An Efficient Data Security System Using Reserve Room Approach on Digital Images for Secret Sharing

Mrs.V.P.Kavitha (Asst. professor, Dept. of ECE in Velammal Engineering College) M.Suganya, K.Suganya, G.Sridevi, D.Suganya (Dept. of ECE in Velammal Engineering College)

Abstract**—** This paper presents enhancement of data protection system for secret communication through common network based on reversible data concealment in encrypted images with reserve room approach. In this paper was implemented for true color RGB image and reserve room approach under multi scale decomposition. The Blue plane will be chosen for hiding the secret text data. Then image is then separated into number of blocks locally and lifting wavelet will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption method. The proposed encryption technique uses the key to encrypt an image and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After image encryption, the data hider will conceal the secret data into the detailed coefficients which are reserved before encryption. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using a symmetric key method. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into the encrypted image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted pixels to extract the data. By using the decryption keys, the image and extracted text data will be extracted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

Index Terms**—***Reversible data hiding, Lifting wavelet transform, chaos encryption, Adaptive LSB replacement*

*****

I. INTRODUCTION

Reversible data hiding is a process in which original cover image can be losslessly recovered without any loss after the embedded message is recovered. This technique is widely used in secrete data communication in defense, research institute, Medical information protection. Here data and the original cover image will be recovered without any loss.

In [1] to overcome the drawbacks of Reversible Data Hiding Kalker and willems introduced a recursive code construction, which does not reach the expected bounds. In [2] Zhang improved recursive code construction by designing a data embedding for all zero-covers and a more efficient compression algorithm, it reaches the average bound.

In [3] Tian's difference expansion technique is a high capacity, reversible method for data embedding. In this method he improved the redundancy in digital images in order to achieve very high embedding capacity, and keeps the distortion low.

The above method suffers from undesirable distortion at low embedding capacity. To overcome this problem Thodi [4] introduced a technique called Prediction- error expansion. His new technique better exploits the correlation inherent in the neighborhood of a pixel than the difference expansion scheme. To avoid the drawbacks of PEE [5] Yang and Zeng further investigated the PEE they proposed a two new strategies named, adaptive embedding and pixel expansion. Unlike conventional PEE which embeds data uniformly they proposed to adaptively 1 or 2 bits into expandable pixel according to the local complexity. This avoids expanding pixels with large prediction-errors, and thus, it reduces embedding impact by decreasing the maximum modification to pixel values.

In [6], Zeng proposed a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image. Thus Good performance is observed both theoretically and experimentally.

In [7], Zhang partitioned an encrypted image into blocks, and each block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data extraction and image recovery can be achieved by examining the block smoothness. This process can be realized with the help of spatial correlation in decrypted image. Hong and Chen [8] Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction, but this method adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work.

In the above two methods, the data extraction depends on the image decryption but in [9], Zhang proposed a method, in that the image is encrypted by the content owner by using encryption key. The data hider can hide the data in the encrypted image to obtain the space to hide the data by using data hiding key. At the receiver side the data can be retrieved using the data hiding key by decrypting an image.

The above two methods are used to "vacate the room after encryption. However, since the entropy of encrypted images has been maximized, [8]-[9] or generate marked image with poor quality for large payload But the encrypted image unchanged still it is decrypted using the encryption key. The receiver who has both the encryption and data hiding keys can access the data embedded as well as the original image. In [10], Kede Ma and Zhang, in which they first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data.

This paper is organized in the following manner. Section II briefly introduces previous methods proposed in [8]–[9]. The novel method is elaborated in Section III followed by Section IV. The paper is concluded in Section

II. PREVIOUS ARTS

The methods proposed in [8]-[9] can be summarized as the framework.

Hong and Chen [8] Zhang's work did not fully exploit the pixels in calculating the smoothness of each block and did not consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction, but this method adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits. The experimental results reveal that the proposed method offers better performance over Zhang's work.

In the above two methods, the data extraction depends on the image decryption but in [9], Zhang proposed a method, in that the image is encrypted by the content owner by using encryption key. The data hider can hide the data in the encrypted image to obtain the space to hide the data by using data hiding key. At the receiver side the data can be retrieved using the data hiding key by decrypting an image.

