National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

Digital Image Watermark Protection and Self-Recovery using Discrete Wavelet Transformand SPIHT Coding

B.Uma[1], M.S.Monisha[2]

[1,2]M.E – Communication Systems, Department of ECE, Adhiyamaan College of Engineering, Hosur,-635109.

Abstract— *Embedding a watermark in the original image has been widely used to avoid tampering or damaging in the area of image forensics. This paper explains about detecting the damaged/tampered area of the received image and a technique to recover the lost information in the tampered areas. Since the Most Significant Bits/ Reference bits contains the entire information about the image, the Least Significant Bits/check bits are used to find the tampered zones. But if the reference bits are lost, the whole image gets corrupted or erased. So an appropriate channel code is used to protect the reference bits. In the proposed method, RS (REED-SOLOMON) channel coding is used. While doing so, parity bits are added to the reference bits. Also by knowing the tampered location, erasure error can be found from an image tampering model. Recovering an image includes the detection of erasure locations with the help of redundancy bits at the decoder side. Our proposed method is simple to implement and better performance is achieved in the retrieval of tampered image at the time of recovery.*

Keywords— Digital Watermarking, DWT, Embedding an image, LSB Detection, RS channel coding, SPIHT algorithm.

I. INTRODUCTION

Recent years, the attention is increased towards the protection of the multimedia information. For this, internet is widely used for endless copying, tampering and distribution is carried by the author day by day. For this reason, we go for more number of methods to protect the information especially in forensic image recovery from the hackers. Hackers have the opportunity to get the electronic material from different sources and through the internet modify the information easily. The existing method to protect the multimedia data is watermarking in spatial domain with increased embedding robustness. In multimedia, the secret of the digital pictures has been labeled using watermarking technique despite of its disadvantages.

So we go for newly proposed method namely, SPIHT (Set Partitioning In Hierarchical Tree) algorithm technique using spatial direction tree it generates the efficient zero tree structure for wavelet coefficients accurately. The efficiency of the compression technique is large and the coding complexity is reduced. Here we also used the 2-Discrete Wavelet Transform. It is used to convert the image in spatial domain into frequency domain. After this, SPIHT compression algorithm is applied to an image in order to partition the decomposed image wavelets into insignificant and significant partitions.

SPIHT is a simple, efficient compression algorithm compared with any other compression techniques. It provides better quality of image and increased peak signal to noise ratio (PSNR) value. SPIHT technique is more effective in the identification of zero trees to increase the chance of forming flexible zero trees. In the existing methods there are two drawbacks, namely

- Watermarking in spatial domain
- Embedding robustness

1.1 Watermarking in spatial domain

Hiding process of digital information in an image is known as watermarking. This type of hidden process does not contain any relation to an image. Watermarking is simply a technique used to verify the owner's data and authentication from the nature and non-nature image to ensure the symbol of owner-ship. Using this method, we verify the owner data i.e., signature, facsimile, etc. This identifies the original owner by extracting and detecting from the watermarked images. Owner can ensure the multimedia data which belongs to them using embedding the watermark into the original image. The human eye cannot differentiate the watermark from the watermarking image. Based on the domains used in the embedded watermarks, the

National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

watermarking is classified into transform and spatial water marking. Higher data embedding applications uses spatial domain watermarking. The transform domain technique is suitable for the application where the robustness is a crucial concern. The basic block diagram of the watermarking is shown in fig 1.

