Data Hiding in Image using Multilevel 2-D DWT and ASCII Conversion and Cyclic Mathematical Function based Cryptography

Abbas F. Tukiwala
M.E Student of Computer Department
Sigma Institute of Engineering, Vadodara

Sheshang D. Degadwala
Assistant Professor of Computer Department
Sigma Institute of Engineering, Vadodara

ABSTRACT
The preserving secrecy of sensitive data becomes very important in today digital communication. Steganography is the discipline of exchanging top secret information by embedding it into a multimedia carrier and Cryptography is the art of protecting information by transforming it into an undetectable form. The ultimate aim, here is to hide the very existence of the embedded information within seemingly innocuous carriers and transmit in such a way that the existence of information is undetectable. In this paper, proposed method extracts by combining the features of cryptography and steganography. Cryptography using Modified ASCII Conversion & Mathematical Function involves converting the secret message into unprintable form of same size as original message in any cases. Steganography is then applied using multilevel 2-D DWT to embed this encrypted data into a cover media using High Frequency Coefficients of each Dimension at all levels of 2-D Haar DWT and hides its existence. Finally, Performance can be measured by using statistical parameters peak signal noise ratio (PSNR) and Mean Square error (MSE). This proposed method provides all three aspects of data hiding such as capacity, security and robustness.

Keywords
2-D DWT, Haar DWT, ASCII Conversion, Cyclic Mathematical Function, PSNR, MSE

1. INTRODUCTION
Security of information becomes one of the most important factors of information technology and communication because of the huge rise of the World Wide Web and the copyrights laws. Cryptography was originated as a technique for securing the confidentiality of information. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret and the concept responsible for this is called steganography [2]. Steganography is the practice of hiding secret message within any media. Most data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. If both the techniques: cryptography and steganography is used then the communication becomes double secured [2].The main difference between Steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret. ASCII Conversion & cyclic mathematical function based cryptography is a new cryptographic algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or hashing function [11].

This paper uses Modified concept based on this cryptography algorithm for data encryption, where the data will be converted into an unprintable form, which will be then hidden into an image file. In order to enable large capacity of data and maintaining good visual quality of the cover image, the embedding is applied by modifying the diagonal details coefficients (High frequency coefficients) in transform domain of Multilevel Two-Dimensional Haar Discrete Wavelet Transform (HDWT). The advantages of using this system are that it does not require the original cover image for successful extraction of the secret message.

The outline of the paper is as follows: An overview of Related Works in Section 2. Methodology was discussed in Section 3. The proposed Work was presented in Section 4. Measurement of Image Steganography was listed in Section 5. Expected results and conclusions are presented in Sections 6 and 7, respectively.

2. RELATED WORKS
Review of literature survey has been conducted on evaluating the performance of Multilevel 2-D DWT based Steganography and ASCII Conversion & Cyclic Mathematical Function based Cryptography. This section describes the previous work which had been done for data hiding.

Mehdi Hussain et al., (and other) [1] critically analyzed various steganography techniques and also covered steganography overview, its major types, classification and application.

Firas A. Jassim [2] proposed method to hide the secret message inside the cover image using five modulus methods. The main advantage of that novel algorithm is to keep size of cover image constant while secret message increased in size.

Chaithra h et al., [3] developed proposed system is to hide message using FMM along with genetic algorithm and Visual Cryptography to ensure improved security and reliability. The major merit of that system is to increase the embedding capacity and secure the information.

Rahul Joshi et al, [4] introduced the concept of steganography using LSB method. This method is easy to implement but has some disadvantages. One of the major disadvantage is that intruder can change LSB bit of all image pixels. Hidden message will be destroyed by changing the image quality. It is not immune to noise and compression technique.

Shivani kundra and Nishi madaan [5] performed analysis of different image steganography techniques and their comparison is done. They found that performance of the Hash LSB would be more secure than other techniques and RSA algorithm itself is very secure that no one can break it easily.

