# A Modified High Capacity Colored Image Steganography in RGB Color Space

Moh Moh Zan[1], Nyein Aye[2]

***Abstract*—**Data hiding can be done by cryptography, steganography and watermarking. We are here only considering steganography and cryptography. Steganography is the most used technique for data hiding. It can be implemented using any cover media like text, images and videos. Proposed paper presents Image Steganography using Discrete Wavelet Transform in RGB Color Space, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Two dimensional Discrete Wavelet Transform (2D-DWT) is performed on cover image of size M × N. The secret message is encrypted using Blowfish encryption algorithm. The system proposes the new encoding algorithm and the new insertion method. The proposed insertion technique will apply only in LL section of DWT and all pixel block will be divided into 2*2 blocks type as well. It improves the image quality and imperceptibility. It can measure the quality of container image with secret image after image hiding process PSNR values. Extensive testing is performed using different sizes of images and presented our results in payload and Peak Signal to Noise Ratio values.

***Keywords*—**Blowfish Encryption, DWT – Discrete Wavelet Transform, 2D-DWT– Two Dimensional Discrete Wavelet Transform, PSNR– Peak Signal Noise Ratio, Steganography.

## I. Introduction

DATA hiding can be done by cryptography, steganography and watermarking. Here only considering steganography, which literally means "covered writing". The steganography is science of data hiding within another one, so that its presence is undetectable and suffers less security threats or attacks. It hides the content in cover media as not to provoke any doubt that there is some information or message hidden in the media [1]. In encryption the content is not hidden but not readable by the reader if the key is not known to him. But the encrypted content can be intercepted by anyone and chances always present that he will try to decode it or affect it by attempting to decode it for a purpose or just for the sake of curiosity. Whereas, steganography gives us more freedom to communicate and send secret information without leaving any evidence that opponent will intercept and try decoding your information. For this, different cover media can be used like, text, image, video etc. The content to be covertly sent is payload which is called stego text after application of any steganographic technique and media used is called stego image/text/video/protocol (depending on the choice of media). The opposite of it is steganalysis, which is out of the scope of this paper. The most popular cover object is image to perform steganography. Image steganography is divided into spatial and transform domain. In spatial domain messages are embedded in the intensity of image pixel like in LSB. Whereas in transform domain, image is first transformed and then message is encoded like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and many others. Many different image file formats exists, but jpeg format proved to be the best among all [2].

Moh Moh Zan[1] is with the Faculty of Information and Communication Technology in University of Technology (Yatanarpon Cyber City), Near Pyin Oo Lwin, Mandalay Division, Myanmar (email:mohmohzan@gmail.com).

Nyein Aye[2] is now with Faculty of Computer Technology in University of Computer Studies (Mandalay), Mandalay Division, Myanmar (e-mail:nyeinaye@gmail.com).

## II. Background Theory

### A. Wavelet Transform

DWT transform have been extensively used in many digital signal processing applications. Wavelet transform gives the best result for image transformation [3]. The transform of a signal is just another form of representing the signal. It decomposes signal into a set of basic functions. There are two flavors of wavelet transform, one is discrete and other is continuous. Wavelet transform converts an image from time or spatial domain to frequency domain. The Wavelet Transform is obtained by repeated filtering of the coefficients of the image row-by-row and column-by-column. For proposed system, it focuses on discrete wavelet transform. In DWT, there are many levels such as 1-D, 2-D… n-D levels. 2D-DWT is used in proposed research work. It uses the scaling and wavelet functions of 1D-DWT. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL, LH, HL and HH.

Wavelet transform divides the information of an image into approximation and detail sub signals. The LL band includes the low pass coefficients and represents a soft approximation to the image and other three detail sub signals shows the vertical, horizontal and diagonal details or changes in the images. The LL sub-band is the low frequency portion and hence looks very similar to the original image. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various

http://dx.doi.org/10.15242/IIE.E0314127

levels can offer corresponding resolution needed. Fig. 1 illustrates the 2D-DWT level. It can increase levels at the cost of complexity. It is two times decomposition of original signal via sub-division.

