*ISSN (e): 2250 – 3005 || Volume, 07 || Issue, 10|| October – 2017 ||*
*International Journal of Computational Engineering Research (IJCER)*

# An Enhanced Steganography Method For Digital Images

Sandeep Kaur, Dr.Akshay Girdhar
*Guru Nanak Dev Engg.College Ludhiana*
*Guru Nanak Dev Engg.College Ludhiana*
*Corresponding Author: Sandeep Kaur*

## ABSTRACT

Steganography is derived from the Greek word steganographic which means covered writing. Steganography is defined as the study of imperceptible communication. Steganography abstractly implies that the message to be transmitted is not visible to the eye. The main objective of steganography is essentially concerned with the protection of hidden information. Security of confidential information has always been the intent theme for researchers to send data without revealing it to anyone other than the receiver. In the proposed work, a superior technique of image steganography i.e. LSB (Least Significant Bit) with RSA and DCT (Discrete Cosine Transform) with RSA algorithm has been implemented. There are different types of steganography techniques along with their strengths and weakness. A DCT transformation technique is used to convert the cover image from spatial to frequency domain. A public key cryptography is combined with steganography to provide more security. A public key encryption algorithm was developed by three scientists Ronald Rivest, Adi Shamir and Leonard Adleman. This algorithm uses public key cryptography; it uses two keys private key and public key. In this thesis work, experiments have been performed on greyscale images to evaluate quantitative and qualitative effect of DCT and LSB+1 with RSA algorithm. Each data set contains colored and greyscale images. The DCT and LSB+1 with RSA algorithm have better quality than existing algorithms. The main intent of thesis is to study and implement the operations used in steganography scheme to enhance data security. The quality of image has been analyzed using the quality metrics such as PSNR (Peak Signal Noise Ratio), and NC (Normalized Correlation).

**Keywords**: Steganography, Image Steganography, cryptography, and stego image

---------------------------------------------------------------------------------------------------------------------------------------

Date of Submission: 10-10-2017 Date of acceptance: 27-10-2017

---------------------------------------------------------------------------------------------------------------------------------------

## I. INTRODUCTION

Steganography is an art and science of invisible communication. This is accomplished by hiding information in another data. The word steganography has been derived from two Greek words “stegos” means “cover” and “grafia” means “writing” defining it as “covered writing” [1]. Steganography protects information from unauthorized access. The key concept behind steganography is that the message to be transmitted is not detectable to the naked eye. Fig 1 shows the information hidden inside an image.Each steganographic communication system consists of an embedded and an extracting algorithm. To accommodate a secret message, the original image also called the cover-image, is slightly modified by the embedding algorithm. As a result, the stego-image is obtained. With the recent advances in Internet computing and its intrusion in our day to day life, the need for private and personal communication has been increased. For this purpose, existing technologies like cryptography offer a solution by scrambling the confidential information so that it can’t be read by anyone else except the intended recipient. However, the cryptographic data lacks the required logical sense and can be easily recognized, to overcome this issue, the encryption key is used. Such an illegible data can attract undue attention from eavesdropper, which is a threat for private and confidential communication. Thus privacy and confidentiality is being lost by the nature of cryptographic solutions. For more privacy and confidentiality in communication, information hiding techniques like steganography has shown some promising solutions to address above security issue. Steganographic communication is not an easy task to trace, this makes the hacker’s job much difficult, rather than just encrypted communication they have to track from all network communication channels [2]. This steganographic feature increases the level of privacy and security by making the confidential communication invisible.

