BCH Coding Watermarking Based on Discrete Wavelet Transform

Jinyu Lu [1, a *]and Tao Qu [2, b]

[1]College of Engineering Bohai University Liaoning, Jinzhou, China

[2]School of Electronics & Information Engineering University of Technology Liaoning Liaoning, Jinzhou, China

[a]156241142@qq.com, [b]54333928@qq.com

Keywords: Watermark image; DWT; BCH error control coding; Robustness

Abstract. The traditional watermark is replaced with a novel coding watermarking scheme, which is focusing on BCH error control coding for increasing the security of the digital products. The pretreatment of watermark image is to be done first of all; iris image is transferred into the binary sequence. And then the binary sequence is to be on discrete cosine transform, the value of the discrete cosine is encoded to BCH error control coding. The BCH codes are embedded into the coefficients of discrete wavelet-transformed host image. Many results show that proposed method can extract the watermark effectively and illustrate its security and robustness.

Introduction

With the internet, computer and smartphone age coming, more and more communication and interaction between people are digital information and digital products. Above all, widely applying the smartphone, the digital information and digital products spread more widely and easily. In order to protect the rights of the authors, the security problem of digital products becomes more and more important. Although a lot of organizations offer their digital products in the internet, they also have the ownership rights proved by their manner. But digital watermarking is still the more important means to accomplish the same. According to visibility, watermark is divided into the visible and invisible watermark. The visible watermark due to visibility, people with the naked eye can identify and determine the style and position of watermark, in order to distinguish the copyright. But also because of the visibility, the attackers can more easily obtain the watermark information and maliciously modify and distort the watermark. Compared with the defect of visible watermark, the invisible watermark has the apparent advantage. Thus, the invisible watermark is widely used.

Researchers usually have embedded the invisible watermark into the spatial domain or transform domain. Robustness and perceptibility is a pair of contradiction to the watermarking whether the spatial domain or transform domain. There is a general consensus among researchers:Using the watermarking technology in the spatial domain, the watermarking technology have a lower robustness function, otherwise, the watermark can easily be found; Using the watermarking technology in the transform domain, the watermarking technology have a higher robustness function, the watermark is embedded into the host image, which is to be found difficultly. The researchers follow the transform domain with interests.

Widles, R.P, et al. have proposed an emerging automated iris biometric recognition[1-3]. Daugman has proposed the working mechanism of iris recognition[4,5]. Boles and Boashash have proposed the application of iris recognition in the wavelet transform[6]. Now some research institutions are in the research of iris recognition, for example Carnegie Mellon University, Lion’s Eye Institute (LEI), Universities of Bath and Chinese Academy of Sciences-Institute of Automation (CASIA).

Firstly the iris image is pretreated. The results of pretreatment is that person’s eye images are transferred into binary BCH (255,207) code. The whole process is divided into three steps: The first step, person’s eye images are changed into iris biometric templates. The second step: the templates are performed on the discrete cosine transform. The third step, the value of discrete cosine transform is transferred to BCH-based coding. Then binary watermark is embedded in the host image. Embedding intensity and location depends on the key. The experiments show that the scheme is robust against popular attacks.

Watermark Pretreatment

The database of many eye images is used from university of Bath. Except iris, there still are pupil, sclera, and eyelid and so on in any eye image. It is necessary that these adverse factors are removed in order to normalizing prior to coding. We apply a minimum bounded isothetic rectangle (MBIR) format to eye image for eliminating these factors. Thus, we obtain rectangular iris templates which are normalized to a size of 120×200 pixels by MBIR format[9, 10]. The normalized 120×200 iris image are applied with row–wise, 1D DCT and retaining of DC value of each row, to obtain a 1×200 set of pixels[11].

The DCT of a row of the iris matrix is defined as

$$Z_i^n(\alpha,\beta)=u(\alpha)\sum_{\beta=1}^{N}v(n,\beta)\cos\frac{(2\beta-1)(\alpha-1)}{2N},\ \alpha=1,2,\cdots N \tag{1}$$

Where $v(n,\beta)$ is βth template of the signal in the nth row of the ith iris biometric image, N is the column size.

$$u(\alpha)=\begin{cases}\sqrt{\dfrac{1}{N}} & \alpha=1\\ \sqrt{\dfrac{2}{N}} & 2\le\alpha\le N\end{cases} \tag{2}$$

Then, this 1×200 DC values are encoded to binary string, which is 8×200 bits format with BCH-based error control code Fig. 1.

