International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Hybrid Domain Steganography for Multiple Images using DWT-LSB Method

Shashikiran B S, Shaila K, Venugopal K R

Abstract: ***The technique of hiding information with coexistence of other information is called Steganography. Users usually stores their documents in the form of images so this can be achieved using steganography. Image steganography can be performed in spatial-domain, Transformation-domain and hybrid domain. A new hybrid domain based steganography for hiding multiple image in a single image is proposed in this paper. The properties of Discrete wavelet transforms is used for developing the algorithm that provides security and also reduces the storage capacity in huge databases. While storing various documents of a user in a huge database confidential and integrity has to be Maintained. Possibility of mismatching of document in huge databases is very common and data storage for maintaining those documents are challenging task. In this Approach, multiple secret images are embedded in a single cover image to get stego image using hybrid domain. Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) techniques are used in embedding multiple images that reduces the storage capacity along with, enough security. The proposed algorithm provides acceptable Peak Signal to Noise Ratio (PSNR) ratio and data capacity of hidden information is more compared to existing methods.***

Keywords : *Cover Image, DWT, LSB, PSNR, Secret Image Steganography, Stego Image*

I. INTRODUCTION

Steganography [1-3] is a technique of embedding data such that it doesn't draw the attention of the hackers. Steganography means covered writing and is originated from two Greek words with ‘Steganos’ means covered and ‘graphia’ means writing. In cryptography data is hidden by scrambling it so that it is unreadable but gives a clue to the hacker.

In recent era, information exchange takes place electronically where new issues, requirements and opportunities are emerged. It is intended that only the authorized person has rights over the data during communication so that unauthorized persons cannot seize the information. Hence, steganography is used to hide the data in other data for secure communication. Consider a person who wishes to deliver some information to recipient such that no one else knows about the information, this can be achieved using steganography technique.

Different types of steganography methods used for embedding information are:

Text Steganography: It allows the user to embed text behind other files by altering the format of text or a file to generate an arbitrary character within the text file. In this technique a text file is preferred as a cover media wherein the secret data is embedded. In this technique, the data is more susceptible to the hackers. Since, the hacker recognize the pattern and decodes the secret data easily. The process of text steganography is difficult since it lacks a large-scale redundancy of information when compared to audio, image and video-based steganography.

Image Steganography: The image steganography technique has gained much attention in the field of steganography. Image steganography techniques are of three types:

1. **Spatial-Domain Steganography:** In this some bits of both cover image and secret image are directly manipulated for embedding secret data.
2. **Transformation-Domain Steganography:** The first and foremost thing is to convert the spatial-domain images to transformation-domain and then embeds the secret data.
3. **Hybrid-Domain Steganography**: Both spatial domain and transformation-domain techniques are employed for hiding secret image in cover image. Initially cover image is converted to Transformation-domain and then the concept of spatial-domain is applied to hide the secret image.

Video Steganography: Embedding information in a video is similar to image steganography where different frames of video are considered to embed information in it.

Audio Steganography: The Audio steganography is most interesting technique as it involves Human Auditory System. Best way to achieve the audio steganography is to use Ultrasound range to transmit secret information.

The aim of this work is to hide the information in image by providing security and to reduce the storage capacity in huge databases. Consider, a bank where customer’s data like, account details, photo, Aadhar, PAN and few more details has to be collected and maintained in database. Similarly, in defense, medical field, colleges, some public and private sectors where multiple data of a person or user are stored in databases as image. First, the database is secured using cryptography. If at all hackers can attack and get information about individuals steganography provides the security at next level.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

Shashikiran B S*, Research Scholar, Dept of ECE, VTU-RC, VKIT, Bangelore, Karnataka, India. Email: shashikiran.bisileri@gmail.com

Dr. Shaila K, Professor and research head, Dept of ECE, VKIT, Bangalore, Karnataka, India.

Dr. Venugopal K R, Vice Chancellor, Bangalore University, Bangalore, Karnataka, India.

Next, the memory required to store the data of individual is again a challenging issue as it contains more information in the form of multiple images. Similarly, data security and storage issues are more challenging in most of the applications or systems. In some social networks the most preferred technique is batch steganography [4] where a secret image is embedded to multiple cover image for transmitting over a communication channel. This was implemented and developed by [5-6] in which the user can embed the secret information in a batch of images.

The idea of having a single image that is embedded with all information of an individual such that only photo of individual is visible to unauthorized person gives better security and as the number of images are reduced to one, memory required for storage is less compared to having three or four images. Many algorithms are developed in image steganography ranging from spatial-domain to Transformation-domain and extended to hybrid domain. Proposed method uses hybrid domain steganography for embedding multiple images in a single image.

A. Motivation

Steganography has widespread application in hiding secret information, When a digital image is considered the main advantage is that (i) it is composed of bit planes and pixels. The MSB of the pixels or MSB Bit planes corresponds to maximum information of the image and LSB contributes less information of the image in time domain. (ii) when DWT is applied on image it is divided into different frequency sub bands. like MSB in time domain i.e., LL sub-band coefficents comprises the highest information of the image and other sub-bands contains very less information about image. The LSB and sub bands are used for hiding secret information. Many steganography algorithms discuss about for hiding a single image and not for multiple images [1-18]. Similarly, many compression algorithms exists but these are not combined with steganography. The main idea is to hide multiple images in a single image so that when image steganography is performed memory required to store the secret images is reduced. The storage space required to store one image is now sufficient to store an image that contains the secret images.

B. Contribution

In recent years, large scale of information has been transferred through digital media where safety and security is the major issue to be considered. Many security algorithms are used for providing security. One such security is to hide information in other information so that intruder fails to get the secret information. With the growing technology digital documentation is preferred over paper documents. Storing multiple documents or information as a image with confidentiality is a challenging task and memory constraint is one more issue. In this paper, we have steganography technique to develop an algorithm to hide multiple key images in a single image to provide security and to reduce the storage space using DWT and LSB technique.

