International Research Journal of Advanced Engineering and Science

ISSN: 2455-9024

Analysis of Different Steganography Algorithms and Security Issues

Harneet Kour khajuria[1], Loveneesh Talwar[2], Akhil Vaid[3]
[1, 2]Department of Electrical Engineering, YCET, Jammu, J&K, India-180004
[3]Department of Electronics Engineering, SSCET, Pathankot, Punjab, India-145001
Email address: [1]harneet.destiny@gmail.com, [2]loveneeshtalwar@gmail.com, [3]akhilvaid20@gmail.com

***Abstract*— *The data transfer through internet aims to provide faster data transfer rate and accuracy of data being transferred. In addition to it when security of the data is prime concern while communicating without any alterations, the data transfer technique aims to provide sufficient security while transferring data which is achieved by employing certain approaches and one such approach is steganography which is discussed in this paper. Steganography is an encryption technique used to hide only the messages (that requires to be kept secretive) in innocent looking public communication such as in image so that their presence remain undetected and protect them from prevailing security attacks. In this paper we tend to present the comparative analysis of different steganography algorithms such as DCT transform, Wavelet transform etc. and also discuss various security issues involved and hence evaluate the existing techniques limelight and drawbacks.*

***Keywords*— *DCT Transform Image, Cryptography Steganography, and Security attacks.*

I. Introduction

In present scenario, internet is integral part of each and everyone's life irrespective of their profession or in person even to store their works or personal information for references in the internet database which further requires to be protected owing to the need of maintaining the confidentiality and integrity of an individual's work or information to avoid copyright violation. Integrity and confidentiality of data is prime concern to avoid above copy right violations and others accreditations. This is achieved by Digital steganography technique that tend to provide the protection of the digital information uploaded on the internet by the user and is defined as an art of hiding desired data into another data by embedding into each other [1]. Digital steganography is used mainly by the corporations to protect their copyright further avoiding any illegal use of them by others thereby making a good reputation as well [1], [2]. In this paper a comparative analysis of various steganography algorithms are discussed. In addition to it, in this paper a brief discussion about various security issues or challenges to be considered with emerging trend of steganography techniques is also included. The steganography technique is applicable worldwide in almost every field both in corporate world as well as in the internet world for personal applications such as social networking sites as facebook etc. It has global application in Govt. data base such as in Scientific Research or Defense field etc. where integrity of data is must and requires to be confidential as well as secretive [1-3].

A. *Cryptography versus Steganography*

Both Cryptography and Steganography are data encryption techniques that tends to provide protection and enhance the security of data to maintain its integrity and confidentiality but differ in their applications since cryptography encodes the data or information in a way that no one else than the authorized person with authentic key can read the contents and ensures that the information transmitted is not modified while its transit. Another main difference between two is that in cryptography the hidden message is visible as information being encoded is in plain text unlike steganography [2], [4] where the hidden message does not appear visible as clear from given table I.

TABLE I. Steganography versus cryptography.

S.No	**Context**	**Steganography**	**Cryptography**
1	Host files	Images, Audio, Text etc.	Mostly text files
2	Hidden files	Images, Audio, Text etc.	Mostly text files
3	Result	Stego files	Cipher text
4	Types of attack	Steganalysis	Cryptanalysis

II. Background

Steganography has been used widely even in the past for communicating secret messages. It includes examples like writing with invisible ink which appears blank to the average person and when heated contents become visible and peel wax off tablet to view the secretive content. With more advancements and growth of digital revolution such as DSP techniques etc, the steganographic techniques applied also become digital and is called digital steganography more precisely [1], [2]. This digital steganography technique aid in creating an environment of corporate vigilance and spawning interesting applications for further evolution and also benefitting the cyber criminals indirectly. Getting rid of emerging cybercrimes has essentially become the need of the hour. So in order to strengthen the existing steganography techniques, frequent attacks are carried out and it is called as stegnalysis. Steganalysis is done to ensure optimal results for steganography technique applied [3], [4]. This paper gives an account of different steganography algorithms and stegnalysis as well.

III. Stegnalysis and Steganography

Stegnalysis is the art to discover and render useless covert messages that help to identify the hidden messages encoded in the suspected information stream and recover it as well. To be more precise it is the process to detect the steganography by looking at variances the bit patterns and files of unusually large sizes [2], [3]. Stegnalysis combats the steganography in many ways except for detection of messages but the problem to uncover messages still needed to be resolved by stegnalysis. Figure 1. shows stegnalysis and steganography relation.

