ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MATHEMATICAL TRANSFORMATIONS WITH SPIHT ALGORITHM FOR STEGANOGRAPHY TECHNIQUES

[1]NAJI MUTAR SAHIB, [2]TAHA MOHAMMAD HASAN, [3]MENA MOHAMMED ABOOD

[1]Department of Computer Sciences, College of Science, Diyala University, Diyala, Iraq

[2]Department of Computer Sciences, College of Science, Diyala University, Diyala, Iraq

[3]Department of Computer Sciences, College of Science, Diyala University, Diyala, Iraq

E-mail: [1] al.sahib@sciences.uodiyala.edu.iq, [2]dr.tahamh@sciences.uodiyala.edu.iq ,

[3]menamohammedabood@gmail.com

ABSTRACT

Due to the rapid and immense development within information transmission and communications, there is a growing need for the usage of steganography techniques which greatly stimulated the emergence of intensive research activities to study steganography. The current paper submits a new system for steganography technique which relies on discrete transforms with SPIHT (Set Partition in Hierarchical Trees) algorithm. The system is able to hide secret massages in a colored cover image. This picture is split up into pixel blocks in the ratio 8x8. Haar wavelet transforms, DCT (Discrete Cosine Transform) and SPIHT algorithm are in turn used on each lock in order to get our (LIP) list, which points out the unnecessary pixels, which represent the optimum locations for hiding the secrete massage. The paper presented two ways for hiding, the first is in (band Blue) and the second is in (band Blue and Green), and we made a comparison between the results of the two methods. Another approach, which is based off of DWT (Discrete Wavelet Transform) as well as Haar wavelet transforms with SPIHT algorithm, is also presented in this paper. The two approaches were compared through capacity, correlation, PSNR and MSE.

Keywords: *Steganography, DCT, DWT, Haar Wavelet Transform, SPIHT Algorithm.*

1. INTRODUCTION

Today, information security becomes one of the most significant aspects of communication and information technology because of the massive height of the WWW and the copyright laws. Cryptography was produced as a technique for securing the privacy of information. Unfortunately, sometimes it is insufficient to maintain the contents of a message secretly, so other means may also be needful to maintain the secrecy of the message, and the term responsible for this is called steganography [1].

Steganography is one of the most and secure effective data communications. It protects the secret messages by embedding them into digital media and making them invisible and inconspicuous to eavesdroppers [2]. In contrast to the classical cryptography which results in hiding the content of secret messages being exchanged between the two sides of communication, steganography aims to hide not only the content but also its very existence. Therefore, it offers a better security in many ways. There are couple other technologies that are connected in a close manner to steganography are fingerprinting and watermarking [3] which involve the information embedded in some media. Mainly, these technologies concerned with protecting intellectual property; hence, the requirements of algorithms are different than steganography requirements [4]. The type of information covered by objects when using watermarking technique are usually an ownership for the purpose of copyright protection or signature to signify origin [5]. On the other hand, the use of fingerprinting involves unique, different marks embedded in distinct copies of the carrier objects which are supplied to different customers [4].

The most important aim of steganography is the improvement of security in communication by embedding some secret messages within a digital image, as well as to modify the nonessential pixels in said image [6]. The image is so-called stego-image, after the secret message is embedded, a public channel will carry it to a particular receiver.

Generally, two approaches exist for image steganography, the first is spatial domain technique, while the second technique is frequency domain. In image steganography, the cover image is where the secrete data is embedded.

One of the most common and understandable known method is Least Significant Bit (LSB) technique, where the secret data takes the place of LSB of the cover image [7]. However, this technique for secret data hiding is considered to be inefficient due to the loss of data that occurs after file transformation [8]. A new method has been introduced, it is based on (DCT) Discrete Cosine Transform transformation [9]. The major focus was on increasing the capacity of hiding the secret data.

2. AIM, OBJECTIVES AND EXPECTED RESULTS

The aim of the paper is to provide a new algorithm that includes two different approaches to hide information in binary media based on a discrete mathematical transform and SPIHT algorithm
The objective with the paper are to:

- Obtaining high security for information, efficiency and performance of the proposed algorithm
- Evaluate different kinds of information carriers, i.e., file formats, in respect of efficiency and performance.
- Identify detection methods for different carriers and media.

The expected results with this paper are to show the possibilities and threats with steganography. The result shall give an indication about the strength of hiding data in streaming media.

3. LITERATURE SURVEY

- Chu, Y.P., et al [2004] [10]: a VQ compressing process is applied with the intention to compress a secret gray-level picture as a pre-embedding procedure. The next step is the encryption process which is taken out on the secret image as mentioned before. Next the image is embedded into DWT coefficients of the cover image. In the event that the stego-image is damaged, yet the PSNR is still below 36dB, a recovery strategy for the mentioned image is undergone.
- **Mythreyi S, et al [2007] [11]:** the Gabor coefficient of the picture is changed so that the secret messages may be embedded in the proposed steganography scheme.
- **Abdelwahab and Hassan [2008] [12]:** both the secret messages and the images go through the **DWT** process which involves hiding data within the **DWT** domain. One aspect considered to be a drawback however, is that the data extracted differs from the embedded data.
- **Bao P. and Ma X. [2005] [13]:** taking the the singular value decomposition in the wavelet domain of an image in order to embed a watermark.
- **Maity S.P. and Kundu M.K. [2004] [14]:** A billed technique for applying watermarks is proposed to embed redundantly in the multilevel wavelet coefficients of the RR and LL band of the cover image. It is said that the scheme has robustness and the ability of detecting how severe any given external attack which has already happened in the watermarked image, however the value of **PSNR** is not very high.