C. Organization

The rest of this paper is organized as follows: Related works are discussed in Section 2 and 3 respectively. Problem statement defined in section 4 proposed model and algorithm design are explained in section 5. In section 6, proposed model and detailed algorithm is discussed. Experimental results are discussed in section 7. Conclusions are presented in section 8.

II. RELATED WORK

Steganography has been practiced for centuries as the technology improved and people depended on digital technology as part and parcel of their life. The digital technology has moved forward in such a way that everything is available at finger tips. But, the question arises how secure is that digital technology. Though steganography is not a new technique, still it is one of the safe and secure techniques for hiding information when compared to other data securing technique like cryptography. Though different steganography technique are available, Image steganography is widely used and is more secured considering the properties of digital image.

Vikas et al., [7] proposed a (LSB) steganography method using midpoint circle approach to hide information. The method overcomes the drawbacks of basic LSB approach in which it is difficult to identify the secret message and improves the data security level for a single embedded image. Shalu et al., [8] proposed a new algorithm using fractional Fourier Transform to hide scrambled secret information into cover image with wavelet coefficients. Alpha bending technique is used for hiding secret data in cover image after executing Arnold transform on cover image followed by DWT to the cover image and secret image. IDWT is used to generate scrambled secret image. The data capacity is discussed for a single image. Yinan et al., [9] proposed a technique for conserving the histogram of the cover image in the stego image to minimize the visual distortions in it. Gray scale images are decomposed into small fragments based on gray value and the same gray value of key images are embedded into the cover image. Randomization is involved to confirm the conservation of the histogram of cover images. Histogram and distortions are discussed for hiding one secret image. Prabhakarn et al., [10] proposed a steganography technique based on Discret Wavelet and Inverse Wavelet Transformation. Fusion process is employed in hiding key image data into cover image. Several combinations of DWT and IWT are employed on both images to improve the stego quality. It is observed that DWT and IWT technique are used for embedding only one key image in cover image

Bingwen et al., [11] proposed a steganographic technique using binary image to decrease the distortion on texture. In this method, cover vector is generated to get super pixel by dividing the scrambled images. Pattern framework code is employed to reduce the embedding distortion in an image. The rotation, complement and mirroring-invariant local texture patterns are taken from the binary image. The changes in complement, rotation and mirroring-invariant local texture patterns distortion shows a robust relationship with the detectability for hiding a single key image.

Aayushi et al., [12], proposed a DWT technique is used for embedding secret data, focus is on decreasing the complexity in image embedding through DWT technique while providing lesser distortion with better security in the stego image. The five LSB of the LL2 band coefficient of cover image is replaced by five MSB of the secret image pixel with a acceptable data hiding capacity.

Elshazly et al., [13], proposed a secured embedding algorithm using hybrid IWT-LSB embedding technique that embeds bitstream of the secret text into the LL band coefficients of LSBs of integer wavelet transform (IWT) of an image to form stego-images. Median filter is used on stego image and then IWT is applied on the image to perform steganography on the LSB of LL Band coefficients. Only median filter is applied for removing the distortion of stego image. Linjie et al., [14] proposed a class of new functions referred to as Uniform Embedding Distortion function (UED) for secure image steganography. The minimum distortion for the information given with the code word is determined using Uniform Embedding Distortion Function by considering the pattern of frame coding, which instead of random adaptation and tries to distribute the embedding changes uniformly to quantized Discrete Cosine Transform coefficients of all possible magnitudes. Less statistical detectability is accomplished with better PSNR and acceptable data capacity.

Zhang et al., [15], proposed an image embedding algorithm based on DCT and Latent Dirichelt Allocation topic classification. LDA topic model is used for categorizing the database of image which belongs to a particular topic considered and DCT for 8 X 8 block is applied on the images. The robust feature sequence is created with relation between the coefficients in adjacent blocks. Feature sequence, location coordinates and image path is created by an inverted index. To achieve steganography, the secret data is transformed into a binary sequence and divided into segments. The image whose secret information segments. The feature sequence location considered are chosen as the cover image according to the index. Sathisha et al., [16] proposed an image steganography method based on lifting wavelet transform. The mantissa part of cover image is replaced by the secret image. The LWT is performed on cover image and secret image of sizes I * I and 3I * 2I respectively. The mantissa values of HL band, LH and HH band of cover image are converted to real values. The LL band of secret image is embedded in mantissa part of different bands with a better PSNR for hiding sinlge secret image. Fengyong et al., [17], proposed a batch steganography method for hiding data in social network. It is different from the previous steganography methods where a user only considers an individual image. In this method, multiple images can be hidden. To assign payload to multiple images optimal embedding strategy is applied. Feature Back Replacement (FBR) iterative search is used for recovering of secret image. Secret image is hidden in multiple cover images in a batch with good capacity and acceptable PSNR value between cover and stego image.

III. BACKGROUND WORK

Many steganography algorithms are proposed and developed from different researchers, few of the related works are discussed in section II. Existing steganographic algorithms are focused on hiding a single image in other image with an intention of increasing the PSNR to get the quality stego image. But going forward and exploring the steganography algorithms, it is observed that steganography not only means to hide an information indirectly it is a compression algorithm also. With this idea, we are developing a steganographic algorithm to hide multiple images in a single image. By hiding multiple images in a single image, memory required to store a single image is sufficient. In this work, we have proposed a new Hybrid technique algorithm consisting of DWT and LSB techniques for hiding multiple images.

IV. PROBLEM DEFINITION

A. Problem Statement

From the above discussions and survey, it is evident that visible encrypted messages draw the attention of the intruder. This provokes intruders to decrypt the cipher text. However, by embedding the message or information into an image, it is hard to draw the attention of others i.e., whether it is containing any secret information or not as the processed image and original image looks similar in naked eye. This will make the message more secure. But with the development of technology, paperless work has been increased drastically and the digitized information need to be stored securely is a challenging task. Image steganography hides one image in another image so that the memory required store one image is sufficient to save two images. Thus, security can be increased using steganography for digitized information with less storage space.