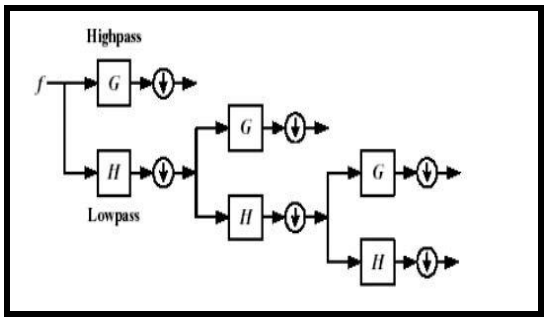


Fig. 1 2D-DWT for image

### B. Blowfish Encryption Algorithm

Cryptography is well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. Cryptography scrambles a message so it cannot be understood. Blowfish algorithm is a very secure technique for cryptography. This algorithm can be optimized in hardware applications though it's mostly used in software applications. It was designed by a cryptologist named Bruce Schneier and made it accessible for public. It was intended to be an attractive alternative to DES (Data Encryption Standard) or IDEA. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. The block size is 64 bits, and the key can be any length up to 448 bits. It is only suitable for applications where the key does not change often, like a communications link or an automatic file encryptor.

It has two parts. A first deal with the key expansion and second part performs the encryption of information. Key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Data encryption consists of 16 Feistel-like iterations. Each iteration operates on a 64-bit data block, split into two 32-bits words. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Although Blowfish is one of the faster block ciphers for sufficiently long messages, the complicated initialization procedure results in considerable efficiency degradation when the cipher is rekeyed too frequently. It increases contrast value in image by reducing the redundant information. In [4], it is presented that blowfish performs outclass compared to other encryption algorithms like AES, DES. Proposed system has selected blowfish to fulfill need of encrypted information.

### C. Related Works

Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar in [6] presented a novel technique using DWT transform for the cover image transformation and then Huffman is used on secret message before embedding. It uses only high frequency coefficients for embedding message bits and neglected low ones to get better image quality. Another image steganographic method using wavelet and Microsoft Utility for RC4 encryption [5] proposed which proves to be more secure. M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa in 2004 [7] utilizes wavelet transforms that map integers to integers and proposed an algorithm that embeds the message bit stream into the LSB's of the integer wavelet coefficients of a true-color image. Proposed system can give the high invisibility even with large message size. The paper [8] proposes hybrid steganography (HDLS) which is an integration of both spatial and transforms domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial to transform domain using DCT/DWT/FFT and embedded in a special manner, the components of cell II retained in spatial domain itself.

## III. PROPOSED SYSTEM ARCHITECTURE

### A. Proposed Steganography Method

Although steganography is applicable to all data objects that contain redundancy, in this paper, JPEG images are considered only. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks. (Visual attacks mean that steganographic messages can be seen on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images). Fig. 2 shows a general representation of the proposed steganography method.

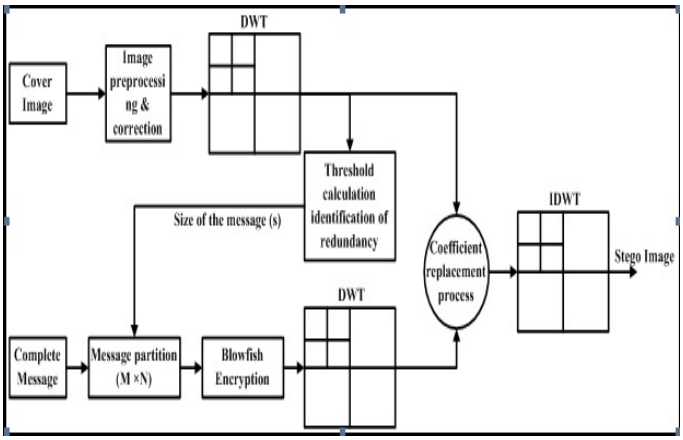


Fig. 2 General representation for proposed steganography method

*B. Proposed System*

In this paper, the problem of unauthorized data access is minimized by combining cryptography and steganography. In cryptography, this system is used Blowfish algorithm with its symmetric key and the cipher text is produced that is in Hexadecimal format. That hexadecimal output needs to convert into 3-bits encoding process of octal number. After achieving cipher text to 3-bit stream then insertion process starts. Firstly, initialization of initial array of octal ($2^3$) process is composed. After that, encoded octal number stream is allocated into specify array. Finally, system will get encoded bit stream of cipher text is achieved. This encoded binary string is used to insert in insertion process.

The extraction process is also reverse of insertion process as well. Firstly, extract the results using cover image and stego image. After that, it needs to transform back into octal number and then to hexadecimal format. The output hexadecimal format of cipher text can be decrypted by Blowfish decryption algorithm process. The contribution of proposed system is a new encoding technique and a new insertion method for hiding data in cover image and is more secure than inserting LSB of the image directly into steganographic system. Proposed system features will go on with the following steps and it can be divided into two sections; stego-insertion and extraction section as shown in Fig. 3.