4. SPIHT ALGORITHM

In 1996 William Pearlman and Amir Said developed the **SPIHT** algorithm [15] (Set Partitioning into Hierarchical Trees). This compression algorithm is based on the following concepts:

- The partial order of the transformed elements from the images magnitude as well as passing on the ordered information.
- The transmission of ordered bit plane.
- To what extent the degree of similarity is found to be in regards to the coefficient as well as various levels of the wavelet is applied. Each must describe the same point of origin.

4.1 The Spatial Orientation Tree

A chosen structure in the form of a tree, which can be referred to as orientation tree [16], shown in Figure 1, depicts a visual representation of the transformed image. The nodes of the tree act in accordance with a coefficient as their identification is relative to of the positioning of these points. When looking upon the wavelet level directly after the previous wavelet, the coordinates which attach directly continue to keep the same spatial direction

Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of representation. This in turn owns more detailed resolution. As has been shown, there are two directions which this can go in: either there are four descendants (represented as leaves), or zero. The descendants make up a group of (2 × 2) coordinates which are adjacent. The highest nodes, in accordance with the hierarchy, represent the only exceptions, where there were no descendants for the coordinates in the low – low band. The coordinates which are within one wavelet level match up with the nodes at the same hierarchy level

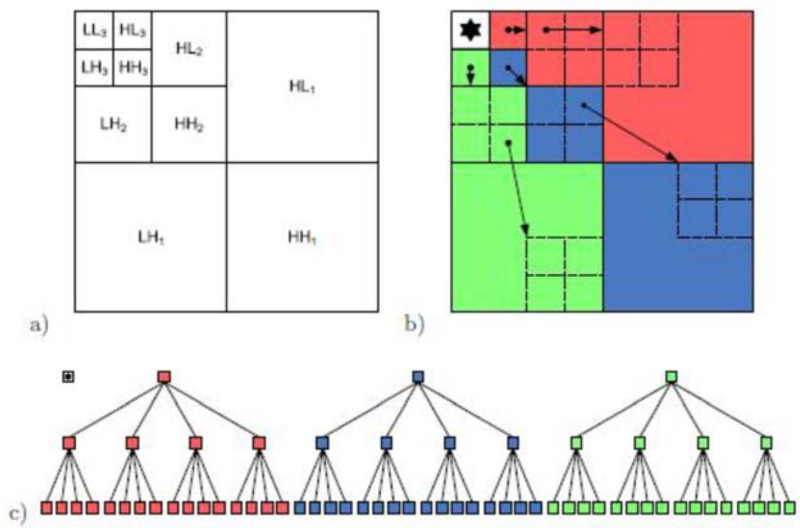


Figure 1: Building the Spatial Orientation Tree [15]: (a) Pyramidal form Created by the Wavelet Transformation, (b) Relationship Between Offspring, (c) Transformed Image Represented as Tree.

4.2 The SPIHT Algorithm

These are the coordinate sets which play an essential part in the SPIHT algorithm [15], [17]:

- H (i, j) coordinate set representing tree roots, the nodes which are in the highest level of all the wavelets
- O (i, j) = {(2i, 2j), (2i, 2j +1), (2i+1, 2j), (2i+1, 2j +1)}, the coordinates representing the node's children (i, j)
- D (i, j) represents all the descendants of node (i, j)
- L (i, j) = D (i, j) \ O (i, j) representing all descendants, excluding the children of node (i,j).

The usage of this function is to indicate the significance of specific coordinates T.

$$S_n \ (T) = \begin{cases} 1, & MAX\{|c_{i,j}|\} \geq 2^n \\ 0, & otherwise \end{cases} \qquad (1)$$

In order to make significant information stored, three ordered sets are utilized:

- The coordinates in **LIP,** the list of insignificant pixels, are not so vital in regards to the current threshold.
- On the other hand, important or relevant coordinates of the coefficients (in regards to the current threshold), are placed in the list **LSP** which contains significant pixels.
- The list **LIS** contains the location points of the roots from insignificant sub trees. The coefficients in **LIS** are all refined in a compression stage, and those that are shown to be important or relevant after this procedure are taken from **LIP** a placed in **LIS**.

5. MATHEMATICAL TRANSFORMS

5.1 DCT

In JPEG compression, **DCT** coefficients are use. It divides the image into segments, each of which holds different importance. It transforms a ∑ into frequencies of low, high and middle values. The sub-band of low frequency, the most vital visual pieces of an image are contained in low frequency, where the major part of signal energy is lying. Whilst in this sub-band (of high frequency), the components of the image, which themselves are at higher frequencies, are generally taken out through noise attacks and compression. So by modifying the coefficients of the middle frequency sub-band, the secret message is embedded, so that no effect will appear on the visibility of the image. The following equation defines a common equation for a 1D (N data items) **DCT**: [18] [19].

