AN EFFICIENT IMAGE WATERMARKING SYSTEM BASED ON ERROR CORRECTING CODES IN DCT DOMAIN

Pranab Kumar Dhar[(1)], Mohammad Ibrahim Khan[(1)] and Sujan Chowdhury[(1)]

1. Department of Computer Science and Engineering, Chittagong University of Engineering and Technology.

E-mail: pranab_cse@yahoo.com, muhammad_ikhancuet@yahoo.com, sujan_cse_04@yahoo.com

ABSTRACT

Digital watermarking has drawn extensive attention for copyright protection of multimedia data. This paper proposes a new watermarking system for digital images using efficient systematic linear block codes (SLBC) in discrete cosine transform (DCT) domain. The proposed watermarking system using SLBC generates a code sequence of {0, 1} that provides error correction capabilities and then replaces it with a binary watermark sequence of {-1, 1}. This achieves more robust invisible image watermarks and requires a small storage unit for binary sequence numbers. The generated watermark sequence is then used as an input for our proposed watermarking system which consists of watermark embedding process and watermark detection process. Experimental results indicate that the invisible watermark embedded with the proposed system are very robust against various kinds of attacks such as white Gaussian noise, JPEG compression, median, and mean filtering, by showing similarity values ranging from 0.7 to 0.8.

KEY WORDS: *Digital Watermarking, Linear Block Code, Copyright Protection.*

1.0 INTRODUCTION

In recent years, rapid development of information technology and computer networks, the privacy of copyrighted digital data has become an important issue in the digital industry. Multimedia data such as audio, video or image can be easily distributed over the Internet. However, many publishers may be reluctant to show their work on the Internet because multimedia data can be easily duplicated without the owner's consent. In order to overcome this copyright-protection issue, digital watermarking techniques have received considerable attentions. A digital watermark is an invisible signature embedded inside an image to show the authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should also be robust against many image manipulations, such as filtering, noise attack, and compression.

A significant number of watermarking techniques have been reported in recent years. Some methods embed the watermark in the spatial domain of an image [1-2]. Other watermarking techniques use transform methods, such as the fast Fourier transform (FFT) [3], discrete cosine transform (DCT) [4-6], to embed the watermark. Recent implementations have also used the human visual system (HVS) to improve the watermark performance [7-8].

In this paper, we propose efficient systematic linear block codes (SLBC) for the invisible image watermarking in the DCT domain. SLBC has been widely used in digital communication since it performs well for error correction when information is transmitted over a noisy channel [10]. However, SLBC generates a code sequence of {0, 1} which is not effective for embedding in DCT components since the watermark 0's cannot change the DCT components in (5) on Section 3.1. Thus, we replace the code sequence of {0, 1} with a binary watermark sequence of {-1, 1} which not only provides robustness to generate new watermarked DCT coefficients but also requires minimal storage for binary sequence numbers. The generated watermark sequence is then used as an input for our proposed watermarking system which consists of watermark embedding process and watermark detection process. Simulation results indicate that our proposed system shows strong robustness against several image processing attacks such as white Gaussian noise, JPEG compression, median, and mean filtering. It achieves similarity values ranging from 0.7 to 0.8.

The rest of the paper is organized as follows. Section 2 discusses the background information regarding linear block code, generator matrix, and error correction using SLBC. Section 3 introduces our proposed watermarking system including watermark embedding process and watermark detection process. Section 4 presents our experimental results, and finally section 5 concludes this paper.

2.0 BACKGROUND INFORMATION

2.1 SYSTEMATIC LINEAR BLOCK CODE

Systematic linear block code is a parity check code that can be characterized by the (n, k) notation where a block of k message bits is encoded into a longer block of n codeword bits. The encoding procedure assigns to each of the 2k message to one of the 2n code word [10].

