Indian Journal of Science and Technology, *Vol 9(5), DOI: 10.17485/ijst/2016/v9i5/87189, February 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

9/7 IWT Domain Data Hiding in Image using Adaptive and Non Adaptive Methods

V. Thanikaiselvan*, Tushar Bansal, Prateek Jain and Shounak Shastri

School of Electronics Engineering, VIT University, Vellore - 632014, Tamil Nadu, India;
thanikaiselvan@vit.ac.in, bansaltushar121@gmail.com, prateek.jain28@yahoo.com,
shounak.mangeshkalika2015@vit.ac.in

Abstract

Background/Objectives: The advancement of information exchange through internet has made it easy to transfer the exact information faster to the destination. Exchange the information safely to the destination with no alterations, there are many approaches like Cryptography, Steganography and Watermarking. **Methods/Statistical Analysis:** Steganography is a method of hiding a secret data in other cover medium. Digital Images are popular for cover medium than other because of their frequent use on the internet. In this paper a transform domain steganography with 9/7 Integer Wavelet Transform (IWT) is proposed. A pixel adaptive embedding method using LSB (Least Significant Bit) method is employed to increase the security of the secret data embedded in the a cover medium. Graph Theory is used to select the coefficients randomly for embedding the secret messages. **Findings:** It is found that the proposed method provides good security and high capacity. This algorithm can be applicable for all kinds of secret communications. Finally Results are compared with 5/3 IWT. **Applications/Improvements:** This method can be applied for all the secret communication applications especially Defence, Telemedicine, etc. This proposed method developed further in terms of robust against various steganalysis tools.

Keywords: Adaptive Embedding, Data Hiding, IWT, Steganography, Security

1. Introduction

In the present patterns of the world, the innovations have propelled so much that a large portion of the people favor utilizing the web as the essential medium to exchange information starting with one end then onto the next over the world. There are numerous conceivable approaches to transmit information utilizing the web: through messages, talks, and so forth. The information move is made extremely basic, quick and precise utilizing the web. Then again, one of the primary issues with sending information over the web is the "security danger" it postures i.e. the individual or private information can be stolen or hacked from numerous points of view. In this way it gets to be critical to mull over information security, as it is a standout amongst the most key elements that need consideration amid the procedure of information exchanging.

Information security essentially implies assurance of information from unapproved clients or programmers and giving high security to avert information adjustment. This range of information security has increased nowadays because of the huge increment in information exchange rate over the web. So as to enhance the security highlights in information exchanges over the web, numerous strategies have been created like: Steganography[1-4], Cryptography[5-7], and advanced watermarking. While Cryptography is a strategy to disguise data by encoding it to "figure messages" and transmitting it to the expected beneficiary utilizing an obscure key, Steganography gives further security by concealing the figure content into an apparently imperceptible picture or different organizations.

Comprehensively talking, there are two manifestations of steganography – spatial domain[8-11] and transform

**Author for correspondence*

domain[12-21]. Every one of them has a few information embedding and good extraction methods. After information embedding, some extra improvement methods can be executed to minimize the error further[8,10]. There are different procedures to embed and extract secret information, with minimum mean square error and more than 35 dB Peak Signal-to-Noise Ratio (PSNR).

Dissimilar to spatial domain steganography where information is embedded inside the pixel values itself, in Transform domain steganography, information is embedded in the transform coefficients (generally Fourier Transform, Discrete Cosine Transform (DCT)[12], Fast Fourier Transform or Discrete Wavelet Transform (DWT))[13] of the cover image. For instance, the DWT converts pixel value into DWT coefficients. In Transform Domain steganography, the DWT is applied to an image and an embedding method is utilized to conceal the secret data on the transformed image. At that point reverse DWT is performed to get back the image in spatial domain which brings about Stego image. At the receiver end, the same method is taken after. The advantages of utilizing transform domain steganography are enhanced security, and better information robustness. On the other hand IWT[14-21] could be utilized to perform the same operation which is explained in the following section. A novel algorithm to embed data in video images using random key encoding function is proposed in[22]. This method gives a better security for the data by embedding the secret bits randomly in the red, green and blue planes of the video images.

In this paper, as opposed to utilizing raster scan strategy, a graph theory method is utilized for irregular choice of the IWT coefficients in the wake of actualizing IWT.