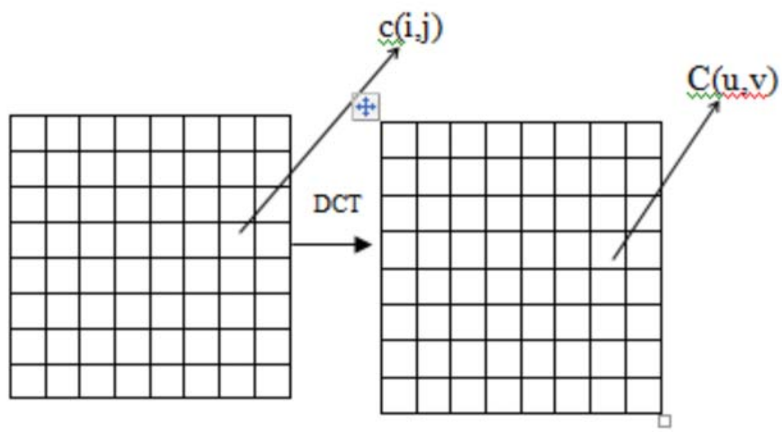


Figure 2: Discrete Cosine Transformation of Images [17].

Although the following is a valid representation of the1D (N data items) **DCT**:

$$C(u) = \sqrt{\frac{2}{N}} \sum_{i=0}^{N-1} \Lambda(i) \cos\left[\frac{4\pi}{2N}\ (2i+1)\right] C(i) \quad (2)$$

The most commonly used equation for a 2D (N by M image) **DCT** is given by the following equation:

$$C\,(u\,,v\,) = \sqrt{\frac{2}{N}}\sqrt{\frac{2}{M}}\ \sum\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} \Lambda(i)\,\Lambda(j).\cos[\frac{\pi u}{2N}\ (2i+1)\cos[\frac{\pi v}{2M}\ (2j+1) C(\,i\,,j\,) \quad (3)$$

5.2. WT

Wavelet transforms (**WT**) refer to the conversion of spatial domain data to frequency domain data. The global frequency distribution of the time signal x(t) is obtained by the Fourier transformed signal XFT (f). In order to reconstruct the original signal, the inverse Fourier transform can be used [20]:

$$X_{FT}(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt \quad (4)$$

$$x(t) = \int_{-\infty}^{\infty} X_{FT}(f) e^{j2\pi ft0} df \quad (5)$$

Previously, before wavelet transformation, Fourier transformation (FT) was the most common and well-known method for this purpose. With its ability to receive both frequency and real time data from a signal, the Short Time Fourier Transform (STFT) surpassed the FT method in terms of what it could achieve. A windowing concept is used in FT along with STFT concept. In this instance, FT is applied to a section of the signal which is covered by a window, where the window over the signal.

$$X_{STFT}(\tau, f) = \int_{-\infty}^{\infty} x(t) g * (t-\tau) e^{-j2\pi ft} dt \quad (6)$$

The local analysis in the wavelet transformation is considered its advantage over the Fourier method**.** The process of analyzing the wavelets, as specified above, is able to uncover essential data such as breakdown points, discontinuities, and more, in a much clearer way than its counterpart.

Two orthogonal functions form the start of a wavelet basis set: the so called father wavelet or scaling function (t) and the mother wavelet or wavelet function ψ(t), a complete basis set is obtained by undergoing a scaling and translation process using the means of these two mentioned functions. These transformations are expressed with the following equation:

$$F(a,b) = \int_{-\infty}^{\infty} f(x) \psi^*_{(a,b)}(x)\, dx \quad (7)$$

Where the * represents the complex conjugate symbol as well as mother wavelet or wavelet function refers to the function ψ.

Discrete transformation of wavelets as well as continuous transformation are the two methods with which the wavelet transformation can be implemented. Continuous wavelet transforms (CWT) can be defined by:

$$X_{WT}(\tau, s) = \frac{1}{\sqrt{|s|}} \int x(t).\psi^*\left(\frac{t-\tau}{s}\right) dt \quad (8)$$

The transformed signal (XWT, s) is a function of the translation parameter and the scale parameter s. ψ is representative of the so called mother wavelet, the * is a representative of the complex conjugate [21].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. THE PROPOSED SYSTEM

The proposed system includes two approaches to hide a secret message in the final image. The first approach (A) uses the base of **DCT** and Haar **WT** with the **SPIHT** algorithm, and the approach (B) is based on **DWT** and Haar **WT** with **SPIHT** algorithm, as shown in Figure (3)