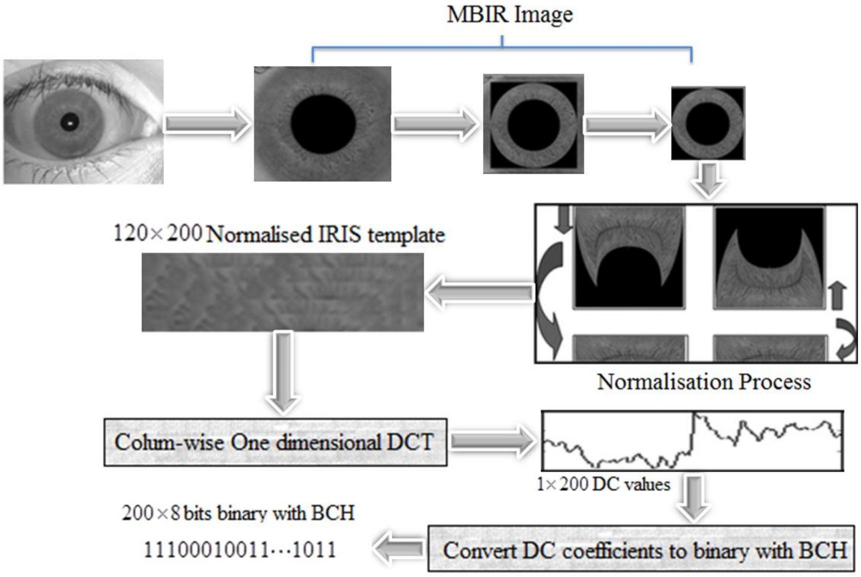
MBIR Image
120× 200 Normalised IRIS template
Normalisation Process
Colum-wise One dimensional DCT
1× 200 DC values
200 × 8 bits binary with BCH
11100010011···1011
Convert DC coefficients to binary with BCH

Figure 1. Iris biometric normalization and coding

In this paper, the watermark image is transferred into a binary sting; the value of binary is 0 or1. In the process of communication, the error transmission is inevitable. In order to improve the robustness of watermarking, error control coding with BCH is applied. In this paper, we use BCH (255,207) code.

For any positive integers $m(m \ge 3)$ and $t(t < 2^m - 1)$, there exists a binary BCH error-control code with the following parameters: Block length: $n = 2^m - 1$, number of parity-check digits: $n - k \le mt$, minimum distance: $d \ge 2t + 1$.

Obviously, the code is capable of correcting any combination of fewer errors in a block of $n = 2^m - 1$ digits. We call this code a t-error-correcting BCH code. The generator polynomial of this code is specified in terms of its roots form the Glois field GF (2^m). For example, $n = 2^6 - 1 = 63$, as shown in table Table 1.

Table 1 Generator Polynomials of the BCH Codes of Length 63

n	k	t	$g(X)$
63	57	1	$g_1(X) = 1 + X + X^6$
	51	2	$g_2(X) = g_1(X)(1 + X + X^2 + X^4 + X^6)$
	45	3	$g_3(X) = g_2(X)(1 + X + X^2 + X^5 + X^6)$
	39	4	$g_4(X) = (1 + X^3 + X^6)\ g_3(X)$
	36	5	$g_5(X) = (1 + X^2 + X^3)\ g_4(X)$
	30	6	$g_6(X) = g_5(X)(1 + X^2 + X^3 + X^5 + X^6)$
	24	7	$g_7(X) = g_6(X)(1 + X + X^3 + X^4 + X^6)$
	18	10	$g_{10}(X) = g_7(X)(1 + X^2 + X^4 + X^5 + X^6)$
	16	11	$g_{11}(X) = (1 + X + X^2)\ g_{10}(X)$
	10	13	$g_{13}(X) = g_{11}(X)(1 + X + X^4 + X^5 + X^6)$
	7	15	$g_{15}(X) = (1 + X + X^3)\ g_{13}(X)$

Algorithm of Embedding and Extraction Watermark

Embedding Algorithm. The watermark is embedded into four subbands which is results of host image by wavelet transform. Embedding intensity and location relies on key. The embedding process is shown in Fig. 2.