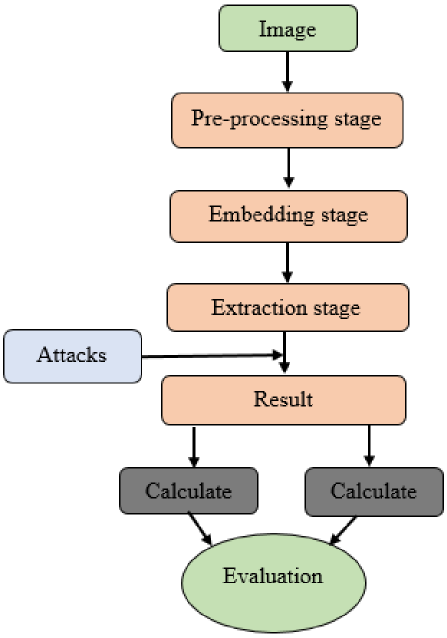

FIG 1: BASIC BLOCK DIAGRAM OF THE WATERMARKING TECHNIQUE

In previous days, the watermarking comprises a sequence of bits and it can be detected using detection theory. On the verification time, the original image is subtracted from the given image, verified and identified. Self-recovery methods for watermarked bits is of two categories: check bits and reference bits, check bits are used to locate the tampered blocks in the image, the reference bits used to restore the original image. In digital watermarking, the main advantage is image authentication. Digital watermarking uses a secret key and the key is used at the decoder to decode the watermarked image. The characteristics of Digital watermarking technique are security, imperceptibility and capacity

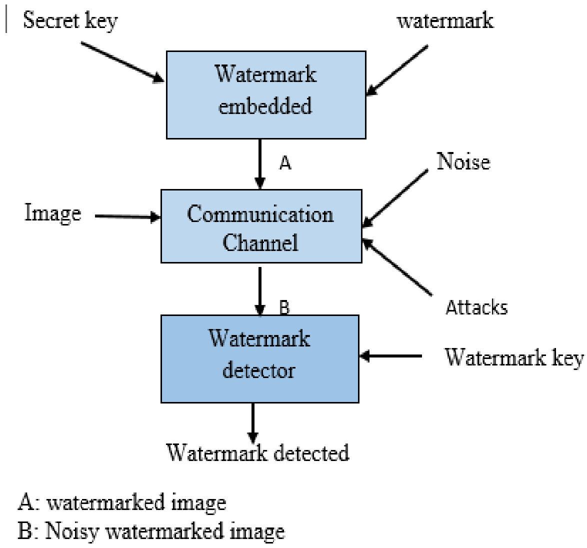

FIG 2 : DIGITAL WATERMARKING PROCESSES

Features of watermarking:

- **Noiselessness:** It is not noticed by simple analyzing.
- **Key distinctiveness:** watermarking keys are statistically independent.
- **Robustness:** Using common signal processing operations, it is efficiently detected.

The spatial domain is used in watermarking method. A common picture cropping operation that may be used to eliminate the watermark is the major disadvantage in spatial domain watermarking. So frequency domain approaches have also been proposed. Multimedia watermarking is also used spread spectrum technique.

1.2 Embedding Robustness:

Robustness is defined as recover the watermark from the watermarking images for after several attacks takes place. For example attacks are cropping, rotation, Gaussian etc. The important issue that needs to be concerned in watermarking is security and robustness [5]. The facility to restrict the embedding, extracting and un-authorized removal from an image is known as security.

II. SPIHT ALGORITHM AND DWT

SPHIT (Set Partitioning in Hierarchical Trees) is a compression algorithm in which the output bit stream is truncated with the desired rate and an appropriate image is generated. The quality of reconstructed image is better with the high output rate. According to the magnitudes, the wavelet transform coefficients are found and then transmitted depending on their bit order. This operation is called sorting. This sorting order is needed to reduce the bit budget.

This algorithm uses the self-similarities between various sub-bands. The similarities are found from the spatial orientation trees. Here the output rate is ns bits/pixel. In order to avoid tampering channel coding is used. If the channel code is perfect without any errors, a maximum signal to noise is achieved. This will be useful while reconstruction of original image at ns bit rate. The advantage of this algorithm is that the adaptive output rate to exploit various compression rates. The block diagram for our proposed method is shown in the Fig 1.

The aim of our algorithm is to avoid damaging/tampering of an image. To do this, the original image is embedded with a watermark. Since this watermark is capable of finding the damaged areas in the received image, so that the recovering of image gets easier. To achieve this, the most significant bits in each pixel are not changed and the remaining bits are used for watermark embedding. To make image recovery easier, the images are compressed using source encoding is used followed by watermarking. Some information may be lost or tampered during transmission, hence the compressed bit stream is encoded using RS channel codes which generates the check bits without changing the MSB bits. These check bits or parity bits are included with channel coded bits forming the Least Significant Bits. At the receiver side, the check bits are used to locate the tampered block which is used in identifying the erasure locations. The erasure decoder finds the compressed image regardless of erasure. Then the image is normally decoded to recover the original image. The average tampering rate used here is

$$\text{TTR}\ (n_s, n_c) = \frac{n-k}{n} = 1 - \frac{n_s}{n_c} \qquad (1)$$

The discrete wavelet transform is used to increase the high ability, better imperceptibility. It gives better localization in both time and frequency domain [6]. The main advantage is that it increases the compression ratio.