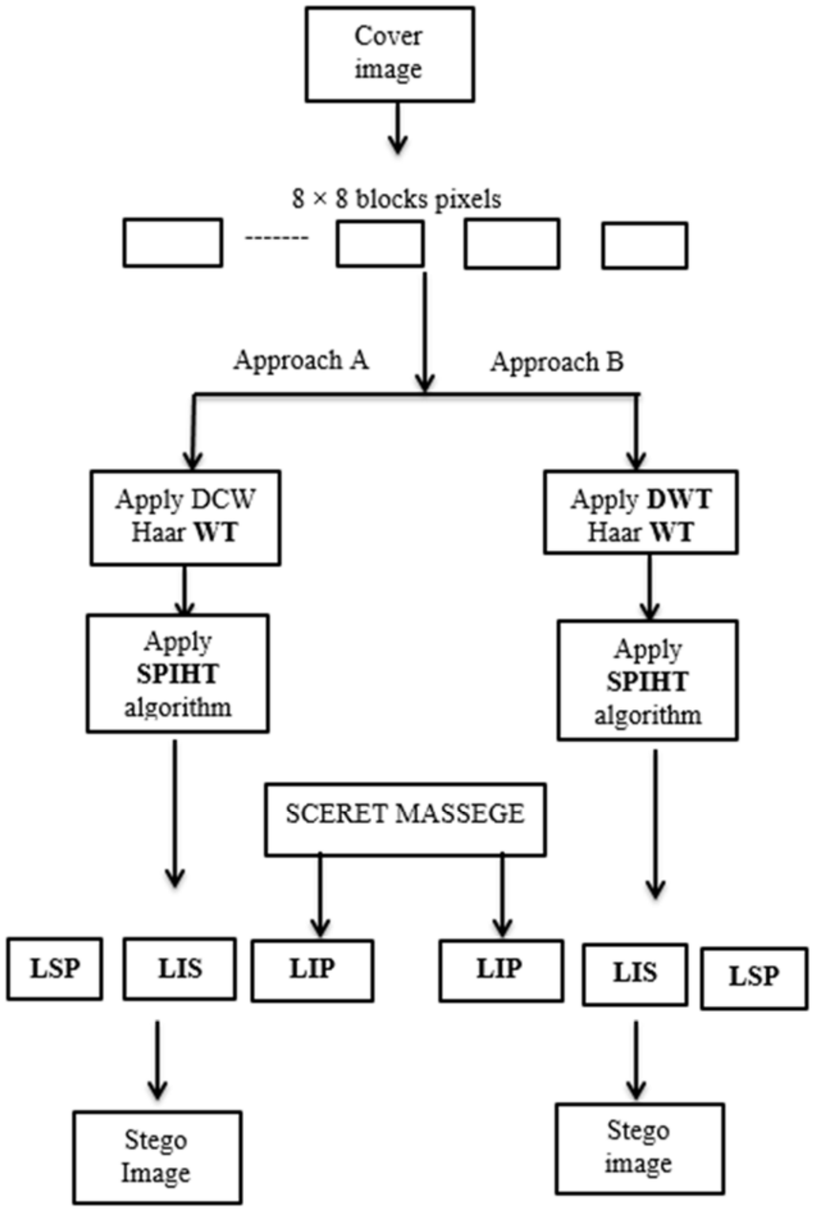


Figure 3: The Proposed System

6.1 Approach A

Part 1: Haar wavelet and **DCT** transform implementation:

In this part, the colored picture is split up into several bo8 x 8 block of pixels. We have used **DCT** in order to convert the 8 x 8 blocks from its spatial to frequency domain. After the conversion, the 8 x 8 blocks are represented as figure (4)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(A)

	1	2	3	4	5	6	7	8
R	192	190	194	198	202	206	208	156
	192	196	198	198	206	206	156	90
	194	196	196	200	204	154	96	88
	190	194	200	200	158	94	82	86
	186	190	198	166	94	84	86	88
	188	192	168	102	84	86	88	94
	222	192	104	86	88	88	96	98
	216	154	88	88	90	92	98	96
B	92	90	90	92	94	100	100	52
	92	92	92	92	96	100	56	14
	92	92	92	94	96	58	26	16
	88	90	96	96	60	22	14	16
	82	84	94	66	18	20	14	16
	86	90	68	26	16	20	16	18
	130	96	24	16	18	16	16	16
	126	66	18	20	16	18	20	24
G	92	90	90	88	92	96	94	72
	96	92	90	90	92	96	74	54
	94	92	90	92	92	76	68	58
	90	90	94	92	72	62	60	60
	90	88	92	76	58	62	56	58
	88	92	76	66	58	64	56	56
	118	96	60	58	60	60	54	56
	108	82	60	60	56	60	58	64

DCT →

(B)

1	2	3	4	5	6	7	8
70	14	0	1	0	0	0	0
12	-3	-6	0	0	0	0	0
1	-3	1	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
70	14	0	1	0	0	0	0
12	-3	-6	0	0	0	0	0
1	-3	1	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
23	-1	0	0	#	#	0	0
-1	1	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
19	2	0	0	#	1	0	0
-1	1	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 4: DCT Implementation (A) Image Data Before DCT (B) After DCT

In order to fulfill the requirement of SPIHT algorithm, the block depicted in figure (4) should be processed by a Haar wavelet filter, Figure (5)

(A)

	1	2	3	4	5	6	7	8
R	192	190	194	198	202	206	208	156
	192	196	198	198	206	206	156	90
	194	196	196	200	204	154	96	88
	190	194	200	200	158	94	82	86
	186	190	198	166	94	84	86	88
	188	192	168	102	84	86	88	94
	222	192	104	86	88	88	96	98
	216	154	88	88	90	92	98	96
B	92	90	90	92	94	100	100	52
	92	92	92	92	96	100	56	14
	92	92	92	94	96	58	26	16
	88	90	96	96	60	22	14	16
	82	84	94	66	18	20	14	16
	86	90	68	26	16	20	16	18
	130	96	24	16	18	16	16	16
	126	66	18	20	16	18	20	24
G	92	90	90	88	92	96	94	72
	96	92	90	90	92	96	74	54
	94	92	90	92	92	76	68	58
	90	90	94	92	72	62	60	60
	90	88	92	76	58	62	56	58
	88	92	76	66	58	64	56	56
	118	96	60	58	60	60	54	56
	108	82	60	60	56	60	58	64