2.2 GENERATOR MATRIX

Since a set of code word which forms a linear block code is k dimensional subspace of n dimensional binary vector space (k<n), it is always possible to find a set of n-tuples, fewer than 2k, that can generate all the 2k code words of the subspace. In general a generator matrix for systematic linear block codes of (n×k) dimension is defined as:

$$\mathbf{G} = \begin{pmatrix} \mathbf{P} & \mathbf{I_k} \end{pmatrix} = \begin{pmatrix} p_{11}\ p_{12} \cdots \cdots p_{1,(n-k)} & 1\ 0 \ldots \ldots 0 \\ p_{21}\ p_{22} \cdots \cdots p_{1,(n-k)} & 0\ 1 \ldots \ldots 0 \\ \cdots \quad \cdots \qquad \cdots & \cdots\cdots \\ p_{k1}\ p_{k2} \cdots \cdots p_{k,(n-k)} & 0\ 0 \ldots\ldots 1 \end{pmatrix} \quad (1)$$

where P is the parity check matrix and Ik is the (k×k) identify matrix. Let [m1, m2, m3,……,mk] be the message word and [u1, u2, u3,……,un] be the code word. Then, the relationship between the message and code words is given by

$$\begin{pmatrix} u_1, u_2, \ldots\ldots u_n \end{pmatrix} = \begin{pmatrix} m_1, m_2, \ldots\ldots m_k \end{pmatrix} \cdot \begin{pmatrix} p_{11}\ p_{12} \cdots \cdots p_{1,(n-k)} & 1\ 0 \ldots \ldots 0 \\ p_{21}\ p_{22} \cdots \cdots p_{1,(n-k)} & 0\ 1 \ldots \ldots 0 \\ \cdots \quad \cdots \qquad \cdots & \cdots\cdots \\ p_{k1}\ p_{k2} \cdots \cdots p_{k,(n-k)} & 0\ 0 \ldots\ldots 1 \end{pmatrix}$$

where

$$u_i = m_1 p_{1i} + m_2 p_{2i} + \ldots\ldots + m_k p_{ki} \quad \text{for } i=1, \ldots\ldots,(n-k)$$
$$= m_{i-n+k} \quad \text{for } i=(n-k+1), \ldots\ldots, n \qquad (2)$$

2.3 ERROR CORRECTION USING SLBC

Let **e** be the error vector and **r** be the received vector resulting from the transmission of **U**. Therefore, **r** can be defined as **r**=**U**+**e**. The syndrome of **r** is defined as **S**= r$\mathbf{H}^T$, where **H** is the parity check matrix such that $\mathbf{UH}^T$ =0. We then have

$$\mathbf{S} = (\mathbf{U}+\mathbf{e})\ \mathbf{H}^T$$
$$= \mathbf{UH}^T + \mathbf{eH}^T \qquad (\mathbf{UH}^T=0) \qquad (3)$$
$$= \mathbf{eH}^T$$

If the syndrome vector is zero, we suppose that no errors are detected. In other words, if it is not zero then errors will be detected in the decoder. To detect the error pattern from the syndrome vector, a reserved syndrome table is used. The error is then corrected by utilizing the error pattern with the received vector.

3.0 PROPOSED WATERMARKING SYSTEM

3.1 WATERMARK EMBEDDING PROCESS

The proposed watermark embedding process is shown in Figure 1. In this process, the input message is encoded by a systematic linear block encoder and the generator matrix of linear block code is used as a watermark key. The output of the watermark encoder is a bipolar sequence of {0, 1}. This bipolar sequence of {0,1} is then mapped to the watermark sequence of {-1, 1} for the effective watermark embedding in the DCT domain. Thus, the watermark sequence X(n) is a sequence of n binary numbers of ±1. The embedding process is implemented in the following three steps:

Step 1: The original image is transformed to the DCT domain to calculate DCT components F(u,v) of original image I(m,n), by the following equation:

$$F(u,v) = \frac{C(u)C(v)}{\sqrt{2N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\frac{(2x+1)u\pi}{2N} \cos\frac{(2y+1)v\pi}{2N} \qquad (4)$$

where C(u) = $1/\sqrt{2}$ for u = 0 and C(u) = 1 for u > 0.

