International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-5, Issue-6, June 2019 Pages 48-50

# Different Algorithms used for Hiding an Image using Steganography with Cryptography

**Manju Kumari Gupta, Vipra Bohara**

***Abstract*—there are a lot of digital techniques exist for sending and storing images. These techniques require privacy, authenticity as well as integrity. Application of images is increasing in the medical field, science field, military field, engineering field, as well as the education field. In this paper, we provide a review and analysis of the different existing methods for hiding an image into another image and video. In this paper, some methods for video steganography and image steganography are used. In video steganography, image is hidden into a video. Video is a collection of frames and frame is represented as an image so in this method, image is hidden into a frame (image) whereas in image steganography image is hidden into the image. This paper represents current trends in steganography, so in the future; we can develop appropriate and more secure steganography algorithms**

***Index Terms*— LSB, MSB, PRNG, Kernel code, LSN, MSN.**

## I. INTRODUCTION

Steganography is a method in which data is hidden into a cover medium, here data can be a text, audio, image, and video and cover medium can be an image, audio, video whereas in cryptography, data is converted into an unreadable form known as cipher text. The cryptography algorithm is classified into two groups one is symmetric key, encryption and decryption process uses the same key. The second one is asymmetric key, encryption and decryption process uses different keys [1].

These cryptography and steganography techniques are used to secure communication but alone cryptography or alone steganography techniques are not appropriate for secure transmission, so we combine both technologies which provide more security and appropriate transmission [2].

The image is a collection of pixels. Each pixel represents with different light intensities. These light intensities vary image to image, depending upon the type of image. Gray scale images have different values and RGB images have different values of light intensities at each pixel. In image steganography, a cover object is an image in which we can hide any secret data.

Video steganography is the extended version of image steganography because the video is a collection of frames and frame represented as an image. So in video steganography, the cover object is an image and secret data is hidden in this cover object. Video also contains audio and audio is used as a cover object also. Here we are using video without concerning about audio. So methods are used for an image hiding in the other image also useful for an image hiding into the video [3].

**Manju Kumari Gupta**, Electronics and communication, Yagyavalkya institute of technology, Jaipur, India
**Vipra Bohara**, Electronics and communication, Yagyavalkya Institute of Technology, Jaipur, India

## II. EXISTING METHODS

Here some existing methods have described for hiding an image into other image and into video. In this paper, video is used for hiding an image. So algorithms used for hiding an image into other image can be used for hiding an image into the video.

### *A. Discrete Cosine Transform Method*

For image processing, for image compression and for steganography technique, DCT holds a key to the success of all these technologies. If changes in images are done in the frequency domain then chances that changes are not detectable. When DCT [4] is applied to images, several coefficients generated at the output. By using these coefficients changes can be done in images without the changes being detected. When a variation in DCT coefficients is less than changes in the image, are not easily detected. DCT coefficients are divided into three degrees of coefficients- Low band coefficients, mid-band coefficients, high band coefficients. Changes done in the mid-band are least detectable so this is the safest band.

**Emlon Ghosh et al. [5]** have used DCT in their proposed algorithm. The author has presented an algorithm that hides R, G, and B image into another R, G, and B cover image by separating both the images in three planes (red, green, blue).

- Embedding phase:-

Each color plane bit of a secret image is hidden into the same color plane of the cover image using discrete cosine transformation. After separating color channels, matrices are divided into cells of the required size. DCT transforms the image into the frequency domain by applying DCT on each block of the cell. For example, if the cover size is 512*512 and the secret image size is 64*64 then cover image needed 8*8 cells so there are 64*64 no of the block of cells and in each block, 1 value is embedded from the 64*64 sized secret image and multiplied by an alpha factor, After an alpha value has chosen. After that IDCT applied on these 8*8 cells. To generate a steganography image combined these modified

components.

- Extraction phase:-

The cover image is not required to obtain a secret image back. The extraction process is blind. The alpha value is used to extract the secret image. Here alpha value is worked as key. To retrieve the secret image, first separate steganography image into R, G, and B planes. Divide R, G, and B components into 8*8 blocks of cells. The same alpha factor value is used as in embedding. After that DCT is applied on 8*8 blocks. Now least detectable position value has been collected which was used during embedding and all value received by each cell divided by the alpha factor and these value considered as an element of the secret image. The combined element represented an original secret image.