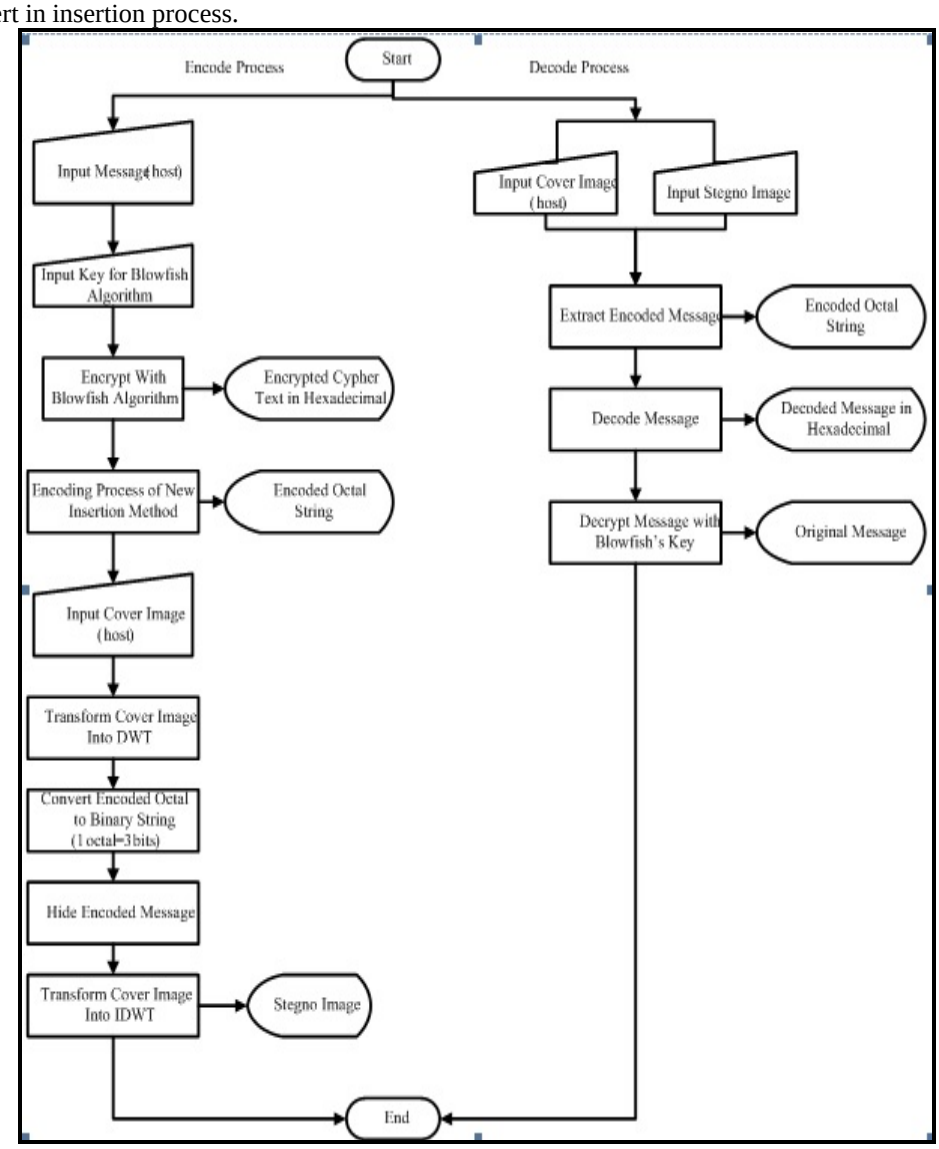


Fig. 3 Proposed system process flow chart

*C. Proposed Encoding Technique*

First, from the output octal number stream "101162707060", it needs to search in left side of stream properties for any same number. If not found in left side array then it is need to search in Initial Array also and when found out the same number properties, there, insert the position of it into encoded bit string array. For '1' at position '0' will enter to its array properties of '2'. For '0' at position '1' will enter to '2'. For '1' at position '2' will enter to '2'. For the next '1' at position '3' will enter to '1'. There, if the position stream value is greater than '7' then, it needs to set that value to '0' and subtract value '7' from array position property until it becomes less than '8'. So, for '6' at position '4' will go to into process of Position=4+7=11, 11-7=4, thus, set '0' and '4' to its array properties. And the rest processes will go as described above. After achieving all stream octal numbers, system needs to

convert that octal value stream into binary array type. The above processing procedure is shown in Fig. 4.