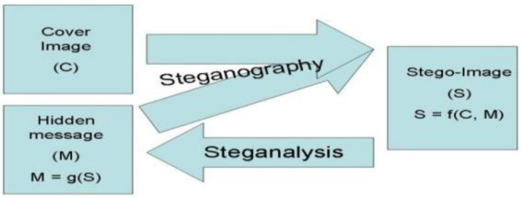

Fig. 1. Stegnalysis and steganography.

Five classes of stegnalysis are summarized as in table below assuming that attacker has the stego object in all classes and stego object is only present in stego-only class where as in known –cover and known-message class, in addition to stego object there is also present an original cover either without the hidden message or along with hidden message respectively. Further in chosen stego and chosen message class, the human or computer knows the algorithm used to hide the message and tries to find them or uses some program to embed his own message to discover similar stegno objects to find the presence of a hidden message.

TABLE II. Classes of stegnalysis.

No extra information	One extra piece of information	Algorithm testing methods
Stego-only	Known-cover	Chosen-Stego
	Known-message	Chosen-message

A. *Limitations of Stegnalysis*

In stegnalysis there exist no certainty that the suspected information stream contain any hidden message or used to transmit any secret message until it is recovered completely and decrypted since the hidden data may not be embedded or it may be noise or irrelevant data encoded into it which makes stegnalysis often a tedious and time consuming analysis which is the only drawback of stegnalysis [3], [4].

IV. STEGANOGRAPHY

Steganography is stronger than stegnalysis due to its inherent properties. The steganography is an encryption technique which tends to hide only the secretive messages that are required to be kept secretive to protect them from prevailing security attacks. It includes hiding information in innocent looking public communication such as in image so that their presence remains undetected and protected from any security threat. The strength of steganography can be determined by its capacity to hide the data, invisibility extent that is human's inability to detect stegno object. Other parameters that judge steganographic strength are undetectability that is computers inability to differ between cover object and the stegno object, robustness, tamper resistance and signal to noise ratio as shown in figure 2. The capacity undetectability and robustness are opposites since increasing one leads to reduction of other and so no steganographic technique can be completely robust or undetectable as well as have maximum capacity thus achieving one goal need a compromise of other two [1], [5], [6]. In most of the applications capacity is less important and robustness along with undetectability is considered as prime goals and robustness achieved by watermarking is preffered. Figure 3 depicts the properties of a good steganography technique that are opposites still required for good steganography**.**

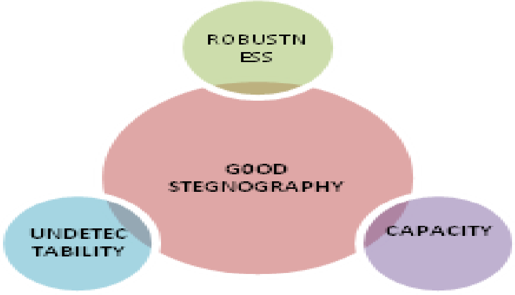

Fig. 2. Key properties of good steganography technique.

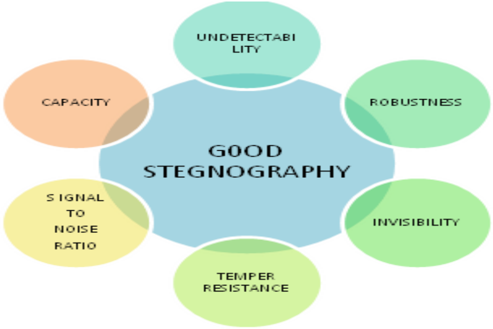

Fig. 3. Opposed properties of good steganography.

A. *Image Steganography*

It is more secure steganographic technique that uses image as the cover image object so that the embedded data leaves no traces of steganography applied and size of the secret message, its format and carrier image content affects directly the visibility of cover image. Figure 4 shows image steganography. The complexity in its detectibility determines its (image steganography) success that ranges from high to low level. And also its robustness that enables the embedded data to preserve its fidelity by surviving when subjected to reprocessing operations for the cover image. There is need to obtain a tradeoff between the capacity and robustness feature for efficient image steganography [5], [6].

B. *Digital Steganography*

Different algorithms are designed to meet with certain requirements before exchanging any digital data over public network securely to the intended recipient without any attack incurred on it thereby fooling the attacker by embedding the secret information into the data in such a way that it remains undetectable and difficult to recover so called in stego object. Figure 5 shows digital steganography stego object is embedded into image or audio file in such a way that the secret message remains unchanged as well as invisible to naked eyes in order to exchange information covertly without being noticed by attackers thereby assuming him to be aware of the hidden data present [1], [5-7]. Modifying the stego object should not affect the watermark embedded by the user on the document.

