Transform Domain Technique in Image Steganography for Hiding Secret Information

Manibharathi. N[1]
(PG Scholar)
Dr.Pauls Engg. College
Villupuram Dist, Tamilnadu, India-605109

Krishnaprasad. S[2]
(PG Scholar)
Dr.Pauls Engg. College
Villupuram Dist, Tamilnadu, India-605109

Famila. S[3]
(Asst. Professor)
Dr.Pauls Engg. College
Villupuram Dist, Tamilnadu, India-605109

***Abstract*--Steganography is an important research field in many applications. Image steganography is the technique used to hiding secret information into a cover image. This paper presents a new approach for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Firstly two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a cover image of size M × N and Huffman encoding is performed on the secret information before embedding. Also, the secret key is used to protect the information from external user. To embed the secret information into cover image various image steganography techniques are given. The proposed algorithm, a system called Transform domain based Stego Imaging System (SIS). This proposed system is tested to see the viability of the proposed algorithm. Different sizes of secret information/data are stored inside the images. Hence this new Transform domain based Stego Imaging System is very efficient to hide the secret information inside the image.**

Keywords—Steganography, Discrete Wavelet Transform, Huffman coding.

I. INTRODUCTION

Steganography technique is a one of the method to hide the secret information inside the cover images. An algorithm is designed to hide all the data inputted within the image to protect the privacy of the data. Then, the system is developed based on the new steganography algorithm. This proposed system provides an image platform for user to input image and a text box to insert texts. Once the proposed algorithm is adapted, user can send the stego image to other computer/user so that the receiver is able to retrieve and read the data which is hidden in the stego image by using the proposed system. Thus, the data can be protected without revealing the contents to other people.

Transform domain based Stego Imaging System (SIS) is a technique that is capable of hiding the Secret information inside the image. The system is using a security password in order to maintain data privacy. Data security is the function of keeping secret data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate information [4]. Privacy, on the other hand, is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively.

Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues. Data privacy issues can arise from a wide range of sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected.

The main Objective of this project is Transferring the Embedded information to the destination without being detected by the un-authorized user or any other system and using the Transform domain technique (DWT) with Huffman coding to improve the secrecy.

An image is essentially a 2-D signal processed by human visual system. The signals are representing in analog form. The signals are representing in analog form. However, in computer applications the analog signal converted into digital form for processing, storage and transmission. A digital image is a 2-D dimensional array of pixels [2]. Image processing plays an important role in society today because a picture gives a much clearer impression of a situation or an object. The objective of image processing includes: Improving the appearance of the visual data (Image enhancement, image restoration), extracting useful information (Image analysis, reconstruction from projection), representing the image in an alternate and possibly more efficient form (Transformation and image compression).

The field of image processing refers to the processing of digital images by means of a digital computer. A digital image comprises of finite number of elements, these elements referred as picture elements or image elements pels or pixels. Pixels represent darkness or brightness of an image at that point. An application of image processing includes: Medical imaging, Earth resources observations, Astronomy, Computer version and Feature detection. Image enhancement is among the simplest and most appealing areas of digital image processing. It used to highlight the certain features of an image. The aim of image enhancement is to improve the interpretability or perception of information in images for human viewers, or to provide `better' input for other image processing techniques. There are two types of Image enhancement techniques. They are, Spatial domain methods, which operate directly on pixels of an image, and Frequency or Transform domain methods are another technique, which operate on the Fourier transform of an image. Image enhancement techniques used as pre-processing tools for other image processing techniques, and then quantitative measures can determine which techniques are most appropriate.

II. TRANSFORM DOMAIN SYSTEM

The transform of a signal is a method for representing the signal in another form. However, the information content present in the signal does not changed. The Wavelet Transform is a method for representation of time-frequency of the signal. The shortcoming of the Short Time Fourier Transform (STFT), is overcome by this wavelet transform. Wavelet transform used to analyze stationary and non-stationary signals. In all frequencies STFT provides the constant resolution, the Wavelet Transform uses multi-resolution technique by which different frequencies are analyzed with different resolutions.