In the Proposed method, the following blocks are involved

- SPIHT Coder
- LSB Detection
- RS Channel encoding block
- Embedded image block
- Watermarking block

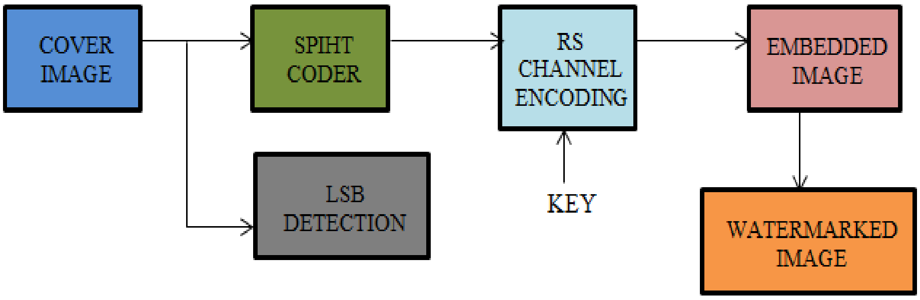

FIG 3: MODIFIED SPIHT ALGORITHM

2.1 SPIHT Coder:

As a first step, the SPIHT coder codes the most important wavelet transform coefficients and transmits the bits to obtain an exact copy of the original image progressively. This is a powerful image compression algorithm that produces an embedded bit stream from which the better images can be reconstructed at various mean square error values and also at various bit rates. The perceptual image quality is not guaranteed to be ideal, since the coder is not designed with the consideration of the human visual system (HVS) characteristics.

2.2 LSB Detection:

Consider an image represented by 8 bit gray scale pixel values. These 8 bits are divided into Most Significant Bits; Check bits (n_c), Source bits (n_s) and Channel code parity/redundancy bits (n_p). The Check bits (n_c), Source bits (n_s) and Channel code parity/redundancy bits (n_p) will form the LSB. The MSB will not be changed at the time of embedding a watermark and later used for image recovery. Since this LSB bits are replaced with watermark bits, it is detected using a LSB detection block and its mean square error is given by

$$MSE(n_w) = \frac{1}{2^{n_w}} \sum_{i=0}^{2^{n_w-1}} \sum_{j=0}^{2^{n_w-1}} (i-j)^2 = \frac{4^{n_w-1}}{6} \tag{2}$$

2.3 RS Channel Encoding:

2.3.1 RS (REED_SOLOMON) Code:

The Reed –Solomon code-words consists of function tables based on uni-variate polynomials. RS channel encoding turns k symbols into a function table with a list of n symbols. Then the first segment of the function table is interpreted by k symbols of polynomials of degree less than k and remaining (n-k) symbols are generated by solving the polynomial at that point. An over determined system is formed by the n transmitted symbols, so the original image is retrieved at the receiver using interpolation technique.

2.3.2 RS Channel Encoding:

The code rate for RS channel code is given by $R=n_s/n_c$, where $n_c= n_s+n_p$. The total channel code is $N_c = N \times n_c$bits. These bits are used to vary and spread over the entire image in such a way that every pixel consists of both source bits and channel coded bits. A key is generated before and after channel coding which is assumed to known by both the transmitter and receiver. Then the LSB bits replaced with channel coded parity bits along with check bits and secret key in the embedding phase. The encoders and decoders are designed by puncturing the RS code using the equation,

$$m = \min_{\hat{m}}(\hat{m} | 2^t - 1 \quad \text{and} \quad \hat{m} > n). \tag{3}$$

National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

2.4 Embedding a Watermark:

There are so many watermarking algorithms used based on the type of application. A general watermark embedding process is shown in fig 4. The bits other than Most Significant Bits (i.e., check bits and channel encoded bits) are used to embed a watermark in the original image. As said in earlier, check bits and channel coded bits generate a secret key which is used to protect it from tampering and secured authentication. It finds application in forensic imagery and defense.