Saeed Ahmed et al., [6] proposed method using Dynamic Substitution and Secret Key is more difficult to attack because of message bits are not inserted in to the fixed position. In their method, the message bits are embedded into deeper layer depending on the environment of the host image and a secret key resulting increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message.

Barnali Gupta and Prof. Samir [7] discussed image steganography using DWT method. It divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. These detailed coefficients can be used to embed secret image.

Yung kuan chan et al., [8] developed proposed method that transform a spatial domain cover image into a frequency domain image using Haar digital wavelet transform method, compresses coefficients of the high frequency band by the Huffman or arithmetic coding method and then embeds the compression data and secret data in high frequency band. This method utilizes the Huffman coding to recover the cover image without any distortion.

Vikas pratap and Prof. Shrikant [9] proposed a new frequency domain method using Haar Wavelet for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. The advantage of this is that the original cover image does not have to be present on the receiver side.

Mrs.D.Mathivadhani and Dr.C.Meena [10] developed hybrid method to hide an image and secret message into a cover image using Discrete Wavelet Transformation (DWT), SLSB (Selected Least Significant Bit) and Visual Cryptography (VC) is proposed. This proposed system can resist various attacks while maintaining the visual quality of the cover image and text message.

Md. Palash et al. [11] developed a Cryptographic Algorithm Based on ASCII Conversions and a Cyclic Mathematical Function is to make the encrypted message undoubtedly unprintable using several times of ASCII conversions and a cyclic mathematical function. The final encrypted message received from three times of encryption becomes an unprintable text without increasing the size of data or loosing of any data. But if size of original message is not divisible by Packet size then size of encrypted message in bits is larger than that of original message. This algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or hashing function.

S.Shanmuga Priya et al. [12] consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain. LSB replacement is a well-known steganographic method. In that embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseuo random number generator (PRNG).

Mr. Vikas Tyagi [13] discussed a technique used on the LSB (least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

Ali and Fawzi [14] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. The basic decomposition step for images using the 2D Wavelet transforms. Also, different levels of Wavelet transform were tried in that paper (up to 5).

Prabakaran. G and Bhavani R. [15] proposed a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is performed to scrambles the secret image. Discrete Wavelet Transform (D WT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image.

G. Prabakaran et al. [16] developed proposed method extracts either Discrete Wavelet Transform (DWT) or Integer Wavelet Transform (IWT) coefficients of both cover image and secret image. After that two extracted coefficient values are embedded by fusion processing technique. Then the stego image is obtained by applying various combinations of DWT and IWT on both images.

Nadiya P and B Mohammed lmran [17] present an advanced method for embedding encrypted secret data in grayscale images to provide high level security of data for communication over unsecured channels. The proposed system combines the features of Cryptography and Steganography. Cryptography involves converting the secret message into a non-recognizable cipher. Steganography is then applied using Double-stegging to embed this encrypted data into a cover media and hides its existence.

Pratibha Sharma and Shanti Swami [18] Present a digital image watermarking based on 3 level discrete wavelet transform (DWT) & compare it with 1 & 2 levels DWT. In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique.

S.Bhargav Kumar and K.Esther Rani [19] propose a new technique of watermarking, combining both Discrete Wavelet Transform (DWT) and Bit-Plane Slicing (BPS) techniques. In the first unit, they decomposed the image to be watermarked in to four dimensional modified DWT coefficients, by adding pseudo-random codes at the high and middle frequency bands of the DWT of an image. In the second unit, a key has been generated from LHLH frequency bands of the 4-Level DWT image and this key is watermarked in to the original gray image. In the third unit, for data compression we used bit plane slicing technique where the original gray image is sliced in to 8 planes and we used bit plane 3 to embed in to the key watermarked image. The embedded key watermarked image is transmitted and the key watermarks are extracted with robustness.

Nikita Kashyap and G.P. Sinha [20] use a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transform techniques. The proposed method is compared with the 1-level and 2-level

DWT based image watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE).

Sree Rathna Lakshmi [21] present a steganalytic algorithm based on III Level DWT with Energy as Feature that detects the stego/normal image with 90% accuracy.