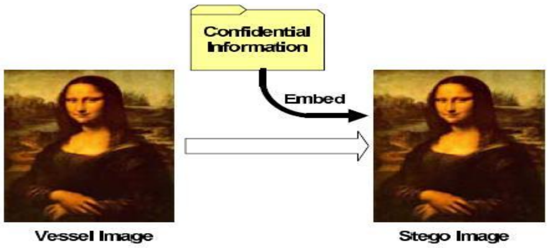

Fig. 4. Image steganography.

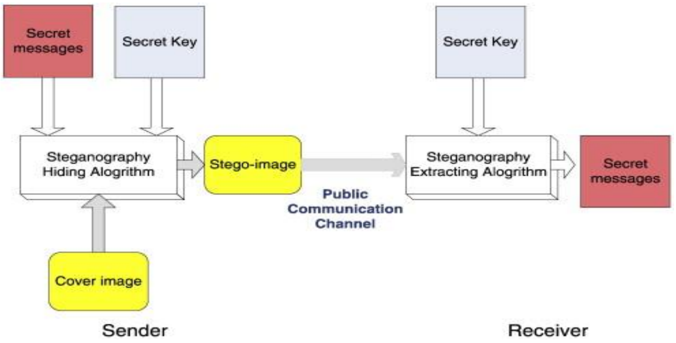
Secret messages
Secret Key
Steganography Hiding Alogrithm
Stego-image
Public Communication Channel
Secret Key
Steganography Extracting Alogrithm
Secret messages
Cover image
Sender
Receiver

Fig. 5. Digital steganography.

V. Different Steganography Algorithims

A. LSB Steganography

In this algorithm, the message is concealed using the least significant bits of the cover media's digital data. It includes LSB replacement technique which simply flips the last bit in each of the data values in order to interpret the hidden message. For example: Let first eight pixels of the original 8-bit grayscale image (bit map) has the gray scale values as below:

11010010 01001010 10010111
10001100 00010101 01010111
00100110 01000011

Now let c be the letter needed to be hidden. Consider its binary value as 10000011. To hide it the LSBs of each gray scale value above is replaced with the binary bits of c to have new grayscale values as:

1101001**1** 0100101**0** 1001011**0**
1000110**0** 0001010**0** 0101011**0**
0010011**1** 0100001**1**

It is also observed that only half the LSBs are needed to change on an average here and hence there will be hardly visible difference between the cover image and the stego image [6-8] as shown in figure 6. LSB steganography also includes LSB matching technique in which the LSB replacement can alter equally the data value by a small amount thereby ensuring to preserve the legal data values range and the difference is that choice can be made at random whether to add or subtract one from the cover image pixel which makes it imperceivable the existence of hidden message [7], [8].

Both LSB replacement and matching leaves the lowest significant bit changed if the message bit matches with the LSB but if it does not match LSB then LSB Replacement replaces the LSB with the message bit whereas on the other side LSB matching lead to increment or decrement the data value by +1 or -1 respectively so called as +-1 embedding as well. There are 256 different grayscale shades between black and white. These shades are used for grayscale bit mapping and since in LSB steganography the LSB of cover image is needed to be substituted by message bit i.e. either 0 or 1, so the 50 PERCENT pixel of LSBs can be changed without any loss [3].

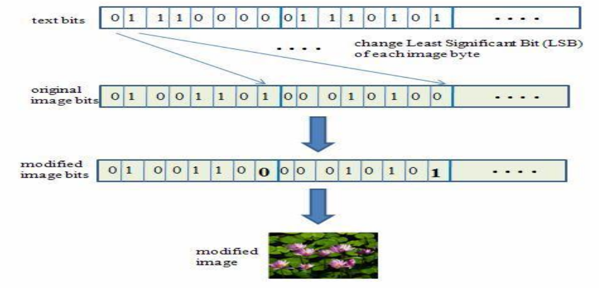

Fig. 6. LSB steganography.

Algorithm

1. Read the image to be embedded and also the image inside which message is embedded i.e. cover image.
2. Set Num Significant Bits equation, n=1, 2
3. Let Size 1= secret message size and Size 2= cover image size.
4. Set the 'Num Significant Bits' equation significant bits of each byte of cover image to zero by using bit by bit AND operation on cover and size1 matrix.
5. Embed the 'Num Significant Bits' most significant bits (MSB) of secret message to create the stego image by using stego equation (cover zero+ secret)/28-n.
6. Recover the embedded image by using bit by shift operation.
7. Display figure of cover image, to be hidden image, stego image and the recovered image.
8. End.

