A Secured Image Steganography Technique using Wavelet Transform

Abhay Dakhole[1] Dr. Sanjay Badjate[2]
[1,2]Department of Electronics
[1,2]S.B.Jain Institute of Technology, Management & Research, Nagpur (M.S) India

Abstract— Image steganography is applicable in department of defense, department of police, department of detective investigation and medical field. In image steganography, generally secret image is not hidden, instead of that a key is generated and that key is hidden in the cover image. By using that key the secret image can be extracted from the cover image. Wavelet Transform (WT) is used to hide the key. Wavelet Transform is very robust and secure because nobody can realize information which is hidden and hidden data cannot be lost because of noise or any signal processing operations. Experimental results show very good Peak Signal to Noise Ratio (PSNR), MSE and maximum error which is a measure of security. In this technique the secret image is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands.

Key words: Steganography, IWT, DWT, PSNR, Lifting Scheme, Bit Plane

I. INTRODUCTION

For confidential Information exchange information security is very essential. There are two ways of achieving confidential information exchange, Steganography and cryptography. Steganography and cryptography are different from each other., The information is unintelligible in cryptography while steganography hide the existence of the data. Because of lack of strength in cryptographic systems research in steganography has mainly been done. Many governments have created laws to prohibit cryptography altogether, so people have to study other methods of secure data transfer. Image steganography is applicable in department of defense, department of police, department of detective investigation and medical field. Avoiding communication through well known channels greatly reduces the risk of information being leaked in transit.

Communicating an encrypted file is more suspicious than hiding information in a photograph of the company picnic. The main objective of steganography is to transfer the information secretly by concealing the existence of information in some other medium such as image, audio or video. Cover object is used to embed information. Stego-object is the cover along with the hidden information. In this paper for both cover object and secret information grey scale images are considered. The secret image is hidden by generating a key and Integer Wavelet Transform (IWT) is used to hide the key.

A. Discrete Wavelet Transform in Images

DWT transforms discrete signal from the time domain into time frequency domain. The transformation product is set of coefficient organized in the way that enables not only spectrum analysis of the signal but also spectral behavior of the signal in time. Wavelet-based coding provides significant improvements in picture quality at higher compression ratios. Fig. 1 shows the 2D DWT for image at various levels.

Image is decomposed into 4 sub bands by using DWT: LL, HL, LH and HH. LL part contains the the majority significant features. If the information is hidden in LL part the stego image can resist compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub bands can be used.

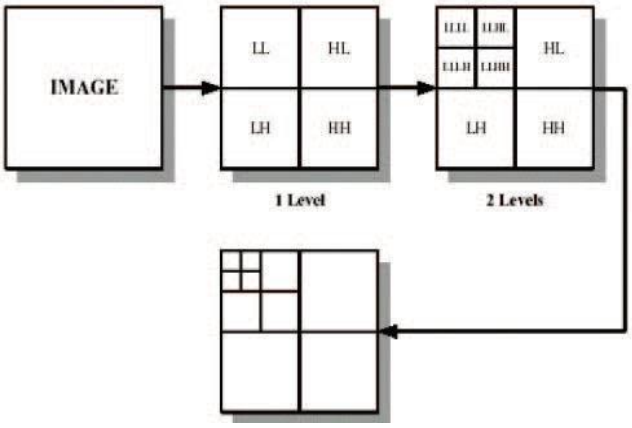

Fig. 1: The 2D DWT for image at various levels

B. Integer Wavelet Transform

IWT is a more resourceful approach to lossless compression. The coefficients in this transform are represented by fixed precision numbers which allows for lossless encoding. This wavelet transforms maps integers to integers. While in DWT, if the input consists of integers, the resulting output does not consists of integers. Thus the perfect restoration of the original image becomes difficult. If the original image (I) is X pixels high and Y pixels wide, the level of each of the pixel at (i,j) is denoted by Ii,j. The IWT coefficients are given by

$$LLi,j = \square (I2i, 2j + I 2i+1, 2j) /2 \quad (1)$$
$$HLi,j = I2i+1, 2j - I2i, 2j \quad (2)$$
$$LHi,j = I2i, 2j+1 - I2i, 2j \quad (3)$$
$$HHi,j = I2i+1, 2j +1 - I2i, 2j \quad (4)$$