3. METHODOLOGY

For high level security, Modified ASCII Conversion and Cyclic Mathematical Function based Cryptography is utilized. And for high payload capacity and robustness, multilevel 2-D Haar DWT is proposed in our technique. In our paper, we are proposing a technique using both multilevel 2-D HDWT and Modified ASCII Conversion and Cyclic Mathematical function based Cryptography.

3.1 Modified ASCII Conversion and Cyclic Mathematical Function based Cryptography

It is a new cryptographic algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or hashing function [11]. It is used to make the encrypted message undoubtedly unprintable using several times of ASCII conversions and a cyclic mathematical function [11]. Dividing the original message into packets. Binary matrices are formed for each packet to produce the unprintable encrypted message through making the ASCII value for each character below 32 [11]. Similarly, several ASCII conversions and the inverse cyclic mathematical function are used to decrypt the unprintable encrypted message [11]. The final encrypted message received from three times of encryption becomes an unprintable text through which the algorithm possesses higher level of security without increasing the size of data or loosing of any data when size of original message is divisible or not by Packet size [11]. Here we modify this algorithm by taking different Mathematical function (M). One for all packets expect last one and second for last packet.

3.1.1 Encryption Phase

In the encryption phase of the proposed algorithm, at first the input characters of the text to be encrypted are divided into several packets of N characters taking in order from the beginning character, where the value of N is less than or equal to 5 which may vary only for the last packet as the last packet contains the remaining characters. Its value may range from 1 to packet size. For example, if a text consists of 13 characters and packet size is 5, the first 5 characters constitute the first packet, the subsequent 5 characters constitute the second packet and the remaining 3 characters constitute the last packet. Secondly, a binary matrix P [N, 8] is formed for each packet using the 8-bit binary equivalent of the ASCII value of each character. The binary value of each ASCII of a packet is then accommodated row wise in the binary matrix. Thirdly, 8 new ASCII values denoted by NewASCII[i] for each packet is evaluated using the matrix P [N, 8] taking the decimal equivalent of the bits belonging to each column of the matrix.

The values of the NewASCII[i] range from 0 to 31 whose equivalent characters are unprintable. Now if we take the equivalent character for each NewASCII[i], then all the printable characters in the original data will become unprintable. Thus, this offers a better security making the cipher text more secured. However, for one step higher security, a cyclic mathematical function has been used to encrypt once again the final ASCII values of the intermediate encrypted data. The mathematical function as shown below is called cyclic because its output is rotated between 0 and 31 for all packets expect last packet. In last packet its output is rotated between 0 to 2^l where l is size of last packet.

$$FinalASCII[i] = (NewASCII[i] + M) \%32 \quad (1)$$

Where, $0<M<32$ for all packets expect last packet and for last packet, $0<M<2^l$ where l is size of last packet.

Finally the 8 FinalASCII[i] values are converted to their equivalent characters whose are undoubtedly unprintable so that the final cipher text cannot be shown at all. This encryption process repeats for each packet of N characters for the original data. Then combining all the encrypted packets as a single it is sent to the receiver.

3.1.2 Pseudo Code of Encryption

1. Input Original Message.
2. Divide original message into several packets of N size.
3. For each packet

a. Convert each character to equivalent ASCII.

b. Create binary matrix P [N, 8] with binary value from ASCII of the characters.

c. Calculate new ASCII as:

```
For (i=0 to 7)
NewASCII[i] =0
For (j=0 to N-1)
        NewASCII[i] += P [j, i]* 2^j
End inner loop
End outer loop
```

d. Re-calculate each NewASCII[i] using cyclic mathematical function:

```
FinalASCII[i] = (NewASCII[i] +M) %32
```

Where, $0<M<32$ for all packets expect last packet and for last packet, $0<M<2^l$ where l is size of last packet.

e. Convert each FinalASCII[i] to its equivalent character

4. End of encryption.

3.1.3 Decryption Phase

In the decryption phase of the algorithm, at first the characters of the received unprintable cipher text are converted to their equivalent ASCII. After which the inverse cyclic mathematical function is applied to the ASCII as shown below:

$$DecASCII\_1 [i] = (ASCII[i] - M + 32) \%32 \quad (2)$$

Where, $0<M<32$ for all packets expect last packet and for last packet, $0<M<2^l$ where l is size of last packet.