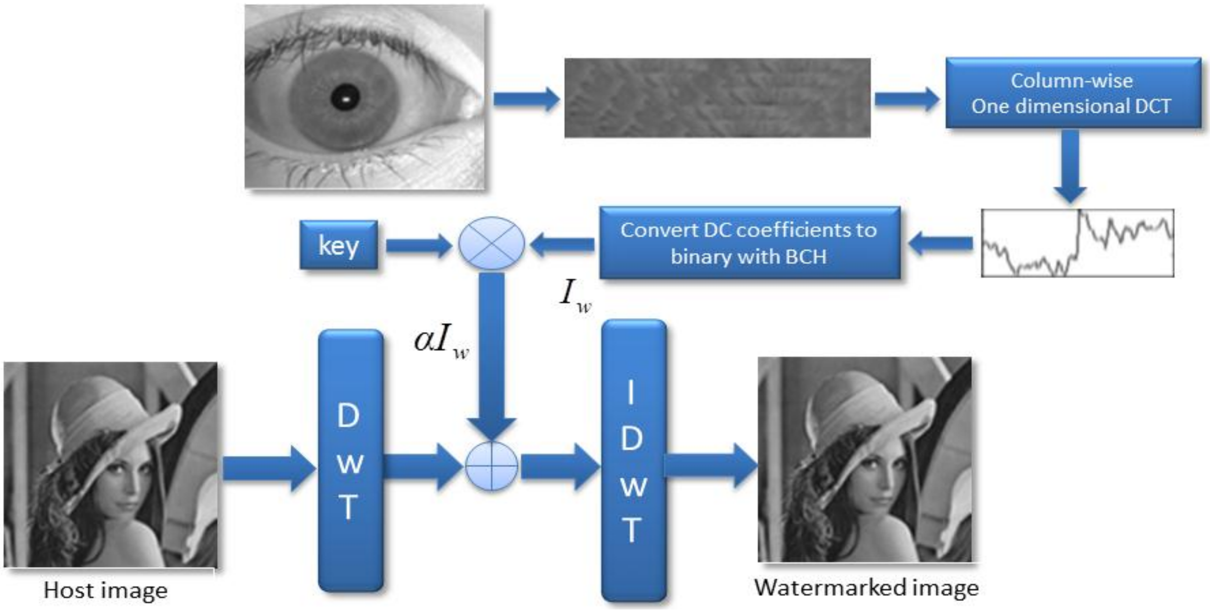

Figure 2. Embedding watermark

Watermark Extraction. Firstly, the watermarked image is decomposed by the wavelet transform. Next, according to the key, the binary string is extracted from each sub-band of the wavelet transform. Then, four sub-bands are extracted to four binary strings; each binary string is implemented by error-correcting and operated on modulo 2, in order to determine which sub-band will be as the detected watermark. Finally, comparing the detected watermark with the Bath database, the ownership of digital products is determined. Watermarked image extraction process is shown in Fig. 3.

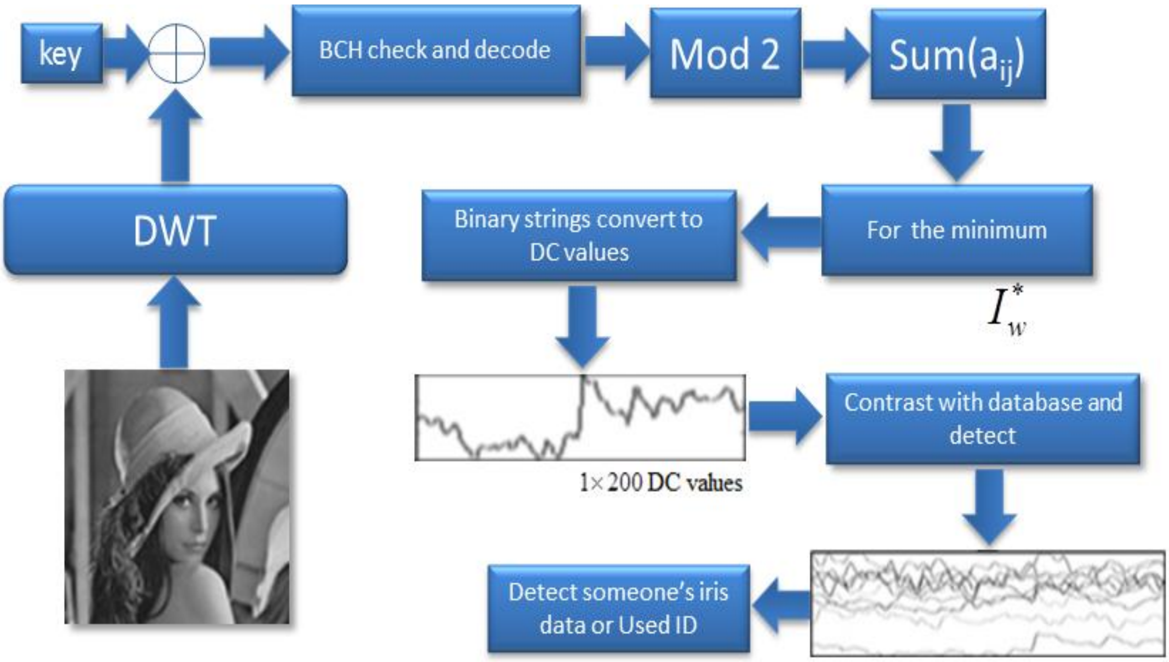
key
BCH check and decode
Mod 2
Sum(a_ij)
DWT
Binary strings convert to DC values
For the minimum
I_w^*
1×200 DC values
Contrast with database and detect
Detect someone's iris data or Used ID

