# An Efficient Data Hiding Approach on Digital Multi Plane Images for Secret Communication

Jaisudha J[1], Keerthana B[2]

[1,2] *UG Student, Department of Electronics and Communication Engineering, Prince Shri Venkateswara Padmavathy Engineering College, Tamilnadu, India*

## ABSTRACT

*This paper proposes the enhancement of security system for secret data communication through encrypted data embedding in colour images. A given input image is converted to any of the R, G or B plane. After plane separation, the encrypted data hider will conceal the secret data into the image pixels. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the input image. Steganography attempts to hide the existence of communication. In the data extraction module, the secret data will be extracted by using relevant key for choosing the image pixels to extract the data. By using the decryption key, the data will be extracted from Input image to get the information about the data. Finally, the performance of this proposal in Colour Image and encryption data hiding will be analysed based on image and Encrypted data.*

**Keyword**: - *Data hiding, Encryption, Compression, Data embedding*

## 1. INTRODUCTION

The idea of hiding secret data is not new, but after the extreme development of the information technology field, steganography became widely used in digital fields and its techniques are developed more and more day by day. Steganography is a branch of the information security field. Another field of information security is cryptography. Steganography and cryptography are somehow related as they both intend to protect information from unauthorized parties. The main difference between them is that steganography is concerned with hiding data and hiding the existence of the data, where cryptography is concerned with transforming data into a not understood form. So, steganography is concerned with not detecting secret data whereas cryptography is concerned with not revealing the visible secret data by altering the structure of the data itself. Of course, they can be combined to make data more secure.

Data can be encrypted is cryptography and then be hidden within a carrier is steganography to provide another layer of protection. In our work we focus on developing a new algorithm that can be used with several types of cover mediums like image, audio, video, text and even network protocols because it depends on the Least Significant Bit (LSB) which can be used with several types.

## 2. EXISTING SYSTEM ANALYSIS

The existing system uses discrete cosine transformation, direct bit replacement process and cryptography.

### 2.1 Discrete Cosine Transformation

A discrete cosine transforms (DCT) expresses finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3 and images (e.g. JPEG), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary condition.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. The DCTs are generally related to Fourier Series coefficients of a periodically and symmetrically extended sequence whereas DFTs are related to Fourier Series coefficients of a periodically extended sequence. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry,

whereas in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT". Its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transform (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transform (MDCT), which is based on a DCT of overlapping data. Multidimensional DCTs (MD DCTs) are developed to extend the concept of DCT on MD Signals. There are several algorithms to compute MD DCT. A new variety of fast algorithms are also developed to reduce the computational complexity of implementing DCT.

Like any Fourier-related transform, discrete cosine transforms (DCTs) express a function or a signal in terms of a sum of sinusoids with different frequencies and amplitudes. Like the discrete Fourie transform (DFT), a DCT operates on a function at a finite number of discrete data points. The obvious distinction between a DCT and a DFT is that the former uses only cosine functions, while the latter uses both cosines and sines. However, this visible difference is merely a consequence of a deeper distinction: a DCT implies different boundary conditions from the DFT or other related transforms.

The Fourier-related transforms that operate on a function over a finite domain, such as the DFT or DCT or a Fourier series, can be thought of as implicitly defining an extension of that function outside the domain. That is, once you write a function as a sum of sinusoids, you can evaluate that sum at any , even for where the original was not specified. The DFT, like the Fourier series, implies a periodic extension of the original function. A DCT, like a cosine transform, implies an even extension of the original function.

However, because DCTs operate on finite, discrete sequences, two issues arise that do not apply for the continuous cosine transform. First, one has to specify whether the function is even or odd at both the left and right boundaries of the domain (i.e. the min-n and max-n boundaries in the definitions below, respectively). Second, one has to specify around what point the function is even or odd. In particular, consider a sequence abcd of four equally spaced data points, and say that we specify an even left boundary. There are two sensible possibilities: either the data are even about the sample a, in which case the even extension is dcbabcd, or the data are even about the point halfway between a and the previous point, in which case the even extension is dcbaabcd (a is repeated).

These choices lead to all the standard variations of DCTs and also discrete sine transforms (DSTs). Each boundary can be either even or odd (2 choices per boundary) and can be symmetric about a data point or the point halfway between two data points (2 choices per boundary), for a total of $2 \times 2 \times 2 \times 2 = 16$ possibilities. Half of these possibilities, those where the left boundary is even, correspond to the 8 types of DCT; the other half are the 8 types of DST. The block diagram for existing figure is shown in fig -1.