Figure 7 shows LSB steganography algorithm.This method is applicable for both 24- bit color and 8- bit gray scale image but here the quality of stego and recovered image will degrade with increase in 'n'which is its limitation [7], [8].

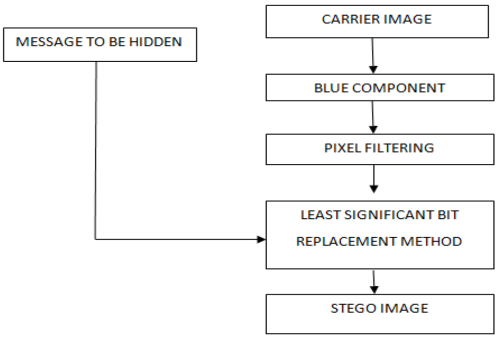

Fig. 7. LSB steganography algorithm.

B. *Enhanced LSB Steganography Technique*

It is more efficient and less prone as shown in figure 8.to distortions compared to simple LSB steganography technique since it is functioning in spatial domain and tends to hide the message in only blue color of RGB carrier image unlike LSB algo which hides the information in LSB of each color of RGB carrier image that in turn causes major distortion due to change in all three colors and hence to overcome this distortion enhanced LSB came into existence [8], [9]. It produces a great balance between the security and good quality of an image improving the computational efficiency and complexity of stego image by improved or modified LSB replacement for data hiding [9].

Enhanced LSB algorithm

1. Select a cover image as an input.
2. The hidden message is embedded in Blue component only of a cover image.
3. Pixel selection filter is used to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Enhanced Least Significant Bit (ELSB) of every pixel to hide information, leaving most significant bits (MSB).
4. Use bit replacement method to hide the message [9].

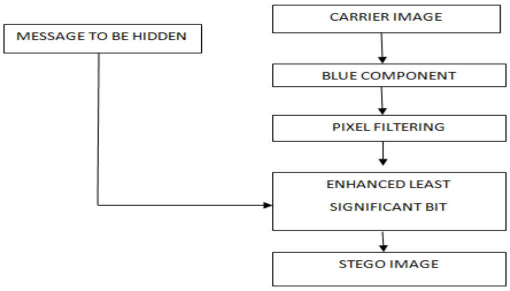

Fig. 8. ELSB steganography algorithm.

C. *DWT Discrete Wavelet Transform*

It is used to represent the signal in time as well as frequency in a compact way that can be efficiently computed and deals with both the approximations that are considered as high scale low frequency components as well as the details that depicts the low scale high frequency components and can be analyzed using a fast pyramidal algorithm related to multirate filter banks [4]. It includes analysis of signal at different frequency bands with different resolutions thereby resulting in decomposition of signal into coarse approximation and detail information.

Mathematically, the DWT is defined as:

$$w(j,k)=\sum_{j}\sum_{k}x(k)2^{-j/2}\varphi(2^{-j/2}n-k)$$

Where φ (t) is a finite energy time function that decays faster called wavelet equation.

Coarse approximation is further decomposed using wavelet decomposition step as a result of successive high-pass [n] and low-pass h[n] filtering of time domain signal defined as:

Output of high pass filter:

$$yhigh[k]=\sum_{nk}x(n)g(2k-n)$$

Output of low pass filter:

$$ylow[k]=\sum_{nk}x(n)g(2k-n)$$

DWT ALGO

a) At transmitter end: DWT is applied for decomposition of the embedded payload as well cover signal thereby resulting into transformation of spatial domain signal to frequency domain and separation of approximation coefficient C[]=c1[]+c2[] and detail coefficient L[]=l1[]+l2[] where l1[]&l2[] are low frequency coefficients and c1[] &c2[] are high frequency coefficients obtained at second stage of fusion of approximation & detail coefficients of both signals. Steganographic signal ss[] is then constructed by applying the inverse wavelet transform. This steganographic signal is decomposed at third stage to A[] and D[] inorder to perform the encryption on it. The detail coefficient vector d[] of the signal combines with the vector R[] =d[]+code used as wavelet to decompose the steganographic signal value which is essential for reconstruction of signal at receiving end [6], [9].

b) At receiver end: Detect the key code {=R[]-d[]} from detail coefficient vector and then steganographic signal is reconstructed using this code and approximation. Now detail coefficient at second stage IDWT is applied on reconstructed steganographic signal in order to reconstruct the payload signal from it with the help of approximate and detail coefficients [6], [9].