The above two methods are used to “vacate the room after encryption. However, since the entropy of encrypted images has been maximized, [8]-[9] or generate marked image with poor quality for large payload But the encrypted image unchanged still it is decrypted using the encryption key. The receiver who has both the encryption and data hiding keys can access the data embedded as well as the original image. In [10], Kede Ma and Zhang, in which they first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data.

III.PROPOSED METHOD

The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in encrypted images with reserve room approach. To preserve an image quality during image recovery, reserving room approach is used to reserve space for embedding a privacy text messages. Here, chaos encryption is used to scramble an image except reserved space to make protection of image details during transmission. After an encryption, the data hider will conceal the encrypted secret data into the reserved coefficients using adaptive LSB replacement algorithm. Finally, image and hidden text will be recovered without any loss based same methods which are used at embedding stage.

A. Introduction to Wavelet:

Over the past several years, the wavelet transform has gained widespread acceptance in signal processing in general and in image compression research in particular. In applications such as still image compression, discrete wavelets transform (DWT) based schemes have outperformed other coding schemes like the ones based on DCT. Since there is no need to divide the input image into non-overlapping 2-D blocks and its basis functions have variable length, wavelet-coding schemes at higher compression ratios avoid blocking artifacts . Because of their inherent multi -resolution nature, wavelet-coding schemes are
especially suitable for applications where scalability and tolerable

degradation are important. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT.

Basically we use Wavelet Transform (WT) to analyse non-stationary signals, i.e., signals whose frequency response varies in time, as Fourier Transform (FT) is not suitable for such signals. To overcome the limitation of FT, Short Time Fourier Transform (STFT) was proposed. There is only a minor difference between STFT and FT. In STFT, the signal is divided into small segments, where these segments (portions) of the signal can be assumed to be stationary. For this purpose, a window function "w" is chosen. The width of this window in time must be equal to the segment of the signal where it is still be considered stationary. By STFT, one can get time-frequency response of a signal simultaneously, which can’t be obtained by FT.
The short time Fourier transform for a real continuous signal is defined as:

$$\text{X (f, t)} = \int_{-\infty}^{\infty} [x(t) w\,(t-\tau) *] e^{-2j\pi f\, t} \text{dt}$$

Where the length of the window is (t-τ) in time such that we can shift the window by changing value of t and by varying the value τ we get different frequency response of the signal segments. The Heisenberg uncertainty principle explains the problem with STFT. This principle states that one cannot know the exact time-frequency representation of a signal, i.e., one cannot know what spectral components exist at what instances of times. This type of problem is called resolution problem. This problem has to do with the width of the window function that is used, known as the support of the window. If the window function is narrow, then it is known as compactly supported. The narrower we make the window, the better the time resolution, and better the assumption of the signal to be stationary, but poorer the frequency resolution:

- Narrow window ===> good time resolution, poor frequency resolution
- Wide window ===> good frequency resolution, poor time resolution

The wavelet transform (WT) has been developed as an alternate approach to STFT to overcome the resolution problem. The wavelet analysis is done such that the signal is multiplied with the wavelet function, similar to the window function in the STFT, and the transform is computed separately for different segments of the time-domain signal at different frequencies. This approach is called Multi-resolution Analysis (MRA) [4], as it analyzes the signal at different frequencies giving different resolutions.

MRA is designed to give good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies. This approach is good especially when the signal has high frequency components for short durations and low frequency components for long durations, e.g., images and video frames. The wavelet transform involves projecting a signal onto a complete set of translated and dilated versions of a mother wavelet Ψ(t). The strict definition of a mother wavelet will be dealt with later so that the form of the wavelet transform can be examined first. For now, assume the loose requirement that Ψ(t) has compact temporal and spectral support (limited by the uncertainty principle of course), upon which set of basic functions can be defined. LWT decomposes the image into different subbands images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of subbands. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. LL subbands contains the significant part of the spatial domain image.