B. Objectives

PSNR is one of the important parameters in deciding the quality of steganographic algorithm. Higher the value of PSNR more secure the secret image. In this work, we have focused on security of the information in an image.
The objectives of the work are:

- To hide multiple images in a single image.
- To get an acceptable PSNR value.

C. Assumption

- Size of secret images is less than or equal to one fourth of the cover image.
- Size of the Cover image is M x M *i.e.*, square image

V. PROPOSED MODEL

The proposed method is to embed multiple images in a single image using hybrid domain steganography such that only authorized person have access to hidden data. In this work, three secret images are hidden in a single cover image. Prerequisite is that all secret images and cover image are color images and secret images size should be half of the cover image. Image is divided into MSB and LSB in which MSB of the image gives maximum information and LSB is used for data hiding. Image is transformed from spatial domain to frequency domain by applying DWT technique. The generated coefficients from DWT are modified to embed secret images.

The proposed method uses Discrete Wavelet Transforms and LSB Technique to encode multiple key images in a single cover image. Red, Green and Blue planes are extracted from the cover image and key images. Each plane of cover image is decomposed into four sub-bands namely, LL, LH, HL and HH using DWT technique. The extracted R-plane of secret images are then embedded into LH, HL and HH sub-bands of R plane of cover image using LSB technique. LL Sub-band contains the significant information of the image and not used for embedding secret image. Next, IDWT is applied on all the four bands to get a stego image in spatial-domain.

To retrieve the secret images from the stego image, first stego image is decomposed into Red, Green and Blue planes and DWT is applied to get the four sub-bands as discussed earlier. Later by using LSB technique secret images are retrieved.

Two metrices such as, embedded rate or data capacity and PSNR are used to validate the quality of the images before and after embedding process. The block diagram for embedding multiple key images into a single cover image is shown in Fgure 1 and extracting secret images from stego image is shown in Figure 2.

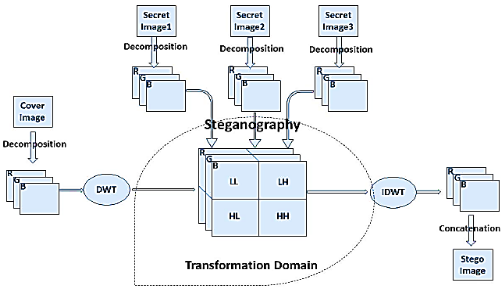


Fig 1: Embedding Process using Hybrid Domain Steganography

The proposed embedded and retrieval process are discussed in the following subsections.

A. Embedded Process

For embedding secret images in cover image, it is assumed that, secret images should be less than or equal to one fourth of the cover image. Single level decomposition of DWT is applied on a cover images to get four sub bands. The first sub-band contains the maximum information of cover image and other three sub bands contains just an attribute of the image and can be ignored. These bands which can be ignored are considered for hiding secret images.

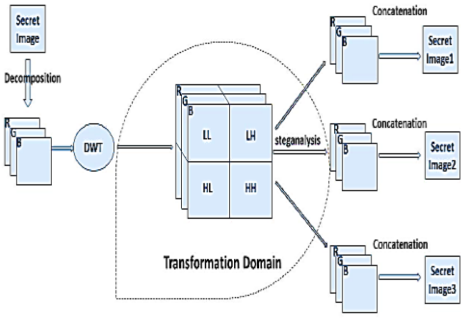


Fig 2: Decryption Process using Hybrid Domain Steganography

The cover image represented by

$$X(i,j) = \begin{bmatrix} X(0,0) & X(0,1) & \cdots\cdots & X(0,N-1) \\ X(1,0) & X(1.1) & \cdots\cdots & X(1,N-1) \\ \vdots & \vdots & & \vdots \\ X(M,0) & X(M,1) & \cdots\cdots & X(M-1,N-1) \end{bmatrix}$$

Here M = N

The key images A, B and C are represented by

$$A(m,n) = \begin{bmatrix} A(0,0) & A(0,1) & \cdots\cdots & A(0,K-1) \\ A(1,0) & A(1.1) & \cdots\cdots & A(1,K-1) \\ \vdots & \vdots & & \vdots \\ A(L,0) & A(L,1) & \cdots\cdots & A(L-1,K-1) \end{bmatrix}$$

Here K = L

Similarly, other two key images $B(m,n)$ and $C(m,n)$ are represented.

Single level decomposition is applied to cover image using DWT to get the sub-bands LL, LH, HL and HH. Among these LH, HL and HH bands values are first converted to UNM between 0 to 255 i.e., 8 bits (1 byte). Lower nibble of each byte is replaced by upper nibble of the key image. Once the embedding process is done IDWT is applied on LL and other three updated sub bands to get the stego image in spatial-domain.

Different sub-bands coefficients of a cover image in transformation domain after applying DWT are represented by

$$\hat{X}(i,j) = \begin{cases} \widehat{X_1}(m,n) \cdots LL\ band \\ \widehat{X_2}(m,n) \cdots LH\ band \\ \widehat{X_3}(m,n) \cdots HL\ band \\ \widehat{X_4}(m,n) \cdots HH\ band \end{cases}$$

Embedding key/secret images into all the sub-bands except LL involves bit wise operation. Image contains R, G and B planes. For all the planes same bit wise operation is performed which is given by

$$f(m,n) = bitand\ (f(m,n), XX)$$
$$g(m,n) = bitshift(g(m,n), Y)$$
$$g(m,n) = bitand(g(m,n), ZZ)$$
$$h(m,n) = bitor(f(m,n), g(m,n))$$

where,

$f(m,n)$ is planes of sub-bands

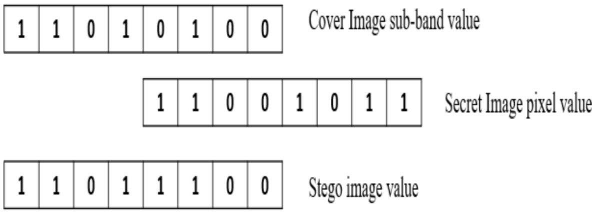
$g(m,n)$ is planes of key image

$h(m,n)$ is sub-band with embedded information

XX, ZZ are 8-bit UNM (Unsigned Number)

Y is an integer

Pictorial representation of embedding process is shown in Figure 3.



