High Imperceptibility Image Steganography Methods based on HAAR DWT

Y. Taouil
EECOMAS
Ibn Tofail
University
Kenitra, Morocco

E.B. Ameur
MSISI-LaRIT
Ibn Tofail
University
Kenitra, Morocco

A. Souhar
MSISI-LaRIT
Ibn Tofail
University
Kenitra, Morocco

A. El Harraj
MSISI-LaRIT
Ibn Tofial
University
Kenitra, Morocco

M.T. Belghiti
EECOMAS
Ibn Tofail
University
Kenitra, Morocco

ABSTRACT

While cryptography keeps unknown the hidden content of information, steganography provides a higher level of data security by making even the existence of hidden information secret, it is the art of dissimulating information in digital media considering it as an unremarkable support. In this paper we propose a new two methods of image steganography by using Haar discrete wavelet transform, the secret data are hidden in the frequency domain to minimize the distortions occurring on the cover during the steganographic process. The floating point in the coefficients of the transform can cause a loss in information. To prevent this problem, data is embedded in the integer part of high frequency coefficients in such a way that increases the imperceptibility.

Extensive experiments on variety of images were performed and the results show that the proposed methods provide better image quality and a high imperceptibility in comparison with prior works. This was achieved using a random key that scrambles the location of the pixels where data is hidden.

Keywords

Steganography, Hiding information, Haar discrete wavelet transform, Imperceptibility, Random key.

1. INTRODUCTION

Nowadays, security of information has become a big concern given that the development of communication technology threatens the confidentiality of information [1]. Cryptography protects data by making the message incomprehensible without having access to decryption algorithms, but a coded message that is unhidden, no matter how strong the encryption, is suspicious and attract attention and it may in itself be a problematic, so this is not enough because the secrecy of the content of information is the heart of data security, hence it has become necessary to keep secret even the existence of information, and that is what steganography is about.

Steganography is the science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message [2]. It is the art of hiding information in digital file called cover. Data is hidden in the areas of the cover file that can be modified without causing a visible modification on its shape; this operation produces a stego file which must be indistinguishable to the cover file [3].

The first approaches of Steganography were based on spatial domain, especially the technique of hiding in the Least Significant Bit (LSB) of the image pixels [4].

Hong [5] proposed a reversible data hiding method based on image interpolation; data is embedded into interpolation errors using the histogram shifting technique.

A semi reversible data hiding method that utilizes interpolation and the least significant substitution technique is proposed in [6].

Hu [7] proposed a high payload image steganographic scheme based on an extended interpolating method.

The prominent disadvantage in spatial domain techniques is the vulnerability to the slight attacks.

In the frequency domain approaches, the message is embedded after applying a transformation on the image, this way the hidden message resides in more robust areas providing a better resistance against statistical attacks.

Singla [8] proposed Steganographic methods based on Discrete Cosinus Transform (DCT).

In Wavelet-based steganographic methods, the message is hidden in the wavelet transform of the image and then the stego image is obtained by applying the inverse transform [9].

A high payload steganographic method based on pixel value differencing (PVD) technique is proposed in [10].

In this work, new steganographic methods based on Haar discrete wavelet transform are proposed. The binary bits of the secret message are distributed among the coefficients of H, V, D bands and hidden in the integer part of the coefficients by two methods having a high imperceptibility. The key chooses a random selection of the pixels where data is embedded. The Mean Square Error and the Peak Signal to Noise Ratio are calculated to evaluate the quality of the hiding process.

In section 2, the parameters used to evaluate a steganographic process (Imperceptibility, Capacity and Robustness) are presented. Section 3 reviews the decomposition and the reconstruction algorithms using 2-D Haar discrete wavelet transform. In section 4 we explain the proposed methods. Section 5 discusses the experiment, the comparison of the results of the method of [10] with the proposed methods based on the parameters presented in section 2. Finally, conclusions and future works are given in Section 6.