Then all the DecASCII_1 [i] are divided into the same number of packets of 8 characters in order as done the encryption phase. Secondly, a binary matrix Q [N, 8] is formed using the equivalent binary of the ASCII value in each packet, where the value of N is 5 which may vary only for the last packet. Its value may range from 1 to 5. The binary value of each ASCII of a packet is then accommodated column wise in the binary matrix. Thirdly, the final N ASCII denoted by DecASCII_Final[i] for each packet is evaluated using the binary matrix Q[N,8] taking the decimal equivalent of the of

the bits belonging to each row of the matrix. Finally, the N DecASCII_Final[i] values for each packet are converted to their equivalent characters whose are undoubtedly same as in the original message. This decryption process repeats for each packet of 8 characters of the encrypted data.

3.1.4 Pseudo Code of Decryption

1. Input Encrypted Message.
2. Convert the characters to their equivalent ASCII.
3. Calculate DecASCII_1 [i] using inverse cyclic Mathematical function:

   DecASCII_1 [i] = (ASCII[i] –M+32) %32

   Where, 0<M<32 for all packets expect last packet and for last packet, 0<M<2^{l} where l is size of last packet.
4. Divide the DecASCII_1 [i] into several packets of 8 characters each.
5. For each packet

a. Create binary matrix Q [N, 8] with binary value from the DecASCII_1

b. Re-calculate new ASCII as:

```
For (i=0 to N-1)
   DecASCII_Final[i] =0;
   For (j=0 to 7)
   DecASCII_Final[i] +=Q [i, j] * 2^(7-j)
      End inner loop
End outer loop
```

c. Convert each DecASCII_Final[i] to its equivalent character

6. End of decryption

3.1.5 Explanation with Example

Encryption:

Let's consider that the user wants to encrypt and then conceal the message BE HAPPY. According to the discussion the algorithm divides the input into 2 packets, where the first one contains the first 5 characters "BE HA" and the last contains the subsequent three characters "PPY" as shown below:

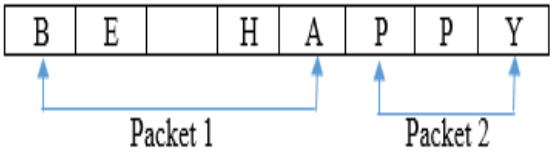


Figure 1: Original Message

As the explanation in the encryption phase the characters of each packet are converted to their equivalent ASCII. Then using the 8-bit binary equivalent of the ASCII the first matrix P1 [5, 8] is formed for the first packet as shown in Fig. 2

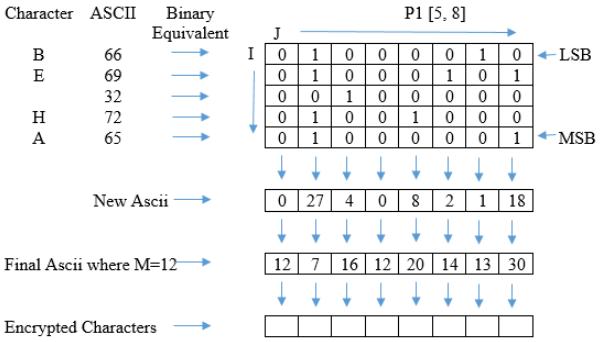


Figure 2: Encryption Steps for first packet

Similarly, using 8-bit binary equivalent of ASCII last matrix P2 [5, 8] is formed show in Figure. 3.