1.1 Related Methods

1.1.1 9/7 Integer Wavelet Transform

The Discrete Wavelet Transform (DWT) is more popular because of its amazing de-correlation property, as a consequence transform stage in many modern image and video compression systems uses the DWT. IWT are the wavelet transforms that map integers to integers. Every sub-band or wavelet transformation is connected with filters of finite length which can be obtained as Lazy wavelet succeeded by lifting steps[14]. The Lazy wavelet divides the signal into even and odd samples. A wavelet transform that maps integers to integers can be obtained by combining the lifting steps and rounding off. This method provided for the design of symmetric short tap filters which gives visually pleasant and smooth outputs. This filter has unequal lengths for the high pass and low pass coefficients, 9 and 7 respectively. Thus the name (9/7) filter is obtained. The following equations are used to implement the 1D IWT with 9/7 filters and these Equations (1) and (2) can be adapted for 2D IWT.

$$d[n] = d_0(n) + \left[\frac{1}{16}\left(\left(s_0[n+2] + s_0[n-1]\right) - 9\left(s_0[n+1] + s_0[n]\right)\right) + \frac{1}{2}\right] \quad (1)$$

$$s[n] = s_0[n] + \left[\frac{1}{4}\left(d[n] + d[n-1]\right) + \frac{1}{2}\right] \quad (2)$$

where's' and'd' are the low frequency and high frequency wavelet coefficients respectively.

There are 3 main steps in the 9/7 IWT

- Splitting the signal into odd and even terms
- Prediction , with the odd terms
- Update, with the even terms

In IWT, Low Frequency (LF) and High Frequency (HF) subbands are created by averaging and differencing techniques separately. First level decomposition of an image gives Approximation (LL), Horizontal (LH), Vertical (HL) and Diagonal (HH) coefficients. LL coefficients are more delicate than the remaining coefficients, so the embedding is done in all the sub-bands with the exception of LL sub-band. Since LH, HL and HH coefficients contain edge data more data can be embedded in these coefficients. The advantage of a lifting scheme like this is that it reduces the execution time of the wavelet transform and the reverse transform is easy to calculate by just reversing the forward equations.

1.1.2 Least Significant Bit Embedding

LSB is one of the most commonly used data-embedding techniques. This technique embeds the bits of secret information directly into the least significant bit plane of the cover image. In the gray level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits so that the embedding procedure doesn't affect the original pixel value greatly. The mathematical representation for LSB Embedding is given in Equation 3.

$$X'(i,j) = X(i,j) - \mathrm{mod}(X(i,j), 2^k) + S(m) \quad (3)$$

For Extraction is given in equation (4)

$$S'(m) = \mathrm{mod}(X'(i,j), 2^k) \quad (4)$$

Where,
X (i, j) – Cover image,
X' (i, j) – Stego image,
S (m) – Secret Data in decimal form,
S' (m) – Extracted Data in decimal form,
Mod – modulus, i and j are the coordinates of the image,
m represents array.
k - number of bits to be embedded in a coefficient.

1.1.3 Graceful Graph for Random Path

A Graph with p vertices (Nodes) and q edges is called as graceful graph. Both vertices and edges of a diagram G (N,E) to an arrangement of (integer or real) numbers, such that some particular property is fulfilled. Here this diagram is utilized to discover the irregular (random) path to insert the secret information. An algorithm is given below for graceful graph:

The total number of edges (E) and total number of nodes (N) are the inputs to this algorithm

Step1: Generate a sequence (S1) of numbers from 1 to N-1

Step 2: Generate a sequence (S2) of random numbers between 0 and 7 and its length must be equal to N.

Condition: If the sequence is starting with higher number, then it will give good result.

Step 3: Add S1 and S2 to produce a new sequence S3.

Condition 1: S3 sequence elements should not equal to N.

Condition *2:* The numbers which are not present in the S2 sequence must available in the S3 sequence.

Step 4: Graceful tree is drawn using S2 and S3 with zigzag scan.

Step 5: Random traversing path is identified from the graceful tree.

Following example illustrates the above algorithm.

Let N=16, E=15

$$Random\ path\ matrix = \begin{bmatrix} 7 & 8 & 9 & 6 \\ 10 & 12 & 13 & 3 \\ 4 & 2 & 11 & 15 \\ 5 & 1 & 14 & 0 \end{bmatrix}$$

Figure 1 shows the procedure for the Graph generation and Figure 2 shows that the Graceful graph of the given example. In the Random path matrix, zero denotes that the first place to embedded secret data and 15 denotes last place for embedding. In each 4 x 4 matrix, we need to start with eighth pixel and finish it with first pixel. This can be extended for the required size by taking N and E values.