Haar WT →

(B)

1	2	3	4	5	6	7	8
23.25	-1.25	0	0	17.75	-1.75	0	0
-0.5	0.5	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
18.75	1.75	0	0	10.25	1.25	0	0
-0.5	0.5	0	0	1	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
11.25	-0.75	0	0	6.75	-1.25	0	0
-0.25	0.5	0	0	0.75	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
8.25	1.25	0	0	1.75	0.75	0	0
-0.25	0.5	0	0	0.75	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
28	11	0	1	0	0	0	0
8	-2	-4	0	0	0	0	0
1	-2	1	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 5: Haar Wavelet Implementation (A) Before Haar WT (B) After Haar WT

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Part 2: SPIHT algorithm implementation.
Select the blocks from the previous part that satisfy the **SPIHT** algorithm conditions. Apply the **SPIHT** algorithm on these blocks, to get three lists **LIP**, **LIS** and **LSP** where:

LIP: the track of the pixels which are to be worked out is kept by this list.

LIS: the list reduced the computation power due to clustering only relative coordinate and set them ready for further processing.

LSP: stores the track of each pixel that has already been evaluated or needs to be re-evaluated is kept within this list.

Part 3 (steganography)

LIP To start implementing steganography, locations are extracted from LIP dropped onto the cover image, In which data is to be embedded. There are two methods to perform the process of hiding the secret messages:

1. Hide the **LSB** in the band blue.
2. Hide the **LSB** in the [band blue, band green].

Embedding Algorithm
Input: An mx n color picture and a message which must remain secret.
Output: An m x n stego image.
Step 1: Write text message and convert it in binary.
Step 2: Select color cover image.
Step 3: The color cover picture is split up into blocks of pixels in the size 8 x 8.
Step 4: DCT and Haar wavelet transform are applied to each block.
Step 5: Choose the blocks that achieved the highest value in the location (0, 0).
Step 6: Apply **SPIHT** algorithm, to get **LIP**, **LIS** and **LSP**.
Step 7: LIP location are taken from each block, which was nominated by the previous step.
Step 8: The location obtained in the previous step are drawn on the cover image location. The locations obtained are used to hide the secret message.
Step 9: Separate the band red, band green and band blue from the selected locations.
Step 10: Calculate **LSB** of each location in band blue (obtained from the previous step) and change it for each part of the encrypted message.
Step 11: Write the stego-image.

Remake:
1. No changes are occurred by the Band red and it is considered the key of the algorithm when a secret message is retrieved.

2. When use the [band green, band blue] in hiding, the same algorithm above just step 10, when replacing the band blue with the [band blue, band green].

Retrieval algorithm
Input: An m x n stego image.
Output: A message which remains secretavie
Step 1: Stego image is read
Step 2: The picture is split up into 8 x 8 block of pixels.
Step 3: DCT and Haar wavelet transform are applided to each block
Step 4: Choose the blocks that achieved the highest value in the location (0, 0)
Step 5: Apply **SPIHT** algorithm, get **LIP**, **LIS** and **LSP**.
Step 6: Separate the blue, red and green locations band from the selected locations (**LIP**)
Step 7: Calulate **LSB** of each location in band blue.

6.2 Approach B
After being split up into 8 X 8 blocks of pixels, **DWT** has been used to convert the cover image from its spatial domain to frequency domain.in **DWT** images are filtered and splatted into high and low frequency. Information of low frequency contains information about some other places of the image, it is very sensitive information where even a small modification affects the reconstructed picture. However if we look at the other sid of things, the information about the edges, corners, etc. of the image are included in high frequency information, hence modifying this information results less noise in the reconstructed image. After applying **DWT** and Haar wavelet transform. An 8 x 8 blocks are resultant as figure 6 (a).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