Step 2: Embed the watermark in the n higher magnitude coefficients in the transform matrix excluding the DC component. This ensures that the watermark is located at the most significant perceptual components of the image. If the watermark is embedded in less significant components, it may be considerably destroyed by compression or other forms of attacks. When the watermark X(n) is embedded into DCT components F(u,v) to obtain new watermarked DCT coefficients F*(u,v), we specify a scaling parameter α which determines the extent to which X(n) alters F(u,v), shown in the following equation [4]:

$$F^{*}(u,v) = F(u,v)[1 + \alpha X(n)] \quad (5)$$

Step 3: Insert back n modified DCT components $F^{*}(u,v)$ and take an inverse DCT transform to get the watermarked image $I^{*}(u,v)$.

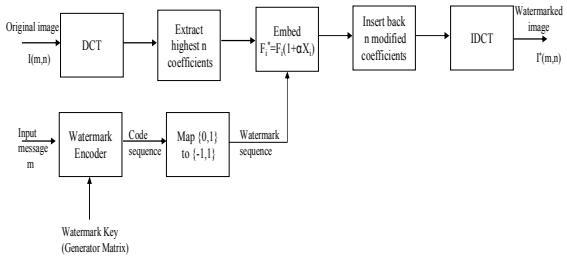


Fig 1: Watermark embedding process

3.2 WATERMARK DETECTION PROCESS

The proposed watermark detection process is shown in Figure 2. The detection process is implemented in the following four steps:

Step 1: Calculate the DCT components of the attacked watermark image $I^{*}(u,v)$ and extract n coefficients of the transform matrix which are located at the same position in the embedding process above.

Step 2: The watermark is then extracted by performing the inverse function of (6), shown in the following equation:

$$Xi^{*} = (F_i^{*} / F_i - 1)/\alpha \quad (6)$$

Step 3: Replace the extracted watermark sequence of {-1, 1} with the code sequence of {0, 1} and then apply to the watermark decoder as an input.

Step 4: Correct the sequence {0, 1} using SLBC which provides error correction capabilities and extract the watermark X*(n) from the corrected sequence.

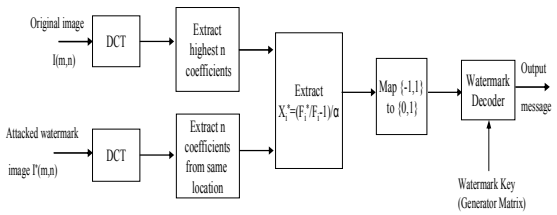


Figure 2: Watermark detection process

4.0 SIMULATION RESULTS

In order to evaluate the performance of the proposed watermarking scheme in terms of the robustness of watermark detection, the correlation coefficient between the original watermark X(n) and the extracted watermark $X^{*}(n)$ is calculated by the following similarity function:

$$SIM(X, X^{*}) = \frac{\sum_n X(n).X^{*}(n)}{\sqrt{\sum_n [X(n).X(n)]}\sqrt{\sum_n [X^{*}(n).X^{*}(n)]}} \quad (7)$$

It is highly unlikely that $X^{*}(n)$ is identical to X(n). To decide whether X(n) and $X^{*}(n)$ match, we determine whether the $SIM(X, X^{+}) > T$, where T is a detection threshold.

In this study, the selected length of the watermark sequence and message signal is 512 and 64, respectively. The structure of the SLBC encoding process used in this simulation is given below:

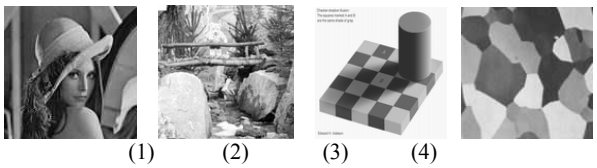
[1×16 bit code sequence] = [1×2 bit message] × [2×16 bit generator matrix]

This encoding process can generate 16 bit code sequence at a time by using two-bit message signal and 2×16 bit generator matrix. By executing this encoding process 32 times, it can generate 32×16= 512 bit code sequence by using two-bit message sequence and 2×16 bit generator matrix.

The generator matrix used in this simulation is

$$\mathbf{G} = \begin{pmatrix} 1\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0 \\ 1\,0\,1\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1 \end{pmatrix} \quad (8)$$

Figure 3 shows four different original images used in this study. Figure 4 shows a qualitative evaluation of the original 128x128 "Lena" image with a watermarked output image in which the watermark is invisible in the watermarked image.