S1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S2	7	7	6	6	7	7	3	4	2	5	4	2	1	1	0
S3	8	9	9	10	12	13	10	12	11	15	15	14	14	15	15

Figure 1. Procedure for graceful graph.

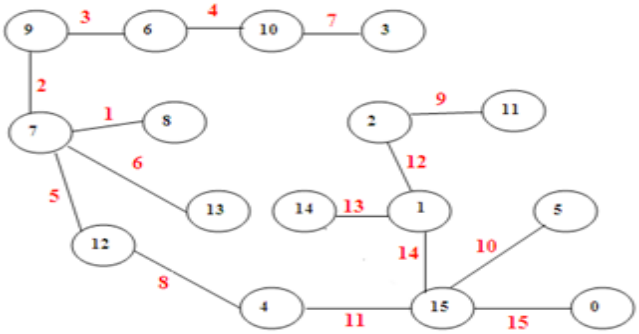

Figure 2. Graceful graph example.

2. Proposed Methodology

2.1 Embedding Algorithm

Figure 3 is the flow diagram of Embedding Algorithm, which is explained below

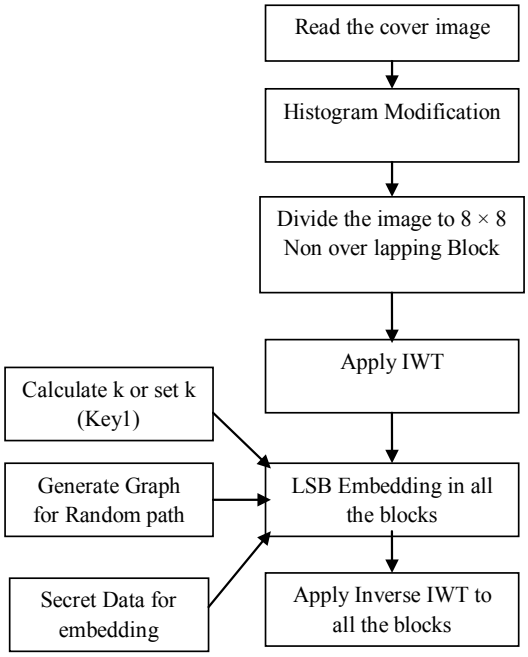

Figure 3. Flow diagram for embedding algorithm.

Input: Cover image

Output: Stego image

Step 1: A gray scale image X(i,j) with the size of 256 × 256 is considered as cover image for this steganography, X ∈ [0 to 255]

Step2: Convert all the pixel values from 15 to 240 using Histogram modification to avoid transform errors, XH ∈[15 to 40].

Step 3: Generate a Random Binary for embedding and consider this as Secret Data, S ∈ [0 and 1]

Step 4: Cover image XH is divided into 8 × 8 sized non-overlapping blocks of pixels. (There is no restriction in this block size).

Step 5: Apply 9/7 integer wavelet transform to each 8 × 8 block to get LL1, LH1,HL1 and HH1 sub-bands in each block. Embedding is to be done in all sub-bands except LL1 sub-band.

Step 6: Generate a Graceful Graph with N=64 and E=63. This is used to select the coefficients in a block for secret embedding. This Random path matrix is considered as key1.

Step 7.1: Non Adaptive bit embedding: Set k value, If k=1, then only one bit will be embedded in the selected coefficient and in all the blocks. This k value may be varied between 1 and 4.

Step 7.2: Adaptive bit embedding: Calculate the number of bits to be embedded in selected coefficient using the following equation

$$k = \begin{cases} 1 & , \quad c < 4 \\ 2 & , \quad 4 \le c < 8 \\ 3 & , \quad 8 \le c < 16 \\ 4 & , \quad 16 \le c \end{cases} \tag{5}$$

Where 'c' is the value of the coefficient value.

Here, data is embedded only in the HH1, HL1, LH1 sub-bands and the LL1 sub-band is extremely sensitive so it is left untouched.

This k is considered as key-2.

Step 8: Inverse IWT is applied to all the 8 × 8 to get Stego image X'(i,j).

2.2 Extraction Algorithm

Figure 4 is the flow diagram of Extraction Algorithm, which is explained below

Input: Received stego image

Output: Secret data.

