

Image Steganography using IWT along with AES Encryption

Samruddhi Yadav¹, Prof.Swati Deshpande², Prof.Smita Bansod³

Information Technology, Shah & Anchor Kutchhi Engineering College, Mumbai

Abstract:

Steganography is a process that involves hiding a secret message in an appropriate carrier like image, audio, video or text in such a way that secret message does not attract attention to itself and remains invisible. Cryptography is an art of protecting information by transforming it into an unreadable format called Cipher text only those possessing a secret key can decipher the message into plain text. A combined approach using Image Steganography and Privatekey Cryptography has been proposed, the cover image is transformed using Integer Wavelet Transform (IWT) and plain text (secret message) is encrypted using Advanced Encrypted Standards (AES). The Encrypted text is then embedded into cover image using proposed assignment algorithm. This system will offer higher security and robustness against image processing attacks and low-pass filtering attacks compared to older system with good embedding capacity, also the stego image and the secret message will have good visual quality. The system will have improved results in terms of PSNR and MSE values.

Keywords — - Encryption, Decryption, AES, 2DHaarIWT, Cryptography, Assignment algorithm.

I. INTRODUCTION

With the current advent of technology, data security is very essential these days. Data security basically means protection of data from unwanted and unauthorized access over the internet. The main targets of Steganography are to hide the secret message into the cover image in such a way that the attacker is not able to sense the hidden message and data remains invisible. The cover image is used to carry the secret message, it uses the fact that human eyes are insensitive to very minute changes to the colours and hence, intelligently embeds the data and transmits it to the receiver. When received, the data is securely retrieved by extraction. Steganography when combined with Cryptography provides double benefits and security, as Cryptography transforms message in to unreadable format called Cipher text and only those possessing a secret key can decipher it, hence secret information remains unreadable as well as hidden.

There are two forms of steganography spatial domain and transform domain. Each one of them has several data embedding and compatible extraction techniques. Unlike spatial domain

steganography where data is hidden within the pixel values itself, in transform domain steganography data is hidden in the transform domain (usually Fourier Transform, Discrete Cosine Transform (DCT), Fast Fourier Transform or Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT)) of the image. For example, the IWT of an image can be represented as an image in frequency domain in terms of coefficients, which basically represents the repetitive nature of the image pixels. In Transform domain steganography, the IWT of an image is taken and an embedding technique is used to hide the secret information on the transformed image. Then inverse-DWT is performed to get back the image in spatial domain which results in Stego image. The Spatial domain techniques provides good embedding capacity but has low robustness against various image processing attacks, as a result of which secret information can fall into the hands of attacked or get damaged, as a result of this Transform domain techniques are preferred over Spatial domain techniques.

Wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands

(HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image, integer wavelet transform maps integers to integers thus the output can be completely characterized with integers. Hence Integer Wavelet Transform (IWT) is used in the proposed system.

Cryptography can be classified into two types Secret Key Cryptography (SKC) which uses a single key for both encryption and decryption and Public Key Cryptography (PKC) which uses one key for encryption and another for decryption. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are most widely used Secret Key Cryptography (SKC) techniques, Advanced Encryption Standard (AES) provides more security, supports larger key size, faster and less prone to attacks and hence is used in proposed system. In the proposed system combination of IWT and AES encryption is used for more security and proposed Assignment Algorithm is used for embedding data into image.

II. BACKGROUND

A. 2D Haar Integer Wavelet Transform (IWT) [2]

In discrete wavelet transform the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image, integer wavelet transform maps integers to integers thus the output can be completely characterized with integers. Thus it is preferred over all wavelet transforms. The IWT will be derived through lifting scheme. First level decomposition of an image gives Approximation (LL), Horizontal (LH), Vertical (HL) and Diagonal (HH) coefficients. LL coefficients are more sensitive than the remaining

coefficients, so the embedding is done in all the sub bands except LL subband. Since LH, HL and HH coefficients contain edge information more information can be embedded in these coefficients.

Here it is shown by using simple truncation, how we can use lifting schemes to obtain invertible integer wavelet transform .The Haar wavelet transform can be written as follow [2]:

$$\begin{aligned} s_{1,n} &= (s_{0,2n} + s_{0,2n+1})/2 \\ d_{1,n} &= s_{0,2n+1} - s_{0,2n} \end{aligned} \quad (1)$$

Where $s_{i,l}$, $d_{i,l}$ are the n th low frequency and high frequency wavelet coefficients at the i th level respectively.