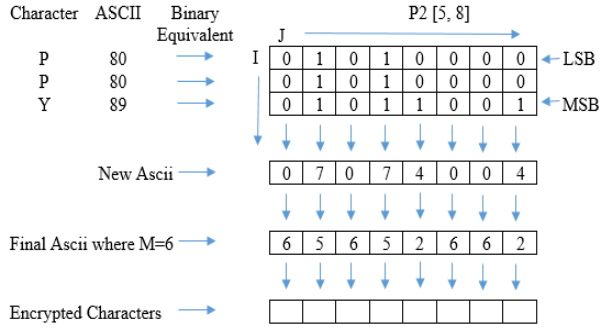


Figure 3: Encryption Steps for Last packet

Finally, the original message is encrypted with a high security which becomes totally unprintable and hidden ensuring the main consent of the developed algorithm. The cipher text contains 16 characters and the binary equivalent of the ASCII for each character is represented by only 5 bits for all packets expect last and only 3 bits for last packets. Since the plaintext contains only 8 characters and the binary equivalent of the ASCII for each character was represented by 8 bits, the cipher text does not require extra bits just same as of the original. That means 8x8=64 and 8x5+8x3=40+24=64.

3.1.6 Decryption:

The cipher text containing 16 characters are converted to their equivalent ASCII each of which is then converted to a new ASCII denoted by DecASCII_1 using the inverse cyclic mathematical function. Then all the DecASCII_1 are divided into 2 packets as discussed in the decryption phase each containing 8 ASCII. After which a Q1 [5, 8] matrix for the first packet and a Q2 [3, 8] matrix for the last packet are formed. From these matrices the original message is decrypted properly as shown below:

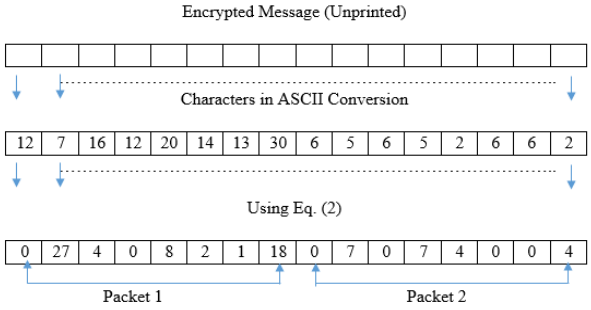
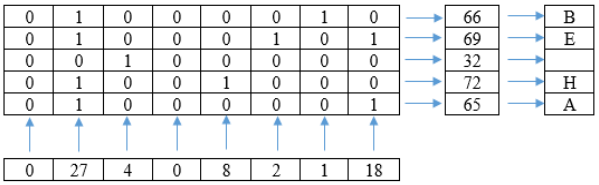


Figure 4: After Inverse Cyclic Math. Function

First Packet Decryption



Last Packet Decryption

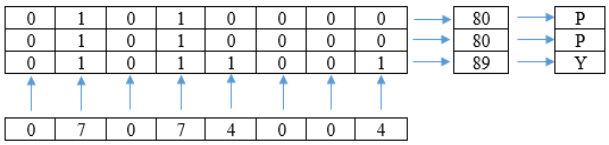


Figure 5: Decryption steps for Encrypted Message

3.2 Multilevel 2-D Haar DWT based Steganography

Two dimensional (2-D) Discrete wavelet transform (DWT) method is one of the most important techniques in transforming a spatial domain image into a frequency domain image [8]. This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level j+1 and the details in three orientations (horizontal, vertical, and diagonal) [8]. HDWT is the easiest and most commonly used method. HDWT can be implemented by two procedures: (1) Horizontal Operation and (2) Vertical Operation [8]. First the Horizontal Operation is utilized to decompose an image into a low frequency band (L) and a high

Frequency band (H). Second Vertical Operation is utilized to partition L and H into LL, LH, HL and HH different frequency bands, each of which possesses ¼ of the original image size [8]. HH represent High Frequency band, LL is low frequency band and LH & HL are middle frequency bands. The coefficients in LL are paramount. If any of the coefficients in LL frequency band are changed, observer can visibly see that the corresponding spatial domain image has been changed [8]. Human eyes are not sensitive to change of HDWT coefficients in HH [8]. For any reason, when any coefficients in HH are altered, an observer can arduously (difficultly) distinguish the change in the spatial domain image [8]. After transform, store message bits into HH frequency coefficients we can use LSB method because it is simplest and very popular method in spatial domain. When using LSB, we does not need original cover image for extracting secret message than that are needed into other methods in spatial domain such as XOR Method.