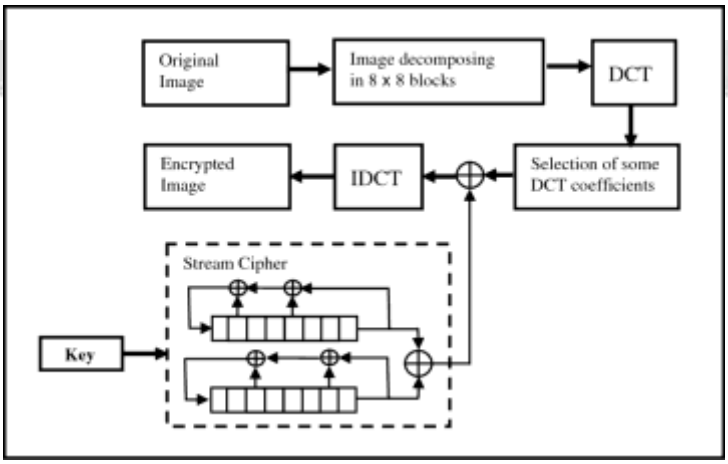


**Fig -1:** Block diagram of existing system

## 3. PROPOSED SYSTEM

Reversible encrypted data concealment in encrypted images using chaos encryption and adaptive least significant bit replacement technique.

### 3.1 Techniques

The techniques used are,

- LWT
- Data Encryption using Chaos Encryption method
- Encrypted Data Embedding in LSB Technique
- Secret Data Extraction
- Image Recovery

Fig -2 describes the embedding process, the input RGB colour image is selected. The plane separation is used to separate the RGB colour image into 3 planes that is R, G and B plane. Any one plane is selected then LWT is applied to that corresponding plane, which will split into 4 sub band images (LL, LH, HL, HH). The LL component is used to avoid noise and distortion. The secret data is encrypted by using chaos encryption and the key is given to it. Using chaos encryption, the plain text is converted into cipher text. The encrypted data is hidden into the output of LWT transformation using LSB technique in the Data embedding process. The output of data embedding is stego-image.

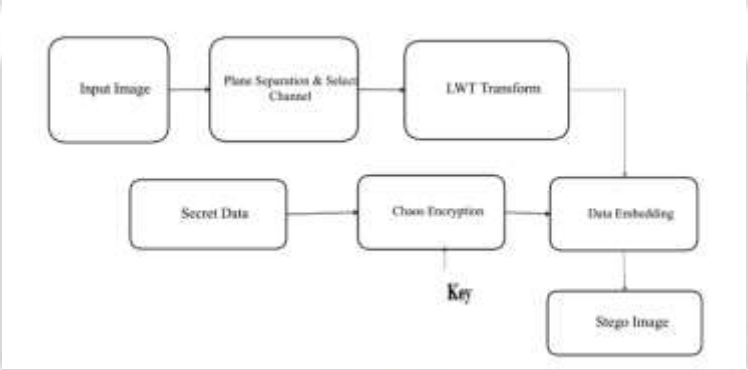


**Fig -2:** Block Diagram of Embedding process

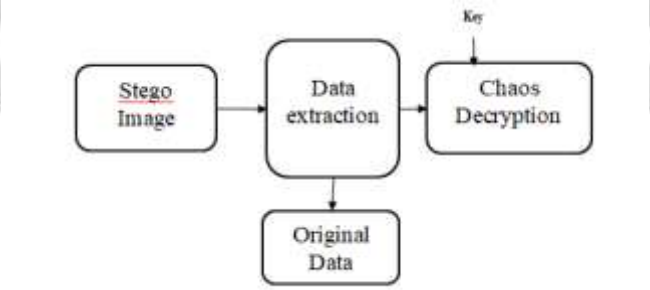


**Fig -3:** Block diagram of Extraction process

Fig -3 describes the extraction process, that is reverse process of embedding process takes place. The output of Data embedding is the input of the extraction process. In the Data extraction process, the secret data is extracted in the stego image. To retrieve the secret data the chaos decryption algorithm is used to convert the cipher text into plain text and the key is given to it then only the secret data retrieved from the stego-image.

### 3.2 Lifting Wavelet Transform

The lifting wavelet transformation is used to decompose the original image into 4 sub band images. One is approximation sub band and another is detailed sub band. The wavelet into spatial operators is called lifting. The

wavelet decompose the image into 4 frequency (LL, LH, HL, HH). The LL component is selected and used to avoid noise and distortion in the image.

### 3.3 Chaos Encryption

Encryption Algorithm

- Step1: secret data selection.
- Step2: ASCII conversion.
- Step3: ASCII to binary conversion.
- Step4: Bit XOR operation.