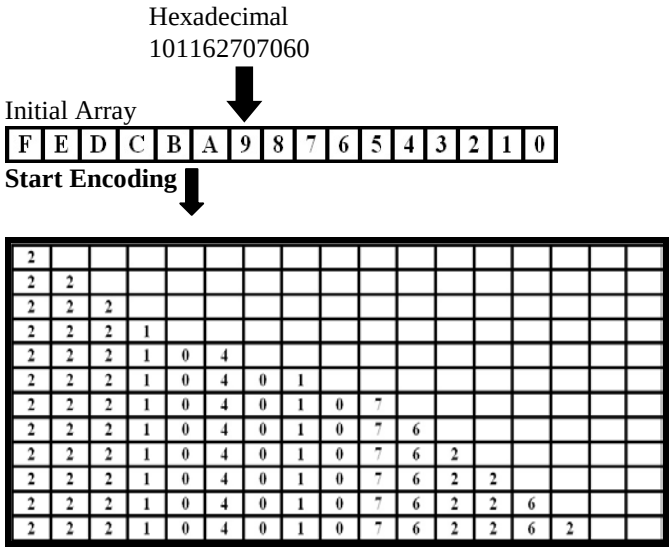


Fig. 4 Proposed encoding method

*D. New Insertion Method Flow*

The detail explanation of the new insertion method is DWT will use 2*2 block (4 pixels) in LL band. So, all of pixel points of input image DWT value will occur into red, green and blue channel of 0-255 range. These values may contain integers and floating numbers. All DWT values must be converted pixel values as it needs to extract clearly in extraction process section and also needs to apply into proposed insertion technique. The cover image pixel values and stegno image pixel values need to differ from each other. Therefore, according to LL section 2*2 block pixel ratio, all of DWT's coefficient values of integers and floating numbers will need to change into converted values.

Firstly, the value of R channel in RGB color space is divided by 4. If the result is 0 or 1, the pixel values in G channel are changed. If the result is 2 or 3, the pixel values in B channel are changed. The pixel values of original image are changed into ±2. So, the changes between the original image and stego image are not significant. It improves the image quality and imperceptibility. For the integer values, it can be directly XOR with 2 to get their ±2 values. For the floating numbers, it is need to multiply with 4, secondly, the multiplication results have to change into binary. That binary have to XOR with binary of 8 and finally it is needed to divide with 4. This is a kind of changing of floating numbers into their ±2 values. For example, floating number of 10.75 will change as follow;

$$10.75 \times 4 = 43 \rightarrow 43 = binary \quad of \ 00101011$$

binary of 8 = 00001000

XOR

00100011 = 35

$$35 / 4 = 8.75$$

After successfully changed all of cover image's DWT coefficients, then it are ready for insertion of encoded octal numbers (encrypted messages). The above pixel value changing process performs if the secret message is 1. If the message is 0, the pixel value is not changed.

*E. Extraction Process Flow*

Extraction process will go as follow;

(a) Extract the pixel values from LL section for both cover and stego image.
(b) Transform the result into octal number.
(c) Convert octal number into hexadecimal format.
(d) Decrypted with Blowfish algorithm.
(e) Find original message.

## IV. Experimental Results

The system will produce a stego image and the user needs to save in his local drive and all these above processes are displaying in Fig. 5.

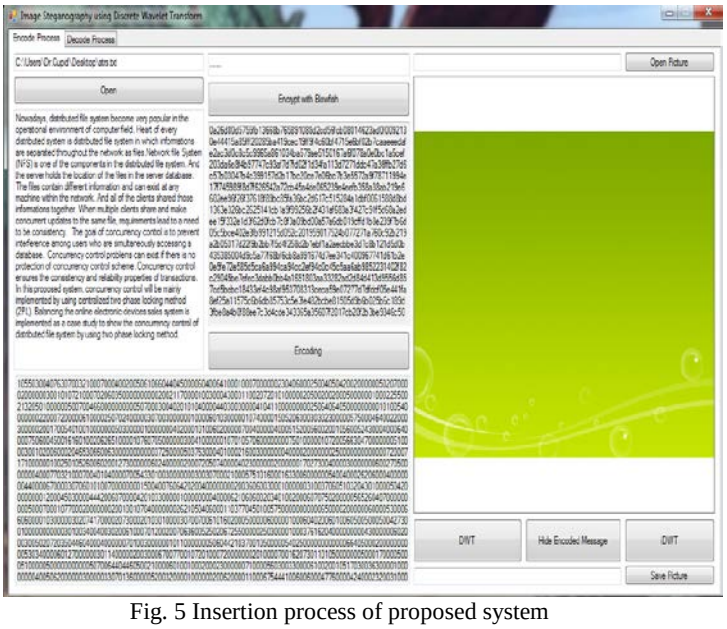


Fig. 5 Insertion process of proposed system

In the extraction section, the user needs to input cover image and stego image altogether. The above describing extraction process flow is displaying in Fig. 6.