In multilevel 2-D HDWT, we can apply 2-D HDWT on NXN image up to k level where $k=\log_2 N$. For ex, if image has 256X256 size then we can apply 2-D HDWT on that image up to $k=\log_2(N)=\log_2 256=8$ levels.

Let's consider image has 8X8 pixel size then decomposition of this image using multilevel 2-D HDWT up to 3- levels shown in Fig.

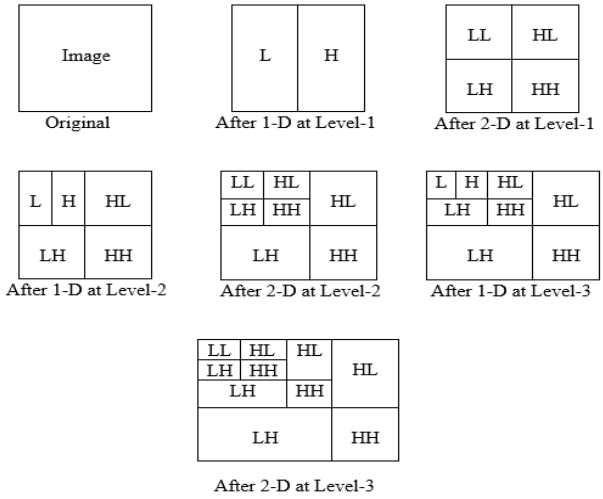


Figure 6: 3- Level 2-D HDWT

4. PROPOSED WORK

In this section, proposed work deals about Modified ASCII Conversion and Cyclic Mathematical function based Cryptography technique and multilevel 2-D HDWT. Advantages of this work are high invisibility even with large message size. Accepted levels of imperceptibility, excellent PSNR values, and high robustness, capacity and security. The proposed data hiding embedding and extracting procedure can also be described as follows.

4.1 Embedding Procedure

Input: An n × n cover image and a secret message.

Output: An n × n stego-image.

Algorithm:

Steps:

1. Read the cover image.
2. Covert it into gray scale image.
3. Read the secret message.
4. Apply Encryption procedure of ASCII conversion and Cyclic mathematical function based Cryptography to create binary message vector.
5. Decompose the cover gray scale image by using Haar wavelet transform up to $k=\log_2 n$ levels.
6. At each level, store secret message bit into high frequency coefficient of each dimension of 2-D HDWT.
7. Apply inverse DWT.
8. Convert gray scale image to prepare stego image for display.

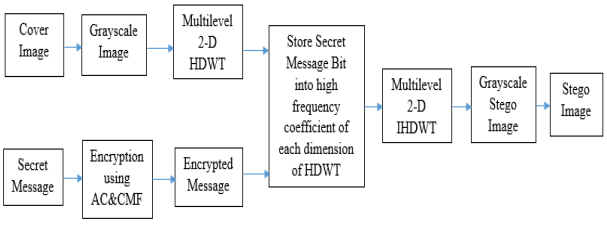


Figure 7: Embedding Procedure

4.2 Extracting Procedure

Input: An n × n stego Image.

Output: A Secret Message.

Algorithm:

Steps:

1. Read the Stego image.
2. Covert it into gray scale image.
3. Decompose the stego gray scale image by using Haar wavelet transform up to k=$\log_2$n levels.
4. At each level, extract secret message bit from high frequency coefficient of each dimension of 2-D HDWT and collect that bit into array.
5. Prepare Message Vector.
6. Apply Decryption procedure of ASCII conversion and Cyclic mathematical function based Cryptography to create original message to display secret message.