Overall conversion: Plain text to cipher text.
Decryption Algorithm

- Step1: Bit XOR operation.
- Step2: ASCII conversion.
- Step3: ASCII to binary conversion.
- Step4: secret data extraction.

Overall conversion: Cipher text to Plain text.

### 3.4 Data Embedding

LSB is considered to be the most common technique in the spatial domain image steganography, because rather than its simplicity, these LSB bits (specially 4-LSB) have lower amount of information than the 4-MSB. In the proposed method, we only deal with colour images which have at least a colour depth of 24-bits at each pixel. We embed 8 bits per pixel (8 bpp). This high embedding rate will lead us to increase the payload capacity within the colour image without sacrificing the imperceptibility. One byte of the secret data is evenly distributed among the pixel's three-colour-components: red, green and blue. Regarding one byte of the secret data to be embedded in the selected pixel, the 1st, 2nd and 3rd bits of that byte are embedded into the 3-LSB bits of the red component's byte. Then the 4th, 5th and 6th bits of that byte are embedded into the 3-LSB bits of the green component's byte. Finally, the 7th and 8th bits of that byte are embedded into the 2-LSB bits of the blue component's byte. This process repeats itself until all the secret data bytes are embedded successfully into the selected pixels.

### 3.5 Data Extraction

The data extraction process is that which convert the cipher text into the plain text by using a secret key. Mapping the pixels into an image is known as extraction method. The requirements for data extraction are watermarked image and the secret key. For extraction process applies the inverse support vector dimension on watermarked image. With the use of a secret key the decryption is done only. Then it transfers the encrypted image to normal image, Extract the original and the retrieved image. The quality of the image doesn't degrade while decompression. The human eyes can't detect easily. It provides the high security to the secret image that cannot alter by hackers or intruder easily.

### 3.6 Results and Analyses

The input image shown in fig -4 which is used to transform the data in encrypted format. To decompose the original image into 4 sub band images, LWT is used. It is a technique for both designing wavelet and perform DWT.

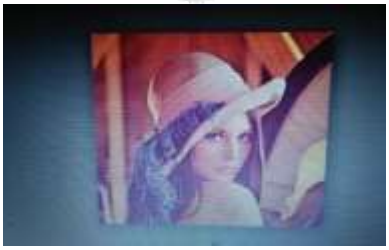

**Fig -4:** Input image

The LWT image is shown in fig -5. The secret data is then hidden in the image through ASCII to binary conversion. A hide known message is pieces of data to protect the information of the data steganography hides

secret message in digital cover files some message is being transmitted. It protects the files. A best media to store data. It provides large capacity for hiding secret information which result into stego image.


**Fig -5:** LWT Image

Secret data is then hidden in the image using chaos encryption. A data extraction is the act of process retrieving data. A data is analysed and retrieve relevant information form data source in a specific pattern. The overall conversion is plain text to cipher text as given in fig -6.


**Fig -6:** Secret Data Hide in Image

The transmitted data is the received and decrypted using the decryption algorithm by converting cipher text to plain text. A data extraction is the act of process retrieving data. A data is analysed and retrieve relevant information form data source in a specific pattern.


**Fig -7:** Extracted Data

Using data extraction, the secret data is extracted from the stego image. The extracted data is shown in fig-7. Finally, the retrieved image is given in fig -8 in which the data is encrypted and transmitted.

**Fig -8:** Retrieved Image

## 4. CONCLUSION

Our proposed encryption algorithm has very good encryption effect and larger secret key space. In addition, experimental results show that our proposed algorithm can resist against noise with different intensity, data lost attack, differential attacks and statistical analysis and comprehensive attacks. All these features show that the proposed method is well suited to encrypt digital images. As the future works, one can study the effect of hybrid clustering-based image encryption and hyper chaotic functions on the encryption performance.

## 5. REFERENCES

[1]. Arun Kumar, Amban, Galgotias University, Greater Noida, Prashant Johri, "Review Paper on Text Sand Audio Steganography Using GA", International Conference on Computing, Communication and Automation, 2015.

[2]. Bassem Bakhache, Dalia Battikh, Milia Habib, Safwan El Assad, "Enhancement using chaos of a Steganography method in DCT domain", 2015.

[3]. Dan Meng, Ling Du, Xiaochun Cao, Xiaojie Guo and Xingxing Wei, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation", IEEE Transactions on Cybernetics, Vol. 46, No. 5, May 2016.

[4]. Gunjan Nehru, Puja Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No.2, January 2012.