1 1 0 1 0 1 0 0 Cover Image sub-band value

1 1 0 0 1 0 1 1 Secret Image pixel value

1 1 0 1 1 1 0 0 Stego image value

Fig 3: Embedding Process in Single Pixel Value

Sub-band coefficents after hiding data in transformation domain can be represented by

$$\left.\begin{array}{l}\widehat{X_1}(m,n)\cdots LL\ band\\ \widehat{Y_2}(m,n)\cdots LH\ band\\ \widehat{Y_3}(m,n)\cdots HL\ band\\ \widehat{Y_4}(m,n)\cdots HH\ band\end{array}\right\} = \hat{Y}(i,j)$$

Applying IDWT to get the image in spatial domain is the stego image represented by

$$Y(i,j) = \begin{bmatrix} Y(0,0) & Y(0,1) & \cdots\cdots & Y(0,N-1) \\ Y(1,0) & X(1.1) & \cdots\cdots & Y(1,N-1) \\ \vdots & \vdots & & \vdots \\ Y(M,0) & X(M,1) & \cdots\cdots & Y(M-1,N-1) \end{bmatrix}$$

B. Decryption Process

For decrypting or recovering key images from stego image, reverse operation is performed on stego image. A DWT is performed on stego image to get sub bands. Except LL band other three bands are converted to UNM between 0 to 255 *i.e.*, 8 bits (1 byte). upper nibble and lower nibble contain the information of cover and secret key images respectively. These nibbles are separated from stego image, upper nibble is appended with zeros for its lower nibble. And separated lower nibble is shifted left by four values and append with four zeros to get key images as shown in Figure 4. The gray color in the Figure 4 shows the appended zeros.

Different sub-bands coefficients of a stego image in transformation domain after applying DWT are represented by

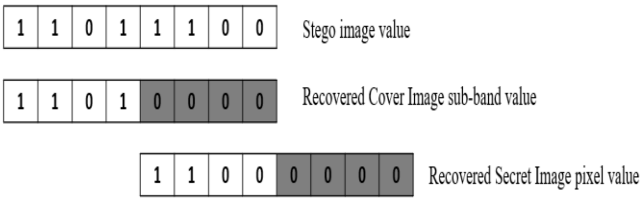
$$\hat{Y}(i,j) = \left\{\begin{array}{l}\widehat{Y_1}(m,n)\cdots LL\ band\\ \widehat{Y_2}(m,n)\cdots LH\ band\\ \widehat{Y_3}(m,n)\cdots HL\ band\\ \widehat{Y_4}(m,n)\cdots HH\ band\end{array}\right.$$

Decrypting secret images from all the sub-bands except LL involves bitwise operation. For all the planes same bit wise operation is performed and given by

$$\hat{h}(m,n) = bitshift\ (\hat{h}(m,n), X)$$
$$\hat{g}(m,n) = bitand(\hat{g}(m,n), YY)$$

where,
$\hat{h}(m,n)$ is sub-band with embedded information
$\hat{g}(m,n)$ is the recovered key image
X is an integer
YY is 8-bit UNM (Unsigned Number)

Pictorial representation of embedding process is shown in Figure 4.



1	1	0	1	1	1	0	0	Stego image value
1	1	0	1	0	0	0	0	Recovered Cover Image sub-band value
1	1	0	0	0	0	0	0	Recovered Secret Image pixel value

Fig 4: Decryption Process from a Single Pixel Value

C. Algorithm

Embedding and extraction process of multiple secret image into a cover image are discussed in algorithm 1 and 2 respectively.

```
Algorithm 1: Embedding Secret Images
Step 1:  Read Cover image and secret images of size M x
         M and M/2 x M/2 respectively
Step 2:  Decompose Cover image in to its RGB planes.
Step 3:  Decompose Secret images in to its RGB planes.
Step 4:  Perform DWT on Cover image RGB planes to get
         Approximate (LL), horizontal (LH), vertical
         (HL) and diagonal (HH) sub bands. So that for
         every plane four sub-bands in
         Transformation-domain are obtained
Step 5:  Resize the RGB planes of secret image as
         required.
Step 6:  Replace LSB of R plane horizontal sub band by
         MSB of R plane of secret image 1
Step 7:  Replace LSB of R plane vertical sub band by
         MSB of R plane of secret image 2
Step 8:  Replace LSB of R plane diagonal sub band by
         MSB of R plane of secret image 3
Step 9:  Repeat steps 6 to 8 for G and B planes
Step 10: Perform IDWT to get new RGB planes
Step 11: Combine all the planes to get a new stego image.
```

```
Algorithm 2: Extracting Secret Images
Step 1:  Read Stego image.
Step 2:  Decompose stego image in to its RGB planes.
Step 3:  Perform DWT on stego image RGB planes to get
         approximate, horizontal, vertical and diagonal
         sub-bands. So that for every plane, four
         sub-bands in Transformation-domain are
         obtained.
Step 4:  Extract LSB of each R plane sub-bands of secret
         image to get R planes of secret images
Step 5:  Extract LSB of Each G plane sub-bands of secret
         image to get G planes of secret images
Step 6:  Extract LSB of each B plane sub-bands of secret
         image to get B planes of secret images
Step 7:  Combine RGB planes separately to get key
         images
```

Different cases can be performed on steganography technique for hiding key image in cover image and the case employed in this work is shown in Figure 5(a) and Figure 5(b) as a flow chart.