2. MEASURES TO ESTIMATE THE PERFORMANCE OF A STEGANOGRAPHIC PROCESS

A steganographic algorithm is evaluated by three important parameters: Imperceptibility, Capacity and Robustness, which are explained below [11, 12, 13]:

Imperceptibility: A steganographic process is imperceptible when human eye cannot distinguish between the cover image and the stego image. This parameter is measured by the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

The Mean square error (MSE) is calculated by the following expression:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{i=1}^{i=M} \sum_{j=1}^{j=N} \left(\mathrm{C}(i,j) - \mathrm{S}(i,j)\right)^2 \qquad (1)$$

Where C is the cover image and S is the stego image, M and N are the numbers of lines and columns of C and S.

The PSNR is computed using the following equation:

$$\mathrm{PSNR} = 10\mathrm{Log}\left(\frac{\mathrm{Max}^2}{\mathrm{MSE}}\right) \qquad (2)$$

where “Max” is the maximum pixel value of the image. The PSNR increases when MSE decreases, this means that a higher PSNR value is a sign of a better degree of imperceptibility of the steganographic algorithm. The human visual system (HVS) cannot detect any distortions in stego-images having PSNR that goes beyond 36 dB.

Capacity: It indicates the amount of secret information that can be embedded in the cover image. The embedding rate is given in absolute measurement such as the length of the secret message [1].

Robustness: It has various definitions; Zollner [14] theoretically proved that the security of a steganographic system is attached to the random nature of the secret message and its independence from the cover image. In short, security of a steganographic system is defined in terms of undetectability, which is assured when the statistical tests cannot distinguish between the cover and the stego-image [12,13].

To Cachin [15] the security of a steganographic process is relative to a parameter measuring the entropy between the probability distribution of cover image (C) and stego image (S), the process is ε-secure if the entropy is smaller than ε. The detectability (security) D(PDc // PDs) is defined by the following expression:

$$\mathrm{D}(\mathrm{PDc}//\mathrm{PDs}) = \int \mathrm{PDc}\,\mathrm{Log}\left(\frac{\mathrm{PDc}}{\mathrm{PDs}}\right) \leq \varepsilon \qquad (3)$$

3. DISCRETE WAVELETS TRANSFORM

Multi-resolution Analysis is the main theory in wavelets that analyzes a signal in frequency domain in detail. In this transform, spatial domain is passing through low pass and high pass filter to extract low and high frequencies respectively. Applying one level 2D wavelet transform on image, decompose the cover image into four non overlapping sub bands by namely A, H, V and D as shown in the figure 1.

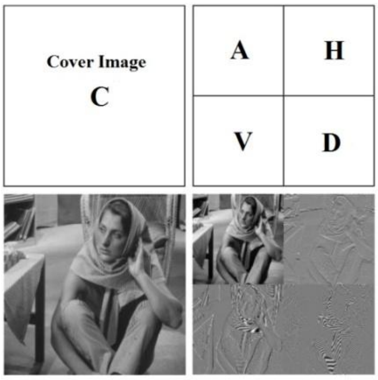


Fig 1: Decomposition Process of DWT

The sub bands A include the low pass coefficient and presents a soft approximation of image. The other three sub bands show respectively horizontal, vertical and diagonal details. In this paper Haar wavelet was chosen as a case study.

The decomposition algorithm of Haar Discrete Wavelet Transform (DWT) is given by the following equations:

$$\begin{cases} \mathrm{A}(i,j) = \dfrac{\mathrm{C}(2i-1,2j-1) + \mathrm{C}(2i-1,2j) + \mathrm{C}(2i,2j-1) + \mathrm{C}(2i,2j)}{2} \\ \mathrm{H}(i,j) = \dfrac{\mathrm{C}(2i-1,2j-1) + \mathrm{C}(2i-1,2j) - \mathrm{C}(2i,2j-1) - \mathrm{C}(2i,2j)}{2} \\ \mathrm{V}(i,j) = \dfrac{\mathrm{C}(2i-1,2j-1) - \mathrm{C}(2i-1,2j) + \mathrm{C}(2i,2j-1) - \mathrm{C}(2i,2j)}{2} \\ \mathrm{D}(i,j) = \dfrac{\mathrm{C}(2i-1,2j-1) - \mathrm{C}(2i-1,2j) - \mathrm{C}(2i,2j-1) + \mathrm{C}(2i,2j)}{2} \end{cases} \qquad (4)$$

