논문-03-08-4-10

Enhancing Robustness of Information Hiding Through Low-Density Parity-Check Codes

Yu Yi*, Moon Ho Lee*, Ji Hyun Kim* and Gi Yean Hwang*

Abstract

With the rapid growth of internet technologies and wide availability of multimedia computing facilities, the enforcement of multimedia copyright protection becomes an important issue. Digital watermarking is viewed as an effective way to deter content users from illegal distributions. In recent years, digital watermarking has been intensively studied to achieve this goal. However, when the watermarked media is transmitted over the channels modeled as the additive white Gaussian noise (AWGN) channel, the watermark information is often interfered by the channel noise and produces a large number of errors. So many error-correcting codes have been applied in the digital watermarking system to protect the embedded message from the disturbance of the noise, such as BCH codes, Reed-Solomon (RS) codes and Turbo codes. Recently, low-density parity-check (LDPC) codes were demonstrated as good error correcting codes achieving near Shannon limit performance and outperforming turbo codes with low decoding complexity. In this paper, in order to mitigate the channel conditions and improve the quality of watermark, we proposed the application of LDPC codes on implementing a fairly robust digital image watermarking system. The implemented watermarking system operates in the spectrum domain where a subset of the discrete wavelet transform (DWT) coefficients is modified by the watermark without using original image during watermark extraction. The quality of watermark is evaluated by taking into account the trade-off between the chip-rate and the rate of LDPC codes. Many simulation results are presented in this paper, these results indicate that the quality of the watermark is improved greatly and the proposed system based on LDPC codes is very robust to attacks.

Ⅰ. Introduction

The fast development of multimedia applications on the internet, combined with the simplicity of duplication and distribution of digital data, has recently stimulated many research efforts towards the design and study of sophisticated digital media protection methodologies. A new emerging technology, digital watermarking[1], protects digital media by embedding or hiding a robust signal or some other distinguishing piece of information directly into the media, thus providing a promising way to protect the digital media from illicit copying and manipulation. Much work done in this field in the past decade have resulted in the advancement of robust, unperceivable, watermarking strategies[2] and many algorithms have been derived for watermarking images, audio, video, and VRML models.

With the advancement of watermarking techniques, they already have many applications, including copyright protection, information hiding and steganography. For different kinds of applications, digital watermarking should show different properties. In these applications, for example, copyright protection is the most prominent application in digital watermarking, so for this kind of application, digital watermarking should have properties such as invisibility,

* Institute of Information & Communication, Chonbuk National Univ.

※ This work was partially supported by ITRC and KOSEF (No. 303-15-2).

robustness, high detection reliability, etc[3].

However, when the watermarked media is transmitted over the watermark channel modeled as the AWGN channel, the watermark information is often interfered by the channel noise and produces a large number of errors. So many error-correcting codes have been applied in the digital image watermarking system to protect the embedded message from the noise, such as BCH codes, Reed-Solomon (RS) codes and Turbo codes. LDPC codes were demonstrated as good error correcting codes achieving near Shannon limit performance and outperforming turbo codes with low decoding complexity. As we all know, in the communication system, LDPC encoder plays a role of adding parity bits to information data for the purpose of protecting information data. LDPC decoder plays a role of recovering information data after correcting errors occurred by the noisy channel from transmitted data including parity check bits. Digital watermarking is a distinguishing piece of information that is adhered to image for protecting rightful ownership of image. In this paper, in order to mitigate the channel conditions and improve the quality of watermark, we proposed the application of LDPC codes as channel codes on implementing a fairly robust digital image watermarking system because of their advantages. The implemented watermarking system operates in the spectrum domain where a subset of the DWT coefficients is modified by the watermark without using original image during watermark extraction. The quality of watermark is evaluated by taking into account the trade-off between the chip-rate and the rate of LDPC codes. Many simulation results are presented in this paper, these results indicate that the quality of watermark is improved greatly and the proposed system based on LDPC codes is very robust to attacks.

This paper is organized as follows: section 2 introduces the proposed digital image watermarking system used in this paper, which includes watermark generation, watermark embedding and watermark extraction. In section 3, LDPC codes and the iterative decoding algorithm are described in detail. Various simulation results are presented in section 4. Finally, section 5 gives the conclusion.

Ⅱ. Digital Image Watermarking System

An abstract block diagram of digital image watermarking system model used in this paper is shown in Fig. 1.

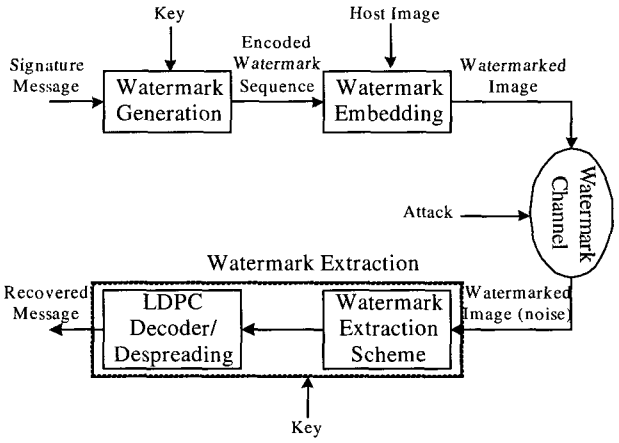

Fig. 1. An abstract block diagram of digital image watermarking system based on LDPC codes

As indicated in Fig. 1, there are three main stages in the design of the proposed digital image watermarking system: watermark generation, watermark embedding and watermark extraction.

Watermark generation is the generation of the watermark sequence to be embedded in the host or cover image. Besides signature message (watermark), the watermark sequence also depends on secret keys. As we all know, the secret keys involved in the generation of the watermark not only provide the security, but also can be used as a method of distinguishing different data owners from each other. In our work we use the watermarking scheme that is similar to spread-spectrum (SS) communication at the watermark generation stage. Two ways generating the spread watermark sequence can be chosen, one is based on the pseudo-random sequence and the other is based on the pseudo-noise

sequence. We use the second approach that is the signature message consists of a number of bits, which are modulated by pseudo-noise sequence in this paper to generate the watermark sequence. However, when the watermarked host image is transmitted over the noisy channel, we can find out the spread watermark sequence embedded in the host image is interfered by channel noise and produces a large number of errors. So we apply the LDPC codes technique in this proposed system to correct the errors in the embedded watermark sequence. Especially, LDPC encoder is used in watermark generation. The spread watermark sequence is transformed to the encoded watermark sequence by LDPC encoder. According to the above description, in our watermarking system, the watermark generation consists of spread spectrum watermark function and LDPC encoder.