Figure 5(a) represents the flow diagram and the process of proposed algorithm for embedding multiple images in a single image. Similarly, Figure 5(b) represents the flow diagram and the procecss of proposed algorithm for recovering key images from stego image. Both the process involves spatial and transformation domains.

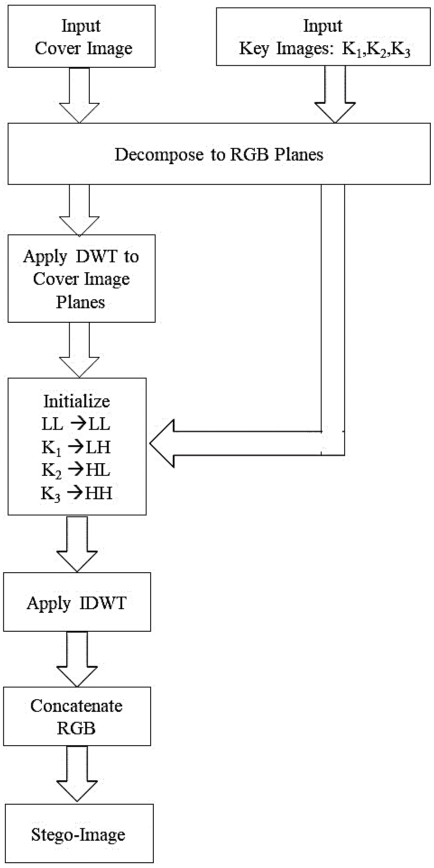


Fig 5(a): Embedding Multiple Images using DWT and LSB Technique

VI. PERFORMANCE EVALUATION

A. Performance Metrics

Hiding Capacity or embedded rate (ER): It is the maximum amount of key information that can be hidden in an embedded cover image and is represented in number of bits or bytes given by,

$$ER = \frac{K}{M \times N} \text{ bpp}$$

Where,

K : Total number of bits embedded
M = N : Size of cover image

Mean Square Error (MSE): It is the square of error between cover image and stego image and is calculated by

$$MSE = \frac{1}{M \times N} \sum_{1,j=1}^{M,N} (X(i,j) \; - \; Y(i,j))^2$$

Where,

$X(i,j)$: Cover pixel value
$Y(i,j)$: Stego pixel value
M=N : Size of the image

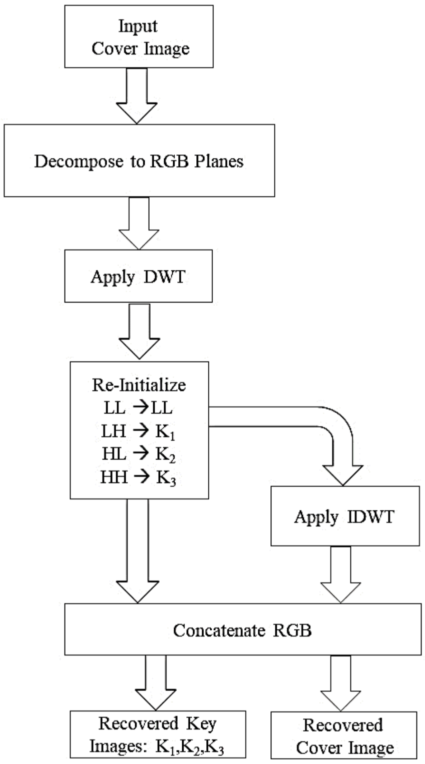


Fig 5(b): Recovering Multiple Key Images and Cover Image from the Stego-Image

Peak Signal to Noise Ratio (PSNR): It is the peak signal to noise ratio used to determine the quality of the image before and after steganography. The acceptable value of PNSR for a typical 8 bit image is 30 to 50 dB and is given by

$$PSNR = 20.log_{10}(Max_I) - 10.log_{10}(MSE)$$

Histogram(H): Histogram represents the tonal distribution in an image *i.e.,* graphical representation of number of pixels in an image at different graylevels.

Entropy (E): Entropy is the measure of uncertainty or randomness of an image given by