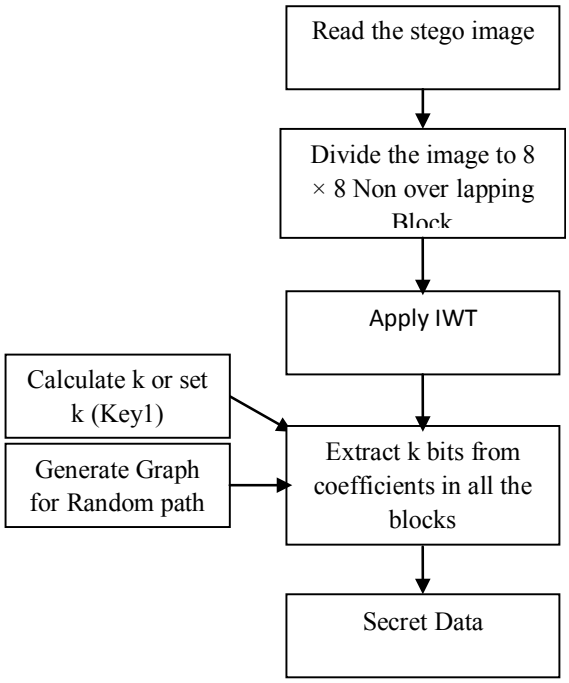

Figure 4. Flow diagram for extraction algorithm.

Step 1: Receive the stego image X' (i, j).

Step 2: Divide the entire image into 8×8 non overlapping block pixels.

Step 3: Apply 9/7 Integer wavelet transform to each 8×8 block and get the LL1, HH1, LH1, HL1 sub-bands.

Step 4: Generate Random path key using Graph theory for Random selection of coefficients to extract k bits using key 1 and key 2.

Step 5: Binary bits are concatenated to get the secret data.

3. Results and Discussions

A few investigations have been performed on the image to assess the performance of the proposed algorithm. Here six gray scale images are brought with size of 256 × 256 as cover image for secret information hiding and all are given in Figure 5. In this technique, the images are separated into 8 × 8 non overlapping blocks. 9/7 IWT is applied to all the blocks. Random Binary information is considered as secret information and is embedded inside the transformed coefficients. Inverse IWT is applied to all the 8 × 8 blocks for getting stego image. Mean Square Error (MSE) and PSNR are utilized to assess the performance of the algorithm and visual nature of the stego image. The MSE and PSNR can be calculated for the image by the following formula.

$$MSE = \frac{1}{M * N} \sum_{j=1}^{N} \sum_{i=1}^{M} (X(i,j) - X'(i,j))^2$$

$$PSNR = 10 \log_{10} \frac{255 * 255}{MSE} dB$$

Where X and X' are cover image and stego image respectively, M and N are the size of the image.

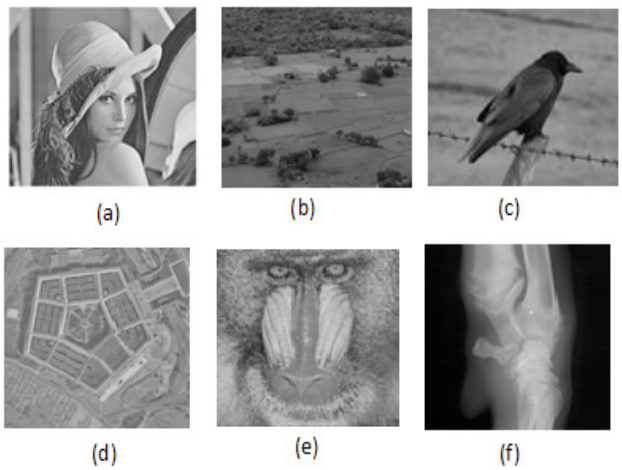

Figure 5. Cover images for steganography, **(a)** Lena **(b)** Farm, **(c)** Crow, **(d)** Galaxy, **(e)** Baboon, **(f)** Medical image.

In this proposed methodology, All kind of results are compared with 5/3 IWT and tabulated in Tables 1 to 3. 1 bit is embedded in 3 sub-bands (LH, HL and HH) of IWT coefficients then the total bits embedded is 49512 with average PSNR around 51 dB. Similarly for Two bits, total bits embedded is 98304 with average PSNR around 45 dB, for three bits, total bits embedded is 147456 with average PSNR around 39 dB, for four bits case, the total bits embedded is 196608 bits and for the adaptive bit embedding total number of bits will be varied according to the nature of the cover image but it will provide extra security to this algorithm.