The reconstruction algorithm or inverse Haar Discrete Wavelet Transform (IDWT) is given by the following equations:

$$\begin{cases} \mathrm{C}(2i-1,2j-1) = \dfrac{\mathrm{A}(i,j) + \mathrm{H}(i,j) + \mathrm{V}(i,j) + \mathrm{D}(i,j)}{2} \\ \mathrm{C}(2i-1,2j) = \dfrac{\mathrm{A}(i,j) + \mathrm{H}(i,j) - \mathrm{V}(i,j) - \mathrm{D}(i,j)}{2} \\ \mathrm{C}(2i,2j-1) = \dfrac{\mathrm{A}(i,j) - \mathrm{H}(i,j) + \mathrm{V}(i,j) - \mathrm{D}(i,j)}{2} \\ \mathrm{C}(2i,2j) = \dfrac{\mathrm{A}(i,j) - \mathrm{H}(i,j) - \mathrm{V}(i,j) + \mathrm{D}(i,j)}{2} \end{cases} \qquad (5)$$

4. PROPOSED WORK

In this work, a new steganographic scheme based on transform domain is proposed. The aim of this work is the development of a new method to dissimulate texts in images in such a way that provides a strong resistance to steganalysis processes with a high or acceptable capacity of embedding. Since human eyes are much sensitive to the low frequency part (A sub-image), A is the most important component in the decomposition process and to not be used in the embedding. Therefore, we chose to embed data in the most robust zones of the image H, V and D using Haar discrete wavelet transform.

Embedding data in the wavelets coefficients H, V and D is the same as adding a number to each one to produce a new coefficient. The stego-image S is obtained by the reconstruction algorithm after the embedding data as follows:

$$\begin{cases} S(2i,2j) & = \dfrac{A(i,j) + (H(i,j) + h) + (V(i,j) + v) + (D(i,j) + d)}{2} \\ S(2i,2j+1) & = \dfrac{A(i,j) + (H(i,j) + h) - (V(i,j) + v) - (D(i,j) + d)}{2} \\ S(2i+1,2j) & = \dfrac{A(i,j) - (H(i,j) + h) + (V(i,j) + v) - (D(i,j) + d)}{2} \\ S(2i+1,2j+1) & = \dfrac{A(i,j) - (H(i,j) + h) - (V(i,j) + v) + (D(i,j) + d)}{2} \end{cases} \quad (6)$$

Where h, v and d are the numbers added to the coefficients H, V and D by the hiding process.

By using the equations of the reconstruction algorithm, we obtain:

$$\begin{cases} S(2i,2j) & = C(2i,2j) + e1 \\ S(2i,2j+1) & = C(2i,2j+1) + e2 \\ S(2i+1,2j) & = C(2i+1,2j) + e3 \\ S(2i+1,2j+1) & = C(2i+1,2j+1) + e4 \end{cases} \quad (7)$$

Where $\begin{cases} e1 = \frac{h+v+d}{2} \;,\; e2 = \frac{-h+v-d}{2} \;, \\ e2 = \frac{h-v-d}{2} \;\text{ and }\; e4 = \frac{-h-v+d}{2} \end{cases}$

In many image processing applications the input data consists of integer samples. Unfortunately wavelet filters return floating point values as wavelet coefficients. When one hides data in their coefficients any truncations of the floating point values of the pixels that should be integers may generate a loss of the hidden information which may lead to the failure of the data hiding method. To overcome the difficulty of floating point, we chose the values of h, v and d so that those of ei are integers.