$$E(I) = \sum P_i log_2 \frac{1}{P_i}$$

B. Performance Analysis

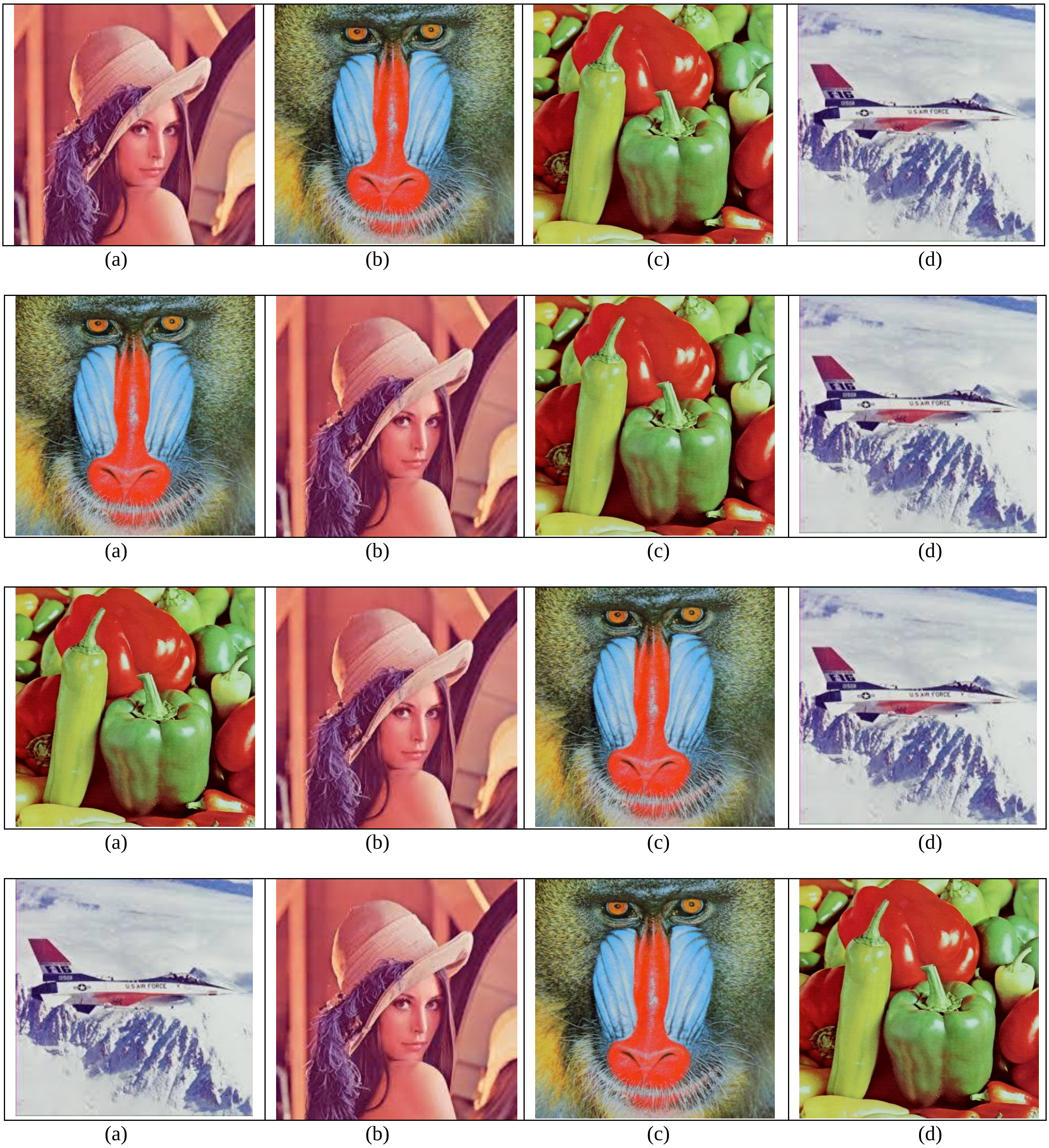
For the performance analysis, the images named Lena, Mandril, Peppers and Jet are considered as shown in Figure 6. The embedding process is performed by hiding three images in another image. The performance parameter such as hiding capacity, MSE and PSNR is calculated.

Hiding Capacity for a regular 512*x*512 gray scale cover image of 8-bit pixel and a secret image of size 256*x*256 with 8-bit pixel, the embedded rate or hiding capacity is 0.375, 0.468, 0.5625 bpp (depending on the number of bits used to embedded in cover image).

MSE and PSNR for different images is computed and tabulated in the results. Higher the hiding capacity inturn decreases the PSNR value. PSNR is maintained around 38 dB in the proposed algorithm. Histogram of both cover image and stego image is calculated and represented in graphical way.

Both histograms looks similar in pattern ensuring that even after modification to cover image to get stego image both looks like identical.

Difference in the Entropy of Cover Image and Stego image is calculated to know the deviation of information.


(a) (b) (c) (d)

(a) (b) (c) (d)

(a) (b) (c) (d)

(a) (b) (c) (d)

Fig 6 (a): Cover Image, (b) Key Image1, (c) Key Image2, (c) Key Image3

Images used for the experimental purpose are shown in Figure 6. Figure 6(a) is the cover image with size M x N and 6(b-d) are key images of size M/2 x N/2. When one image is used as cover image other three images are used as key images.

VII. RESULTS

The algorithm proposes a secure image steganography technique for embedding multiple secret images in a cover image using a hybrid domain technique comprising of DWT-LSB algorithm. The proposed algorithm is developed using m-scripts and performed on standard set of images. Higher the PSNR value data recovered is more, hence PSNR value of key image is also calculated in the proposed algorithm. For different embeded rate and number of images hidden, the PSNR value is tabulated in the Tables 1 to Table 5 with difference in entropy for hiding 3 images.

For different cover images and secret images the PSNR calculated is given in Table 1 to Table 4 and PSNR for multiple images is shown in
Table 5.

Table- I: PSNR Obtained for Lena Image for Hiding Single Key Image with Different ER

Lena Image			
Secret/Key image	*PSNR of cover image in dB*	*PSNR of Secret image in dB*	*Embedded Rate in bpp*
Pepper	40.5605	29.3239	0.125
Jet	36.3193	29.208	0.125
Mandril	39.1067	29.1183	0.125
Pepper	35.4641	34.3638	0.25
Jet	32.4918	39.6165	0.25
Mandril	34.616	35.1469	0.25

Table- II: PSNR Obtained for Pepper Image for Hiding Single Key Image with Different ER

Pepper Cover Image			
Secret/Key image	*PSNR of cover image in dB*	*PSNR of Secret image in dB*	*Embedded Rate in bpp*
Lena	39.8843	28.9086	0.125
Jet	36.5017	28.9466	0.125
Mandril	39.2944	28.9125	0.125
Lena	35.3859	34.8076	0.25
Jet	32.8793	36.1076	0.25
Mandril	35.0984	34.1932	0.25

Table-III: PSNR Obtained for Jet Image for Hiding Single Key Image with Different ER

Jet Cover Image			
Secret/Key image	*PSNR of cover image in dB*	*PSNR of Secret image in dB*	*Embedded Rate in bpp*
Lena	39.6796	28.9883	0.125
Pepper	40.5537	29.2924	0.125
Mandril	39.1127	29.0539	0.125
Lena	34.8982	35.8968	0.25
Pepper	35.4675	34.7601	0.25
Mandril	34.6374	35.8439	0.25

Table- IV: PSNR Obtained for Mandril Image for Hiding Single Key Image With Different ER