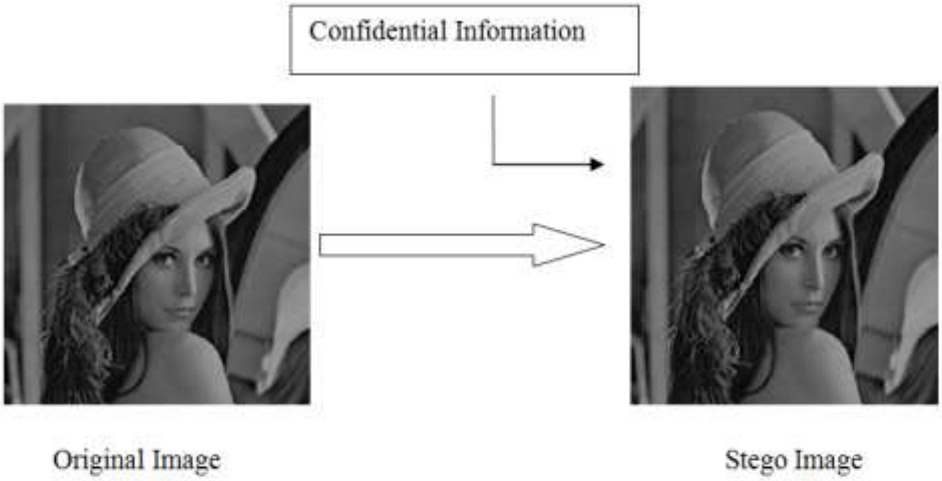

**Fig.1: Steganography of an image**

## II. CLASSIFICATION OF STEGANOGRAPHY

Steganographic systems use multimedia objects like image, audio, video etc., as the cover media, because people often transmit digital pictures over email and other Internet communication. Images are the mainly accepted wrap items used for steganography. In the field of digital media (image), a lot of dissimilar image file extensions exist, the majority of them has been used for particular application. For these different image file formats, different steganographic algorithms exist.

### 2.1 IMAGE STEGANOGRAPHY

An image is a 2-D signal defined by the mathematical function *f (x, y)* where *x* and *y* are two co-ordinates horizontally and vertically and *f* is called the intensity of the image at that level. Digital image is composed of finite number of elements called pixels. Each of which has particular location and value. Image can be described in terms of vector graphics or raster graphics. An image started in raster form is sometimes called a bitmap. Colored and grayscale images use 8 bits for every pixel and are proficient to show 256 dissimilar colors or shades of grey. Digital color images are usually stored in 24-bit files and use the RGB color model, also called real color. All color deviations for the pixels of a 24-bit image is the result of three primary colors: red, green and blue, and every primary color is equal to 8 bits. Hence in a single pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors in certain pixels, [6]. The common techniques are: -

- Least significant bit insertion
- Masking and filtering
- Redundant pattern encoding
- Encrypt and scatter
- Algorithms and transformations

Each of these methods can be useful, with varying degrees of achievement.

### 2.2 AUDIO STEGANOGRAPHY

When secret data is embedded into digital sound, this technique is known as audio steganography. This method embeds the secret message in WAV, AU and MP3 sound files. Enclosing secret data in digital sound is frequently an additional complex procedure than inserting text in different media, such as digital images. To conceal the text profitably, different methods for data in digital audio have been defined [7]. These methods range from simple algorithms that insert information in the form of signal noise to more powerful methods that develop sophisticated signal processing techniques to hide information. The lists of techniques that are usually used for audio steganography are discussed below.

- Least significant bit coding
- Phase coding
- Spread spectrum
- Echo hiding

### 2.3 TEXT STEGANOGRAPHY

A secret message or data will be concealed into an input image by applying an embedding algorithm to produce an output or stego text. Then stego text will be transmitted. Fig.2shows to embed and receive text using algorithms.

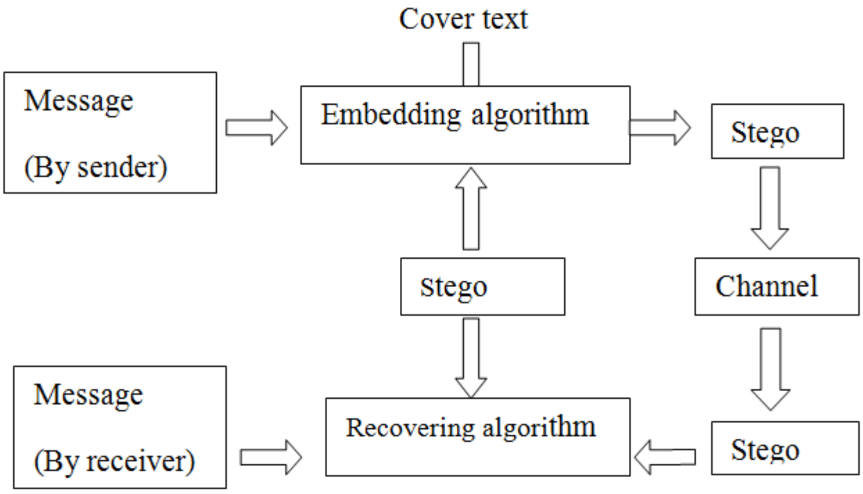

**Fig. 2: Text steganography process**

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word in a sentence. Hiding a data in the simple content can be done in several dis-similar methods which involve the alteration of a manuscript, policy such as nth character or the changing the quantity of white space subsequent to lines or among the terminology [8].Another possible way of storing a secret message inside a text is using publicly available cover source, a book or a newspaper.

| For example | Text | **g**uru **n**anak **d**ev **c**ollege |
|---|---|---|
| | Message | gndc |
| | Output | gndc |

### 2.4. VIDEO STEGANOGRAPHY

Video files are generally a collection of images and sounds, so most of the obtainable techniques on images and audio can be implemented to video files too. The most important advantages of video steganography are the large amount of information that can be embedded inside the images and sounds at receiver to transfer receiver side.