### B. *Bit Plane Slicing Through (7, 4) Hamming Code*

The first cover video converted into no of frames. Each frame of video separated into R, G, and B plane and then (3*3) pixel blocks are formed. After that, each color plane is divided into 4bit planes starting from the LSB plane. PRNG (pseudo-random number generator) function with random seed K2 is used for the random selection of pixel's positions of the cover image for hiding secret data. Embedding capacity is an important metric for data embedding. It is measured by the number of secret bits that can be embedded into a cover image. The embedding capacity is calculated as ER= L/M × N bpp [6] where L is the length of the secret message

Before embedding the secret data, we take 36 bit secret key k1 which is known to both the sender and the receiver, to encrypt the secret data bit using symmetric key encryption. Before hiding, secret data is converted into a 1D array. After this, secret data is XORed with 36 bits key. Now data is embedded into the cover frame using the Hamming code. By these method 36 bits, secret data can be inserted into (3*3) pixel block. So lots of bits can be inserted into the cover frame. In the extraction phase first video is separated into frames. By using PRNG function with the same seed K2, steganography pixels of a random sequence are determined, after that pixel's R, G, B components are separated. 4-bit plane slicing has performed from LSB within (3*3) pixel blocks. Data is decoded from (7, 4) Hamming code after this encrypted data is retrieved by XORing with the same key k1.

**Ananya Banerjee et al. [7]** have introduced a method of data hiding into the video stream using bit plane slicing through (7, 4) Hamming code and by using a shared secret key. In this, a binary logo image is embedded into a cover video for authentication.

### C. *Parallel LSB Technique With Open CL Parallel Programming Technique*

In this technique, a 24bit color image is used as cover data to hide a large secret image. A parallel LSB technique is used for hiding and extracting. Here steganography image and the header of the secret image are sent by the sender. The header acts as a key that is used to decode the hidden image. Due to parallelism, encryption and decryption process are done in milliseconds.

- In the embedding phase:-

Each pixel's R, G, B bits of the secret image is hidden parallel in the least significant bit of cover image pixel's R, G, and B bits. This process is done using kernel code where work is done in parallel. The header of the secret image is a text file, which is shared with the receiver. In the extraction phase, the LSB of each bit of the R, G, and B components of each pixel of the steganography image is taken and combined in parallel to form one byte of R, G, and B components of each pixel of the secret image. The header provides information about the size of the secret image.

- In the extraction phase:-

The header information of s provides the size of the image. To make one byte of the R, G, B component of each pixel of the secret image, extract the LSB of each byte of the R, G and B components of every 8 pixels of the steganography-image.

**N. Gopalakrishna Kini et al. [8]** have used this technique to hide an image into the cover image. Here both images are used in this paper are a colored image.

### D. *Image Hiding using LSN and MSN Algorithm*

In this algorithm, two 24 bit cover image has chosen for hiding an image. Most significant nibble (MSN) and the least significant nibble (LSN) of the secret image have embedded randomly into two different cover images using a 4-4-4 hiding technique. Chaotic theory [9] has been used for encryption of both steganography images with a private key; this key creates confusion so named as confusion key. Encrypted steganography images have transmitted. The receiver has decrypted both the steganography images using reverse chaotic theory with the same key. MSN and LSN have separated from steganography images. MSN and LSN have merged to obtain a secret image.

**Radha S. Phadte et al. [10]** have used this algorithm to hide a secret image into two cover images. In this first 24 bit, the secret image split into three planes: red, green and blue. Each r, g, b plane is then converted into two parts at bit level of each pixel, named as secret MSN (most significant nibble) and secret LSN (least significant nibble). Two 24 bit cover image is chosen for embedding both secret MSN and secret LSN in randomized order using 4-4-4 data hiding technique of steganography, after that, both steganography images are encrypted using chaotic theory and a secret key.

### E. *Logical Stratified Steganography Technique*

In this technique, an image is hidden into the cover image. OR operation is used to combine the cover image and hidden image. In this technique, the right shift operation is performed on pixels of the hidden image by 4bits. 4LSBs of the pixel of the cover image are replaced with zeroes. OR operation is performed on the pixels of a cover image containing 4LSB bits zeroes with the right shifted 4MSB bit of secret image which is modified into the 4LSB bit. The steganography image is created after a secret image embedded into the cover image. At the receiver side, 4LSBs are retrieved and are shifted left 4 times so MSB bits can be formed. The hidden

image is retrieved by this corresponding intensity.

**M. Radhika Mani et al. [11]** have proposed a paper based on this technique. In this paper, author has used gray scale images for hiding. For testing the integrity and robustness, the proposed method is applied to various images like human faces, textures, and medical images. Various performance measures are used

### *F. Histogram Shifting Method*

A histogram is a pictorial representation of pixel intensity variation that exists in the image. Histogram of the cover image generated after these maximum repetition pixels in an image is chosen. Minimum repetition pixels and their locations in an image are used to hide the secret image. Before embedding, the secret image is encrypted through the Arnold cap map method with a secret key. The secret image is embedded into the cover image. After embedding the encrypted image, those pixels are converted back into their decimal equivalent which is responsible in an image. These pixels are restored along with their location in encrypted images. These pixel indexing values are considered as a secret key, which helps decode the secret image at the receiver side. For receiving the original secret image, pixels location is selected using embedded keys, from here encrypted image received. By using pixel indexing value, the original secret image decrypted.