Watermark embedding is a method of inserting the encoded watermark sequence from the watermark generation into the host image to get the watermarked image. Based on the scheme of embedding, digital watermark embedding can be classified as: spatial domain watermarking and spectrum domain watermarking[4]. In spatial domain watermarking schemes, the watermark is embedded by modifying the pixel value of an image directly. Though they are simple and don't need the original image to extract the watermark, spatial domain watermarking schemes are not robust to the signal processing operations, since the watermark doesn't spread all over the image and some common signal processing operations can easily erase the embedded watermark without affecting the quality of the watermarked image. On the contrary, spectrum domain watermarking schemes involve embedding the watermark by modifying the spectrum coefficients, after the image has been transformed to the spectrum domain, such as the Discrete Cosine Transform (DCT) domain, Discrete Fourier Transform (DFT) domain and Discrete Wavelet Transform (DWT) domain. Since these transforms de-correlate the spatial value of an image, most of the energy of the image is put on low frequency components in the spectrum domain. The watermark is usually inserted into the low frequency and middle frequency coefficients and the modifications will spread throughout the image. Because low and middle frequency coefficients are less likely to be affected during common signal processing than high frequency coefficients, the spectrum domain watermarking schemes are more robust than the spatial domain watermarking schemes. Because of the advantage of spectrum domain watermarking schemes, they are used in the watermark embedding and we can get the watermarked host image from the host image based on the DWT and encoded watermark sequence. Then it is transmitted over the watermark channel modeled as the AWGN channels and attacked by the channel noise.

Watermark extraction is the recovery of the signature message from the watermarked host image. Besides the watermarked host image, the presence of the secret keys involved in the watermark generation is required. In this paper, the signature message is extracted without the original cover image. So as mentioned in the watermark generation stage and the watermark embedding stage, we can know that the watermark extraction consists of watermark extraction function, LDPC decoder and the dispreading function. LDPC decoder is used to correct the errors in the recovered signature message from the watermark extraction function. Finally, we can get the recovered signature message from the dispreading function.

1. Watermark Generation

In this section, watermark generation is described in detail. The generation of the watermark sequence is in many aspects similar to the spread-spectrum (SS) modulation scheme. In the spread spectrum communication, a narrow band signal is transmitted over a much larger bandwidth such that the signal energy present in any single frequency is undetectable [4]. The spreading is accomplished by methods of a spreading sequence. Also, the same sequence is used at the receiver side for dispreading and data recovery. Similarly the watermark bits are spread by a large factor called

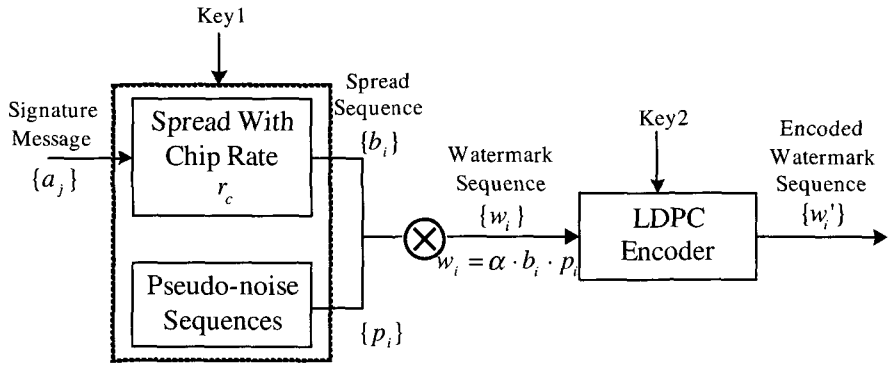

Fig. 2. A block diagram of watermark generation

chip-rate so that it is imperceptible. The block diagram of watermark generation is shown in Fig. 2.

According to the above Fig. 2, some notations are described as follows[6], let M be the total number of pixels in a cover image, a total of L signature message bits be embedded in the host image and r_e be the chip-rate used to spread the message bits.

$$r_e = M/l \tag{1}$$

The chip-rate is considered as a parameter to study watermark because it clearly affects watermark robustness and watermark capacity. For a fixed number M of modified coefficients, the number of L of embedded signature message bits, for instance, the watermark quality increases as the chip-rate decreases. However, a decrease in the chip-rate results in a lower energy of each message bit, and therefore leads to a loss in watermark robustness. After repeating each message bit r_e times, the resulting sequence of consecutive +1's and 1's is reordered in a random fashion. This reordering is done by the key that is the dependent random permutation and provides increased watermark security. Without the knowledge of the correct key, it is impossible to extract the hidden message, since one does not know where the corresponding bits are embedded. So in the proposed system the spread spectrum watermarking sequence is formed with key1 and LDPC encoder are applied with key2. Let $\{a_j\}$ be the sequence of signature message bits that has to be embedded into the cover image. Each data element a_j is either represented by +1 or 1. This discrete signal is spread by a large factor, that is the chip-rate r_e, to obtain the spread sequence $\{b_i\}$:

$$j \cdot r_c \le i \le (j+1) \cdot r_c \tag{2}$$

The purpose of spreading is to add redundancy by embedding one bit of information into r_e pixels of the image. The spread sequence $\{b_i\}$ is then modulated by a pseudo-noise sequence $\{p_i\}$, where $p_i \in \{-1, 1\}$ $\{p_i\}$ serves for frequency spreading. The modulated signal is scaled with a factor α :

$$w_i = \alpha \cdot b_i \cdot p_i \tag{3}$$

Where w_i is the spread spectrum watermark sequence, which is arranged into a matrix with size equal to the image size. However, modern communication infrastructure supports the possibility of delivering quality signals. The different noises in channel of communication will interfere the hidden message, LDPC codes are used as channel codes in our proposed watermarking system to detect and correct the errors caused by the noise. The spread watermark sequence w_i is transformed by LDPC encoder to the encoded watermark w'_i to protect from the noise.