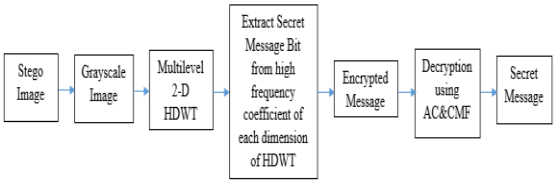


Figure 8. Extracting Procedure

5. MEASUREMENT OF IMAGE STEGANOGRAPHY

5.1 Mean Square Error (MSE)

MSE is used to measure the distortion (Difference) between the original cover image and the stego image.

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{j=1}^{\mathrm{M}} \sum_{k=1}^{\mathrm{N}} (\mathrm{X_{j,k}} - \mathrm{X'_{j,k}})^2 \quad (3)$$

5.2 Peak Signal to Noise Ratio (PSNR)

The PSNR computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a stego-image. The higher the PSNR, the better the quality of the stego, or reconstructed image.

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \mathrm{DB} \quad (4)$$

5.3 Normalized Cross Correlation (NCC)

Normalized Correlation coefficient (NCC) between recovered and original secret image, is used as a metric for performance evaluation. The value of NCC lies between -1 and +1. If two images are identical, then its value will be +1, if they are completely opposite then its value will be -1 and it will be 0 if images are completely uncorrelated.

$$\mathrm{NCC} = \sum_{j=1}^{\mathrm{M}} \sum_{k=1}^{\mathrm{N}} (\mathrm{X_{j,k}} - \mathrm{X'_{j,k}})^2 \frac{1}{\sum_{j=1}^{\mathrm{M}} \sum_{k=1}^{\mathrm{N}} (\mathrm{X_{j,k}})^2} \quad (5)$$

5.4 Average Difference (AD)

It is used to measure average difference between original cover image and stego image.

$$\mathrm{AD} = \sum_{j=1}^{M} \sum_{k=1}^{N} \frac{(X_{j,k} - X'_{j,k})^2}{MN} \quad (6)$$

5.5 Structural Content (SC)

It is used to give structural content between original cover image and stego image.

$$\mathrm{SC} = \sum_{j=1}^{\mathrm{M}} \sum_{k=1}^{\mathrm{N}} (\mathrm{X_{j,k}})^2 \Big/ \sum_{j=1}^{\mathrm{M}} \sum_{k=1}^{\mathrm{N}} (\mathrm{X'_{j,k}})^2 \quad (7)$$

5.6 Maximum Difference (MD)

It is used to measure maximum difference between original cover image and stego image.

$$\mathrm{MD} = \mathrm{MAX}(|X_{j,k} - X'_{j,k}|) \quad (8)$$

5.7 Normalized Absolute Error (NAE)

It has observed acceptable security and imperceptibility.

$$NAE = \sum_{j=1}^{M} \sum_{k=1}^{N} (|X_{j,k} - X'_{j,k}|) \Big/ \sum_{j=1}^{M} \sum_{k=1}^{N} (|X'_{j,k}|) \quad (9)$$

6. EXPECTED RESULT

In Our Proposed Work, We will try to achieve all three aspects of data hiding by following way.

Security will be achieved by using ASCII conversion and Cyclic Mathematical function based cryptography which provides high level security by converting secret data into unprintable data without using any secret key or public key distribution.

Robustness will be achieved by using Haar DWT which is one of methods of Frequency domain by converting spatial domain coefficients into Frequency domain coefficients.

Capacity will be achieved by first storing secret data into 1-D High Frequency Coefficients and then storing another secrete data into 2-D high frequency Coefficients at multiple levels of Haar DWT transformation of Cover image.

By using this method, if image has **NxN** pixel size then **(NxN)-1** bits will be stored. This payload capacity has higher value than that can be achieved in existing systems.

If image has NXN size the maximum level is K=$\log_2$N.

For 256X256 image we will perform maximum level up to K=$\log_2$ (256) =8 levels and at each level we use HH Band to store secret data.