BLOCK DIAGRAM:

FIGURE A: Encryption and Embedding:

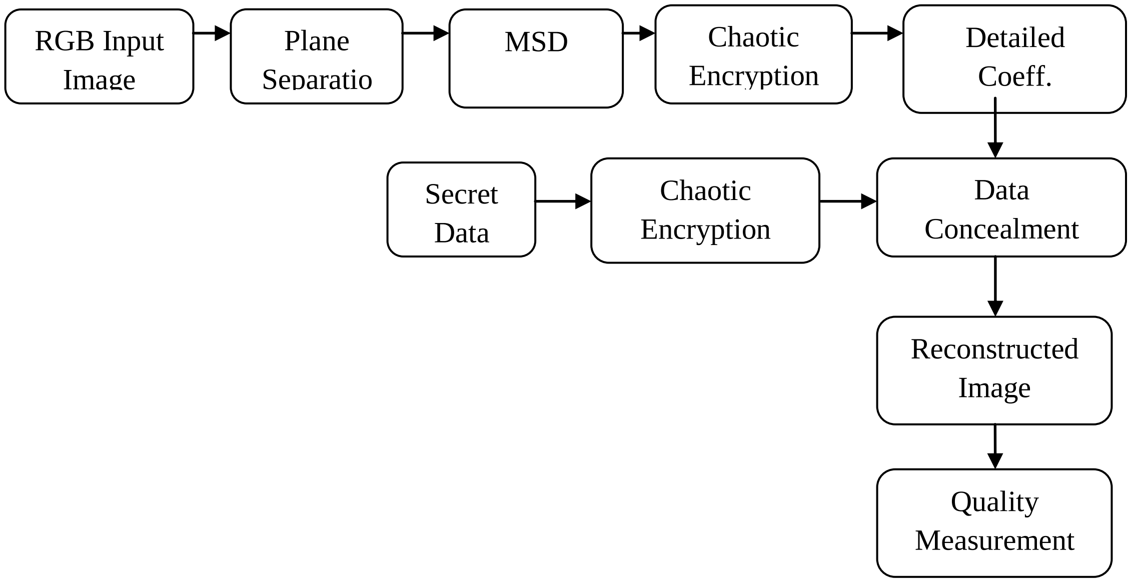


FIGURE B: Decryption and Data Extraction:

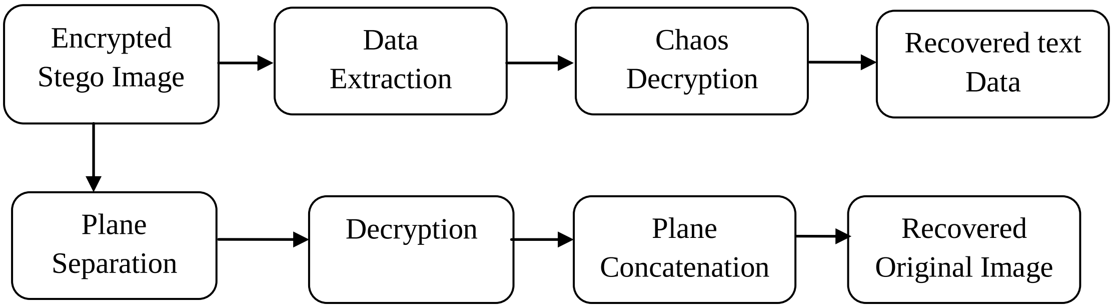


Figure (A).Framework: “Reserving the room for embedding and the image is encrypted”.

Figure (B).Framework: “Decryption for recovering the original image and data extraction”.

High-frequency sub band contains the edge information of input image. These coefficients are selected as reserved space foe hiding the text data. The secret text data is embedded into the wavelet coefficients of high frequency subbands because it is non sensitive to human visual system. The basis set of wavelets is generated from the mother or basic wavelet is defined as:

$$\Psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \quad ;$$

Where a, b $\in \Re$ and a>0

The variable 'a' (inverse of frequency) reflects the scale (width) of a particular basis function such that its large value gives low frequencies and small value gives high frequencies. The variable 'b' specifies its translation along x-axis in time. The term 1/$\sqrt{a}$ is used for normalization.

***B.2-D Transform*:**

The 1-D DWT can be extended to 2-D transform using separable wavelet filters. With separable filters, applying a 1-D transform to all the rows of the input and then repeating on all of the columns can compute the 2-D transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. As depicted in Figure 3.2(c), the four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass or high pass filter to the rows, and the second letter refers to the filter applied to the columns.

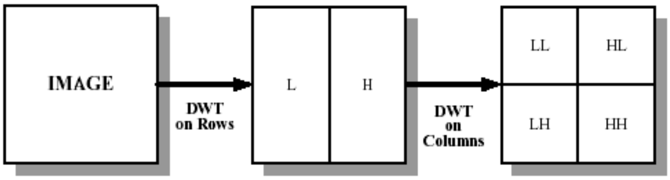


Figure 2 Block Diagram of DWT (a) Original Image (b) Output image after the 1-D applied on Row input (c) Output image after the second 1-D applied on row input.