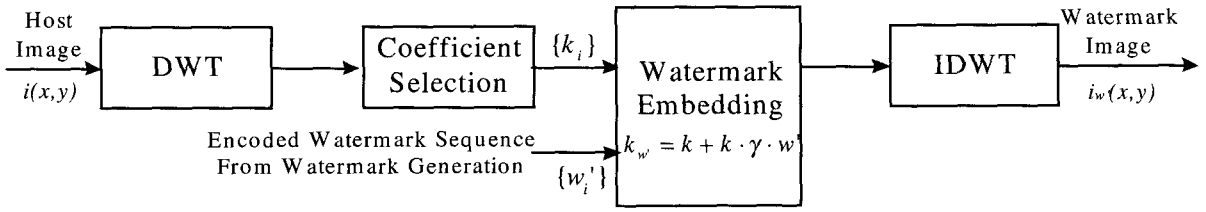

Fig. 3. A block diagram of watermark embedding

2. Watermark Embedding

In this paper, the spectrum domain watermarking is considered as the watermarking embedding scheme based on DWT to improve the robustness of watermark channels. The block diagram of watermark embedding is shown in Fig. 3.

According to the Fig. 3, it is well known that the embedding in the low frequency band is more robust to manipulation such as enhancement and image compression. However, changes made to the low frequency components may result in visible artifacts. Modifying the data in a multiresolution framework, such as a wavelet transform, appears quite promising for obtaining good quality embedding with little perceptual distortion. The dyadic frequency decomposition of the wavelet transform resembles the signal processing of the HVS and thus permits to excite the different perceptual bands individually. Here, three levels DWT with a Daubechies filter are used. The selection of the coefficients that are manipulated in the embedding process is determined by the hiding technique and the application. The main distinction is between the approximation image (LL) which contains the low-frequency signal components and the detail sub-band (LH_j, HL_j, HH_jj is the resolution level) that represent the high-frequency information in horizontal, vertical and diagonal orientation. In this work, the message or signature data are encoded by LDPC codes and are embedded by some coefficients in the detail sub-bands, which are above threshold selected according to the numbers of the encoded watermark sequence from the channel. The magnitude values of the selected DWT coefficients are ordered into a sequence of length M. The watermark sequencefrom the LDPC encoder also consists of M elements. Each coefficient is modified proportional to its magnitude, according to an additive-multiplicative embedding rule as proposed in [6]

$$k_{w',i} = k_i(1+\gamma \cdot w') \tag{4}$$

where r controls watermark strength. Also, the parameter r reflects a trade-off between watermark imperceptibility and watermark robustness. Small values $r$of clearly improve watermark transparency, while diminishing the watermark power and making the embedded watermark more susceptible to attacks. Large values of r, however, increase watermark robustness but also watermark visibility.

After the watermark embedding into the set of the selected coefficients, the watermarked image $i_{w'}(x, y)$ is obtained by taking the Inverse Discrete Wavelet Transform (IDWT). Ideally the difference between the host image and the watermarked image $i(x, y)$ should be as small as possible.

3. Watermark Extraction

The watermark extraction can create the estimate of the embedded watermark signal. We can show the diagram of the watermark extraction in Fig. 4.

The watermark could be extracted without using the original image by means of a correlation receiver. But the pseudo-noise sequence $\{p_i\}$ is needed for watermark extraction. The watermarked image is first

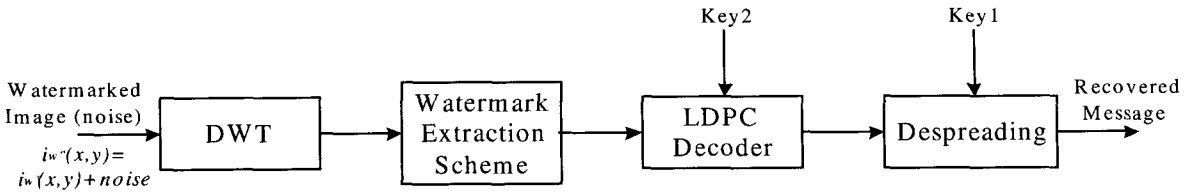

Fig. 4. A block diagram of watermark extraction

high pass filtered to remove major components of the image itself. The second step is de-modulation, which is the multiplication of the filtered watermarked image with the same pseudo-noise sequence $\{p_i\}$ that was used for embedding. This is followed by summation over a window of length equal to the chip-rate, yielding the correlation sum s_j for the jth information bit.

The watermarked image, $k_{w',i}=k_i(1+r\cdot w')$ where w' is from the LDPC encoder. At the receiver, we can get the watermark image disturbed by $i_{w''(x,y)}=i_{w'}(x,y)+noise$. Then, LDPC decoder with key2 and dispreading with key1 are also applied to the extracted watermark message. The high pass filter removes major components of $k_{w'j}$. Therefore, we can get the recovered message in the following[4].

$$s_j=\sum_{i=jr_c}^{(j+1)r_c-1} p_i\cdot w_i=\sum_{i=jr_c}^{(j+1)r_c-1} p_i^2\cdot\alpha\cdot b_i \tag{5}$$

$$s_j=a_j\cdot r_c\cdot\alpha \tag{6}$$

$$sign(s_j)=sign(a_j\cdot r_c\cdot\alpha)=sign(a_j)=a_j \tag{7}$$

This is because $r_c>0$, $a>0$, $p_i^2=1$ and $a_j=\pm 1$. Thus the embedded bit can be retrieved without any loss. This means that the embedded information bit is 1 if the correlation is positive and 1 if it is negative. But since the image cannot be completely removed by the high pass filter, there may be errors in the extracted watermark bits.