A. *Continuous wavelet transform*

The Continuous Wavelet Transform (CWT) is provided by equation1, where x(t) is the continuous time signal to be analyzed. Ψ (t) is the basis function; it also called as mother wavelet. All through translation (shifting) and scaling (dilation or compression).

$$X_{wt}(\tau, s) = 1/\sqrt{|s|}\int x(t).\Psi^*\left(\frac{t-\tau}{s}\right)dt \qquad (1)$$

The mother wavelet used to generate all the basic functions designed based on some desired characteristics associated with that function. Where τ is the translation parameter, it relates to the wavelet function shifted through the signal, and the location of the wavelet function as it is. Thus, it corresponds to the time information in the Wavelet Transform. The scale parameter s is defined as |1/frequency| and corresponds to frequency information. Scaling either dilates (expands) or compresses a signal. Large scales (low frequencies) dilate the signal and provide detailed information hidden in the signal, while small scales (high frequencies) compress the signal and provide global information about the signal. The Wavelet Transform performs the convolution operation and the basis function of the signal. The CWT becomes very useful as in most practical applications, in high frequencies (low scales) do not last for a long duration of the signal and appear as short bursts, while low frequencies (high scales) usually last for entire duration of the signal.

B. *Discrete wavelet transform*

The Wavelet Series is just a sampled version of CWT and depending on the resolution required, its computation may consume significant amount of time and resources. The Discrete Wavelet Transform (DWT), which based on sub-band coding. It found to yield a fast computation method of Wavelet Transform. The implementation of DWT is very easier. It also reduces the amount of resources required and computation time.

Wavelets are functions defined over a finite interval and having an average value of zero. Wavelets provide an efficient means for approximating source signal with a small number of basic elements. The basic idea behind the wavelet transform is to represent any arbitrary function (t) as a superposition of a set of such wavelets or basis functions. In general, the wavelets are a set of functions that are generated from a single function, called the mother wavelet, by dilations or contractions (scaling) and translations (shifts) [2]. The basic functions thus obtained are called baby wavelets. The wavelet transform is computed separately for different segments of the time domain signal at different frequencies.

In CWT, a set of basic functions are used to analyze the signals, which relate to each other by simple scaling and translation function. In DWT, digital filtering techniques are used to obtain the time-scale representation of the digital signal. The analyzed signal is passed through filters with different cutoff frequencies at different scales. The 2-D DWT can be implemented using a set of up-samplers, down-samplers, and recursive two channels digital filter banks. There are many available filters, but the most commonly used are Haar Wavelet filters. Each of these filters decomposes the image into several frequencies. Important properties of wavelet filters in digital image compression are symmetry (used for avoiding artifacts at the borders), orthogonality (fat algorithm), regularity, and degree of smoothness. In Haar-DWT the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels.

C. *Huffman coding*

A number of variations can be used for hiding secret image in transform domain technique. In the first case secret image can be Huffman encoded to reduce the size of the image [1]. Huffman codes are optimal codes that map one symbol to one code word.

For an image Huffman coding assigns a binary code to each intensity value of the image and convert it into a 1-D bit stream of lesser length than the original image. This helps in increasing the embedding capacity as well as security. It also provides a kind of authentication as any single bit change in the Huffman coded bit stream is unable to decode. Then the reduced image is converted into 3-bit blocks and embedded in the DWT-DCT converted cover image based on the size. The 3-bit block is embedded in the DCT coefficients of the 8*8 blocks. This will lead to better security and increase in the capacity of embedding of the secret image.