The inverse transform is given by

$$I2i, 2j = LLi,j - \square HLi,j/2 \quad (5)$$
$$I2i, 2j +1 = LLi,j + \square (HLi,j+1)/2 \quad (6)$$
$$I2i+1, 2j = I2i, 2j +1 + LHi,j - HLi,j \quad (7)$$
$$I2i+1, 2j+1 = I2i+1,2j + HHi,j - LHi,j \quad (8)$$

Where, $1 \le i \le X/2$, $1 \le j \le Y/2$ and $\lfloor \rfloor$ denotes Floor value.

The nearer the stego image to the cover image, the superior the security. It is measured in terms of PSNR.

$$PSNR \ \ (in\ dB) = 10 \log_{10}(\frac{255^2}{MSE})$$

Where L = maximum value, MSE = Mean Square Error.

$$MSE = \frac{\sum_x \sum_y (f(x, y) - f'(x, y))^2}{M \times N}$$

Where X = original value, X' = stego value and N = number of samples. High PSNR value indicates high security. Because no one can suspect the hidden information.

II. RELATED WORK

Abdelwahab and Hassaan projected a data hiding technique in the DWT domain which decomposed both secret and cover images with 1-level DWT. Extracted data is not completely as same as the embedded original version is the disadvantage of this method. This is further improved by Neda Raftari and Amir Masoud Eftekhari Moghadam who suggest a new image steganography technique based on IWT and Munkres' assignment algorithm in which secret image is embedded in frequency domain of cover image with high matching quality. The improvement is obtained with higher computation. El Safy, R.O, Zayed. H. H, EI Dessouki. A, used an adaptive steganographic technique based on IWT, which improves the hiding ability and PSNR compared to DWT technique proposed by B. Lai and L. Chang. PSNR and hiding capacity are further improved by Elham Ghasemi, Jamshid Shanbehzadeh and Bahram ZahirAzami [5], who use a steganographic method based on IWT and Genetic Algorithm.

III. PROPOSED ALGORITHM

A. Algorithm 1

Hiding the secret image in the special domain can easily be extracted by unauthorized user. In this paper, we proposed a first steganography technique using DWT (Discrete Wavelet Transform) for hiding a large amount of data with high security, a good invisibility and no loss of secret message. The basic idea to hide information using DWT is to alter the magnitude of the DWT coefficients of three sub-bands, HH, HL, and LH of cover image.

The cover image considered is grayscale image of size 256X256 and the secret information is also grayscale image of size 128X128. The secret image itself is not hidden, instead a key is generated and the DWT is used to hide the key in the cover image.

1) Key Generation

The following steps are used to generate a key for the secret image:

- Obtain single level 2D DWT of the cover-image C and secret-image S.
- The resulting transformed matrix consists of four subbands CLL, CHL, CLH and CHH and SLL, SHL, SLH and SHH obtained by transforming images C and S respectively.
- The sub-images CLL and SLL are subdivided into nonoverlapping blocks BCk1 ($1 \leq k1 < nc$) and BSi ($1 \leq i < ns$) of size 4x4 where nc, ns are the total number of nonoverlapping blocks obtained from sub-images CLL and SLL respectively.
- Every block BSi, is compared with block BCk1. The pair of blocks which have the least absolute difference is determined. Here, subtracts each element in BSi from the corresponding element in array BCK1 and returns the absolute difference of blocks into the output array t(j). If BSi and BCk1 are integer arrays, elements in the output that exceed the range of the integer type are truncated. A key is used to determine the address of the best matched block BCk1 for the block BSi. Then IDWT is applied to get cover C.

2) Key Embedding using DWT

The generated key is hidden in the cover using the watermarking technique proposed in using DWT. Since in steganography, the cover image is not required at the receiver once the secret information is extracted, some of the bit planes of the transformed coefficients of the cover can be entirely modified to hide the secret information. This increases the hiding capacity.