The output of “(1)” is not integer, the Haar wavelet transform in “(1)” can be rewritten using lifting in two steps to be executed sequentially:

$$\begin{aligned} d_{1,n} &= s_{0,2n+1} - s_{0,2n} \\ s_{1,n} &= s_{0,2n} + d_{1,n}/2 \end{aligned} \quad (2)$$

From “(1)” and “(2)” we can calculate the integer wavelet transform according to:

$$\begin{aligned} d_{1,n} &= s_{0,2n+1} - s_{0,2n} \\ s_{1,n} &= s_{0,2n} + [d_{1,n}/2] \end{aligned} \quad (3)$$

Then the inverse transform can be calculated by:

$$\begin{aligned} s_{0,2n+1} &= d_{1,n} + s_{0,2n} \\ s_{0,2n} &= s_{1,n} - [d_{1,n}/2] \end{aligned} \quad (4)$$

B. AES Algorithm

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the

state. Most AES calculations are done in a special finite field. The block diagram of AES is shown in 'figure 1'. The algorithm steps are given below:

Algorithm steps:

Encryption Algorithm:

1. Key Expansion: round keys are derived from cipher key. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round: Add RoundKey-each byte of the state is combined with a block of the round key using bitwise xor

3. Rounds:

a: Sub Bytes-a non-linear substitution step where each byte is replaced with another according to the lookup table.

b: Shift Rows-a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c: Mix Columns-a mixing operation which operates on the column of the state combining the four bytes in each column.

d: Add RoundKey.

Decryption Algorithm:

1. input: inverse cipher input

2. irstart: state at start of round[r]

3. is_box: state after InvSubBytes()

4. is_row: state after InvShiftRows()

5. ik_sch: key schedule value for round[r]

6. ik_add: state after AddRoundKey()

7. ioutput: inverse cipher output

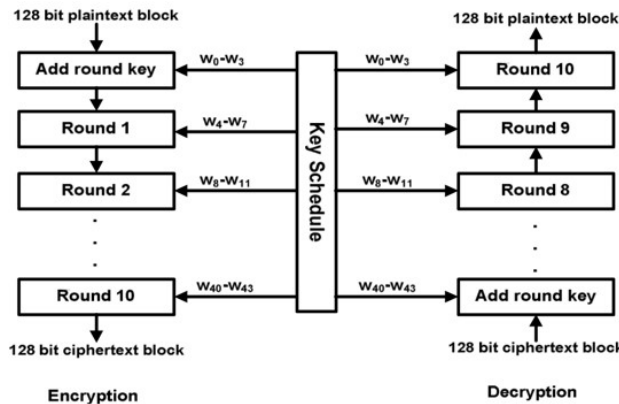


Figure 1. The block diagram of AES

C. Assignment Algorithm

The assignment algorithm is used to embed the data into the IWT coefficients of the cover image. The steps of the assignment algorithm are given below:

Step 1. For each row of the matrix, find the smallest element and subtract it from each element in its row.

Step 2. Find a zero in the resulting matrix. If there is no starred zero in its row or column, star that zero. Repeat for each zero in the matrix.

Step 3. Cover each column containing a starred zero. If n columns are covered, the starred zeros describe a complete set of unique assignments. In this case, stop, otherwise continue with step 4.

Step 4. Find an uncovered zero and prime it. If there is no starred zero in the row containing this primed zero, go to Step 5, Otherwise, cover this row and uncover the column containing the starred zero. Repeat this process until there are no uncovered zeros left. After saving the smallest uncovered value go to Step 6.

Step 5. Construct a path of alternating primed and starred zeros as follows. Let Z0 represent the uncovered primed zero found in Step 4. Let Z1 denote the starred zero in the column of Z0 (if any). Let Z2 denote the primed zero in the row of Z1 (there will always be one). Continue until the series terminates at a primed zero that has no starred zero in its column. Unstar each starred zero of the series, star each primed zero of the series, erase all primes and uncover every line in the matrix, return to Step 3.

Step 6. Add the value found in Step 4 to every element of each covered row, and subtract it from every element of each uncovered column. Return to Step 4 without altering any stars, primes, or covered lines.