Huffman coding is an entropy-encoding algorithm used for lossless data compression. The variable-length code table for encoding a source symbol such as a character in a file. Based on the estimated probability of occurrence in a particular way for each possible value of the source symbol, the variable-length code table has derived. The representation for each symbol has chosen by the specific method in the Huffman coding. Resulting in a prefix code or prefix-free codes, representing some particular symbol in the bit string is not a prefix of that bit string. If representing any other most common source symbols using shorter strings of bits. Huffman design the most efficient compression method of this type: smaller average output size does not produce individual source symbols to unique strings of bits when the actual symbol frequencies agree with those used to create the code. The Huffman's method running time is efficient; it takes operations to construct it. A later found method was to design a Huffman code in linear time and input probabilities sorted with the weights.

Before embedding the secret image into cover image, it encoded using Huffman coding. Huffman codes are optimal codes that map one symbol to one code word. For an image, Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2. Image is converted to a 1-D bits stream with length LH < M2 × N2.

Huffman coding used to serve the following:

Lossless Compression –It increases the embedding capacity. **Security by means of encoding** – Huffman encoded bit stream cannot reveals anything. **To extract the exact meaning** –Huffman table is required to decode. In Huffman coded stream, if any single bit changed; it provides one type of authentication, and Huffman table is unable to decode.

III. PROPOSED STEGO IMAGING SYSTEM

A. *Concept of steganography*

Steganography is the heart of science for hiding information. The concept of steganography based on cryptography. The main goal of cryptography is to make data unreadable by an un-authorized user. The steganography is to hide the information in the sense data or image from an un-authorized user.

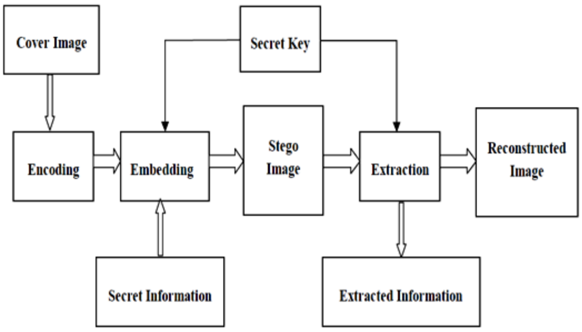


Figure 1: Basic block diagram of Steganography system

The Fig.1 shows the block diagram of Steganograhy system. Here the cover image encoded with the secret information and the secret key embedded into the secret information. From the resultant of stego image, the same key used to extract the Secret information.

There are many number of steganographic method used in our day-to-day life. Most of that methods are familiar with (especially for a large number of spy movies), ranging from microdots and invisible ink to secreting a hidden information in spread spectrum radio communication [4]. There are so many ways to hiding information in computers and networks: They are,

- Covert channels (e.g., Loki and some distributed denial-of-service (DOS) tools use the Internet Control Message Protocol (ICMP), as the communications channel between the Unknown user or system and a compromised system).
- Hidden text files within the Web pages.
- Hiding the important information in "plain sight".
- Zero ciphers (e.g: to form a hidden message using the first letter of each word otherwise innocuous text).

B. *Transform domain based stego imaging system (SIS)*

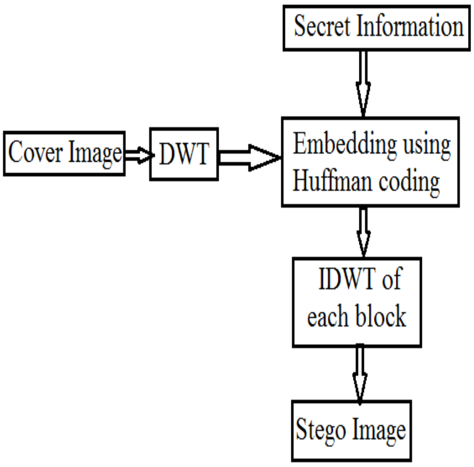


Figure 2: Block diagram of proposed Stego Imaging system

The cover Image is an Image file in which we will hide the Secret information, which may also been encrypted using the stego key. The resultant output file is the stego image (which will, of course be the same type of file as the cover Image). Generally, the cover medium is typically image or audio files. Here, I focused on image files and will; therefore, the cover medium and stego medium are referring to the *cover image* and *stego image*.