D. *DCT (Discrete Cosine Transform) Steganography*

a) DCT: It’s a common JPEG compression technique that leads to transformation of spatial domain image or signal into the frequency domain. i.e. high, middle and low frequency components of an image as shown in figure 9.

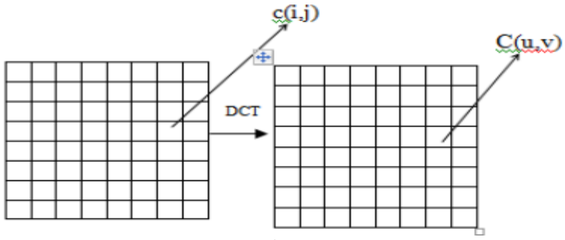

Fig. 9. DCT of an image.

Here, C(u,v) is the DCT coefficient of DCT matrix of row u and column v
C(i,j) is pixel intensity in row i and columns j

Signal energy is represented by lower frequency components in image lying at upper left corner of DCT and lower right half represents higher frequency component that are small enough to be neglected there by achieving required compression.

DCT for 1 D image is obtained as:

$$C(u)=\alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right]$$

where u = 0, 1, 2,…, N-1 for n data items
DCT for 2 D (N*M) image c(i.j) is obtained as:

$$\mathrm{C}(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

where u,v= 0,1,2…N-1

b) DCT and steganography: In steganography, DCT technique is used to obtain the DCT coefficients in which the secret messages are embedded. First the image is broken into 8*8 pixel blocks to which is applied DCT on block basis from left to right and top to bottom. Quantization table is used to compress each block and scale the DCT coefficients. These DCT coefficients are embedded with the message that is to be kept hidden and this is called as DCT steganography since here steganography requires DCT coefficients which are obtained by DCT algo and message is embedded in DCT coefficients using given algorithm:

Algorithm to create stego image

1. Cover image and secret message is read and then converted to its binary.
2. Cover image is converted to 8*8 block of pixels.
3. From each pixel block, 128 is subtracted starting from left to right and top to bottom.
4. DCT is applied to each block to obtain compression using the quantization table i.e. DCT coefficients.
5. LSB of each DC coefficient is first calculated and then replaced with each bit of secret message.
6. Stego image is then created.

Algorithm for text message retrieval

1. Stego image is read and then divided into 8*8 pixel blocks.
2. Starting from left to right and top to bottom, 128 is subtracted from each pixel block.
3. DCT is applied to each block and compressed through quantization table.
4. LSB of each DC coefficient is calculated.
5. Retrieval of each 8 bit and then conversion of each 8 bit into character [6], [7], [9].

VI. Security Issues

Hidden information analysis by attackers includes Detection of secret information, extraction and destruction or modification of hidden information. Depending upon the type of information available to the stegnalyst for stegnalysis [1-4]. Security attacks are classified as:

A. *Types of Security Attacks*

a) Basic attacks: Loop holes while designing techniques are root cause of basic attacks. For example change in audio length without alteration of the pitch of audio quality is effective against the attacks for audio files that need synchronization since such audio files may lose data just by adjusting parameters that are required to achieve synchronization.

b) Robustness attacks: Water marking techniques are prime targets of robustness attacks that tend to destroy the watermark without changing the image since watermark lose its content if a series of minor distortions are applied. Robustness attacks can be handled by creating multiple copies of the mark using inverse transformations which increase its resistance against robust attacks.

c) Presentation attacks: It prevent the detection of water mark on digital images and requires that the original image file that splits into a matrix have minimum value of cells and the size of cell can't be further reduced by attacks if the cell size is minimum which prevents the diminishing of watermark thereby making its detection possible since the watermark could be lost if the size of cells I a image matrix are very small.

d) Interpretation attacks: The attacks where it becomes difficult for attacker to interpret the owner of document. Let a digital image is created by the user who embeds the image with a watermark then that watermark belongs to the only user. Assume that the attacker or any second user adds a watermark to the same digital image there by showing that the watermarked image is owned by him. So the actual owner of document is difficult to decide. Such types of attacks are prevented by using a strong watermarking technique so that no fake watermark can be added by attacker.

e) Implementation attacks: The attacks targeted at the marks existing in the data due to loopholes or faults present in the mark detection software that make it feasible for attackers to generate the secret information [2-4].