Figure 3. Watermark extraction

Experimental Results

In this paper, the iris digital watermarking algorithm based on DWT, but the iris image is transferred into BCH code after the binary sequence as the watermark is embedded into the wavelet transform coefficient of the host image. Embedding strength and position depend on the key. A total of 200 person and 70 times is 28000 samples. 13 times, false accepted watermark is zero in the 700 times experiments. The result is shown in Table 2.

Table 2 The result of Aspect Ratio

Aspect ratio	Correct detection	False rejection	False acceptance
95%	687	13	0
90%	691	9	0
85%	692	8	0

Respond to crop attacks, correct detected watermark is more than 691 times, false rejected watermark is less than 7 times, false accepted watermark is less than one time, in the 700 times experiments. The result is shown in Table 3.

Table 3 The result of Crop

JPEG	Correct detection	False rejection	False acceptance
95%	681	18	1
90%	689	11	0
85%	692	8	0

Respond to filtering attacks, correct detected watermark is more than 694 times, false rejected watermark is less than 6 times, false accepted watermark is less than one time, in the 700 times experiments. The result is shown in Table 4.

Table 4 The result of Filtering

Filterin	Correct detection	False rejection	False acceptance
95%	694	6	0
90%	695	4	1
85%	698	2	0

Many experimental results show that, the paper proposed scheme has stronger robustness against common attack.

Conclusions

Using BCH coding watermarking based on discrete wavelet transform is processed before embedded into wavelet transform of the original gray image. The experimental results show that the proposed scheme is robust against popular attacks. Because the algorithm is easier, the watermark can be blind detected.

References

[1] Chi Xiao-fang, Feng Gui; Dong Xiao-hui: Journal of Huaqiao University(Natural Science),Vol.36(2015)No.5,p.534

[2] S. Yin, X. Li, H. Gao, O. Kaynak, Data-based techniques focused on modern industry: An overview,IEEE Transactions on Industrial Electronics,62(1):657-667, 2015.

[3] Yu Min, Chen Jun; Application Research of Computers, vol.33(2016)No.9

[4] S. Yin, Z. Huang, Performance monitoring for vehicle suspension system via fuzzy positivistic C-means clustering based on accelerometer measurements, IEEE/ASME Transactions on Mechatronics, 20(5):2613-2620, 2015.

[5] Chen G, Ma H J, Chen N. A blind watermarking algorithm based on singular value decomposition and quantization[C] Proc. of the 10th World Congress on Intelligent Control and Automation. 2012: 4887-4890

[6] S. Yin, X. Zhu, O. Kaynak, Improved PLS focused on key performance indictor related fault diagnosis, IEEE Transactions on Industrial Electronics, 62(3):1651-1658, 2015.

[7] S. Yin, X. Zhu,?Intelligent particle filter and its application on fault detection of nonlinear system, IEEE Transactions on Industrial Electronics, 62(6):3852-3861, 2015

[8] Su Q, Niu Y, Wang G, et al. Color image blind watermarking scheme based on QR decomposition [J]. Signal Processing, 2014, 94(1): 219–235.

[9] S. Yin, O. Kaynak, Big data for modern industry: challenges and trends, Proceedings of the IEEE, 102(3):143-146, 2015.

[10] Tsougenis E D, Papakostas G A, Koulouriotis D E, et al. Performance evaluation of moment based watermarking methods: a review [J]. Journal of Systems and Software, 2012, 85(8): 1864-1884.

[11] Singh C, Ranade S K. Rotation invariant moments and transforms for geometrically invariant image watermarking [J]. Journal of Electronic Imaging, 2013, 22(1): 13-34.