Ⅲ. Low-Density Parity-Check (LDPC) Codes

LDPC codes were first introduced by Gallager in 1963[7], in which two ideas are exploited: iterative decoding algorithms and the constrained random code construction. LDPC codes have been almost forgotten for about thirty years, in spite of their excellent properties. Recently, LDPC codes were rediscovered by Mackay[7] as good error correcting codes achieving near Shannon limit performance and outperforming turbo codes. Comparing with turbo codes, LDPC codes possess several distinct advantages: (1) it is easy to create LDPC codes with almost any rate and block length, but turbo code should look for a good interleaver; (2) the simpler decoder based on belief propagation decoding algorithm of LDPC codes is fully parallelizable and accomplishes at a greater decoding speed; (3) the decoding complexity of LDPC codes is lower than that of turbo codes[9].

The LDPC code is a linear block code specified by a very sparse parity-check matrix. In this paper, LDPC codes are defined by $M\times N$ parity-check matrix as (N, K, j, k) LDPC, where K=N-M is the original information bits, j is the column weight and k is the row weight. Note that the code rate is R=K/N. Also, LDPC codes can be represented by a Factor Graph, called as Tanner Graph, which can contains two types of nodes: the bit nodes and the check nodes. Each bit node corresponds to a column of a parity-check matrix, which represents a parity-check equation. An edge between a bit node and a check node exists if and only if the bit participates in the parity-check equation represented by the check node. We can show an example of a parity-check matrix, H and its' corresponding bipartite

Parity Check Matrix

$$H=\begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array} \begin{matrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \end{matrix}$$

Fig. 5. An example of the (9, 6, 2, 3) H matrix

Bipartite Graph

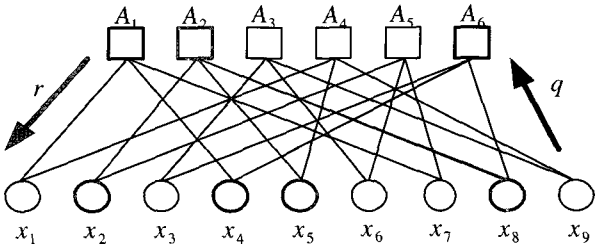

Fig. 6. The bipartite graph

graph in Fig. 5 and Fig. 6, respectively.

In the family of LDPC codes, two kinds of LDPC codes are paid attention to, one is regular LDPC code and the other is irregular LDPC code[11]. Regular LDPC codes are defined that the degrees of all message nodes are equal, and the degrees of all check nodes are equal. This means that the parity-check matrix of the code described above contains the same number of ones in each row and the same number of ones in each column. However, irregular LDPC codes are defined that the degrees of the nodes on each side of the graph can vary widely. In terms of the parity-check matrix H, the weight per row and column is not uniform, but instead governed by an appropriately chosen distribution of weights. In this paper, regular binary LDPC codes are used to implement the proposed watermarking system.

1. LDPC Codes Construction

We use the method to construct a LDPC code in this paper called as random design, which is depicted in[11]. A parity check matrix is divided into three submatrices, each containing a single 1 in each column. The first of these submatrices contains 1's in descending order; i.e., the ith row contains 1's in the columns (i-1)k+1 to ik, where k is the row weight. The other submatrices are merely column permutations of the first submatrix. The permutations of the 2nd submatrix and the 3rd submatrix are independently selected.

We can show the minimum distance of this code[14]. As block length n increases, the probability distribution function of minimum distance is upper bounded by a unit step function at $\theta\in(0,1)$. Thus, for large n, the minimum distance of LDPC codes in the ensemble has at least $n\theta$.

Let $\alpha : m/n, \alpha\in(0,1)$. For $\theta\in(0,1)$ the average distance distributions

$$b_\theta := \lim_{n\to\infty}\frac{1}{n}\ln A_d := H(\theta)+p_\theta^\alpha \tag{8}$$

$H(\theta)$ is the natural entropy

$$H(\theta)=\lim_{n\to\infty}\frac{1}{n}\ln\binom{n}{\theta n}=-\theta\ln\theta-(1-\theta)\ln(1-\theta) \tag{9}$$

For random codes, we can give the following description, Let for $\theta\in(0,1)$

$$p_\theta^\alpha=\alpha\ln\left(\frac{(1+t)^k+(1-t)^k}{2t^{\theta k}}\right)-\alpha k H(\theta) \tag{10}$$

Where t is the only positive root of

$$\frac{(1+t)^{k-1}+(1-t)^{k-1}}{(1+t)^k+(1-t)^k}=1-\theta \tag{11}$$

Then, for k even

$$b_\theta=H(\theta)+p_\theta^\alpha \tag{12}$$

and for k odd

$$b(\theta)=\begin{cases} H(\theta)+p_\theta^{\alpha}, & if\theta\in(0,\dfrac{k-1}{k}) \\ -\infty, & otherwise. \end{cases} \quad (13)$$

For example[15], we show average normalized distance distribution for (3, 6) LDPC codes in Fig. 7

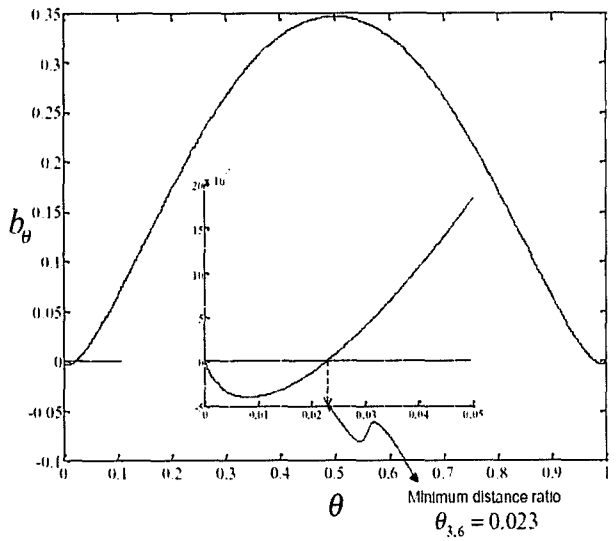

Fig. 7. Average normalized distance distribution for (j, k)=(3, 6)-regular LDPC codes

In this case, the minimum distance ratio is $\theta_{3,6}=0.023$ which is first zero crossing and the minimum distance increases linearly with the codeword length n. When block length n is 1008, we can calculate the distance distribution of this code.

$$d_{\min}=\theta_{j,k}\cdot n \quad (14)$$

$$d_{\min}=0.023\times 1008=24 \text{ and } A_{24}=1 \quad (15)$$

According to the set of $(\theta_{jk}, b(\theta))$ in Fig. 7, we can get the next distance spectrum (d, Ad) as $(26, 4)$, $(28, 14)$, $(30, 45)$, $(32, 156)$, $(34, 559)$. We can show this distance spectrum in Fig. 8.