VII. Comparison of Secret Communication Techniques

Encryption and Steganography are mistaken mostly as ambiguous concepts though both are different techniques developed with a common goal. "Encryption" refers to encoding data in a way that only the intended recipient can determine its intended meaning which remains undetermined for others. In contrary to this in steganography, an attempt is made to prevent the unintended recipients from suspecting the existence of data [1-3] Steganography rather tends to prevent the visibility of data from the attacker without altering the data unlike encryption where data encoding is done to maintain the privacy and security of the data [2], [11].

TABLE III. Difference between secret communication techniques.

Technique	Confidentiality	Integrity	Un removabiltity
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

The core difference between encryption digital signature and steganography techniques is tabulated as shown in table III.

VIII. CONCLUSION

Secure communication is desired in almost every field whether military or in personnel communication which is obtained using secure communication techniques rather than the traditional communication techniques. Steganography is one of my secret communication technique that are developed with a common goal of protecting data from unintended users or attackers, when data is required to be maintained secure and for providing secure communication. The detection of secure data can be made complicated by integrating the different secure communication techniques such as cryptography along with steganography since many such techniques are not independently robust enough to prevent detection and removal of embedded data alone. This paper tend to present the secure communication by employing different steganographic algos which make secure communication more simple and easy and can be applied for defense and military applications in addition to the personal as well as professional point to point or multipoint secure communication. Different security attacks to be considered while designing the algo are discussed such as basic attacks, robustness attacks presentation attacks etc.and a comparative analysis of steganography algo with other secure communication techniques concludes that there are some advantages as well as limitation of each secure communication technique such as if high payload is to be embedded then image steganography is preferred where as low capacity requirement for embedding data is met using spread spectrum steganography. Similarly DCT, wavelet and LSB, ELSB steganographic techniques uses a stego object for embedding secret messages covertly into it. The steganographic technique with lowest delectability is a new image steganographic technique based used commonly for secure internet communication based on chaotic sequences and most efficient results are obtained with simple LSB steganographic technique.

REFERENCES

[1] R. Poornima and R. J Iswarya, “An overview of digital image steganography,” *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 4, no. 1, pp. 23-31, 2013.

[2] T. Morkel, J. H. P Eloff, and M. S. Olivier, “An overview of image steganography,” in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, 2005.

[3] J. Fridrich, *Multimedia Security Technologies for Digital Rights Management*, in Academic Press, ch. Steganalysis, pp. 349-381, 2006.

[4] J. Fridrich, R. Du, and M. Long, “Steganalysis of LSB encoding in color images,” *in Proceedings of the IEEE International Conference on Multimedia and Expo. Newyork*, USA, IEEE Society Press, 2000.

[5] V. K. Sharma and V. Shrivastava, “A steganography algorithm for hiding image in image by improved LSB substitution by minimize detection,” *Journal of Theoretical and Applied Information Technology (JATIT)*, vol. 36, no. 1, pp. 001-008, 2012.

[6] N. Tiwari and Dr. M. Shandilya, “Evaluation of various LSB based methods of image steganography on GIF file format,” *International Journal of Computer Applications (IJCA)*, vol. 6, no. 2, pp. 1-4, 2010.

[7] V. L. Reddy, Dr. A. Subramanyam, and Dr. P. C. Reddy, “Implementation of LSB Steganography and its evaluation for various file formats,” *International Journal of Advanced Networking and Applications (IJANA)*, vol. 2, no. 5, pp. 868-872, 2011.

[8] T. Kumar and K. Verma, “A theory based on conversion of RGB image to gray image,” *International Journal of Computer Applications (IJCA)*, vol. 7, no. 2, pp. 7-10, 2010.

[9] S. Gupta, G. Gujral, and N. Agawam, “Enhanced least significant bit algorithm for image steganography,” *International Journal of Computational Engineering and Management (IJCEM)*, vol. 15, no. 4, pp. 40-42, 2012.

[10] A. Kumar, S. Chokhandre, and Dr. A. Mishra, “Discrete wavelet transform based signal steganography and encryption,” *International Journal of Engineering Science and Technology (IJEST)*, vol. 4, no. 5, pp. 2417-2420, 2012.

[11] K. B. Raja, C. R Chowdary, K. R. Venugopal, and L. M. Patnaik, “A secure steganography using LSB, DCT and compression techniques on raw images,” in *IEEE International Conference on Intelligence Sensing and Information Processing*, pp. 171-176, 2005.