The Two-Dimensional DWT (2D-DWT) converts images from spatial domain to frequency domain. At each level of the wavelet decomposition, each column of an image is first transformed using a 1D vertical analysis filter-bank. The same filter-bank is then applied horizontally to each row of the filtered and sub sampled data. One-level of wavelet decomposition produces four filtered and sub sampled images, referred to as sub bands. The upper and lower areas of Fig. 3.3(b), respectively, represent the low pass and high pass coefficients after vertical 1D-DWT and sub sampling. The result of the horizontal 1D-DWT and sub sampling to form a 2D-DWT output image is shown in Fig.3.3(c). We can use multiple levels of wavelet transforms to concentrate data energy in the lowest sampled bands. Specifically, the LL sub band in fig 2.1(c) can be transformed again to form LL2, HL2, LH2, and HH2 sub bands, producing a two-level wavelet transform. An (R-1) level wavelet decomposition is associated with R resolution levels numbered from 0 to (R-1), with 0 and (R-1) corresponding to the coarsest and finest resolutions.

The straight forward convolution implementation of 1D-DWT requires a large amount of memory and large computation complexity. An alternative implementation of the 1D-DWT, known as the lifting scheme, provides significant reduction in the memory and the computation complexity. Lifting also allows in-place computation of the wavelet coefficients.

2-D transform hierarchy:

The 1-D wavelet transform can be extended to a two-dimensional (2-D) wavelet transform using separable wavelet filters. With separable filters the 2-D transform can be computed by applying a 1-D transform to all the rows of the input, and then repeating on all of the columns.

LL1	HL1
LH1	HH1

Fig. 2.1SubbandsLabelling Scheme for a one level, 2-D Wavelet Transform .

***C. Lifting wavelet computation*:**

In order to obtain an efficient wavelet computation, it is important to eliminate as many unnecessary computations as possible. A careful examination of the forward and reverse transformsshows that about half the operations either lead to data which are destroyed or are null operations (as in multiplication by 0).

The one-dimensional wavelet transform is computed by separately applying two analysis filters at alternating even and odd locations. The inverse process first doubles the length of each signal by inserting zeros in every other position, then applies the appropriate synthesis filter to each signal and adds the filtered signals to get the final reverse transform.

Forward Transform:

H = (Co-Ce); L = (Ce+H/2)

Where Co and Ce is the odd column and even column wise pixel values.

Step 1: Column wise processing to get H and L

Step 2: Row wise processing to get LL,LH,HL and HH, Separate odd and even rows of H and L, Namely, Hodd – odd row of H, Lodd -odd row of L, Heven- even row of H, Leven – even row of L.

LH = Lodd-Leven; LL = Leven + (*LH* / 2)

HH = Hodd – Heven; HL = Heven + (*HH* /2)

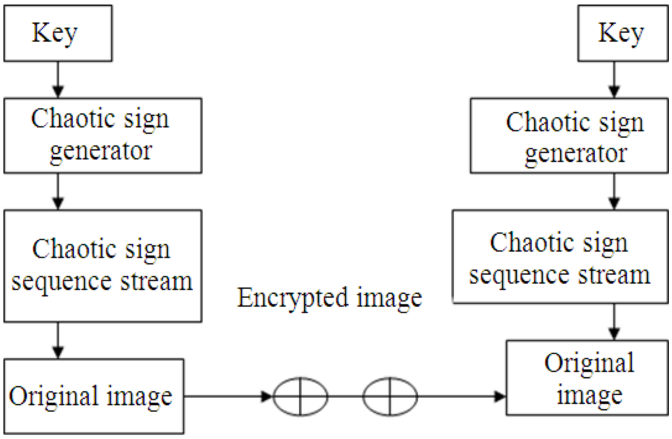
Reverse Lifting scheme:

Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

D. Image Encryption:

This method is one of the advanced encryption standard to encrypt the image for secure transmission .It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit XOR operation . Here logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The chaotic systems are defined on a complex or real number space called as boundary continuous space. Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression.

Chaotic Encryption Scheme:



The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is High level security. The encryption is achieved by iteration. Whereas the requirement of large cipher storage and slow in speed are considered the major disadvantages.