III. THE PROPOSED SCHEME

In the proposed system, we overcome the problems of the existing system and introduce Image Steganography using 2D Haar Integer Wavelet Transform and Advanced Encryption Standards (AES) Encryption method. An image is first selected which is called as cover image, this image is then transformed using 2D Haar IWT. After applying IWT the image is decomposed into four

sub-images such as approximation coefficients (CA), horizontal detail coefficients (CH), vertical detail coefficients (CV) and diagonal detail coefficients (CD). A text file which needs to be hidden in the image is selected which is called as secret text, the secret text is encrypted using AES encryption. The sub images and the encrypted text is then divided in blocks of size 2×2 . The best matched block of the secret text of minimum error in approximation band blocks is searched by using the root mean squared error (RMSE). After finding all the error blocks, then for each error block the best matched block in horizontal band blocks is searched by proposed assignment algorithm. The data is then hidden in those blocks.

The steps of embedding procedure are as follows:

Step 1. Decompose the cover image into four sub-images (ICA, ICH, ICV, ICD) using 2D Haar integer wavelet transform. Select the secret text and encrypt it using Advanced Encryption Standards.

Step 2. The sub-images and the encrypted text is decomposed into size of (2×2) blocks.

Step 3. For each text block, the best matched block of minimum error in ICA (approximation band) is searched by using the root mean squared error (RMSE).

Step 4. After finding all of the error blocks in step3, then for each error block, the best matched block in ICH (horizontal band) is searched by Munkres' assignment algorithm. The data is then embedded in best matched block.

Step 5. After embedding all of blocks in step 4, apply the inverse IWT to the ICA, ICV, ICD, and the modified sub-image ICH to obtain the stego image. "Fig. 2" shows the block diagram of the embedding algorithm.

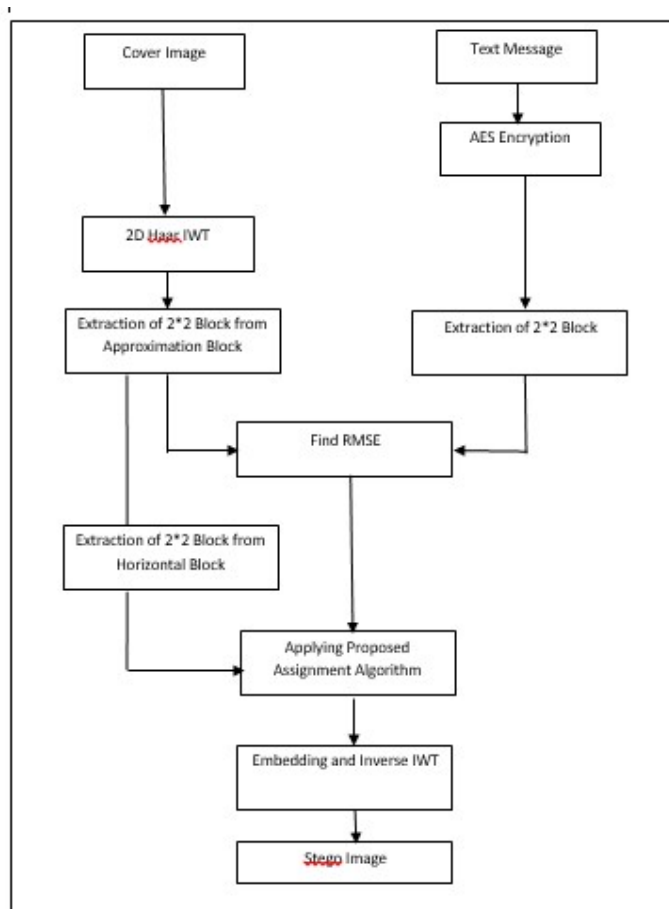


Figure 2. The block diagram of the embedding algorithm

IV. RESULTS

Following are the analysis parameters:

1. Different types of images:

The images are of different formats like Joint Photographic Experts Group (JPEG), Exchangeable Image File Format (EIFF), Tagged Image File Format (TIFF), Graphics Interchange Format (GIF), Bitmap format (BMP), Portable Network Graphics (PNG), etc. These image formats are used for testing the system. The cipher text is hidden in these formats and the efficiency of the assignment algorithm is evaluated by testing the stego image by calculating Peak Signal to Noise Ratio (PSNR) and Mean Square error.

2. Different image sizes:

Different size of cover image like (512×512) , (256×256) then (128×128) is taken and cipher text

is hidden in those image, efficiency of the assignment algorithm is evaluated by testing the stego image by calculating Peak Signal to Noise Ratio (PSNR) and Mean Square error.