The Fig.2 shows the block diagram of Transform domain based Steganography Imaging System (SIS). Here Discrete Wavelet Transform used as the Transform domain. Embed the secret information into the cover image by using Huffman coding. To provide the higher security the password is created after that of the secret information hidden into the cover image.

The terminologies used in Image steganography are as follows:-

Cover-Image: It is original image, which used as a carrier for hidden information.

Secret Information: It is actual information, which used to hide into images. Message could be a plain text or some other image.

Stego-Image: Stego-image is an image generated after embedding the secret information into cover image.

Stego-Key: It is a secret key that are used for embedding or extracting the information from cover-images and stego-images.

The uses of steganography system are many and one of the most widely used applications is *digital watermarking*. A watermark is a method that uses a replication of an image, logo or text on paper stock. So the source of the document authenticated partially [3]. The same function accomplished by the digital watermark scheme. The communications between the underground communities are done by using stego image. There are several reports explains the steganography is used to embed messages for the group within images.

Steganalysis is the science of detecting hidden information from the stego image [4]. The main objective of Steganalysis is detection of stego image and break steganography. Almost all steganalysis algorithms rely on the Steganographic algorithms introducing statistical differences between cover and stego image.

C. *Algorithm for proposed stego imaging system*

Step 1: Input: select the cover image.
Step 2: Then apply the discrete wavelet transform to the cover image.
Step 3: The DWT separates the cover image into different sub band images (LL, LH, HL, and HH).
Step 4: In order to apply the secret information with use of Huffman coding.
Step 5: Hide the secret information into the cover image and generate the security key to provide high security.
Step 6: From this result the stego image is generated.
Step 7: Using the stego image by provides the security key as same as the previously used to extract the secret information
Step 8: Output: Get the secret information hided into the cover image.

The above algorithmic steps describes the process of the proposed Transform domain based Steganography Imaging System (SIS).

IV. RESULTS AND DISCUSSION

In this section, I present simulation results to demonstrate the highly secured Transform domain based Stego Imaging System (SIS). This proposed stego imaging system produces better result from this algorithm. The output results are obtained by using MATLAB software. The simulation results shown below:

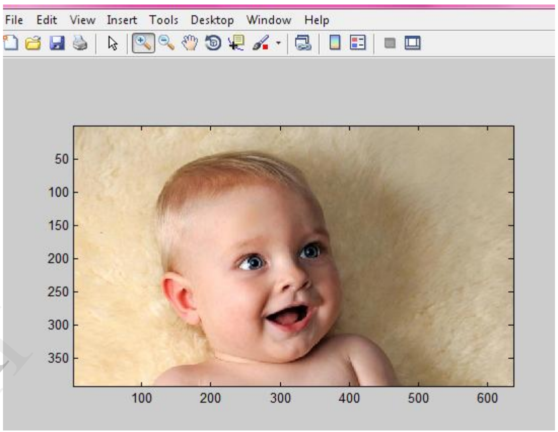


Figure 3: Input Cover image (without secret information)

The Fig.3 shows the Input Cover Image. It does not contain any secret information within the image.