On the other hand, The coefficients ei { i=1,2,3,4} added to the reconstruction algorithm are factors of the error MSE, then in order to have an imperceptible method we must minimize the error MSE, which means we have to choose the values of h, v and d minimizing E for each iteration of the reconstruction algorithm, while E is:

$$E = |e1|^2 + |e2|^2 + |e3|^2 + |e4|^2 \quad (8)$$

Since $h = e1 + e2$, $v = e1 + e3$, $d = e1 + e4$ and ei are integers, hence h, v, d must also be integers, we conclude from this that the hiding is performed in the integer part of the Haar DWT coefficients.

In order to keep E minimal the values of h, v, d must be in {0,1}, but in that case the ei can be non integer. As an example if h=d=0 and v=1 then e1 = 0.5 which is not integer.

4.1 First method

The secret message m is sequentially divided into packets of 3 bits m1 m2 m3 where mi is in {0,1}. To have ei integers and minimal we choose h, v and d as multiple of 2, so data is embedded in the second LSB of the integer part of Haar DWT coefficients:

For example let H be the selected coefficient, then $h = \mathrm{sign}(H)(mi \oplus c)$ where c is the second LSB of H and $\oplus$ is the "xor" bit-wise operator.

In this case the value of E is in {0,4,7,12}, while E is the accumulated error of four pixels.

The maximum absolute value of ei is 3, this means that if a pixel of the cover image is <3 or >252 then after the hiding process the stego pixel can fall off [0,255]. To avoid this problem we keep, before hiding data, the pixels of the cover in [3,252]:

$$\begin{cases} C(i,j) = 3 & \text{if } C(i,j) < 3 \\ C(i,j) = 252 & \text{if } C(i,j) > 252 \end{cases} \quad (9)$$

4.2 Second method

In this method, the secret message m is sequentially divided into packets of 2 bits m1 m2 where mi is in {0,1}. To minimize the value of E even more than the first method we use, among (h, v, d), two parameters to store data with values in {0,1}, and the third one we deduce its value from the two others to satisfy that e1, e2, e3 and e4 are all integers, Therefore we chose (h,v) for hiding and d is given depending on (h,v) by the following equation: $d = h \oplus v$.

The values of h and v are in {0,1}, and this means that data is hidden in the LSB of the integer part of Haar DWT coefficients, this keeps the value of E in {0, 2}, the MSE is reduced in comparison with the first method but the capacity of embedding will also be reduced since just two sub bands are used for hiding data.

The maximum absolute value of ei is 1, so if a pixel of the cover image is equal to 0 or 255 then after the hiding process the stego pixel can become -1 or 256. To prevent this we keep, before embedding data, the pixels of the cover in [1,254]:

$$\begin{cases} C(i,j) = 1 & \text{if } C(i,j) = 0 \\ C(i,j) = 254 & \text{if } C(i,j) = 255 \end{cases} \quad (10)$$

Since the random nature of the hiding process provides more resistance to the steganalysis attacks, the order of selection of pixels during the embedding and the extracting operations is given by a random key that scrambles the hiding location, and this for the purpose of strengthening the security of the proposed methods.

4.3 Embedding algorithm

Step 1: Read the cover image as two-dimensional file (matrix).

Step 2: Transform the text into a binary sequence appending to it the key and the message's length.

Step 3: Apply the key to select the pixels where text bits are going to be dissimulated.

Step 4: Adjust the values of pixels and just those where data is going to be hidden, between 1 and 254 or between 3 and 252.

Step 5: Calculate the Haar discrete wavelet transform.

Step 6: Insert the binary sequence in the DWT coefficients as explained before according to the method chosen (first or second).

Step 7: Apply the Haar inverse discrete wavelet transform to obtain the stego-image.

4.4 Extracting algorithm

Step 1: Read the stego image as two-dimensional file (matrix).

Step 2: Calculate the Haar discrete wavelet transform of the stego-image.

Step 3: Extract the key to select pixels where secret data is embedded.

Step 4: Extract bits from the integer part of the DWT coefficients: from the second LSB for the first method or from the LSB for the second method.