3. Comparing Cover image and Stego Image:

The stego image is compared with the cover image to check the quality of image.

4. Comparing Histogram of the Cover Image and Stego Image:

The histogram is used to compare original and the cover image to check whether the data is hidden properly or not. The deviation of cover image from the stego image is checked.

Table 1: (512*512) JPEG Cover Image

Cover image name	(512*512) JPEG Image		
	PSNR	SNR	MSE
Leena	62.1738	57.0362	0.1156
Monalisa	61.8783	57.2012	0.1435
Einstein	62.3865	54.4136	0.1554
Vegetables	61.8128	53.0986	0.1651

Table 2: (256*265) JPEG Cover Image

Cover image name	(256*256) JPEG Image		
	PSNR	SNR	MSE
Leena	62.0831	56.8849	0.1203
Monalisa	61.7924	57.1295	0.1416
Einstein	62.4212	54.4658	0.1577
Vegetables	61.7964	53.0950	0.1659

Table 3: (128*128) GIF Cover Image

Cover image name	(128*128) GIF Image		
	PSNR	SNR	MSE
Leena	62.1440	56.9573	0.1233
Monalisa	61.9742	57.2844	0.1419
Einstein	62.5274	54.5720	0.1509
Vegetables	61.6528	53.9660	0.1639

Table 4: (512*512) PNG Cover Image

Cover image name	(512*512) PNG image		
	PSNR	SNR	MSE
Leena	62.2253	57.0877	0.1197
Monalisa	61.8831	57.2060	0.1404
Einstein	62.5419	54.5689	0.1540
Vegetables	61.7308	53.0168	0.1637


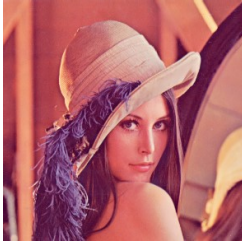




Table 5: (256*256) BMP Cover Image

Cover image name	(256*256) BMP image		
	PSNR	SNR	MSE
Leena	62.0443	56.8464	0.1193
Monalisa	61.9292	57.2665	0.1411
Einstein	62.5935	54.6382	0.1538
Vegetables	61.5998	53.8987	0.1634

The Cover Image Leena of size (512*512) JPEG, Monalisa (256*256) GIF and Einstein (128*128) PNG are compared with their Stego image which is

in BMP format. The comparison table is shown in table 6.

Table 6: Comparing Einstein Cover Image and Stego Image.

Cover Image	Stego Image
	
	
	