In order to increase the robustness and security the middle bit planes of the higher frequency components of the transformed cover image are used.

The steps to hide the key are as follows:

- Find the discrete wavelet transform of the cover image
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image
- Replace the middle bit planes of the higher frequency components of the transformed image by the bits of the key.
- Obtain the inverse DWT of the resulting image to get the stego image.The embedding process is explained graphically in Fig. 4.1.

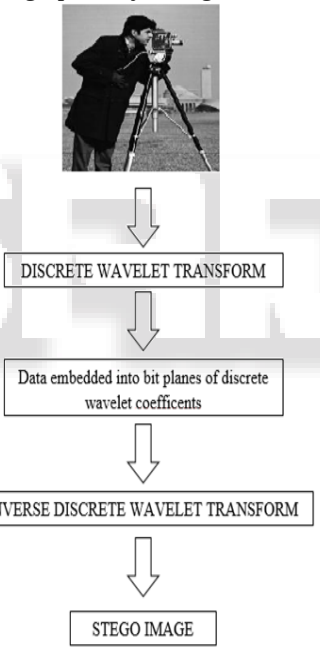

Fig. 2: The embedding process in steganography technique by using DWT

The extraction process also consists of two steps:

3) Key Extraction

The steps are as follows:

- Find the discrete wavelet transform of the stego image.
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image
- The middle bit planes of the higher frequency components contain the key.

4) Secret Image Generation

- Transform the stego-image into single level 2D DWT.
- This transformation results in four sub-bands GLL, GHL, GLH and GHH. Divide the sub-band image

GLL into 4x4 non overlapping blocks. The key is used to obtain the blocks that have the nearest approximation to the original blocks in secret image.
- The obtained blocks are then rearranged to obtain the sub-band image SLLnew. Assuming SHLnew, SLHnew, SHHnew are zero matrices of dimension similar to SLLnew. 2D IDWT is obtained.
- The resultant image is the secret image S.

B. Proposed Algorithm 2

1) Key Generation

Same procedure performed in algorithm 1

2) Key Embedding using IWT

The steps to hide the key are as follows:
- Find the integer wavelet transform of the cover image
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image
- Replace the middle bit planes of the higher frequency components of the transformed image by the bits of the key.
- Obtain the inverse IWT of the resulting image to get the stego image.

The embedding process is explained graphically in figure 4.2.

The extraction process also consists of two steps:

3) Key Extraction

The steps are as follows:
- Find the integer wavelet transform of the stego image
- Construct the binary image using the middle bit planes of the higher frequency components of the transformed image
- The middle bit planes of the higher frequency components contain the key.

4) Secret Image Generation
- Transform the stego-image into single level 2D DWT.
- This transformation results in four sub-bands GLL, GHL, GLH and GHH.
- Divide the sub-band image GLL into 4x4 nonoverlapping blocks. The key is used to obtain the blocks that have the nearest approximation to the original blocks in secret image.
- The obtained blocks are then rearranged to obtain the sub-band image SLLnew. Assuming SHLnew, SLHnew, SHHnew are zero matrices of dimension similar to SLLnew. 2D IDWT is obtained.
- The resultant image is the secret image S.