The properties of chaos are slightly producing some changes in the entire cryptography. Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches. The chaotic encryption method is proposed by (Baptista, 1998). It seems to be a much better encryption algorithm than traditional algorithms were used. We first identify the mapping scheme for a trajectory to encrypt the message. Subsequently decide the initial state and parameters for the key.
We assume the initial condition as the current route (trajectory). Iterate the chaotic equation until the path reaches the target site and then store the amount of iterations as a code for each message symbol. Encrypt the next message by iterating the recent trajectory. Produce the next cipher according it and so on.

Data hiding using LSB:

Image embedding Methods:

Three Data hiding methods will be explored:

- Least Significant Bit Insertion.
- Reversible Data Embedding using Difference Expansion.
- Reversible Data Hiding.

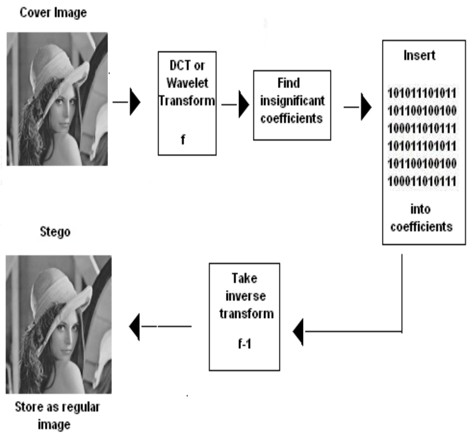
Maintain the secrecy of digital information when being communicated over the internet is presently a challenge. Given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on cipher-text. An ideal steganography technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message.

This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new steganalytic approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed steganalytic approach, bounds on estimation errors are developed.

Furthermore, the vulnerability of the new approach to possible attacks is also assessed, and counter measures are suggested. A detailed algorithm is presented along with results of its application on some sample images.

Let us see how to encode and decode the hidden data:

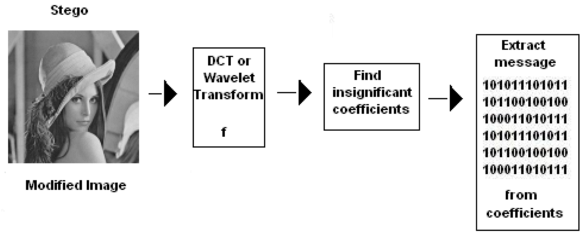
To Encode the Hidden Data:



1. Take the DCT or wavelet transform of the cover image
2. Find the coefficients below a certain threshold
3. Replace these bits with bits to be hidden (can use LSB Insertion)

4. Take the inverse transform
5. Store as regular image

To Decode the Hidden Data:



1.

Take the transform of the modified image.

2. Find the coefficients below a certain threshold.

3. Extract bits of data from these coefficients

4. Combine the bits into an actual message

Least significant bit insertion:

In random LSB insertion methods, a pseudo-random number generator is used to randomly distribute and hide the bits of a secret message into the least significant bits (LSBs) of the pixels within a carrier image, called the cover image. A popular approach to achieve this is the random interval method. Both communication parties share a stegokey, k usable as a seed for a random number generator. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. This is usually accomplished with two complementary techniques:

- Encryption of the message, so that who extracts it must also decrypt it before it makes sense.
- Randomizing the placement of the bits using a cryptographically random function (scattering), so that it's almost impossible to rebuild the message without knowing the seed for the random function.

In this way, the message is protected by two different keys, acquiring much more confidentiality than before. This approach protects also the integrity of the message, being much more difficult (we could say at least computationally infeasible) to counterfeit the message.

Simplified Example with a 24 bit pixel:

1 pixel:

(00100111 11101001 11001000)

Insert 101: (00100111 11101000 11001001)

(Red - Green - Blue)

Simplified Example with an 8 bit pixel:

1 pixel:

(00 01 10 11)

{White- red- green –blue}

Insert 0011:

(00 00 11 11)

{White-white-blue- blue}

Advantages of LSB Insertion:

A major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software developed which work around LSB color alterations via palette manipulation. LSB insertion also works well with gray-scale images.

LSB substitution:

The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 28=256 variations. The weighting configuration of an 8-bit number is illustrated in Figure 1.