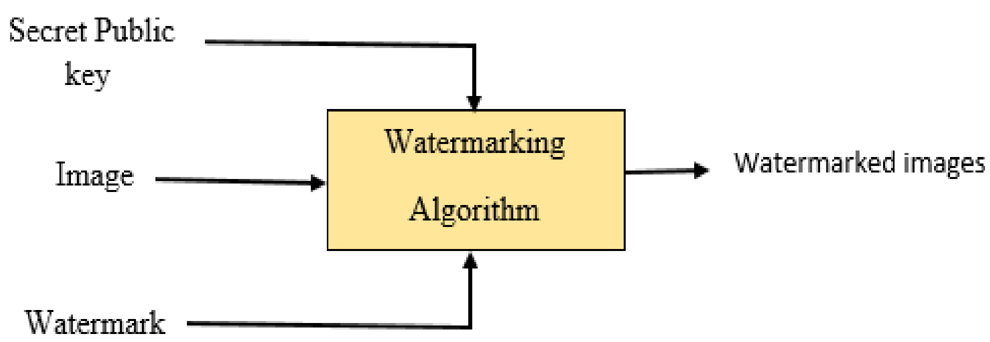

FIG 4: EMBEDDING PROCESS

2.5 Receiver side - Decoding process:

The receiver side process is very simple. From the image received, the LSB bits are processed to identify whether tampering of image is present. The decoding process at the received side is shown in fig 5.If so, tampered area is located using the check bits.

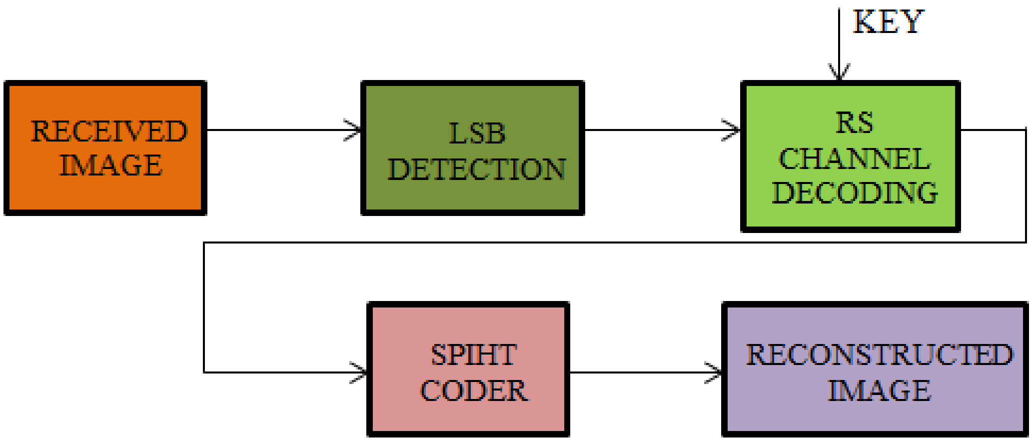

FIG 5: RECONSTRUCTION OF RECEIVED IMAGE

Once the tampered location is known, channel encoded bits are decoded using the same key by the RS channel decoding algorithm to decode the tampered area. Then the SPIHT coder reconstructs the original image from the digitally embedded watermarked image. A general watermarking detection is shown in fig 6.

National Conference on Information, Communication, VLSI and Embedded systems (ICVE 2K16)
(16 - 17 March 2016)
International Journal of Engineering Research & Science (IJOER)
ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