## III. DIFFERNCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. Cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something. In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. Steganography and cryptography differences are briefly summarized following in Table I.

**Table I. Difference between Cryptography and Steganography**

| CRYPTOGRAPHY | STEGANOGRAPHY |
|---|---|
| Known message passing | Unknown message passing |
| Common technology | Little known technology |
| Technology still being developed for certain Formats | Most of algorithm known by all |
| Cryptography alter the structure of the secret message. | Steganography does not alter the structure of the secret message |

## IV. METHODS OF STEGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes”. It is the art of discovering and rendering useless covert messages [9]. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information, unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message.

### 4.1 VISUAL DETECTION

Most steganographic programs embed message bits either sequentially or in some pseudo-random fashion. In most programs, the message bits are chosen non-adaptively independently of the image content. If the image contains connected areas of uniform color or areas with the color saturated at either 0 or 255, we can look for suspicious artefacts using simple visual inspection after pre-processing the stego-image. Even though the artefacts cannot be readily seen, we can plot one bit-plane (for example, the LSB plane) and inspect just the bit-plane itself [10].This attack is especially applicable to palette images for LSB embedding in indices to the palette.

### 4.2 STATISTICAL DETECTION

Statistical attack that can be applied to any steganographic technique in which a fixed set of Pairs of Values (PoVs) are flipped into each other to embed message bits[11]. These methods use first or higher order statistics of the image to reveal tiny alterations in the statistical behaviour caused by steganographic embedding and hence can successfully detect even small amounts of embedding with very high accuracy.

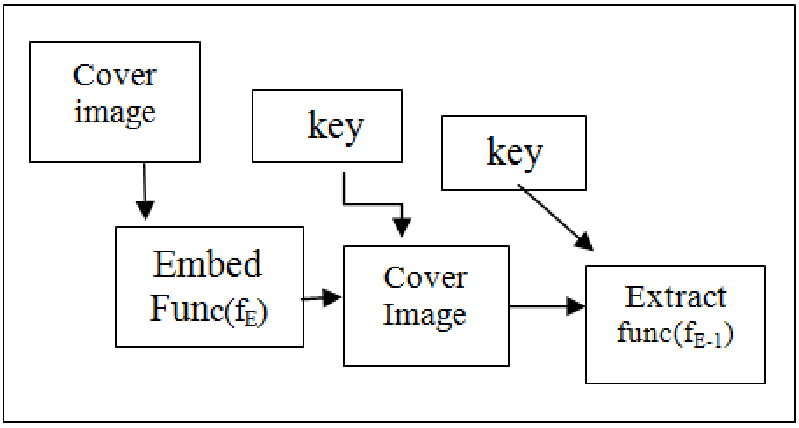

**Fig-3: Process of Steganalysis**

## V. RSA ALGORITHM

Encryption using RSA, to encode the information that is concealed in an image. Hackers cannot identify hidden data in images easily and at most they can get encrypted data from images which will not reveal any confidential information. Care should be taken during the selection of prime numbers, so that hacker will not able to reveal key to decrypt. Fig 4: demonstrates Encryption process and Fig 5: Demonstrates decryption process.

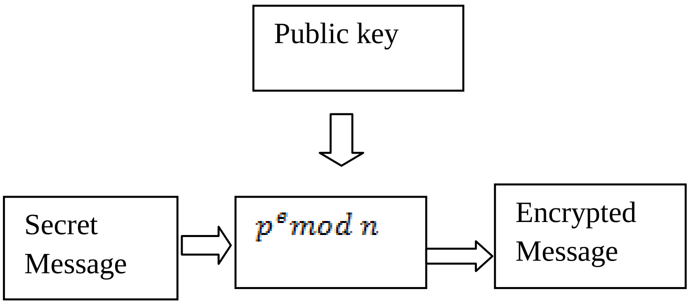

**Fig-4: Encryption process**

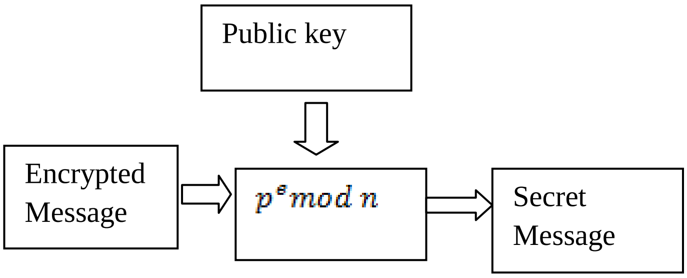

**Fig-5: Decryption process**

## VI. PROPOSED METHOD

The first task is to load the captured image and send it as input to the proposed encoding image steganography algorithm. In proposed method LSB and DCT with RSA rule to construct a safe steganography algorithm which is more secure than various systems being used for the intent of secretly transfer the information [12]. The proposed encryption process use in DCT and LSB for Image steganography is explained in the further part of algorithm design and other subsequent sections.