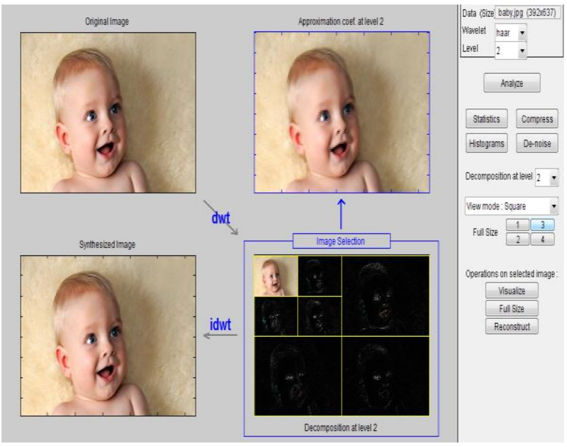
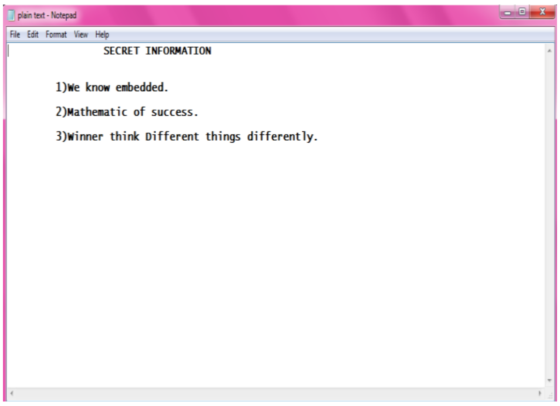

Data (Size) baby.jpg (392x637)
Wavelet haar
Level 2
Decomposition at level 2
View mode : Square

Figure 4: Cover image split by the 2Level DWT

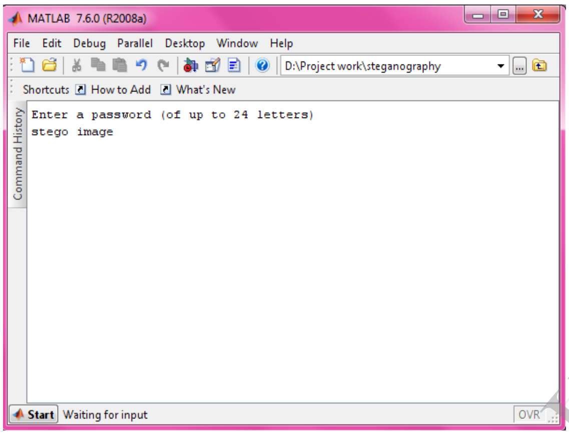
The Fig.4 shows the input of the cover image split by the 2Level DWT using Haar wavelets.



```
            SECRET INFORMATION

    1)We know embedded.
    2)Mathematic of success.
    3)Winner think Different things differently.
```

Figure 5: Secret Information

The above Fig.5 shows secret information. This secret information is embedding into the cover image.


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window Help
D:\Project work\steganography
Shortcuts How to Add What's New
Command History
Start Waiting for input
OVR

```
Enter a password (of up to 24 letters)
stego image
```

Figure 6: Creating Password key

The Fig.6 shows the creation of password key on embedding process. This security password helps to provide the higher security.

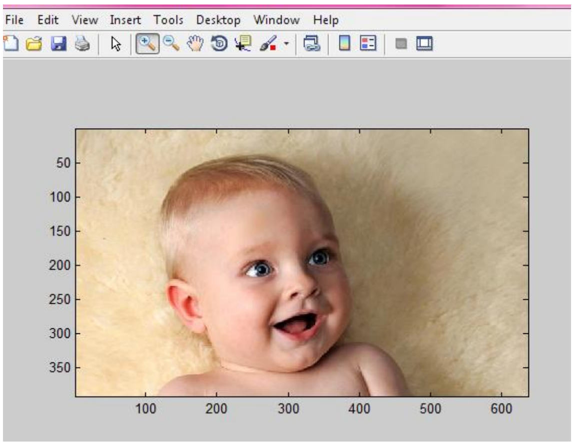
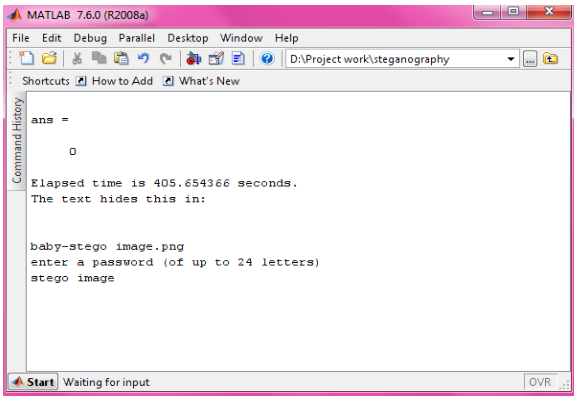