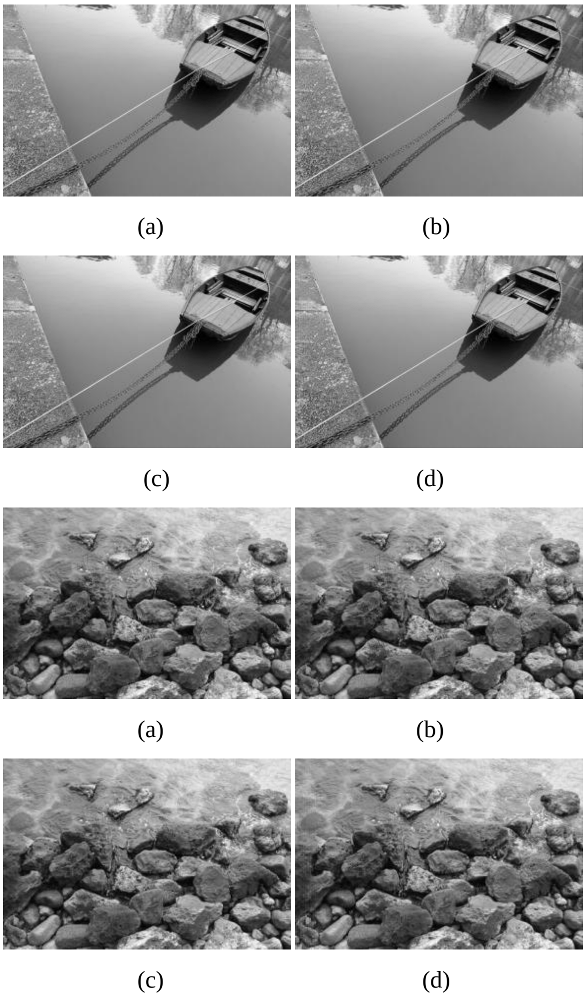
Step 5: Regroup the data extracted by blocks of 8 bits to obtain the information hidden.

5. EXPERIMENT RESULTS AND DISCUSSION

In this section, experiments were accomplished to test the performance of the proposed methods, we used a set of images with a size of around 512x512 pixels, and we dissimulated in those images a text of 1000 bytes. The implementation of all algorithms is performed using MATLAB R2009a.

The PSNR, MSE, the ε-security and the capacity of hiding are calculated in order to evaluate the quality of our proposed work, and are considered as parameters of comparison with the method of [10] as shown in the figures below.

The figure 2 show some of the cover images we used and their stego images associated to the first and the second proposed methods and the compared method respectively from left to right.

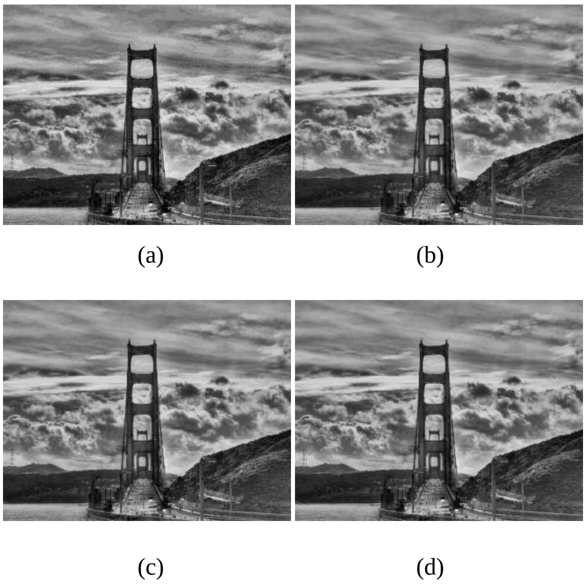


(a) (b)

(c) (d)

(a) (b)

(c) (d)



(a) (b)

(c) (d)

Fig 2: Cover images and associated stego-images (boat, stone, bridge), (a) cover image, (b) stego image by the first proposed method, (c) stego image by the second proposed method, (d) stego image by the compared method [10].