Mandril Cover Image			
Secret/Key image	*PSNR of cover image in dB*	*PSNR of Secret image in dB*	*Embedded Rate in bpp*
Lena	39.008	28.9883	0.125
Pepper	39.7559	29.2654	0.125
Jet	35.9955	29.2323	0.125
Lena	33.9493	35.1186	0.25
Pepper	34.3685	34.5115	0.25
Jet	32.0938	39.5985	0.25

Table-V: PSNR and Difference in Entropy Obtained for Hiding Three Key Image With ER = 0.375

Hiding three images for ER = 0.375				
Cover Image	*PSNR in dB*	*Secret Image*	*PSNR in dB*	*Diff in Entropy*
Lena	33.4955	Pepper	29.391	0.0325
		Jet	29.111	
		Mandril	29.178	
Pepper	33.7105	Lena	29.13	0.0284
		Jet	28.844	
		Mandril	29.097	
Jet	33.9841	Lena	29.15	0.1609
		Pepper	23.461	
		Mandril	29.247	
Mandril	31.8817	Lena	29.047	0.0092
		Pepper	29.355	
		Jet	29.078	

Histogram of cover image and stego image obtained for hiding multiple images are represented in Figure 7 (a-d). Histogram shows the pixel distribution of image before and after steganography.

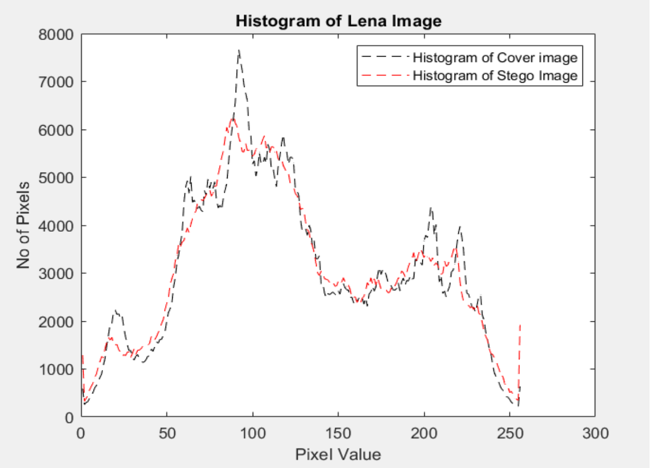


Fig 7(a): Histogram of Lena Image Before and After Hiding Multiple Images

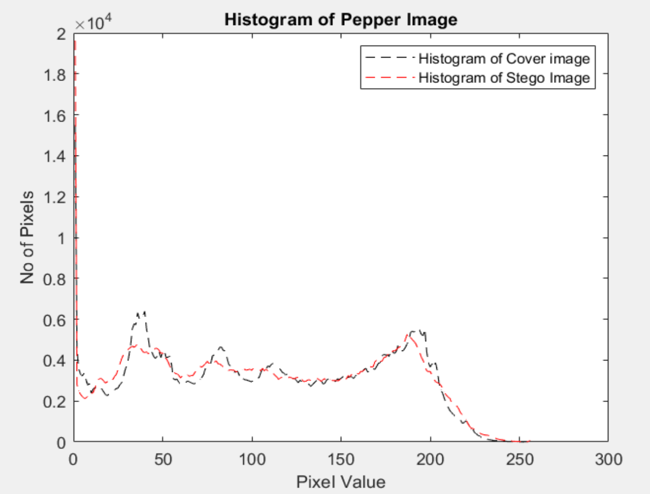


Fig 7(b): Histogram of Pepper Image Before and After Hiding

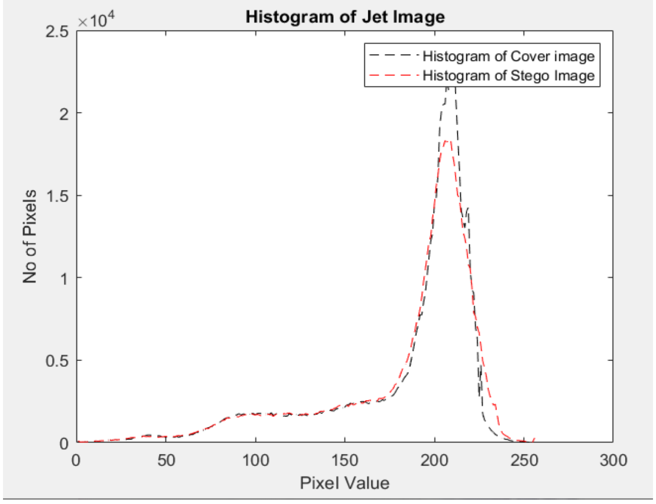


Fig 7(c): Histogram of Jet Image Before and After Hiding Multiple Images

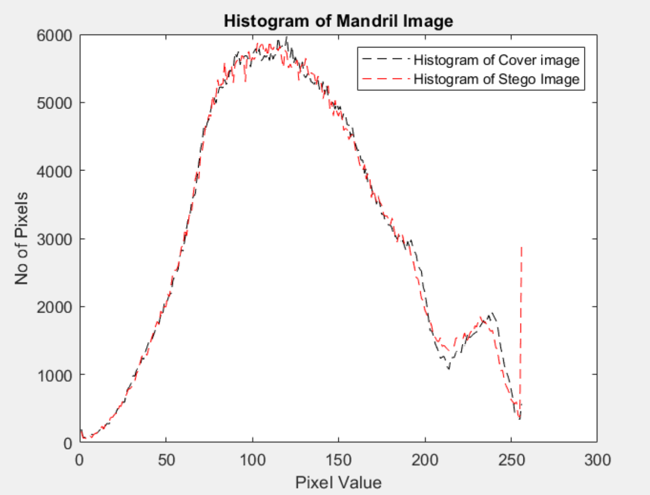


Fig 7(d): Histogram of Mandril Image Before and After Hiding Multiple Images

VIII. CONCLUSION

Multiple secret images are embedded into a single image and PSNR for cover and secret images in the proposed algorithm is in acceptable range. the algorithm is proposed for data security and to reduce the storage capacity with a acceptable PSNR value between 29 to 32. Memory required to store four images in database now can be replaced by a single image by reducing the memory as well securing the data.