Using upper bound for the word error probability of linear block codes,

$$P_e \le \sum_{d=d_{\min}} \frac{1}{2}A_d e^{-dR\frac{E_b}{N_0}} = \frac{1}{2}\left[A(X)-1\right]_{X=e^{R\frac{E_b}{N_0}}} \quad (16)$$

we can estimate the upper bound of this code in (17).

$$P_e \le \sum_{d=d_{\min}} \frac{1}{2}A_d e^{-dR\frac{E_b}{N_0}} \quad (17)$$

$$=\frac{1}{2}e^{-24R\frac{E_b}{N_0}}+\frac{4}{2}e^{-26R\frac{E_b}{N_0}}+\frac{14}{2}e^{-28R\frac{E_b}{N_0}}+\frac{45}{2}e^{-30R\frac{E_b}{N_0}}+\frac{156}{2}e^{-32R\frac{E_b}{N_0}}+\frac{559}{2}e^{-34R\frac{E_b}{N_0}}$$

The word error probability upper bound is shown in Fig. 9.

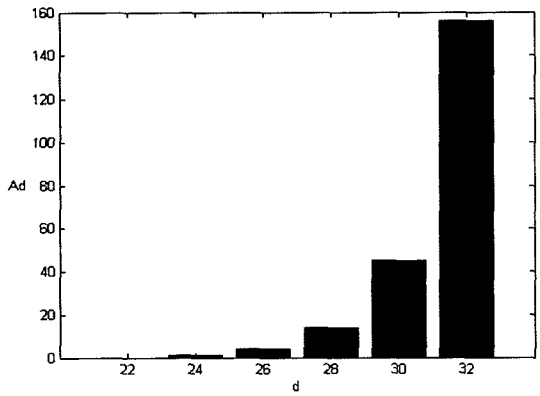

Fig. 8. Weight distribution of (3, 6)-regular LDPC codes up to 32 when block length is 1008

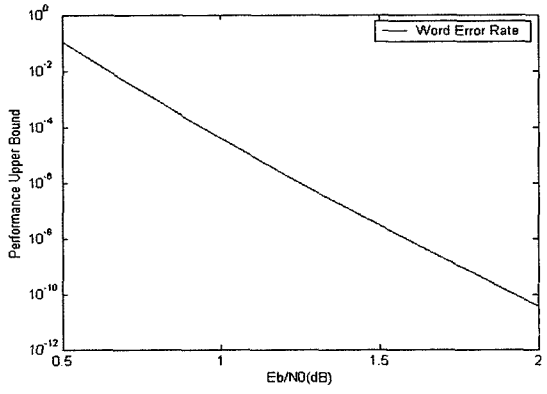

Fig. 9. Performance upper bounds for the (3, 6)- LDPC codes when block length is 1008

2. LDPC Encoder

Given a binary data vector, u, having length k, we can select a transmitted vector length n, giving a k/n code. This means we are introducing m=n-k parity check bits. The transmitted vector, t, is created by multiplying the source vector by a transformed generator matrix G^T, such that $t = G^T u \bmod 2$. The generator matrix is derived from the parity-check matrix, A, which can be randomly constructed. Gaussian elimination and reording of the columns of A are used to produce an equivalent parity-check matrix, H, of the form $H = [P \mid I_m]$, where P is a $m \times k$ matrix containing the actual parity checks and I_m is the $m \times m$ identity matrix. From this form of the parity-check matrix, we can create the generator matrix as[12],

$$G^T = \begin{bmatrix} I_k \\ P \end{bmatrix} \tag{18}$$

Where I_k is the $k \times k$ identity matrix.

3. LDPC Decoder

Considerable work in investigating LDPC iterative decoding algorithms such as Gallager's bit flipping (BF) decoding, weighted MLG decoding and sum product algorithm have been reported in[13]. The optimum-decoding algorithm usually used is belief propagation (BP) algorithm that has been received significant attention recently, commonly known as sum product algorithm (SPA). So in this section, SPA is described in detail.

We describe the notations for the SPA as follows. $M(l)$ denotes the set of check nodes that are connected to bit node l, i.e., positions of "1"s in the lth column of the parity-check matrix; and $L(m)$ denotes the set of bits that participate in the mth parity-check equation, i.e., positions of "1"s in the mth row of the parity-check matrix. $L(m) \setminus l$ represents the set $L(m)$ with the lth bit excluded. $q^0_{l \to m}$ and $q^1_{l \to m}$ denote the probability information that bit node l sends to check node m, indicating and respectively; and denote the probability information that mth check node gathers for the lth bit being 0 and 1, respectively. Generally speaking, $r^0_{l \to m}$ or $r^1_{l \to m}$ is the likelihood information for $x_l = 0$ or $x_l = 1$ from the mth parity-check equation, when the probabilities for other bits are designated by the $q^0_{l \to m}$'s. Therefore, $r^1_{m \to l}$ can be considered as the extrinsic information for the lth bit node from the mth check node. The a posteriori probability for a bit is calculated by gathering all the extrinsic information from the check nodes that connect to it, which can be obtained by the following iterative belief propagation procedure.

3.1 Initialization

Each bit node l is assigned an a priori probability p_l. In the case of equiprobable inputs, $p(x_l \mid H)$ is the same for $x_l = 0$ and $x_l = 1$. Therefore, on a memoryless additive white noise channel,

$$p_l^0 = P(y_l \mid x_l = 0),\ p_l^1 = P(y_l \mid x_l = 1); \tag{19}$$

For every position (m, l) such that, $H_{ml} = 1$, $q_{l \to m}$ are initialized as:

$$q^0_{l \to m} = p^0_l,\ q^1_{l \to m} = p^1_l; \tag{20}$$

3.2 Check nodes to bit nodes

Each check node m gathers all the incoming information $q_{l \to m}$'s, and updates the belief on the bit l based on all other bits that are connected to check node m.