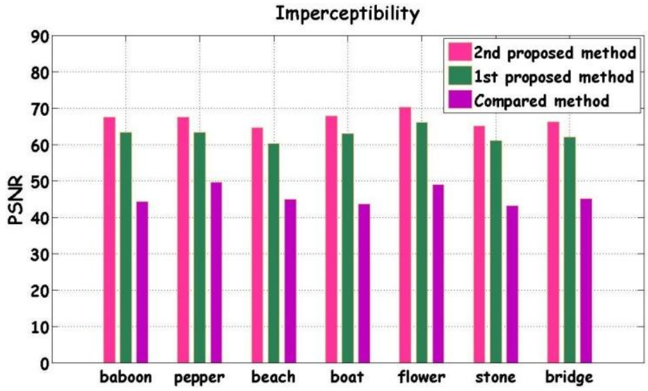


Fig 3: PSNR for the three methods

Imperceptibility: A steganographic process is imperceptible if the PSNR is above 36 dB, the results in the table 1 and in the figure 3 show that the proposed methods give a high value of PSNR proving that they have a high level of imperceptibility. In comparison with the method developed by [10], there is a large difference in PSNR going beyond 15 dB

Table 1: MSE, PSNR and security for the proposed methods and the compared method

	Image	MSE	PSNR	Entropy x10^{-5}
Compared method	**Baboon**	2.437	44.262	11.841
	Pepper	0.717	49.571	7.0897
	Beach	2.113	44.881	27.766
	Boat	2.782	43.685	3.9953
	Flower	0.827	48.952	5.5758
	Stone	3.204	43.072	16.627

	Bridge	1.981	45.161	7.2474
First proposed method	**Baboon**	0.030	63.301	3.4926
	Pepper	0.029	63.365	3.9890
	Beach	0.062	60.173	41.819
	Boat	0.028	63.613	5.4835
	Flower	0.016	66.025	1.0170
	Stone	0.050	61.071	9.2205
	Bridge	0.041	61.991	2.0567
Second proposed method	**Baboon**	0.011	67.491	2.0567
	Pepper	0.012	67.474	2.8249
	Beach	0.023	64.556	14.362
	Boat	0.010	67.827	2.5243
	Flower	0.006	70.180	0.5565
	Stone	0.019	65.156	7.3862
	Bridge	0.015	66.182	4.3243

In the figure 4 PSNR is calculated for the image (pepper) while changing the length of data embedded from 100 bytes to 2000 bytes. The second method give the best values, and they are not far from those of the first method, the PSNR of [10], although they are good, are way smaller than the PSNR of the proposed methods.

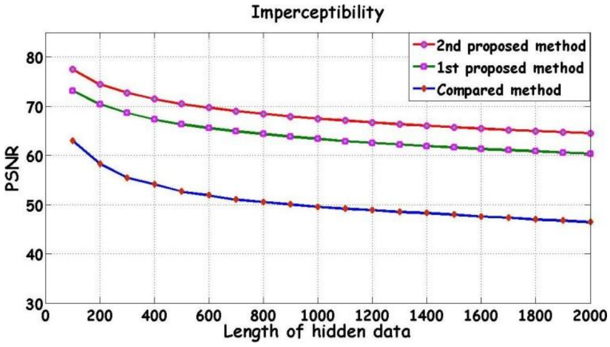
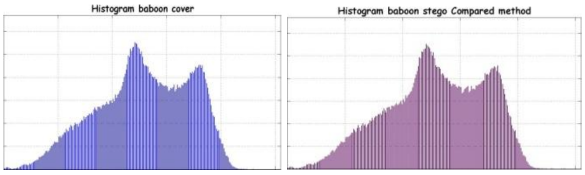
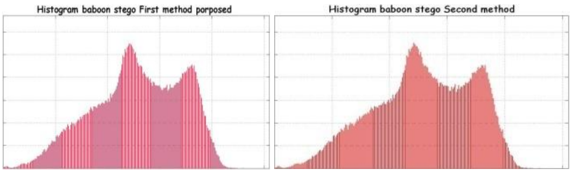


Fig 4: PSNR by length of data in the three methods for the image pepper

Security: In the table 1, the second method has the smallest values of the ε-security (entropy between the cover image and the stego image), followed by the first method then the compared method, proving that the modifications on the histogram generated by the proposed methods are very slight as shown in the figure 5. The proposed methods are more secure.