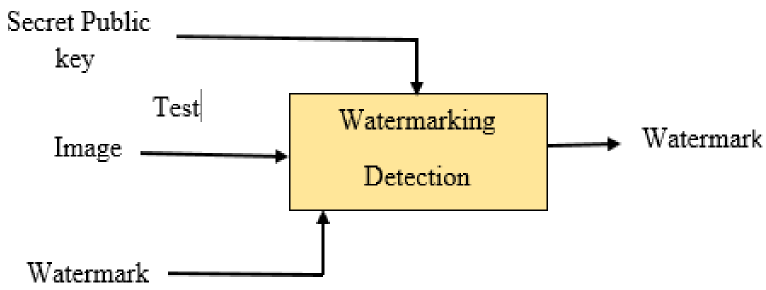

FIG 6: DECODING PROCESS

III. RESULTS AND ANALYSIS

Consider a color image,

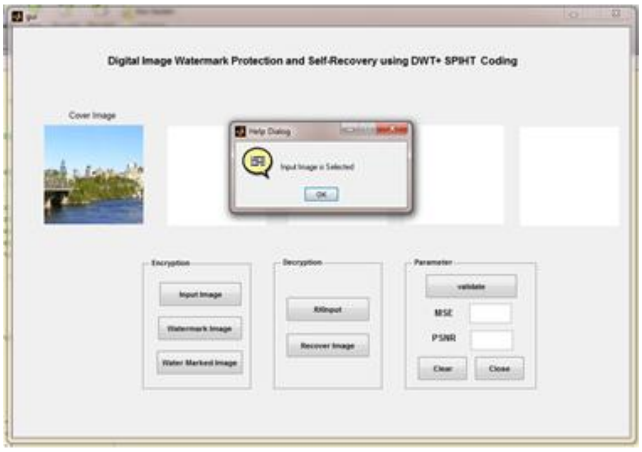

FIG 7.1 COVER IMAGE SELECTION

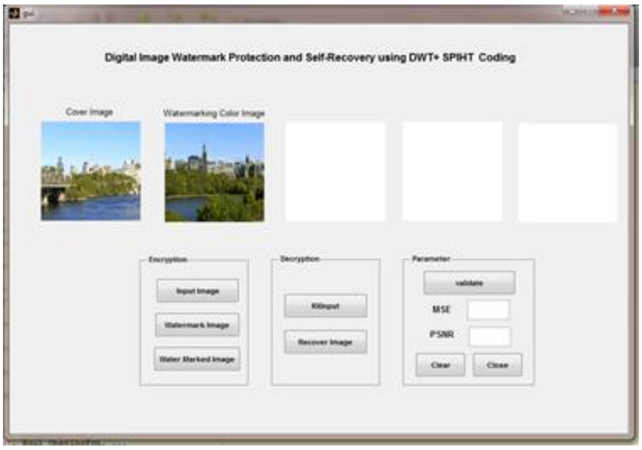

FIG 7.2 WATERMARK IMAGE

FIG 7.3 AFTER WATERMARKING

FIG 7.4 STEGO IMAGE AT RECEIVER SIDE

ISSN: [2395-6992] [Vol-2, Issue-3 March- 2016]

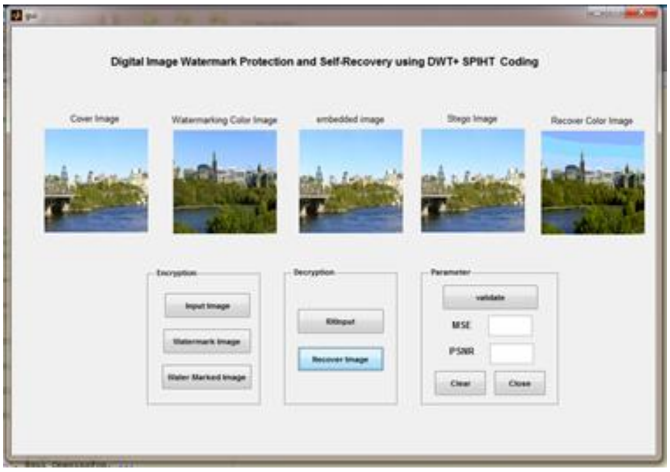

FIG 7.5 RECOVERED WATERMARK IMAGE(DATA)

FIG 7.6 VALIDATION OF MSE AND PSNR

IV. CONCLUSION

In this paper, the SPIHT compression algorithm is used to source code the actual image. An 8×8 pixel in an image is splitted into Most Significant Bit (MSB) and Least Significant Bit (LSB). Further, a modified watermarking scheme is used to protect the original image from damaging/tampering. Then the LSB bits are divided into source encoder bits, check bits and channel encoder bits. This modified scheme uses the check bits present in the LSB bits to locate the tampered zone and the RS channel coded bits are used to recover the image in that tampered area. A tampering model is modeled to find the erasure error. This error is utilized by the RS channel decoder in recovering the original image. In this paper, the implementation of encoder and decoder circuits is simple. The peak signal to noise ratio is high compared with the proposed method. A better image recovery is achieved using these techniques. In Future, various improvements in SPIHT algorithm can be made in the areas of speed with high PSNR, resilience and memory requirement.