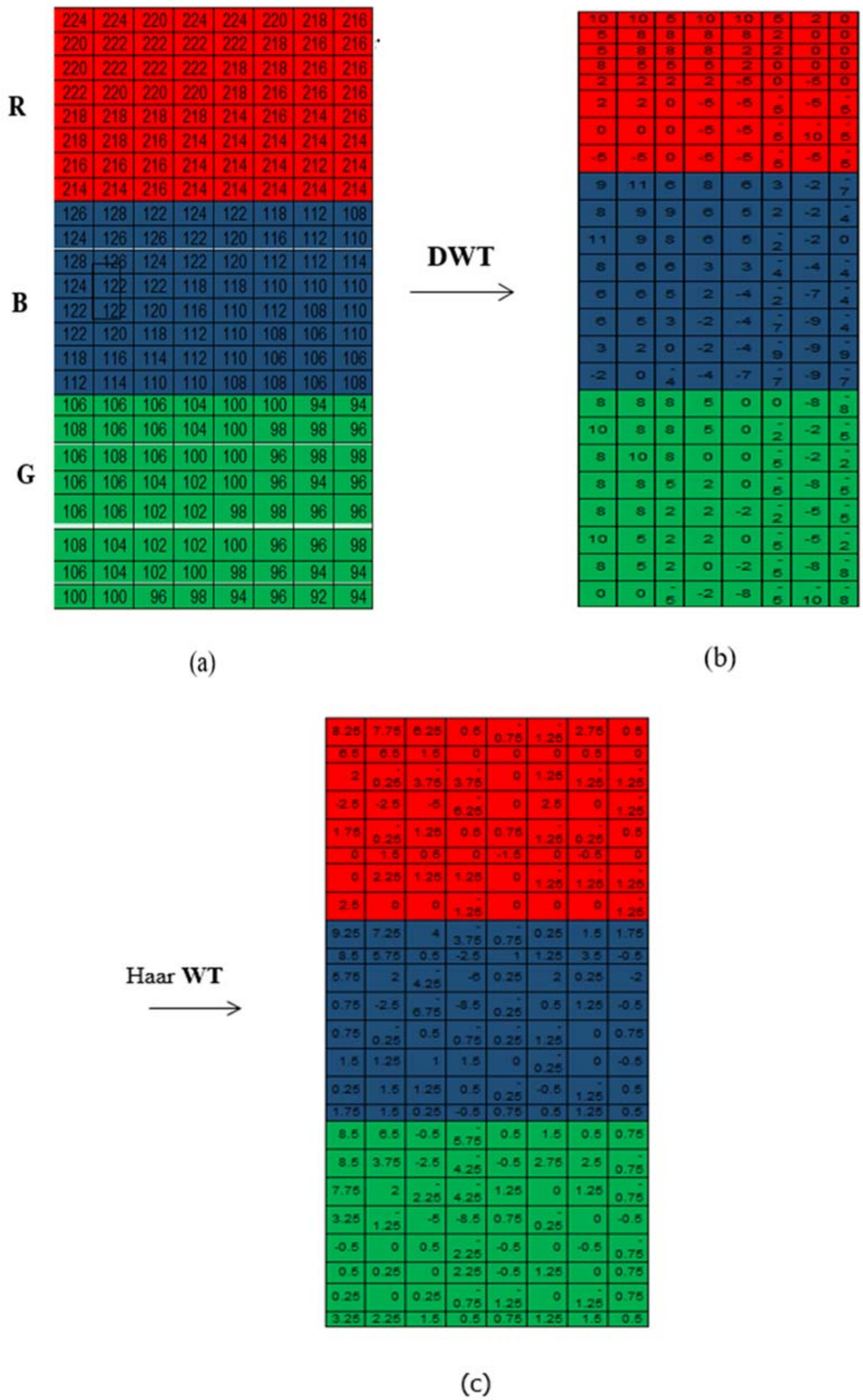


Figure 6: DWT Implementation (A) Image Data (B) After DWT (C) After Haar WT

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SPIHT algorithm is applied to the resulting blocks which achieves a higher condition in the location (0, 0), to get **LIP**, **LIS** and **LSP**. Actions to hide the secret message are performed same to approach A.

7. PERFORMANCE MATRICES

We compare the performance level of the individual methods using the mean square error peak signal to the computation time and noise ratio.

7.1 The Mean Square Error

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR), are used in order to compare the image compression. The MSE represents the accumulated squared error within the original image and the compressed image.

Mean Square Error =
sum(sum(error))) ^2/size (original image) (9)

7.2 Peak Signal to Noise Ratio

The mean-squared error is found first using the equation, as stated below, to compute the peak signal to noise ratio(PSNR),

Then the block computes the PSNR using this equation:
*PSNR=10*log10(255*255/Mean Square Error)* (10)

8. RESULTS AND ANALYSES

The simulation of the findings was performed using Visual Basic 2013 programming language. This paper discusses the performance of mathematical transforms with SPIHT algorithm for steganography techniques. Applying the SPIHT algorithm makes it possible to enhance the PSNR with decreased mean square error. Previous works are compared with the findings and outcomes found within this paper.

The SPIHT algorithm was implemented for 100 iterations. After the iterations are carried out, a higher value for PSNR is obtained. In compression with DWT, the DCT technique using SPIHT algorithm with band (1) generated the maximum PSNR, but because DWT hiding is undergone using an approximation of the coefficient, it is much safer as well as less prone to attacks. 335 characters must be used in order to hide the message in trial pictures.

Through the results described in the table 1, showing that PSNR, MES, and Time of approach A (DCT based SPIHT algorithm), and the results described in the table 2, showing PSNR, MES and Time of approach B (DWT based SPIHT algorithm). The results of Figure 8 ,9 give higher PSNR of band1 than PSNR of band2, and give better MES of band 1 than band 2. The result of Figure 10 ,11 gives higher PSNR and MES of band1 than band 2. The result of Figure 12 compared the PSNR of approach A and approach B, gives better PSNR of approach A. The result of Figure 13 compared the MES of approach A and approach B, gives better MES of approach A. The result of Figure 14 compared the time of approach A and approach B, gives better time of approach B.

Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

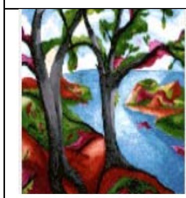
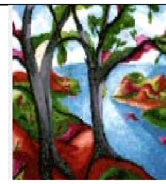
Cover image	Secret message	Stege imag approach band 1	Stege imag approach band 2	Stege imag approach band 1	Stegeo image Pproach B band 2
	Hellow				
	My dear				
	How ar you				
	I am ver happy				

Figure 7: Stege Image Of Approach A And Approach B

Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: PSNR, MSE and TIME Approach A

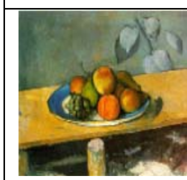
APPROACH A					
Cover image	PSNR band1	PSNR band2	MES band1	MES band2	Time Span
	85.5037904	84.2544030	0.000183105	0.000244140	00:00:02.0280036
	80.422355	42.1607946	0.00059006	3.953674316	00:00:01.9032033
	78.813722	78.6116887	0.000854492	0.000895182	00:00:02464040
	77.0528100	34.8519365	0.001281783	21.2758382	00:00:02.2620040

Table 2: PSNR, MSE and TIME Approach B

		APPROACH B			
Cover image	PSNR band1	PSNR band2	MES band1	MES band2	Time Span
	44.9125338	45.9919808	2.098103841	1.63672884	00:00:00.6240011
	39.3925	41.5618817	7.478637	4.538289388	00:00:00.5148009
	34.815089	34.8215771	21.45709	21.425089	00:00:00.5148009
	78.4186372	77.3376954	0.000935872	0.001200358	00:00:00.5148009