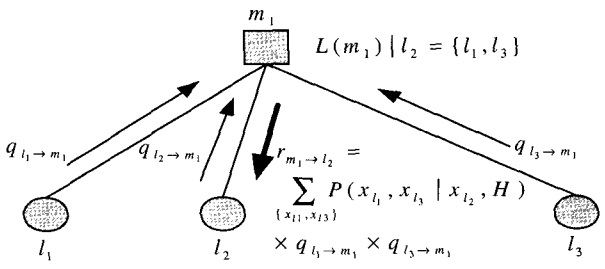

Fig. 10. Belief propagation from check nodes to bit nodes

According to the above Fig. 10, we can get the following formulas:

$$r^0_{m\to l} = \sum_{x_{l'}:l'\in L(m)\backslash l} P(\{x_{l'}\}\,|\,x_l=0,H)\times \prod_{L(m)\backslash l} q^{x_{l'}}_{l'\to m}, \quad (21)$$

$$r^1_{m\to l} = \sum_{x_{l'}:l'\in L(m)\backslash l} P(\{x_{l'}\}\,|\,x_l=1,H)\times \prod_{L(m)\backslash l} q^{x_{l'}}_{l'\to m} \; ; \quad (22)$$

The exclusion of the $q_{l\to m}$ from the product for the $r_{m\to l}$ is necessary for $r_{m\to l}$ to contain only the extrinsic information. $p(\{x_l\}\mid x_l=0,H)$ and are actually indicator functions, i.e,

$$P(\{x_{l'}\}\,|\,x_l=0,H)=\begin{cases}1 & if \sum\oplus\{x_{l'},0\}=0;\\ 0 & otherwise,\end{cases} \quad (23)$$

$$P(\{x_{l'}\}\,|\,x_l=1,H)=\begin{cases}1 & if \sum\oplus\{x_{l'},0\}=0;\\ 0 & otherwise\ ,\end{cases} \quad (24)$$

Where $\sum\oplus$ denotes modulo-2 sum. Therefore $r^0_{m\to l}$ and $r^1_{m\to l}$

$$r^0_{m\to l} = \sum_{\substack{x_{l'}:l'\in L(m)\backslash l\\ \in\sum\oplus\{x_{l'}\}=0}} \prod_{L(m)\backslash l} q^{x_{l'}}_{l'\to m}, \quad (25)$$

$$r^1_{m\to l} = \sum_{\substack{x_{l'}:l'\in L(m)\backslash l\\ \in\sum\oplus\{x_{l'}\}=1}} \prod_{L(m)\backslash l} q^{x_{l'}}_{l'\to m}. \quad (26)$$

3.3 Bit nodes to check nodes

Each bit node l gathers the probability information from the check nodes that connect to it, and updates its APP.

According to the above Fig. 11, we can get the following formulas:

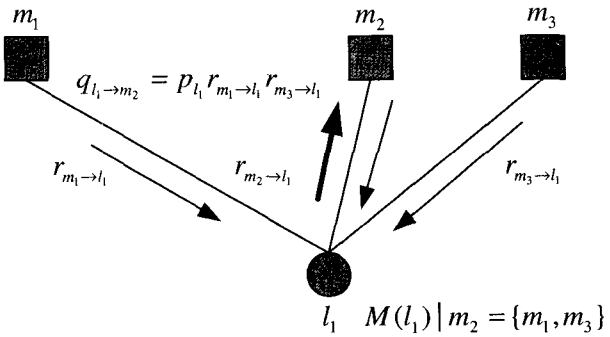

Fig.11. Belief propagation from bit nodes to check nodes

$$q^0_l = \eta_l p^0_l \prod_{m\in M(l)} r^0_{m\to l}, \quad (27)$$

$$q^1_l = \eta_l p^1_l \prod_{m\in M(l)} r^1_{m\to l}, \quad (28)$$

Where the normalization factor η_l is chosen such that $q^0_l+q^1_l$. Two terms contribute to the APP: the initial information p_l, and the "extrinsic" information, $r_{m\to l}$, coming from the connected check nodes. The belief that bit node l propagates back to check node m should not include the information coming from check node m; therefore, $q_{l\to m}$'s are updated as

$$q^0_{l\to m} = \eta_{ml} p^0_l \prod_{m\in M(l)\backslash m} r^0_{m'\to l}, \quad (29)$$

$$q^1_{l\to m} = \eta_{ml} p^1_l \prod_{m\in M(l)\backslash m} r^1_{m'\to l}. \quad (30)$$

Where the normalization factor η_{ml} is chosen such that $q^0_{l\to m}+q^1_{l\to m}=1$.

3.4 Stop criterion

Hard decision is made on each bit's APP q_l, and the resulting decoded input vector $\hat{x}$: otherwise, it repeats 2-3.

Ⅳ. Experiment Results

In this section, we present some results for the proposed watermarking system. The 59177 signature image and 256256 cover image shown in Fig. 12 are chosen for simulation. In this paper, we use LDPC codes as error-correcting scheme to protect the signature message and we lay emphasis on the analysis of the recovered watermark image quality improvement using LDPC codes, LDPC codes with different code rate and block size are applied The signature image is first spreaded and modulated by pseudo noise sequences, the output sequence is then coded by LDPC codes to generate watermark sequence. Fig. 13 shows the watermarked image and the difference between the original image and the watermarked image is illustrated in Fig. 14.