Algorithm of DCT with RSA
Step 1: Load input image.
Step 2: Split the concrete picture into 8x8 chunks of pixels.
Step 3: Alter the input image from spatial domain to frequency using two dimensional DCT with RSA.
Step 4: Calculate the DCT coefficients by divide using parameter into the rounded value.
Step 5: Encodes the secret image using RSA algorithm.
Step 6: Split up the encoded image into 8x8 parts.
Step 7: Implant this information in the mid DCT coefficients of input image.
Step 8: Implement two dimensional DCT to analysis it in the spatial domain.

Algorithm of LSB **+1** with RSA
Step 1: Load and read the cover image
Step 2: Write the text to be embedded.
Step 3: Generate public and private key by using RSA algorithm

Step 4: Apply encryption function on plaintext to create cipher data.

Encryption key P;!d>>bD;'1b&!d>,
Step 5: Change it into binary bits.

Sandeep Kaur gndec
⇩
0 110 010001111

Step 6: Message bits are taken from step 5 to embed into the erratic and multiple LSBs of the sample of the wrap icon.

Step 7: Embedding procedure, the most significant bit of input sample is tested.

Step 8: When most significant bit is “0” after that utilizes 6 LSBs**+1** for information embed.

Step 9: When most significant bit is “1” after that utilizes 7 LSBs**+1** for information embed.

Step 10: Generate decryption key by using RSA algorithm

Step 11: The customized input text segments are then recorded to the folder and obtained in the output image.

| **QUALITY MERTICES**<br>**IMAGES** | **PSNR for DCT WITH RSA** | **PSNR for LSB+1WITH RSA** |
|---|---|---|
| BARBARA | 53.777 | 84.834 |
| LENA_STD_BW | 54.902 | 82.316 |
| BIRD.BMP | 55.076 | 82.678 |
| BOAT | 52.251 | 80.063 |
| BABOON | 47.709 | 80.981 |
| GOLDHILL | 52.085 | 79.961 |
| PEPPERS | 50.044 | 79.575 |
| CLOWN_LUMI | 55.727 | 82.871 |
| FRUIT_LUMI | 53.253 | 79.668 |
| ELAINE | 64.9427 | 89.5287 |
| BUILDING | 65.8639 | 65.8639 |
| DOWNLOAD | 63.3257 | 87.1311 |
| GIRLFACE | 63.2314 | 86.4056 |
| CROOKEDROAD PALETT | 60.5518 | 86.4056 |
| GRAYSCALE | 65.8797 | 90.8549 |
| LION | 63.781 | 86.6342 |
| CUTE-BABY-GIRL | 62.7883 | 86.4056 |
| NATURE | 61.3422 | 88.892 |
| DENA | 63.7853 | 87.6922 |
| CAMERAMAN | 61.8109 | 84.9126 |
| FLOWER | 59.9087 | 78.3717 |
| CAT | 63.1966 | 80.7326 |
| CALVINGREY | 65.7937 | 83.7429 |
| BRIDGE | 64.3256 | 84.2544 |
| ORIGINAL | 64.3077 | 80.9808 |
| GREY | 64.0335 | 82.8714 |
| TREES | 62.1292 | 81.484 |
| MARILYN | 66.3568 | 84.2544 |
| HOUSE | 62.8009 | 80.7326 |
| JELLYFISH | 65.7591 | 84.5347 |