(1) (2) (3) (4)

Fig.3: Four different original images used in the study

Fig.4: Original Lena image, watermarked Lena image and difference image

Fig. 6 and 7 shows the original message signal and detected message signal when no attack is applied to watermarked Lena image.

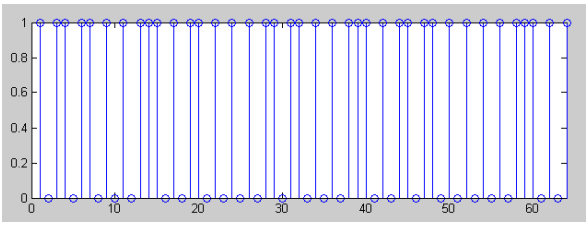


Fig.6: Original message signal

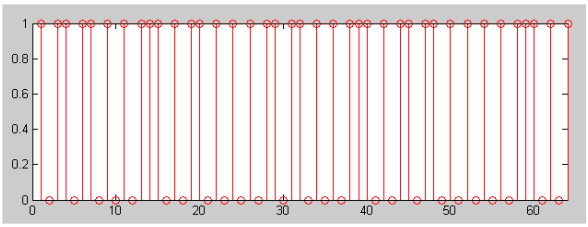


Fig.7: Detected message signal

Fig. 8 shows the original watermark sequence and detected watermark sequence represented by a 32×16 image when no attack is applied to watermarked Lena image.

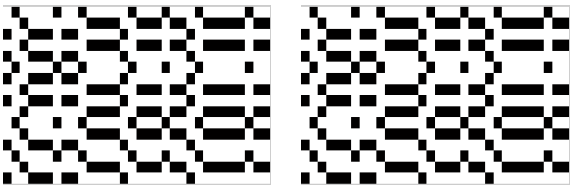


Fig.8: Original watermark sequence and detected watermark sequence

Table 1 shows the results of the watermark detection when no attack is applied to four different types of watermarked images as shown in Fig. 7. Thus, our proposed system can perfectly detect the watermark sequence when no attack is applied to each watermarked image.

No Attack	SIM
Image 1	1
Image 2	1
Image 3	1
Image 4	1

Table 1: Watermark detection without attack

In addition to the qualitative evaluation, a quantitative evaluation must be done because the similarity between the original watermark X(n) and the extracted watermark $X^*(n)$ is the best subjective measure for determining the robustness of the proposed watermarking scheme. In order to evaluate the performance of our proposed scheme, it is tested against several kinds of image processing attacks such as white Gaussian noise, JPEG compression, mean, and median filtering.

4.1 NOISE ATTACK

For the noise attack, white Gaussian noises with zero mean and different variances (100, 300, 600, and 900) were added into the watermarked Lena image as shown in Figure 9. Table 2 illustrates the similarity results of the proposed scheme against the white Gaussian noise attack. Our proposed system achieves similarity values ranging from 0.77 to 0.80.

Fig 9: Results of adding different Gaussian noises to the watermarked Lena image

$N(\mu, \sigma^2)$	SIM			
	Image 1	Image 2	Image 3	Image 4
N(0,100)	0.8077	0.8051	0.8093	0.8084
N(0,300)	0.8052	0.8019	0.8071	0.8068
N(0,600)	0.7927	0.7969	0.7968	0.7868
N(0,900)	0.7868	0.7747	0.7936	0.7742

Table 2: Similarity results of the proposed system against the white Gaussian noise attack

4.2 JPEG COMPRESSION ATTACK

Figure 10 shows results of applying JPEG compression to different watermarked images.

Table 3 shows similarity results of the proposed system against the JPEG compression attack. Our proposed system achieves similarity values ranging from 0.80 to 0.81.