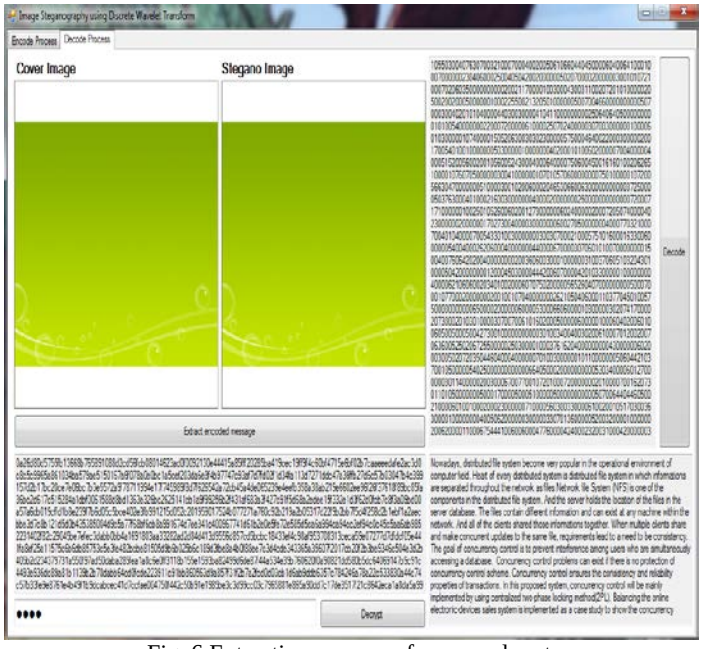


Fig. 6 Extraction process of proposed system

The following table shows the comparison of PSNR values of various image size and message size.

TABLE I
THE COMPARISON OF PSNR VALUES

| Image Size / Message Size | 275*183 | 300*300 | 540*720 |
|---|---|---|---|
| | PSNR | PSNR | PSNR |
| 1K | 51.12dB | 55.25dB | 67.17dB |
| 5K | 43.37dB | 49.16dB | 58.13dB |
| 10K | 39.51dB | 45.22dB | 52.64dB |

## V. CONCLUSIONS

Steganography and cryptography are used for secure communication. This paper presents a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding. Secret message embedding is performed in DWT domain than the DCT as DWT outperforms than DCT. This method provides double security by involving blowfish, which satisfies the need of imperceptibility. And the new encoding technique and insertion method is presented for getting better invisibility and security of communication. That proposed insertion technique based on the changing of hexadecimal based to octal and binary step by step flows. Future work may be carried out to increase the payload and maintain the higher PSNR values.

## ACKNOWLEDGMENT

The first author thanks full to the Principal of University of Technology in Yatanarpon Cyber City Dr. Aung Win and the Head of Information and Communication Technology Department Dr. Soe Soe Khaing who support to complete the entire research work well.

## REFERENCES

[1] N. Provos, P. Honeyman, "Hide and seek: "An introduction to steganography", IEEE Security Privacy Magazine (2003), Volume: 1, Issue: 3, Publisher: IEEE Security & Privacy, Pages: 32-44. http://dx.doi.org/10.1109/MSECP.2003.1203220

[2] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998. http://dx.doi.org/10.1109/MC.1998.4655281

[3] Wavelet Transform and Denoising: 152858/unrestricted/ Chapter4.pdf. http://scholar.lib.vt.edu/theses/available/etd-12062002 52858/unrestricted/Chapter4.pdf.

[4] Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[5] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[6] Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science an and Security, (IJCSS), Volume (4): Issue (6).

[7] M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa, "Using No.Integer Wavelet Transforms in Colored Image-Steganography", IJICIS Vol. 42, July 2004.

[8] K B Shiva Kumar, K B Raja and Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", International Journal of Computer Applications (0975 – 8887) Volume 19– No.7, April 2011.