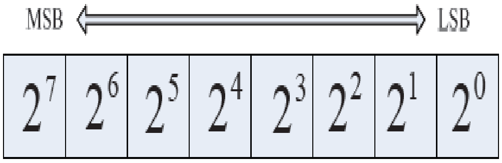


Figure 1. Weighting of an 8-bit pixel

The basic concept of LSB substitution is to embed the confidential data at the right most bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB method is: *x* represents the *i*th pixel value of the stego-image, *i x* represents that of the original cover-image, and *i m* represents the decimal value of the *i*th block in confidential data. The number of LSBs to be substituted is denoted as k. The extraction process is to copy the k-rightmost bits directly. Hence, a simple permutation of the extracted *i m* gives us the original confidential data. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

E.QUALITY MEASURES FOR IMAGE:

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE} = \sigma_q^2 = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image.

From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

F. Keys used in encryption and decryption:

Cryptography:

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the “key” in this case being the knowledge of the method being employed (security through obscurity). steganography books are filled with examples of such methods used throughout history. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern in hiding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. First we start with a few definitions.

Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a “key” the receiver can decode the encrypted message (decrypting) to retrieve the original message. Stenography improves on this by hiding the fact that a communication even occurred. The message m is imbedded into a harmless message c which is defined as the cover-object. The message m is then embedded into c, generally with use of a key k that is defined as the Stego-key.

Steganography:

Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the Stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible.

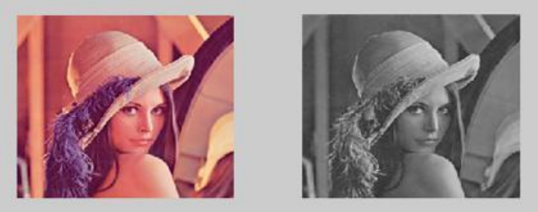
“*Steganography is the art of hiding information in ways that prevent the detection of hidden message*”.

Cryptography VS Steganography:

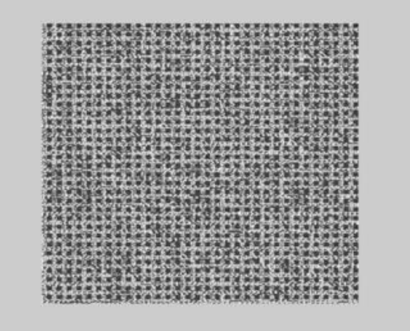
Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn’t vary even after the information is hidden. Information to be hidden + cover object = stego object. To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

Simulated result:

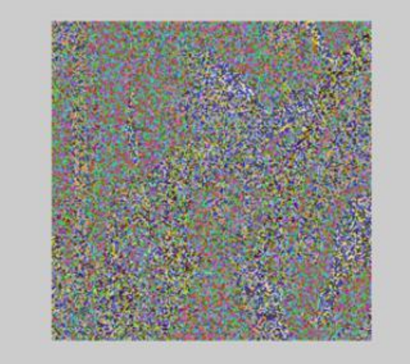
a) Original Image and its B Plane:



b) Reserved Spaces (Dark Region) using LWT :



c) Encrypted Image and its Recovery:



VI. Conclusion

The project presented that protection of image quality and hidden data during transmission based on approach of reserve room technique and chaotic crypto system with LSB based data concealment. Here, lifting wavelet transform was used to reserve space for concealing data effectively and chaos encryption was used as to protect image contents. This system was generated the stego image with less error under maximum data hiding capacity. Finally, the performance of system was evaluated with quality metrics such as error and SNR factor. It was better compatible approach and flexibility with better efficiency rather than prior method.

IV.REFERENCES

[1]. T. Kalker and F. M. Willems, “Capacity bounds and code constructions for reversible data-hiding,” in *Proc. 14th Int. Conf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.

[2].W. Zhang, B. Chen, and N. Yu, “Capacity-approaching codes for reversible data hiding,” in *Proc 13th Information Hiding (IH’2011), LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.

[3].J. Tian, “Reversible data embedding using a difference expansion,”
IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug. 2003.

[4].D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[5].X. L. Li, B. Yang, and T. Y. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec.2011.

[6].W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[7].X. Zhang, “Reversible data hiding in encrypted images,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[8].W. Hong, T. Chen, and H. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[9].X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEETrans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[10].Kede Ma, Weiming Zhang, Xianfeng Zhao, “Reversible Data Hiding In Encrypted Images by Reserving Room Before Encryption,”*IEEETrans.Inf. Forensics Security*, vol. 8, no. 3, pp.553-562, March 2013.

.