REFERENCES

1. L. Guo, J. Ni, and Y. Shi, “Uniform Embedding for Efficient JPEG Steganography," IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, pp.814-825, 2014.
2. V. Sedighi, R. Cogranne and J. Fridrich, “Content-Adaptive Steganography by Minimizing Statistical Detectability", IEEE Transactions on Information Forensics and Security, vol.11, no. 2, pp. 221-234, 2016.
3. M. Sadek, A. Khalifa, M. Mostafa, “Video Steganography: a Comprehensive Review," Multimedia Tools and Applications, vol. 74, no. 17, pp. 7063- 7094, 2015.
4. A. Ker, “Batch Steganography and Pooled Steganalysis," In Information Hiding, 8th International Workshop, vol. 4437, pp. 265- 281, 2006
5. T. Pevný and I. Nikolaev, “Optimizing Pooling Function for Pooled Steganalysis," in Proceedings of IEEE InternationalWorkshop on Information Forensics and Security, pp.1-6, 2015
6. A. Ker and T. Pevný, “Batch Steganography in The Real World," in Proceedings of 14th ACM Workshop Multimedia Security (MM&Sec), pp.1-10, 2012.
7. VikasVerma, Poonam Rishma and Chawla, “An Enhanced Least Significant Bit Steganography Method using Midpoint Circle Approach,” International Conference on Communications and Signal Processing, pp. 105-108, 2014.
8. ShaluGarg and Monika Mathur, “Chaotic Map Based Steganography of GrayScale Images in Wavelet Domain,”International Conference on Signal Processing and Integrated Networks, pp. 689 – 694, 2014.
9. Yinan Wang, Weirong Chen, Yue Li, Wei Wang and Chang Tsun Li, “HPS: Histogram Preserving Steganography in Spatial-Domain,” International Workshop on Biometrics and Forensics, pp. 1 – 4, 2014.
10. Prabakaran G,Bhavani R, S Sankaran, “Dual Wavelet Transform in Color Image Steganography Method,” International Conference on Electronics and Communication Systems, pp. 1 -6, 2014.
11. Bingwen Feng, Wei Lu and Wei Sun, “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture,”IEEE Transactions on Information Forensics and Security,pp. 243-255, 2014.
12. Aayushi Verma,Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, “Implementation of Image Steganography Using 2-Level DWT Technique”, International Journal of Computer Science and Business Informatics, ISSN: 1694- 2108, vol. 1, no. 1. may 2013.
13. Elshazly Emad, Abdelwahab Safey, “A Secure Image Steganography Algorithm Based on Least Significant Bit and Integer Wavelet Transform”, IEEE Journal of Systems Engineering and Electronics, Vol. 29, No. 3, pp. 639 – 649, June 2018.
14. Linjie Guo, Jiangqun Ni and Yun Qing Shi, “Uniform Embedding for Efficient JPEG Steganography”, IEEE transactions on information forensics and security, vol. 9, no. 5, may 2014.
15. X. Zhang, F. Peng and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification", *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, 2018.
16. N Sathisha, K Suresh Babu, K B Raja and K R Venugopal, “Image Steganography Based on Mantissa Replacement using LWT”, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 4 no. 2, pp 457-465, February 2015.
17. Andrew D. Ker Tomas pevny, “Batch steganography in the real world” *Multimedia and Security’12*, pp 1-10, 2012
18. F. Li, K. Wu, X. Zhang, J. Yu, J. Lei and M. Wen, "Robust Batch Steganography in Social Networks with Non-Uniform Payload and Data Decomposition", *IEEE Access*, vol. 6, pp. 29912- 29925, 2018.

AUTHORS PROFILE

Shashikiran B S., Research Scholar at Visvesvaraya technological University. He obtained his M.Tech in Bio-Medical Signal Processing and Instrumentation from R V College of engineering, Bangalore and B.E. from UBDT college of Engineering, Davanagere. He has over 6 years of teaching experience and 2 years of Industry experience. He also work as technical freelancer at Banglore

Dr. Shaila K, Processor in Department of Electronics and Communication and was the Head of the Department, Vivekananda Institute of Technology. She obtained her Ph. D in Computer Science and Engineering from Bangalore University, M.E in Electronics and Communication from University Visvesvaraiah College of Engineering, Bangalore University and B.E from PES Institute of Technology, Bangalore University, Bangalore. She has over twenty years of teaching experience. She has authored Digital Circuits and Systems published by Tata McGraw Hill, New Delhi and Secure Data Communication Techniques by LAP LAMBERT publishers, Germany. She has published papers in refereed International Journals and International Conferences. She has received Best Teacher and Best Researcher Award. Her name appears in Marquis Who’s Who in the World Science and Engineering. She is the Life member of ISTE, iMAPs, Member of ACM, IEANG and reviewer for conference and journals. Her research areas include Wireless Sensor Networks, Adhoc Networks and Image Processing.

Dr. Venugopal K. R., Vice Chancellor, Bangalore University. He has Eleven Degrees with Ph.D. in Computer Science Engineering from IIT-Madras, Chennai and another Ph.D. in Economics from Bangalore University. He has degrees in Law, Mass Communication, Electronics, Economics, Business Finance, Computer Science, Public Relations and Industrial Relations. He has authored and edited 64 books and published more than 700 papers in refereed International Journals and International Conferences. He has supervised 630 M.E. dissertations, 25 Ph.Ds and filed 101 Patents. He was a Post Doctoral Research Scholar and a visiting Professor at University of Southern California, USA. He has been conferred Fellow of IEEE, USA and ACM Distinguished Educator for contributions to Computer Science Engineering and Electrical Engineering Education.