Figure 7: Stego image (with secret information)

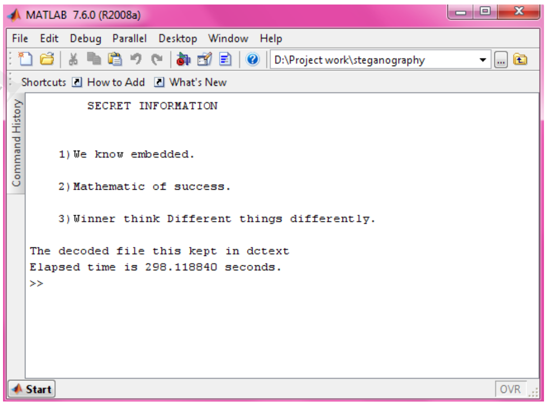
The above Fig.7 shows the resultant output of stego image having secret information inside the image.


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window Help
D:\Project work\steganography
Shortcuts How to Add What's New
Command History
Start Waiting for input
OVR

```
ans =

     0

Elapsed time is 405.654366 seconds.
The text hides this in:


baby-stego image.png
enter a password (of up to 24 letters)
stego image
```

Figure 8: Steganalysis of secret information

The Fig.8 describes the steganalysis of secret information from the stego image using same the password as we are using at the time embedding the secret information.


MATLAB 7.6.0 (R2008a)
File Edit Debug Parallel Desktop Window Help
D:\Project work\steganography
Shortcuts How to Add What's New
Command History
Start
OVR

```
        SECRET INFORMATION


    1)We know embedded.

    2)Mathematic of success.

    3)Winner think Different things differently.

The decoded file this kept in dctext
Elapsed time is 298.118840 seconds.
>>
```

Figure 9: Extracted Secret information

The Fig.9 shows extracted secret information from the stego image.

V. CONCLUSION

Image Steganography methods in spatial domain LSB substitution system does not provide the basic demand of secrecy. The attacker can easily destroy the secret information by applying signal-processing techniques. The proposed Transform domain based Stego Imaging System (SIS) provide the higher security for protecting the secret information from the external user. The secret password given at the time of secret information embedded in to the cover image. In the process of steganalyst the same password is used to extract the secret information from the stego image. In addition, the time consumed for the extraction of secret information is less than that of time taken for embedding the secret information.

As a scope of future work, Embedding the secret image into the cover image using the watermarking technique to embedding the secret image.

REFERENCES

[1] Mukta Goel and Rohit Geol, "Current Image steganograhy techniques for higher compression and robustness", *VSRD International Journal of Computer Science & Information Technology*, Vol. 3 No. 2 Feb 2013.

[2] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge adaptive image steganography based on LSB matching revisited," in *IEEE Transactions on Information Forensics and Security*, vol.5, no.2, June 2010.

[3] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security ,* 5 ,1, PP 187–193, 2010.

[4] Matthew L.Miller, Ingemar J.Cox, "Digital Watermarking and Steganography":Second Edition, Morgan Kaufmann Publishers.

[5] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image" *International Conference on Information and Communication Technology*, PP 238–241, 2007.

[6] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.

[7] D. Wu and W. Tsai, "A steganographic method for images by pixel value differencing," *Pattern Recognit. Lett.*, vol. 24, pp. 1613–1626, 2003

[8] D. Artz, "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, 4, 2, PP 127- 135, 2001.

[9] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, "Reversible data hiding" , *IEEE Transactions on Circuits and Systems for Video Technology*, PP 354–362,2006.