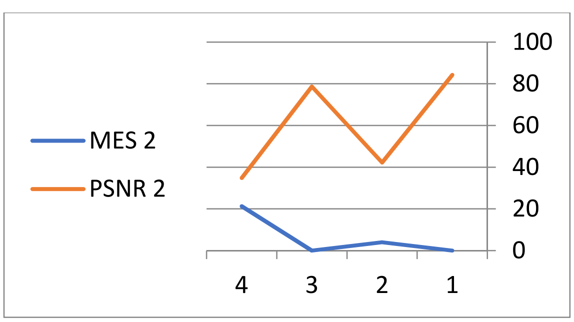


Figure 8: Result PSNR and MES Band 1approach A

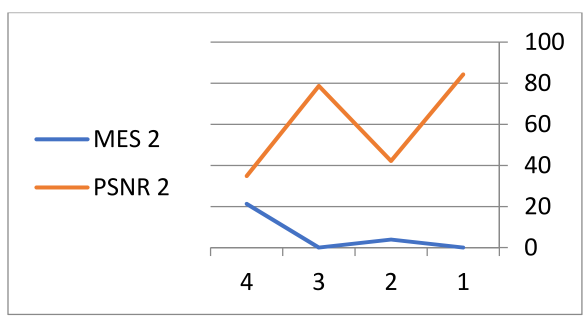


Figure 9: Result PSNR and MES Band 2 approach A

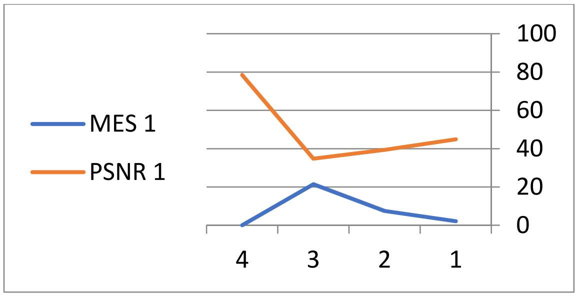


Figure 10: Result PSNR and MES Band 1 of approach B

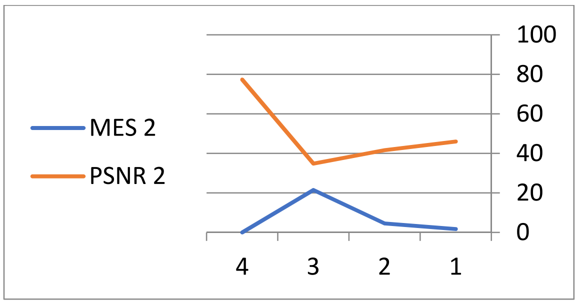


Figure 11: Result PSNR and MES Band 2 of Approach B

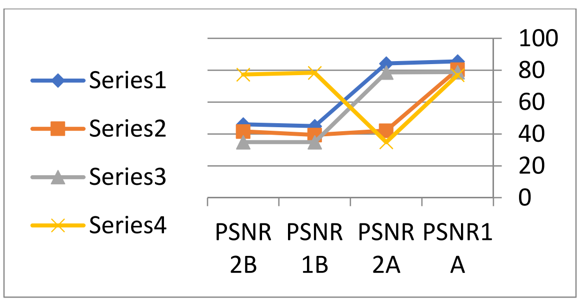


Figure 12: Graphical Comparison of PSNR

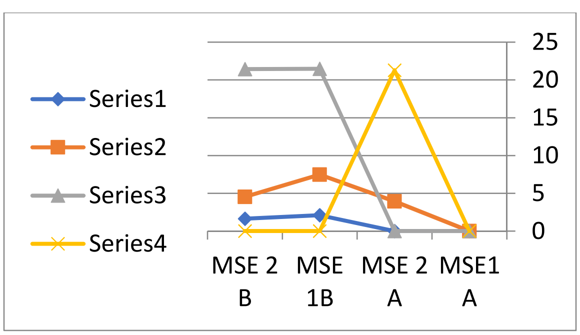


Figure 13: Graphical Comparison of MSE

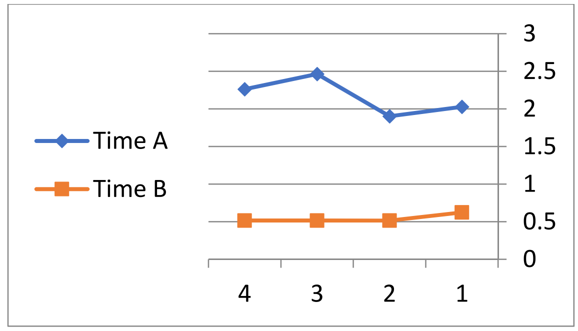


Figure 14: Comparison of Computation Time (in seconds)

9. CONCLUSION

The basic steganography techniques are compared in this paper. The DCT based SPIHT technique (approach A) gives better Performance compared to the DWT based SPIHT technique (approach B). The SPIHT is analyzed in this paper on DCT, the PSNR result was better when compared with others. Hence, the performance is enhanced by the SPITH algorithm with significant SPNR. Through implementing the technique of SPIHT, the DCT gives a very good payload capacity. The use of DCT in SPIHT provides high PSNT, but more time is consumed by DCT compared to DWT. Based on that, the future works will be about to decrease the computation time with an improved PSNR.

10. CONTRIBUTION

A new algorithm has been used to implement steganography which is SPIHT algorithm, the proposal of this paper was built upon using the power of this algorithm to hide data in different wave left levels that describes the same origin; the due to the capability of SPIHT Algorithm to reveal these levels.

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

REFERENCES:

[1]H. N. Abed, N. H. Hassoon, A. L. Ahmed and I. S. Albayaty ,"Hiding Information in an Image Based on Bats Algorithm", Iraqi Journal of Information Technology, vol 8, No2 ,pp 128-141, 2018.

[2] Tian, Lei; Zhou, Ke; Jiang, Hong; Liu, Jin; Huang, Yongfeng; and Feng, Dan, "An M-Sequence Based Steganography Model for Voice over IP" (2008). *CSE Technical reports.* Paper 68.

[3] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal Processing* 90, no. 3 (2010): 727-752.

[4] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," *in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005 (Published electronically)

[5] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing*, *8:08*, 1999

[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998 .

[7] C.S. Lu, "Multimedia security: steganography and digital watermarking techniques for protection of intellectual property". *Artech House, Inc.* (2003).

[8] J.J. Chae and B.S. Manjunath, "Data hiding in Video" Proceedings of the 6th *IEEE International Conference on Image Processing, Kobe, Japan* (1999).

[9] Provos, N., Honeyman, P., "Hide and Seek: An Introduction to Steganography" *IEEE Security & Privacy Magazine 1* (2003).

[10] Chu, Y.P., Guo, S.W., Chan, Y.K. and Wu, H.C. "Image Hiding Based on a Hybrid Technique of VQ Compression and Discrete Wavelet Transform", International Computer Symposium, 313-317 ,2004.

[11] Mythreyi S and Vaidehi V. "Gabor Transform based Image Steganography", IETE Journal of Research, 53(2):. 103 – 112,2007.

[12] A.A. Abdelwahab, L.A. Hassan. "A discrete wavelet transform based technique for image data hiding", in: Proceedings of 25th National Radio Science Conference, Egypt, 2008.

[13] Bao, P and Ma, X. "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition", IEEE Transaction on Circuits and Systems for Video Technology, 15(1):2005

[14] Maity S.P. and Kundu M.K., "A Blind CDMA Image Watermarking Scheme in Wavelet Domain" IEEE International Conference:2633 – 2336,2004.

[15] A. Said and W. A. Pearlman, "A New fast and efficient image codec based on set partitioning in hierarchical trees", IEEE Transaction On Circuits and Systems for Video Technology, vol. 6, no.3 pp 243-250, Jun. 1996.

[16] Tobias Blaser, Stephan Senn, Philipp Stadelmann,"Wavelet-based Compression using the **SPIHT** Algorithm",Chip Design Project, 1st April 2006.

[17] F. Khélifi N. Doghmane And T. Bouden, "Compression Of The Color Images By **SPIHT** Technique", 0-7803- 8482-2©2004 IEEE.

[17] MamtaJuneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on **LSB** Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[19] K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray, Sabyasachi Pattnaik, **"**Coherent Steganography using Segmentation and **DCT**", IEEE-978-1-4244- 5967-4/10/$26.00 ©2010."

[20] Mrs. Archana S. Vaidya, Pooja N. More., Rita K. Fegade, Madhuri A. Bhavsar, Pooja V. Raut, GES's R. H. Sapat College of Engineering, Management Studies and Research, Nashik, "*Image Steganography using **DWT** and Blowfish Algorithms*", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 8, Issue 6 (Jan. - Feb. 2013), PP 15-19

[21] Chui, C. K. (Ed.). Wavelets: *A Tutorial in Theory and Applications*. San Diego, CA: Academic Press, 1992.