Table 1. Comparison of 5/3 and 9/7 IWT PSNR Value for 1 bit and 2 bits case

	Total Bits = 49152 (1 bit in 3 sub-bands)		Total Bits = 98304 (2 bits in 3 sub-bands)	
Image Name	**5/3 IWT (PSNR in dB)**	**9/7 IWT (PSNR in dB)**	**5/3 IWT (PSNR in dB)**	**9/7 IWT (PSNR in dB)**
Lena	50.89	51.45	45.1	45.23
Farm	50.88	51.45	45.07	45.23
Crow	50.69	51.78	44.96	45.18
Baboon	50.94	49.54	44.08	43.92
Galaxy	50.93	49.67	45.22	44.97
Medical image	51.16	51.61	44.61	44.77

Table 2. Comparison of 5/3 and 9/7 IWT PSNR value for 3 bits and 4 bits case

	Total Bits = 147456 (3 bits in 3 sub-bands)		Total Bits = 196608 (4 bits in 3 sub-bands)	
Image Name	**5/3 IWT (PSNR in dB)**	**9/7 IWT (PSNR in dB)**	**5/3 IWT (PSNR in dB)**	**9/7 IWT (PSNR in dB)**
Lena	39.46	39.54	33.29	33.54
Farm	39.46	39.54	33.3	33.44
Crow	39.53	39.66	33.03	33.64
Baboon	39.23	38.88	33.36	32.98
Galaxy	39.61	39.59	33.2	33.12
Medical image	38.57	39.34	33.95	33.86

Table 3. Comparison of 5/3 and 9/7 IWT PSNR value for adaptive bits case

Image/ Transform	**Lena**		**Baboon**	
	No. of Bits	**PSNR (dB)**	**No. of Bits**	**PSNR (dB)**
5/3 IWT	130339	40.1	145777	38.5
9/7 IWT	131022	40.3	144843	38.2

4. Steganalysis

Steganalysis is the blind assessment of hidden information in stego image. This proposed system is exceedingly powerful against the blind attacks. This technique is a transform domain method, so that secret information can't be removed from the spatial area. Key 1 and Key 2 give very random embedding. Thusly proposed system is exceptionally powerful against Blind steganalysis procedures. Total number of iteration for Blind extraction of this method has been calculated and tabulated in Table 4.

Chi-square analysis is used to test the stego image, because this is a familiar method for statistical steganalysis. In Figure 6 and Figure 7, X-axis denotes the percentage of

Table 4. Comparison of Complexity Analysis of the Proposed Algorithm

	Total No. of iterations for Blind extraction
Proposed Method	(8*8)!*(32*32)*5 (after applying IWT)
Other raster scan Procedures	only one raster scan

embedding and Y-axis denotes probability of embedding. This graph denotes the performance of the proposed method and shows the high robustness against the blind steganalysis. So hackers may not interpret any details contained in the cover image. The graphs shown below in Figure 6 and Figure 7 are the chi-square graphs of the image baboon with embedded data as well as without data. There isn't much difference found in the chi square graphs of the cover image and stego image. This shows the robustness of the proposed algorithm.

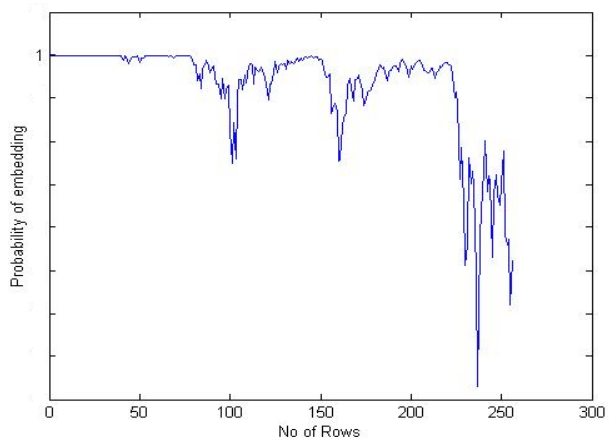

Figure 6. Chi square analysis of Baboon cover image.

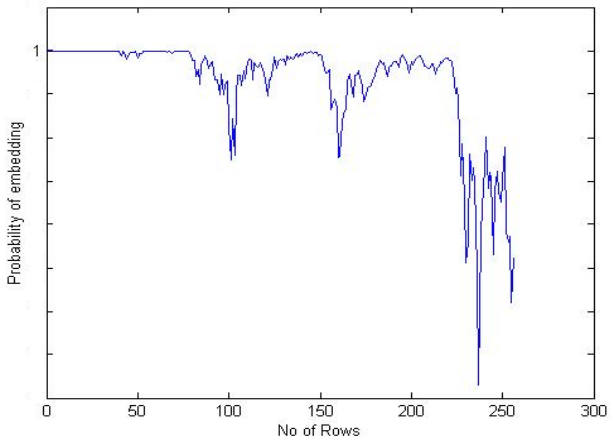

Figure 7. Chi square analysis of Baboon stego image.