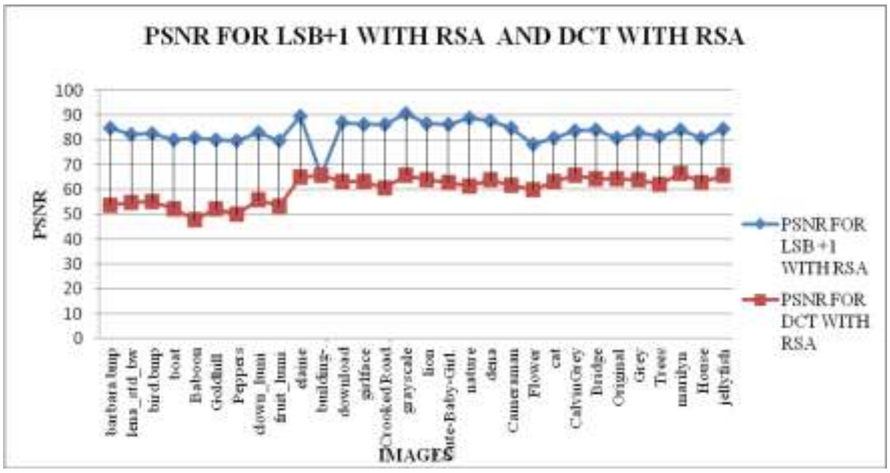

**Fig.6: Comparison of LSB+1 with RSA and DCT with RSA**

In proposed work text data is hiding into cover image and get stego image after. In this analysis of LSB+1 with RSA and DCT with RSA based steganography has done on the basis of parameter like PSNR and NC. PSNR computes the peak signal to noise ratio in decibels of the images. If PSNR ratio is higher than the quality of images are enhance. DCT with RSA schemes works perfectly with minimal distortion of image quality. In comparison of LSB+1 with RSA based steganography and RS encryption is used for security purpose with the help of RSA encryption hidden information transfer security from sender to receiver.

## VII. CONCLUSIONS

In the current effort, LSB with RSA and DCT with RSA has been implemented for enclosing secret data in conceal image without changing the image quality. This approach is a better way to hide data in image with greater security. In this endeavour, RSA algorithm is used to encode the secret information. At present, this application supports hiding data in lossless bmp, jpg image formats. RSA algorithm independently is very secure which is used to boost the security of hidden data. The proposed technique has been analysed by the quality metrics such as PSNR and MSE values.

## ACKNOWLEDGEMENT

I thanks to a great many people who helped and supported me during writing of this paper. My deepest thanks to Dr. Akshay Girdhar Associate professor of Information Technology Guru Nanak dev Engineering College Ludhiana, Punjab. Who guided and supported me in every phase of writing this paper. I am grateful to my parents who are inspirational in their understanding patience and constant encouragement.

## REFERENCES

[1] B. Li, J. He and J. Huang, "A Servey of Image Steganography and Steganalysis," Journal Of Information Hiding And Multimedia Signal Processing, vol. 2, pp. 142-172, 2011.

[2] S. Gupta and A. Goyal, "Information Hiding Using Least Significant Bit Steganography and Cryptography," I.J.Modern Education and Computer Science, vol. 6, pp. 27-34, 2012.

[3] J. Kaur and G. Ira, "Steganography Using RSA Algorithm," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 3, no. 3, pp. 75-79, 2013.

[4] A. M.Mehta and S. Lanzisera, "Steganography in 802.15.4 Wireless Communication," IEEE international conference on image processing, 2009.

[5] M. Karim, S. Rahman and M. Hossain, "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 14th International Conference, pp. 286- 291, 2011.

[6] M. Asad, J. Gilani and A. Khalid, "An Enhanced Least Significant Bit Modification Technique For Audio Steganography," Computer Networks and Information Technology (ICCNIT) International Conference, pp. 143 - 147, 2011.

[7] Aissi, M. K. Chandra and Cherif, "Implementation of the RSA algorithm and its cryptanalysis," American Society for Engineering Education Gulf-Southwest, 2002.

[8] E. Y. Kumar and P. Padmaja, "RSA Based Secured Image Steganography Using DWT," Journal of Engineering Research and Applications, vol. 4, no. 8, pp. 1-4, 2014.

[9] E. Emam and N. Nameen, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm," Journal of Computer Science, vol. 3, no. 4, pp. 223-232, 2007.

[10] G. Gunasekaran and B. R. Kumar, "Encrypting And Decrypting Image Using Computer Visualization Techniques," Asian Research Publishing Network Journal of Engineering and Applied Sciences, vol. 9 no. 5, pp. 646-650, 2014.

[11] M. Zodape and P. Shukla, "Analysis Of Triple DES And RSA Algorithm In Securing Image Steganography," International Journal of Computer Architecture and Mobility, vol. 1, no. 8, 2013.

[12] R. Bamal and V. S. Kaushal, "steganography: a modern day artand science for data hiding," International Journal of Latest Research in Science and Technology, vol. 2, no. 4, pp. 9-14, 2012.

International Journal of Computational Engineering Research (IJCER) is UGC approved Journal with Sl. No. 4627, Journal no. 47631.