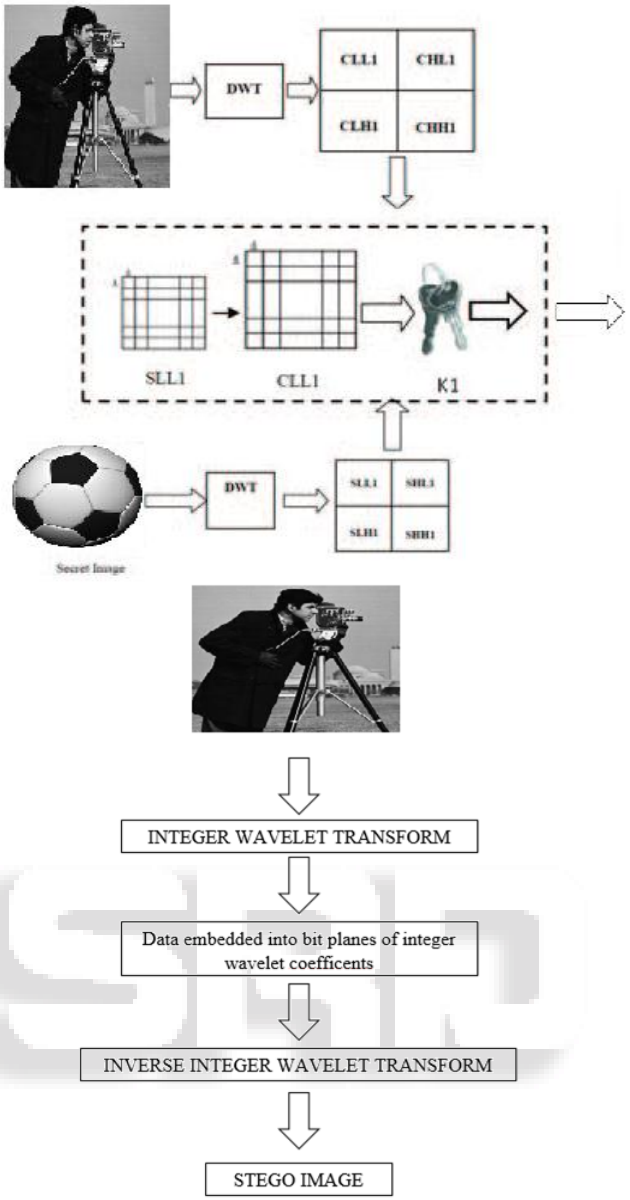

Fig. 3: The embedding process in steganography technique by using DWT and IWT.

IV. Experimental Results

We have performed experiments on Windows 7. All experiments are performed in MatLab 2012a.

Sr No	Bit Plane	PSNR (dB)	MSE	MAX ERROR
1	1	34.9823	20.6468	67.75
2	2	34.9538	20.7826	67.75
3	3	34.8297	21.3853	67.75
4	4	34.8749	21.1637	67.75
5	5	34.7398	21.8321	67.75
6	6	34.7101	21.9823	67.75
7	7	34.6742	22.1645	67.75
8	8	34.6342	22.3699	67.75
9	16	33.8996	26.4925	67.75
10	32	31.9209	41.7818	67.75
11	64	28.1137	100.391	69.75

12	128	22.9491	329.7369	101.75
13	256	17.2074	1.24E+03	165.75
14	512	11.2776	4.85E+03	293.75
15	1024	5.2892	1.92E+04	549.79
16	2048	-0.7187	7.67E+04	1061.8

Table 1: Performance parameter of cover image and stego image by using DWT Steganography Technique.

Sr No	Bit Plane	PSNR (dB)	MSE	MAX ERROR
1	1	6.5433	1.4413e+04	232.5
2	2	6.5433	1.4413e+04	232.5
3	3	6.5433	1.4413e+04	232.5
4	4	6.5433	1.4413e+04	232.5
5	5	6.5433	1.4413e+04	232.5
6	6	6.5433	1.4413e+04	232.5
7	7	6.5433	1.4413e+04	232.5
8	8	6.5433	1.4413e+04	232.5

Table 2: Performance parameter of original secret image and extracted secret image by using DWT Steganography Technique.

Performance parameter of cover image and stego image at different bit plane by using IWT and DWT Steganography Technique is presented in table 3. Also the extracted image is compared with the original secret image by using PSNR, MSE and MAX ERROR parameters. Performance parameter of original secret image and the extracted secret image at different bit plane by using IWT and DWT Steganography Technique is presented in table 3.

Sr No	Bit Plane	PSNR	MSE	MAX ERROR
1	1	61.9244	0.0417	2
2	2	58.9428	0.0829	2
3	3	52.2978	0.3831	3
4	4	52.7514	0.3451	3
5	5	49.8408	0.6745	4
6	6	48.2703	0.9684	4
7	7	46.4611	1.4688	5
8	8	46.8175	1.3531	6
9	16	40.7384	5.4858	12
10	32	34.7436	21.8133	24
11	64	28.7175	87.3634	48
12	128	22.6912	349.9093	96
13	256	16.6693	1.40E+03	192
14	512	10.5806	5.69E+03	385
15	1024	5.148	1.99E+04	641
16	2048	-0.8729	7.95E+04	1281

Table 3: Performance parameter of cover image and stego image by using DWT and IWT Steganography Technique.

