STEGANOGRAPHY + RSA CRYPTOGRAPHY		HAVE A NICE DAY!	
	IMAGE: Boy1.bmp SIZE: 264 KB DIMENSIONS: 300 X 300 BIT DEPTH: 24 Bit	CHARACTER: 16	IMAGE: msgimage.bmp SIZE: 264 KB DIMENSION:300 X 300 BIT DEPTH: 24 Bit

- ASCII equivalent of message

  72 65 86 69 32 65 32 78

  73 67 69 32 68 65 89 33
- The encrypted message is

  410 958 1497 37
  0 958 0 1267
  4 1182 37 0
  36 958 316 1
- The recovered encrypted message from image is

  410 958 1497 37
  0 958 0 1267
  4 1182 37 0
  36 958 316 1

The decrypted message is: HAVE A NICE DAY!
Above result shows (1) ASCII equivalent of character string (HAVE A NICE DAY!) (2) The encrypted secret message. (3) Recovered encrypted message from Boy1.bmp image or from stego image. (4) Decrypted secret message.

Combination of cryptography and steganography replaces the cover image data by secret message so after data hiding the size of images remain same as well as it is not differing stego image from cover image .

B. Message Image is Hiding Behind Cover Image

Here secret data is store in the form of Image and cover data is also Image. Those images are PNG (Portable Network Graphics), TIFF (Tagged Image File Format), JPEG (Joint Photographic Experts Group), BMP (Windows Bitmap) formats.

Evaluation of image quality

➢ **PSNR And MSE**

The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a reconstructed image. If PSNR is higher, reconstructed image quality is better.

The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. If value of MSE is lower, lower the error.

To compute the PSNR, first calculates the mean-squared error using the following equation:

$$MSE=\frac{\sum_{M,N}[I1(m,n)-I2(m,n)]^2}{M*N} \quad \text{-------- (1)}$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR= 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad \text{---------- (2)}$$

I. Results for PNG images

Table 5(I): Message image hide in cover image by using LSB steganography in PNG Images

Cover image	Message image
	
IMAGE: peppers.png SIZE: 716 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit	IMAGE: lena.png SIZE: 501 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit

Table 5(II): Results for Message image hide in cover image by using LSB steganography in PNG format

Number of bit hiding	Stego image	Extracted Image	PSNR	MSE
1			15.8043	6.8882e +03
2			23.3978	1.1988e +03
3			29.0312	327.6553
4			35.1573	79.9489

In PNG images suspicion might not arise if it is transmitted with LSB steganography. In PNG images can be store large amount of information. As shown in table 5(II) bits of cover image replaced with bits of message image and result shows the effect on stego image as well as extracted images. When data replace with one bit small amount of data is hiding but if hiding 2 or 3 bits replacing quite good information can be embed.

II. Results for GIF Images

Table 6(I): Message image hide in cover image by using LSB steganography in GIF Images

Cover image	Message image
	
IMAGE: cameraman.gif SIZE: 168 KB DIMENSIONS: 512 X 512 BIT DEPTH: 8 Bit	IMAGE: barbara.gif SIZE: 123 KB DIMENSIONS: 512 X 512 BIT DEPTH: 8 Bit

Table 6 (I) represents cover image and secret message image and Table 6(II) represents stego image and extracted images for 1 bit, 2 bits, 3 bits or 4 bits replaced of cover image by message image. Gray scale images have a 8 bit depth. Gray scale GIF image, there are 256 shades of gray. This results in gradual changes in the colors and it is hard to detect.

After replacing LSB in GIF images has the possibility of hiding a large message, but only when the most suitable cover image has been chosen. GIF images are indexed images where the colors used in the image are stored in a palette. Each pixel is represented as a single byte and the pixel data is an index to the color palette. If the LSB of a GIF image is changed using the palette approach, it may result in a completely different color. This is because the index to the color palette is changed. The change in the resulting image is noticeable if the adjacent palette entries are not similar but the change is not noticeable if the adjacent palette entries are similar.

Table 6(II): Results for Message image hide in cover image by using LSB steganography in GIF format.