REFERENCES

[1] AthanasiosNikolaidisioannis pitas, " Region- based image watermarking" IEEE Transactions on image processing, NOV-2001.

[2] Chiou-Ting Hsu AndJa-Ling Wu "Hidden Digital Watermarks in Images" IEEE Transactions On Image Processing, Vol. 8, No. 1, January 1999.

[3] Myasar Mundher1, Dzulkifli Muhamad1, Amjad Rehman2,∗ , Tanzila Saba3 And Firdous Kausar4 "Digital Watermarking For Images Security Using Discrete Slantlet Transform" Appl. Math. Inf. Sci. 8, No. 6, 2823-2830 (2014) 2823 Applied Mathematics & Information Sciences- An International Journal.

[4] M. Kim1, D. Li2 "A Robust Digital Watermarking Technique For Image Contents Based On DWT-DFRNT Multiple Transform Method" International Journal Of Multimedia And Ubiquitous Engineering Vol.9, No.1 (2014), Pp.369-378

[5] Mohan Durvey, DevshriSatyarthi "A Review Paper on Digital Watermarking "International Journal Of Emerging Trends & Technology In Computer Science (IJETTCS)Volume 3, Issue 4, July-August 2014

[6] I. VenkataAnjaneyulu, P. Rama Krishna "Fpga Implementation OfDwt-Spiht Algorithm For Image Compression" International Journal Of Technology Enhancements And Emerging Engineering Research, Vol 2, Issue 3 ISSN 2347-4289

[7] Chandan deep Kaur1, SumitBudhiraja "Improvements of SPIHT in Image Compression-Survey" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume3,Issue1,January2013)

[8] Li-Der Jeng , Yuan-Nung Liu "An Improved Spiht Format For Image Transmission "International Journal Of Information Technology & Computer Science (IJITCS)(ISSN No : 2091-1610) Volume 9 : Issue No : 2 : Issue On May / June, 2013

[9] Ping Liu, Guanfeng Li "An Improved Spiht Algorithm For Image Compression In Low Bit Rate" ommunications and Network, 2013, 5, 245-248http://dx.doi.org/10.4236/cn.2013.53B2045 Published Online September 2013.

[10] Sadashivappa1,Mahesh Jayakar, K.V.S AnandBabu , Dr. Srinivas K "Color Image Compression using SPIHT Algorithm" ,International Journal of Computer Applications (0975 – 8887) Volume 16– No.7, February 2011

[11] Shih-Hsuan Yang And Wu-Jie Liao "Evaluation Of Spiht Coding Parameters"IEEE Transactions On Image Processing, Vol. 24, No. 7, July 2015

[12] Dr.M.Mohamed Sathik1 and S.S.Sujatha2 "An Improved Invisible Watermarking Technique for Image Authentication "international Journal of Advanced Science and TechnologyVol.24,November,2010.

[13] A.Saidand W. Pearlman, “A New Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Tress, ”IEEE Transactions on Circuit and System forVideo Technology, Vol. 6, 1996, pp. 243-250.

[14] Sweldens. W, “The lifting scheme: a custom-design construction of biorthogonal wavelets,” Applied and ComputionalHarmonicAnalysis, Vol. 6, No. 2, 1996, pp.186-200.doi:10.1006/acha.1996.0015

[15] W.B.Fan,J.ChenandJ.N.Zhen, “SPIHT Algorithm Based on Fast Lifting Wavelet Transform in Image Compression,” LNAI,Vol.2,2005,pp.838-844.

[16] Y. F. Yang and Z. X. Su, “An Improved Based on Wavelet Zero tree Image Coding Algorithm, ”China journal of Image and Graphics, Vol. 6, 2001, pp. 542-546.

[17] L.Y.Li, C. L. Zhan and L. Huang, “The Algorithm of SPIHT Coding Based on LS9/7 Lifting Wavelet,” Communication Technology, Vol. 40, 2007, pp. 362-363.

[18] P. Yu, X. H. Ma and J. G. Li, “The Algorithm of Image Compression Based on LS9/7 Lifting Wavelet,” Microelectronics and Computer,Vol.40,2008,pp110-111.