Sr No	Bit Plane	PSNR (dB)	MSE	MAX ERROR
1	1	12.6609	3.52E+03	250
2	2	12.6609	3.52E+03	250
3	3	12.6609	3.52E+03	250
4	4	12.6609	3.52E+03	250
5	5	12.6609	3.52E+03	250
6	6	12.6609	3.52E+03	250
7	7	12.6609	3.52E+03	250
8	8	12.6609	3.52E+03	250

Table 4: Performance parameter of original secret image and extracted secret image by using DWT Steganography Technique.

V. CONCLUSION

Generally, image steganography method does not provide much attention on the basic demand of secrecy and privacy. In this project, the major importance is given on the secrecy as well as the privacy of information. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. These operations provide sufficient secrecy. The goal of this project is to characterize and categorize the new ways of providing security to images while transmission over wireless channels

REFERENCES

[1] N. Provos, P. Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Computer Security 2003, <http://www.citi.umich.edu/u/provos/papers/practical.pdf.
[2] J. C. Judge, Steganography: Past, Present, Future, SANS Institute, <http://www.sans.org/reading_room/whitepapers/steganography/steganography-past-present-future_552.
[3] Hemalatha S, Renuka A, U. Dinesh Acharya, Priya R Kamath. "A Secure Image Steganography Technique Using Integer Wavelet Transform", In Proceedings of IEEE 978-1-4673-4805-8/12, 2012.
[4] Gabriel BUGÁR, Vladimír BÁNOCI, Martin BRODA, Dušan LEVICKÝ, Denis DUPÁK. "Data Hiding in Still Images Based on Blind Algorithm of Steganography." IEEE 978-1-4799-3715-8/14, 2014.
[5] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi. "High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm", In Vol I, Hong Kong, Proceedings of the International Multi-Conference of Engineers and Computer Scientists 2011.
[6] Diop, S. M. Farssi, M. Chaumont, O. Khouma, et H. B. Diouf, "Utilisation des codes LDPC en stéganographie, " CORESA'2012, COmpression et REprésentation des Signaux Audiovisuels, Lille, France, 24-25 mai, 2012.
[7] Jayant Rajurkar,T.K.Khan," Review on Efficient Query processing for Set Predicates of Dynamically Formed Group", International Journal of Advanced Research in Computer Science and Software Engineering

(IJARCSSE), Volume 4, Issue 9, Page No.640-643,2014.

[8] Lalit Dole,Jayant Rajurkar,"A Decision Support System for Predicting Student Performance",International Journal of Innovative Research in Computer and Communication Engineering,Volume 2,Issue 12,Page No.7232-7237,2014.

[9] T. Narasimmalou and Allen Joseph. R, "Optimized Discrete Wavelet Transform Based Steganography", IEEE InternationalConference on Advance Communication Control and Computing Technologies (ICACCCT), pp 88-91, 2012.

[10] S. Kouider, M. Chaumont, et W. Puech, "Stéganographie Adaptative par Oracle (ASO)," CORESA'2012, COmpression et REprésentation des Signaux Audiovisuels, Lille, France, 24-25 mai, 2012.

[11] Fridrich, J., Goljan, M.: Practical steganalysis of digital images – state of the art. In Delp III, E.J., Wong, P.W., eds.: Security and Watermarking of Multimedia Contents IV. Volume 4675 of Proc. SPIE., 2013

[12] J. Kodovský et J.J. Fridrich. "Steganalysis in high dimensions: fusing classifiers built on random subspaces," in Media Watermarking, Security, and Forensics XIII, part of IS&T SPIE Electronic Imaging Symposium, volume 7880, paper. 21, pages L 1–12, San Francisco, CA, January 23-26 2011.