(a) (b)



(c) (d)

Fig 5: Histogram of baboon, (a) cover image, (b) stego image of the compared method [10], (c) stego image of the first proposed method, (d) stego image of the second proposed method.

Capacity: The first method uses three coefficients to hide three bits of secret data, and since the sub band A is not used then we have a hiding capacity of 75% pixels.

On the other hand the second method uses three coefficients to hide two bits of secret data which gives a hiding capacity of 50% pixels for the second method.

While the second method gives a high PSNR than the first, its capacity is smaller than the first's, but generally 50% is a good value, and the imperceptibility is more important than the capacity of embedding.

6. CONCLUSION

We proposed new steganographic methods based on the frequency domain by using the Haar DWT. New techniques are used to solve the problem of the floating point starting from the expression of the MSE and Haar DWT reconstruction algorithm, data is embedded in the integer part of the coefficient of the transform. The results obtained shows that the proposed methods have a high level imperceptibility with a good value of embedding capacity, the imperceptibility increases from the first method to the second one, and the capacity decreases. The security is fortified by using a key giving a random selection of the coefficients where data is hidden providing a strong resistance to the steganalysis processes. The problem to increase the hiding capacity of these methods can be subject of our future works.

7. REFERENCES

[1] C.P.Sumathi, T.Santanam and G.Umamaheswari "A Study of Various Steganographic Techniques Used for Information Hiding" International Journal of Computer Science \& Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[2] Kevin Curran & Karen Bailey "An Evaluation of Image Based Steganography Methods" International Journal of Digital Evidence Fall 2003, Volume2, Issue 2.

[3] N. Ajeeshvali and B.Rajasekhar "Steganography Based on Integer Wavelet Transform and Bicubic Interpolation" I.J. Image, Graphics and Signal Processing, 2012, 12, 26- 33.

[4] Shashikala Channalli, Ajay Jadhav Sinhgad "Steganography, An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1 (3), 2009, 137-141.

[5] Wien Hong & Tung-Shou Chen "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", J. Vis. Commun. Image R. 22 (2011) 131-140.

[6] Ki-Hyun Jung & Kee-Young "Steganographic method based on interpolation and LSB substitution of digital images", Multimed Tools Appl DOI 10.1007/s11042-013-1832-y.

[7] Jie Hu, Tianrui Li "Reversible steganography using extended image interpolation technique", Computers & Electrical Engineering, Volume 46, August 2015, Pages 447–455.

[8] Deepak Singla & Rupali Syal "Data Security Using LSB & DCT Steganography In Images", International Journal Of Computational Engineering Research/ ISSN: 2250-3005.

[9] Bo Yang and Beixing Deng "Steganography in gray images using wavelet" In Proceedings of ISCCSP 2006.

[10] Nur Azman Abu, Prajanto Wahyu Adi and Othman Mohd "Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform" International Journal of Video\&Image Processing and Network Security IJVIPNS-IJENS Vol: 14 No: 02.

[11] A. Cheddad, J. Condell, K. Curran, and P.M. Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Digital Signal Processing, vol.90, no.3, pp.727-752, 2010.

[12] B. Li, J. He, J. Huang, and Y. Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol.2, no.2, pp.142-172, 2011.

[13] R. Roy, S. Changder, A. Sarkar, and N.C. Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", Computing, Management and Telecommunications (ComManTel), pp.21-24, Ho Chi Minh, Vietnam, 2013.

[14] J. Zollner, H. Federrath, H. Klimant, A. Pitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the Security of Steganographic Systems" Information Hiding Workshop, pp.345-355, Portland, USA, 1998.

[15] C. Cachin "An Information theoretic Model for Steganography", Information and Computation, vol.192, no.1, pp.41-56, 2004.