Number of bit hiding	Stego Image	Extracted Image	PSNR	MSE
1			16.9890	5.2437e+03
2			22.8662	1.3549e+03
3			28.9646	332.7217
4			35.2366	78.5024

III. Results for JPEG images

Table7 (I): Message image hide in cover image by using LSB steganography in JPEG Images

Cover image	Message image
	
IMAGE: flower.jpg SIZE: 61 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit	IMAGE: Image (1).jpg SIZE: 61 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit

Table 7(II): Results for Message image hide in cover image by using LSB steganography in JPEG format

Number of bit hiding	Stego image	Extracted Image	PSNR	MSE
1			16.9975	5.2335e +03
2			23.5107	1.1681e +03
3			28.9672	332.5199
4			35.1956	79.2465

IV. Results for BMP images

Table 8(I): Message image hide in cover image by using LSB steganography in BMP Images

Cover image	Message image
	
IMAGE: boy.bmp SIZE: 769 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit	IMAGE: airplane.bmp SIZE: 769 KB DIMENSIONS: 512 X 512 BIT DEPTH: 24 Bit

As Table 8 (I) represents cover image and messag image of BMP images and Table 8 (II) represents stego image and extracted images results for different number of bits are embedded. When images used as carrier for data hiding in steganography it is generally manipulated by changing one or more bits of byte or bytes of image which forms pixels of image. Same as in BMP Images can store good amount of information.

Table 8(II): Results for Message image hide in cover image by using LSB steganography in BMP images

Number of bit hiding	Stego image	Extracted Image	PSNR	MSE
1			16.6419	5.6800e+03
2			24.5389	921.8244
3			29.1719	317.2089
4			35.2933	77.4834

Here Least Significant bits of cover image are replacing with message image. As shown from above figures 1 bit, 2 bits, 3 bits or 4 bits of cover image LSB's replace with message image. If compare till 3 bit of data can hide in image without any suspicion. From four bits onwards stego image disturb its quality and intruder can easily observe that changes. For 1 bit data hiding fewer amounts of data can hide. For BMP, PNG invisibility is higher as well as large amount of data can hide.

5. Conclusion

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.

As presented, LSB Embedding has the advantage that it is simple to implement. This is especially true in the 24-bit bitmap case. It also allows for a relatively high payload, carrying one or many bits of the secret message per byte of pixel data. In addition, it is also seemingly undetectable by the average human if done right. However, the assumption has been that the stego-image is indistinguishable from the original cover image by the human eye. When hide secrete image in cover image by replacing one bit LSB very small changes are occurred there but when we hide $n \geq 4$ cover image quality is disturbed, here intruder can detect hidden message. By combining Steganography and Cryptography one can achieve better security.

References

[1] Vijay Kumar Sharma ,Vishal Shrivastava "A Steganography Algorithm for Hiding Image in Image By Improved LSB Substitution By Minimize Detection", Journal of Theoretical and Applied Information Technology, Volume (36), No. (1), 2012
[2] Li Zlii, Sui Ai Fen Yang Yi Xian "A LSB Steganography Detection Algorithm", The 14th IEEE 2003 International Symposium on Persona1,Indoor and Mobile Radio Communication Proceedings, PP. 2780-2783, 2003
[3] Prof. Samir Kumar Bandyopadhyay, Sarthak Parui "A Method for Public Key Method of Steganography", International Journal of Computer Applications Volume (6), No. (3), PP 7-10, 2010
[4] Ahmed Al-Vahed , Haddad Sahhavi "An overview of modern cryptography" World Applied Programming, Volume (1), No. (1), PP. 55-61, 2011.
[5] Shivangi Goyal "A Survey on the Applications of Cryptography", International Journal of Science and Technology Volume (1), No. (3), PP. 137-140, 2012
[6] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", International Journal of Science and Research (IJSR), PP.170-174, 2013
[7] Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, "Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Computer Science and Security (IJCSS), Volume (5), Issue (3) PP. 298-309, 2011
[8] Shai Simonson, "Public Key Cryptography", 1995
[9] Evgeny Milanov " The RSA Algorithm", PP. 1-11, 2009

[10] Samoud Ali, Cherif Adnen. "RSA Algorithm Implementation For Ciphering Medical Imaging", International Journal Of Computer And Electronics Research Volume (1), Issue (2), PP.44-49, 2012
[11] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh, "Comparative Analysis Of Cryptographic Algorithms", International Journal Of Advanced Engineering Technology, PP.16-18, 2013
[12] Rosziati Ibrahim and Toeh Suk Kuan, "Steganography Algorithm to hide Secret Message inside an Image", Computer Technology and Application PP. 102-108, 2011
[13] Bret Dunbar, "A detailed look at Steganographic techniques and their use in an open systems environment", SANS institute 2002.
[14] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar " Image steganography using least significant bit with cryptography", Journal Of Global Research In Computer Science, Volume (3), No. (3), 2012
[15] Tao Zhang, Yan Zhang, Xijian Ping, Mingwu Song, "Detection Of LSB Steganography Based On Image Smoothness" ICME**,** PP- 1377-1380, 2006
[16] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats, Int. J. Advanced Netwo,rking and Applications", Volume (2), Issue (5), PP. 868-872, 2011
[17] Stuti Goel, Arun Rana, Manpreet Kaur "Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems www.ijcdsonline.com Volume (3), Issue (I), PP.20-30, 2013