Fig 10: Results of applying the JPEG compression attack to different watermarked images

JPEG Compression	SIM
Image 1	0.8019
Image 2	0.8060
Image 3	0.8077
Image 4	0.8101

Table 3. Similarity results of the proposed system against the JPEG compression attack

4.3 MEDIAN FILTERING ATTACK

For the median filtering attack, watermarked images were filtered by a 3×3 median filter as shown in Figure 11. Table 4 shows the similarity results of the proposed system against the median filtering attack. Our proposed scheme achieves similarity values ranging from 0.79 to 0.80.

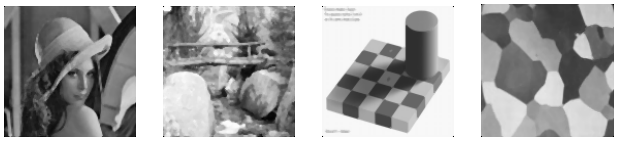


Fig 10: Results of applying the median filtering attack to different watermarked images

Median Filtering	SIM
Image 1	0.7967
Image 2	0.8009
Image 3	0. 8077
Image 4	0. 8043

Table 4: Similarity results of the proposed system against median filtering attack

4.4 MEAN FILTERING ATTACK

For the mean filtering attack, watermarked images were filtered by a 3×3 mean filter as shown in Figure 9. Table 5 shows similarity results of the proposed system against the mean filtering attack. Our proposed scheme achieves similarity values ranging from 0.7 to 0.8.

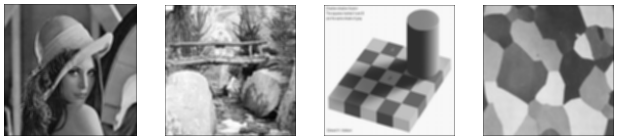


Fig 11. Results of applying the mean filtering attack to different watermarked images

Mean Filtering	SIM
Image 1	0.8109
Image 2	0.7635
Image 3	0. 7927
Image 4	0. 8026

Table 5: Similarity results of the proposed system against mean filtering attack

Overall, the proposed watermarking system shows strong robustness against several kinds of image processing attacks including white Gaussian noise, JPEG compression, median, and mean filtering.

5.0 CONCLUSION

In this paper, a new image watermarking system using efficient systematic linear block codes (SLBC) in DCT domain has been proposed for image copyright protection. Experimental results show that the watermark embedded with the proposed system is invisible. In addition, our proposed system is highly robust against several kinds of image processing attacks including white Gaussian noise, JPEG compression, median, and mean filtering. It achieves similarity values ranging from 0.7 to 0.8. These results demonstrate that our proposed watermarking system can be a suitable candidate for image copyright protection.

REFERENCES

[1] R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," in Proceedings of IEEE International Conference on Image Processing, Vol. 2, pp. 86-90, Nov. 1994.

[2] I. Pitas, "A Method for Signature Casting on Digital Images," in Proceedings of IEEE International Conference on Image Processing, Vol. 3, pp. 215-218, Sept. 1996.

[3] J. O'Ruanaidh, W. Dowling, and F. Boland, "Phase Watermarking of Digital Images," in Proceedings of IEEE International Conference on Image Processing, Vol. 3, pp. 239-242, Sep. 1996.

[4] I. Cox, J. Killian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia Data," IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

[5] S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE Journal on Selected Areas in Communications, vol. 16, No. 4, pp. 573-586, May 1998.

[6] C. C. Wai, "DCT-Based Image Watermarking Using Subsampling," IEEE Transaction on Multimedia, Vol. 5, No. 1, pp. 34-38, 2003.

[7] S. H. Yang, "Filter Evaluation for DWT-domain Image Watermarking," Electronics Letters, Vol. 39, No. 11, pp. 840-841, November 2003.

[8] J. Huang and Y.Q. Shi, "Adaptive Image Watermarking Scheme Based on Visual Masking," Electronics Letters, Vol. 34, No. 8, pp. 748-750, 1998.

[9] J. Delaigle, C. D. Vleeschouwer and B. Macq, "Psychovisual Approach to Digital Picture Watermarking" Journal of Electronic Imaging, Vol. 7, No. 3, pp. 628-640, 1998.

[10] B. Sklar, Digital Communications Fundamentals and Applications, Second Edition, Pearson Education, 2002.