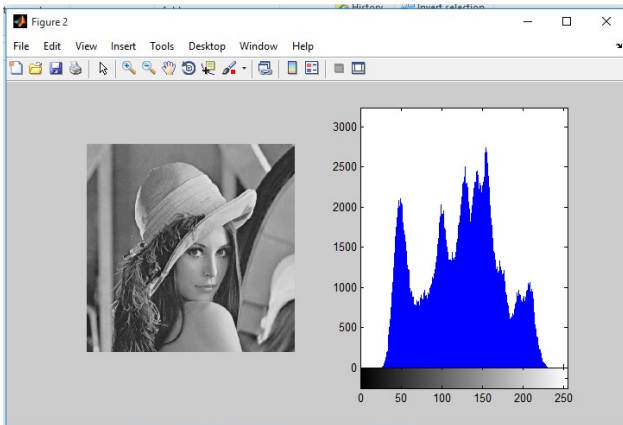


Figure 3: (512*512) JPEG Leena Stego Image

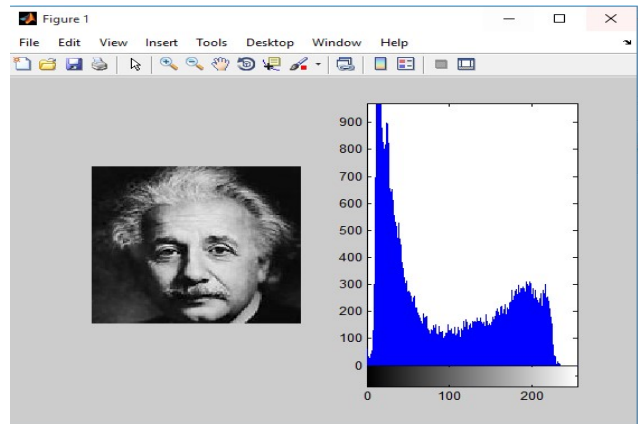


Figure 4: (256*256) PNG Einstein Stego Image

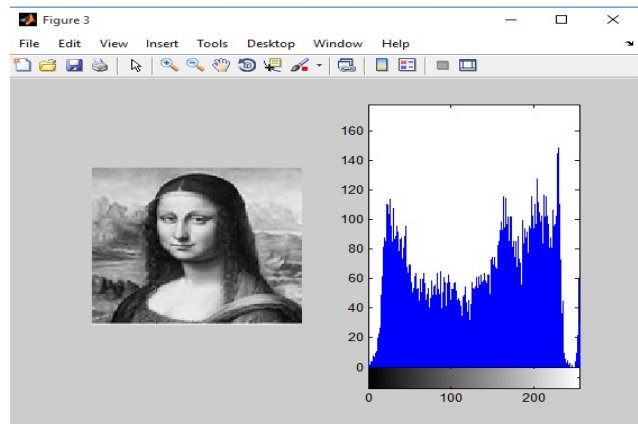


Figure 5: (128*128) GIF Monalisa Stego Image

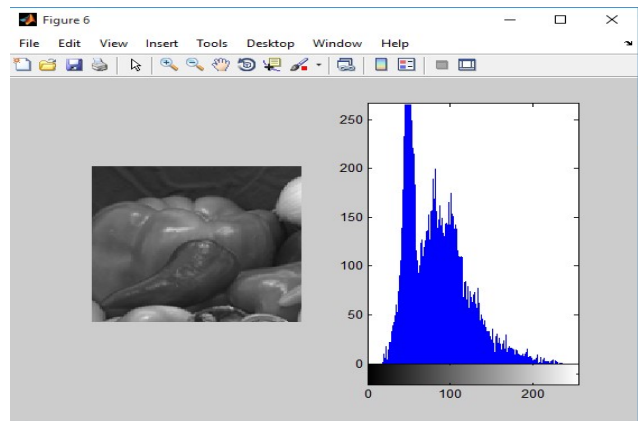


Figure 6: (256*256) PNG Vegetables Stego Image

V. CONCLUSION

Steganography provides security mechanism against unwanted access to important resources by hiding information in some another data such that the information remains invisible to the attacker and he is unable to distinguish between the hidden and the visible data. But Spatial domain steganography are prone to attacks like image compression and low pass filtering even though their embedding capacity is high. In this proposed system Integer Wavelet Transform (IWT) is used which has a high robustness against image processing attacks and compression. Advance Encryption Standards (AES) Encryption is used to enhance more security of the system and provide more protection. Assignment Algorithm is used to enhance the embedding capacity of the system. The proposed system will offer more protection and security to the important hidden information along with high embedding capacity and low distortion of the original image. It will provide better PSNR and MSE than other existing systems.

- International Conference on Informatics, Electronics & Vision, IEEE, 2014.
- [9] Jas R Sheth. "Snake and Ladder Based Algorithm for Steganographic Application of Specific Streamline Bits on Prime Gap Method." International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCCICT), IEEE, 2014.

REFERENCES

- [1] Neda Raftari and Amir Masoud Eftekhari Moghadam. "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm." Sixth Asia Modelling Symposium, IEEE, 2012.
- [2] Thanikaiselvan V and Arulmozhivarman P. "High Image Steganography Using IWT and Graph Theory." International Conference on Signal and Image Processing Applications (ICSIPA), IEEE, 2015.
- [3] S.Thenmozhi and Dr.M.Chandrasekaran. "Novel Approach for Image Stenography Based on Integer Wavelet Transform." International Conference on Computational Intelligence and Computing Research, IEEE, 2012.
- [4] Souvik Bhattacharyya, Avinash Prasad Kshitij, and Gautom Sanyal. "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform.", International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE, 2010.
- [5] Prajanto Wahyu Adi, Farah Zakiyah Rahmanti and Nur Azman Abu. " High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function." International Conference on Science in Information Technology (ICSITech), IEEE, 2015.
- [6] Md. Palash Uddin, Mousumi Saha, Syeda Jannatul Ferdousi, Masud Ibn Afjal and Abu Marjan. "Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography." The 9th International Forum on Strategic Technology (IFOST), IEEE, 2014.
- [7] Nadiya P V and B Mohammed Imran. "Image Steganography in DWT Domain using Double-stepping with RSA Encryption." International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPR], IEEE, 2013.
- [8] Md. Rashedul Islam, Ayasha Siddiq, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain. "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography." 3rd