**Irfanal Haque et al. [12]** have used this technique for hiding secret images. The author has avoided minimum repeated pixel values and only taken maximum repeated pixel values for embedding the secret image. More Number of maximum repeated pixel values in cover object offered the more degree of freedom to embed the secret image.

### *G. Least Significant Bit (LSB) Method*

In this algorithm least significant bit of cover image is replaced with a secret image bit. This method allows for hiding information directly into the cover image. LSB steganography is classified into two methods, first LSB replacement, second LSB matching. These terms first described by T. Sharp [13], in LSB matching [14] each pixel of the cover image is selected in a pseudo-random order, which is selected by a key. If the least significant bit of cover pixel matches the bit of a secret image, no change is required otherwise randomly 1 is added or subtracted from the cover pixel value. If secret image's bits are fewer than no of pixels presented in the cover image, then changes are spread by pseudorandom permutation, uniformly throughout the image. Whereas in LSB, replacement method, last bit of each pixel in the cover object is replaced with secret data bits.

**Deepesh** Rawat **et al. [15]** have proposed an algorithm to hide an 8-bit color image by replacing 4 LSB of the cover color image. The author has also described two algorithms for a 24-bit color image. In the first algorithm, the simple LSB method is used. In This color secret image is hidden by replacing the last 2 bits of R, G, and B in each pixel of the cover image. In these 2 bits of the cover image, 2 MSB of the secret image is hidden within the same color plane.

In an improved LSB method for a 24-bit color image, the first image separated into R, G, and B plane. The aim of this algorithm is, to hide most of the bits of a secret image into a blue plane rather than red and green.

More secure than other methods. Positions of pixels for hiding an image are random so no one can decode video which has any hiding data. PSNR and MSE value are very good than other existing methods. Encryption can be done before and after hiding an image into video, so this can be said that the proposed method is more secure for hiding color image into a video.

## III. CONCLUSION

This paper has presented a review of different steganography techniques for hiding an image. Our main concern is to hide an image into either video or image for secure communication. In this paper, some algorithms support only gray scale image for hiding, some algorithms support RGB and gray scale both, some algorithms support binary logo image. There are two methods of encryption. First, the secret data encrypted before hiding into the cover object. Second, the secret data is encrypted after the steganography operation performed. In this paper, we have presented both encryption methods.

## REFERENCES

[1] Mritha Ramalingam and Nor Ashidi Mat Isa, “A Steganography Approach over Video Images to Improve Security,” Indian Journal of Science and Technology, Vol 8(1), 79–86, January 2015.
[2] R.Nivedhitha, Dr.T.Meyyappan, “Image Security Using Steganography and Cryptographic Techniques,” International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.
[3] Mr. Mandar Digambar Khatavkar, “ A Image Security with Image Steganography using DCT Coefficient and Encryption,” International Journal of Innovations in Engineering Research and Technology [Ijiert] Volume 3, Issue 9, Sep.-2016
[4] Vandana Thakur, “Hiding Secret Image in Video, “International Conference on Intelligent Systems and Signal Processing (ISSP) IEEE2013.
[5] Emlon Ghosh, Diptasree Debnath, and Barnali Gupta Banik, “Blind RGB Image Steganography using Discrete Cosine Transformation,” Springer 2019.
[6] Cao Z, F., Yin Z, S., Hu H, T., Gao X, Wang L, “High capacity data hiding scheme based on (7, 4) Hamming code,” SPRINGER PLUS 5(1), 175 (2016).
[7] Ananya Banerjee and Biswapati Jana, “A Secure High Capacity Video Steganography Using Bit-Plane Slicing Through (7, 4) Hamming Code,” SPRINGER 2018.
[8] N. Gopalakrishna Kini, Gautam and Vishwas G. Kini.: A Parallel Algorithm to Hide an Image in an Image for Secured Steganography. Springer 2019.
[9] Ephin M, Judy Ann Joy, N. A. Vasanthi, “Survey of Chaos based Image Encryption and Decryption Techniques,” Amrita International Conference of Women in Computing (AICWIC’13).
[10] Radha S. Phadte, Rachel Dhanaraj, “Enhanced Blend of Image Steganography and Cryptography. IEEE2017.
[11] M. Radhika Mani and G. Suryakala Eswari, “A Novel Image Hiding Technique Based on Stratified Steganography” Springer 2018.
[12] Amal Saroj, Dr. S Saira Banu, “An Improved Technique for Hiding Secret Image on Color Images Using DWT, DCT, SVD,” IRJET 2018.
[13] T. Sharp, “An implementation of key-based digital signal steganography,” In Proc. Information Hiding Workshop, vol. 2137, Springer LNCS, 2001, pp. 13–26.
[14] R. Chandramouli and Nasir Memon, “Analysis of LSB Based Image Steganography Technique,” IEEE 2001.
[15] Deepesh Rawat, Vijaya Bhandari, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image,”