Table 1: Payload Capacity

Level	Payload Capacity (Bits)		
	After 1-D	After 2-D	Total
1st Level	256x128=32768	128x128=16384	0+32768+16384=49152
2nd Level	128x64=8192	64x64=4096	49152+8192+4096=61440
3rd Level	64x32=2048	32x32=1024	61440+2048+1024=64512
4th Level	32x16=512	16x16=256	64512+512+256=65280

5th Level	16x8=128	8x8=64	65280+128+64= 65472
6th level	8x4=32	4x4=16	65472+32+16=6 5520
7th Level	4x2=8	2x2=4	65520+8+4=655 32
8th Level	2x1=2	1x1=1	65532+2+1=655 35

7. CONCLUSION

Hereby it is concluded that Image Steganography Using multilevel 2-D HDWT Transform is more robust and provides more payload capacity. And cryptography based on ASCII conversion and cyclic mathematical function provides high level security. The security level of this method can be measured based on the PSNR value. Increase payload and increase threshold (α) PSNR value must be increase. Wavelet takes less time than the curvelet and provide more robustness than discrete cosine transform.

8. REFERENCES

[1] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013

[2] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, June 2013

[3] Chaithra H, Manjula Y, M Z Kurian, Dr.K.B.Shivakumar, Nuthan A C, "Hiding Technique Using FMM, Visual Cryptography and Genetic Algorithm", International Journal for Research and Development in Engineering (IJRDE) 2014. Vol2: Issue3

[4] Rahul Joshi, Lokesh Gagnani, Salony Pandey, "Image Steganography with LSB", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013

[5] Shivani Kundra, Nishi Madaan, "A Comparative Study of Image Steganography Techniques", International Journal of Science and Research (IJSR) Volume 3 Issue 4, April 2014

[6] Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam, "A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key", American Journal of Engineering Research (AJER) Volume-02, Issue-09,2013

[7] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, "A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013

[8] Yung-Kuan Chan, Wen –Tang Chen, Shyr-Shen Yu, Yu-An Ho, Chwei-Shyong Tsai, Yen-Ping Chu, "A HDWT – based reversible data hiding method", Elsevier Inc. 2008

[9] Vikas pratap singh, Prof. Shrikant lade, "Haar wavelet domain analysis of image steganography", International Journal of Technical Research and Applications Volume 1, Issue 5 (Nov-Dec 2013)

[10] Mrs.D.Mathivadhani, Dr.C.Meena, "Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method", IEEE, 2010

[11] Md. Palash Uddin, Md. Abu Marjan, Nahid Binte Sadia and Md. Rashedul Islam, "Developing a Cryptographic Algorithm Based on ASCII Conversions and a Cyclic Mathematical Function", 3rd international conference on informatics, electronics & vision 2014

[12] S.Shanmuga Priya, K.Mahesh, Dr.K.Kuppusamy, "Efficient Steganography Method to Implement Selected Lease Significant Bits in Spatial Domain (SLSB – SD)", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012

[13] Mr. Vikas Tyagi, "Data Hiding in Image using least significant bit with cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

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

[15] Prabakaran. G, Bhavani R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012

[16] G. Prabakaran, Dr. R. Bhavani, K Kanimozhi, "Dual Transform Based Steganography Using Wavelet Families and Statistical Methods", IEEE, 2013

[17] Nadiya P v, B Mohammed lmran, "Image Steganography in DWT Domain using Double-stegging with RSA Encryption", International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPR], 2013

[18] Pratibha Sharma, Shanti Swami, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform", Conference on Advances in Communication and Control Systems 2013

[19] S.Bhargav Kumar, K.Esther Rani, "FPGA Implementation of 4-D DWT and BPS based Digital Image watermarking", International Journal of Engineering Trends and Technology- Volume 3 Issue2-2012

[20] Nikita Kashyap, G. R. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", I.J.Modern Education and Computer Science, 2012

[21] N.V.S. Sree Rathna Lakshmi, "A Novel Steganalytic Algorithm based on III Level DWT with Energy as Feature", Research Journal of Applied Sciences, Engineering and Technology, May 15, 2014