5. Conclusion

In this paper secret information is embedded inside a cover image using IWT, namely (9/7) IWT with adaptive and non-adaptive techniques. Various embedding strategies are used for performance evaluation. PSNR value is greater than or equal to 35 for all k values except k=4 and adaptive case. This shows that, proposed method has high capacity and high imperceptibility. Robustness of the algorithm has been proved in terms of chi square analysis number of iterations and different keys. This proposed methodology can be altered with other transforms and performance can be analyzed as a future work.

6. References

1. Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM System Journal. 1996; 35(3&4):313–36.
2. Katzenbeisser S, Petitcolas FAP. Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, MA: Artech House; 2000. p. 239.
3. Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Processing. 2010; 90(3):727–52.
4. Atawneh S, Almomani A, Sumari P. Steganography in digital images: Common approaches and tools. IETE Technical Review. 2013; 30(4):344-58.
5. Schneier B. Applied Cryptography Protocols, Algorithm and Source Code in C. 2nd edition. India: Wiley; 2007.
6. Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JBB. Pixel scattering matrix formalism for image encryption - A key scheduled substitution and diffusion approach. AEU - International Journal of Electronics and Communications. 2015; 69(2):562-72.
7. Kim I, Kwon C-H, Lee W. New watermarking technique using data matrix and encryption keys. Journal of Electrical Engineering and Technology. 2012; 7(4):646-51.
8. Chan CK, Chen LM. Hiding data in images by simple LSB substitution. Pattern Recognition. 2004; 37(3):469–74.
9. Yang CH, Weng CY, Tso H-T, Wang S-J. A data hiding scheme using the varieties of pixel-value differencing in multimedia images. The Journal of Systems and Software. 2011; 84(4):669-78.
10. Amirtharajan R, Rayappan JBB. An intelligent chaotic embedding approach to enhance stego-image quality. Information Sciences. 2012; 193:115–24.
11. Thanikaiselvan V, Arulmozhivarman P, Amirtharajan R, Balaguru Rayappan JB. Horse riding and hiding in image for data guarding. Procedia Engineering. 2012; 30:36-44.
12. Song X, Wang S, Niu X. An integer DCT and affine transformation based image steganography method.

Proceedings of 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP); Piraeus. 2012:102-5.
13. Chen PY, Lin H-J. A DWT based approach for image steganography. International Journal of Applied Science and Engineering. 2006; 4(3):275-90.
14. Adams MD. Reversible integer-to-integer wavelet transforms for image coding. The Vancouver: University of British Columbia; 2002.
15. Calderbank AR, Daubechies I, Sweldens W, Yeo BL. Wavelet transforms that map integers to integers. Applied and Computational Harmonics Analysis. 1998; 5(3):332–69.
16. Yang H, Sun X, Sun G. A high-capacity image data hiding scheme using adaptive LSB substitution. Radio Engineering Journal. 2009; 18(4):509-16.
17. Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transformations on Information Forensics and Security. 2008; 3(3):488–97.
18. Thanikaiselvan V, Arulmozhivarman P, Chakrabarty S, Agarwal A, Subashanthini S, Amirtharajan R. Comparative analysis of (5/3) and haar IWT based steganography. Information Technology Journal. 2014; 13(16):2534-43.
19. Safy ROEI, Zayed HH, EI Dessouki A. An adaptive steganographic technique based on Integer Wavelet Transform. International Conference on Networking and Media Convergence (ICNM'09); Cairo. 2009. p. 111-17.
20. Peng F, Li X, Yang B. Adaptive reversible data hiding scheme based on integer transform. Signal Processing. 2012; 92(1):54-62.
21. Thanikaiselvan V, Arulmozhivarman P. High security image steganography using iwt and graph theory. Proceedings of International Conference on Signal and Image Processing Applications (ICSIPA); Melaka, Malaysia. 2013. p. 337-42.
22. Ramalingam M, Isa NAM. A Steganography approach over video images to improve security. Indian Journal of Science and Technology. 2015; 8(1):79-86.