To retrieve watermark with good quality, the

Fig. 12. Host image and signature image

Fig. 13. Watermarked image

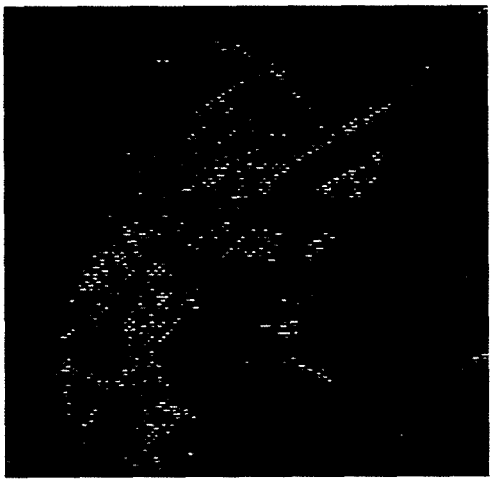

Fig. 14. The difference between the original image and the watermarked image

embedding strength and chip-rate are both the most important factors that should be considered. Embedding strength reflects a trade-off between watermark imperceptibility and watermark robustness. Chip-rate, which is decided by the lengths of signature message and the watermark sequence, can clearly affect watermark robustness and watermark capacity. In this paper, we analyze the probability of error as a function of the embedding strength and the chip-rate. Fig. 15 indicates the relationship between bit error rate and chip-rate under the condition of different embedding strength. From this figure, we can see that an increase in embedding strength results in lower error rates and higher capacity of the watermarking channel.

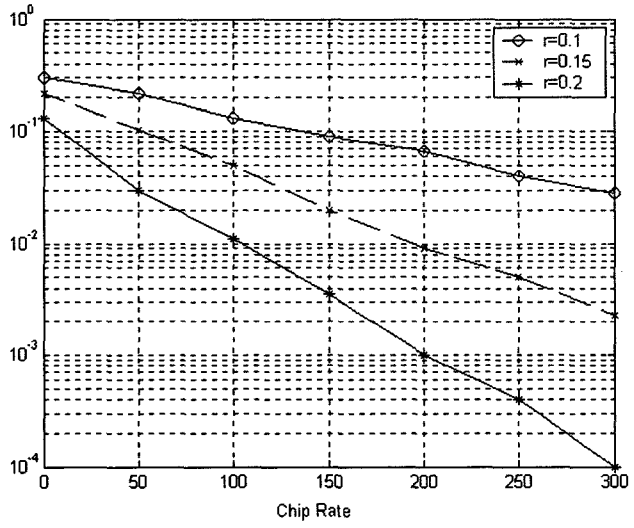

Fig. 15. BER versus Chip Rate with different embedding strength

Signature message is the most important information that should be protected. However, when the covered image embedded spread watermark sequence is transmitted over the noisy channel, it is easily to be attacked by noise and this often results in the quality decrease of recovered watermark information. To correct the errors in the embedded watermark sequence caused by noise, we apply LDPC codes to protect the important signature information. In this paper, we analyze the BER and PSNR performances of the watermarked images. Four cases are studied here: LDPC codes with code rate of 1/2, 1/3 and block size of 512bit and 1024bit are applied in the simulation. From Fig. 16 and Fig. 17, it can be proved that LDPC codes with lower code rate and bigger block size can tolerate higher noise levels.

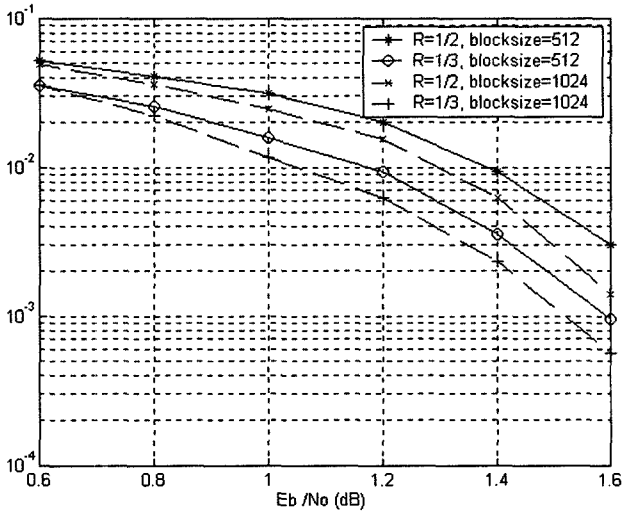

Fig. 16. BER performance of watermarked images

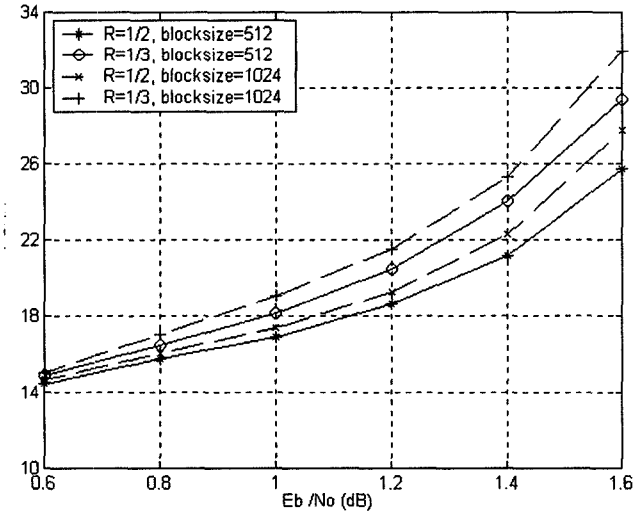

Fig. 17. PSNR performance of watermarked images

By implementing the proposed watermarking system, we can retrieve signature message with good quality at a very lower signal to noise ratio. Figure 16 denotes the

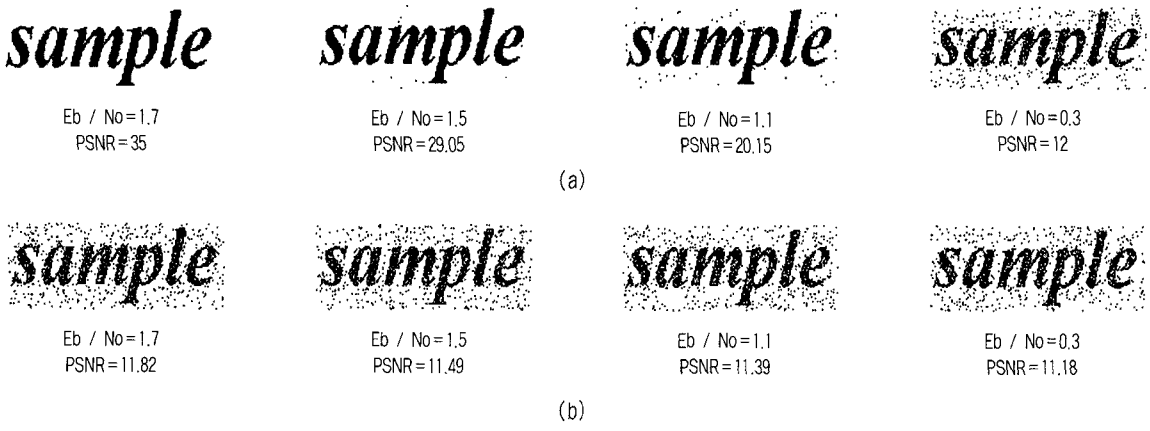

Fig. 18. Reconstructed signature images: (a) protected by LDPC codes with code rate of 1/3 and block size of 1024 (b) without error protection

reconstructed signature images. In this figure, (a) shows the recovered signature images protected by LDPC codes with code rate of 1/3 and block size of 1024, (b) demonstrates reconstructed images without error correcting. It is obvious that the recovered images protected by LDPC codes have much better quality even at a very low signal to noise ratio such as 1.7 and 1.5. The quality of retrieved signature images without error correction is totally unacceptable. Fig. 18 shows that signature information can be extracted successfully when signal to noise ratio is very low by using LDPC codes.

V. Conclusion

In this paper, we propose the application of LDPC codes on implementing a fairly robust digital image watermarking system. As indicated in this paper, the performance of LDPC codes is the best in the family of error correcting codes. So LDPC codes can play an important role of correcting the errors of the embedded message caused by the disturbance of channel noise in the proposed system. At the same time, the spread spectrum technology and DWT are used to implement this system. Many simulation results and figures are presented in this paper, these results indicate the quality of the watermark is improved greatly and the proposed system based on the LDPC codes is very robust to attacks.

References

[1] R.B.Wolfgang and E. J. Delp, Overview of image security techniques with applications in multimedia systems, Proceedings of the SPIE International Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways, November 4-5, 1997, Dallas, Texas, vol. 3228, pp. 297-308.

[2] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, Multimedia data-embedding and watermarking technologies, Proceedings of the IEEE, 86, pp. 1064-1087, June 1998.

[3] J. R. Smith and B. O. Comiskey, Modulation and information hiding in images, in Proc. Of First Int. Workshop on Information Hiding, Lecture Notes in Computer Science, vol. 1174, pp. 207-226, 1996.

[4] I. J. Cox, J.Kilian, F. T. Leighton, and T. Shammon, Secure Spread Spectrum Watermarking for multimedia, IEEE Transactions on Image Processing, 6:1673-1686, December 1997.

[5] Mercy George, Jean-Yves Chouinard, and Nicolas Georganas, Digital Watermarking of Images and Video using Direct Sequence Spread Spectrum Techniques, ICEIC, 1999.

[6] Piva A., M. Barni, F. Bartolini, V.Cappellini and A. De Rosa, Improving the Robustness of Non-additive Watermarks Through Optimum Detection Theory, Proceedings of SPIE, Vol. 3971, 2000.

[7] R.G.Gallager, Low Density Parity Check Codes, MIT Press, Cambridge, Mass., 1963.

[8] D.J.C.Mackay, Good error-correcting codes based on very sparse matrices, IEEE Transaction on Information Theory, vol. 45, pp. 399-431, Mar. 1999.
[9] T. Zhang, Z. Wang, and K. K. Parhi, On finite precision implementation of low-density parity-check codes decoder, in Proceeding of 2001 IEEE International Symposium. On Circuits and Systems, Sydney, May 2001. Available at http:// www. Ece.umn.edu/groups/ddp/turbo/.
[10] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Improved low-density parity-check codes using irregular graphs and belief propagation, in Proceedings of IEEE International Symposium on Information Theory, page 117, 1998.
[11] R.G.Gallager, Low-density parity-check codes, IRE Transaction on Information Theory, vol. IT-8, pp. 21-28, Jan. 1992.
[12] C. Howland and A. Blanksby, Parallel decoding architectures for low density parity check codes, in Proc. Of 2001 IEEE International Symposium On Circuits and Systems, Sydney, May 2001.
[13] Kou, Y, Lin, S, Fossorier, M.P.C, Low-density parity-check codes based on finite geometries: a rediscovery and new results, IEEE Transaction on Information Theory, Volume: 47 Issue: 7, Nov. 2001 Page(s): 2711-2736.
[14] S. Litsyn and V. Shevelev, On Ensembles of Low Density Parity Check Codes: Asymptotic Distance Distributions, IEEE Trans. on Information Theory, vol. 48, no. 4, pp. 887-908, Apr. 2002.
[15] Eunok Lee, Jaebum Kim, Performance of LDPC code based D-blast system,VTC 2003-Spring. The 57th IEEE Semiannual, Volume: 3, April 22-25, 2003.

저 자 소 개

유 이(Yu Yi)

- 2002년 2월 : 중남 민족 대학교 컴퓨터공학과 학사
- 2002년 3월~현재 : 전북대학교 정보통신공학과 석사
- 주관심분야 : LDPC, 채널코딩

이 문 호

- 1967월 2월 : 전북대학교 전기공학과 학사
- 1984년 2월 : 전남대학교 전기공학과 박사
- 1990년 6월 : 동경대학교 전자과 공학박사
- 1980년~현재 : 전북대학교 전자정보공학부 교수 (연구소장)
- 주관심분야 : 디지털 이동통신, 채널코딩 및 암호이론, 영상신호처리

김 지 현

- 2002년 8월 : 전북대학교 전자정보공학부 학사
- 2002년 8월~현재 : 전북대학교 정보통신공학과 석사
- 주관심분야 : 리눅스 보안, 채널코딩 및 암호이론, 영상신호처리

황 기 연

- 1998년 2월 : 서남대학교 전자공학과 학사
- 2001년 2월 : 서남대학교 컴퓨터정보통신학과 석사
- 2003년 2월 : 전북대학교 정보통신공학과 박사 수료
- 2003년 3월~현재 : 전주공업대학 겸임교수
- 주관심분야 : MIMO-OFDM, 이동통신, LDPC