Extension of Structural Watermarks Based on Balanced Incomplete Block Designs

Zhi-Fang Yang, Po-Chen Lee, Wei-Hung Chen, and Jia-Guu Leu

Department of Computer Science and Information Engineering National Taipei University New Taipei City, 237 Taiwan, R.O.C. zfyang@mail.ntpu.edu.tw

Received June 2010; revised May 2011

ABSTRACT. Large number of watermarks is crucial for some real watermarking applications, such as transaction tracking. The purpose of this paper is to enlarge the set of structured watermarks based on balanced incomplete block designs (BIBD). An approach is proposed to generate new structured watermarks by combining existing BIBD-based watermarks. The corresponding recognition rules for the new set of watermarks are designed based on the structure information contained. Experimental results show the properties of the proposed watermarks based on true positive and false positive rates under Gaussian noise.

Keywords: watermark; balanced incomplete block designs (BIBD)

1. Introduction. Digital multimedia is spread over the internet in the current era. Illegal reproduction and modification of digital content thus have become a serious problem. Study of techniques of copyright protection and content authentication has been a hot topic, [2, 3, 10, 12, 13, 18, 19] and digital watermarking is one of the potential techniques [5].

Digital watermarking aims to embed watermarks into digital contents, and expects the information contained in the watermarks to help verify ownership or to improve quality of the transmitted digital content [5]. Thus, robustness of digital watermarks is an important issue. For digital images, robust watermarking is expected to resist volumetric distortion and geometric distortion to a certain degree [5]. Volumetric distortion changes values of pixels without moving them, for instance, additive noise, linear filtering, lossy compression, quantization and so on [5]. Geometric distortion, however, makes pixels leave their original positions, including translation, rotation, scaling, aspect ratio, and so forth [5]. No matter which kind of distortion happens, the working area could be global, local, or random [5].

A variety of researches on robust watermarking has been developed [5, 6, 7, 8, 16]. These techniques can be used at the watermark embedder [5, 6, 7, 16], the watermark extractor [5], or the watermark designer [8]. For examples, hiding watermarks repeatedly [5], using the technique of spread spectrum [6], and embedding at perceptually significant coefficients[7] or at areas of known robustness [16] are methods used at the watermark embedder. For the watermark extractor, several methods can be found, such as exhaustive searching parameters [5], distortion inversion [5], and matching image features. At the watermark designer, invariant watermarks and synchronization patterns [8] are two choices.

In our previous work [29], one kind of structural watermarks is designed to achieve robust watermarking. The basic idea is to discuss whether mathematical structures are good for robust watermarking. The structure depicts relations among members in a data set [20], specifically more than one kinds of relations. We believe that such structures construct multiple relations among data members of the watermark, and thus facilitate robustness of the watermarking system.

The relation between watermarking robustness and structures in watermarks has not At the watermark embedder, watermarking mechanisms been thoroughly discussed. mainly include selecting robust embedding areas [7, 16] or embedding methods such as repetitive embedding and spread spectrum [5, 6]. All these techniques have nothing to do with structures in watermarks. At the watermark designer, methods using random patterns, orthogonal patterns, or message codes all aims to make watermark candidates apart from each other as far as possible; such thoughts focus on relations among watermarks instead of the structure inside one watermark [5]. Other methods of watermark designs include invariant watermarks based on geometric invariant features or moments, periodic watermarks with autocorrelation properties, informative watermarks extracted by some synchronization patterns [5, 15]. All these watermarks are designed without considering relations among data members inside a watermark except the periodic watermark. However, nothing more than the periodic property is adopted to construct the periodic watermark. As for the watermark extractor, the mechanisms adopted depend on the methods used at the watermark designer or at the watermark embedder. That is, structures in watermarks are considered at the watermark extractor only if structural information are used at the embedder or at the designer.

The proposed structural watermark in [29] is designed based on a mathematical structure: the balanced and incomplete block designs (BIBD) [4, 9, 11, 22]. The structural properties of BIBD relate different subsets of the members in a BIBD set, and such properties are used to recognize the watermark. The structural properties of BIBD, namely, balance and incompleteness, are considered beneficial to robustness of digital watermarking in our thoughts, and the experimental results have shown the feasibility of the proposed watermark.

However, the number of BIBD-based watermarks is limited because that each BIBD set can only generate one proposed BIBD-based watermark in [29], and thus the number of BIBD sets is quite limited [20]. Not enough number of available watermarks would be a fatal drawback for some watermarking application, such as transaction tracking in which large number of watermarks may be required to represent all the transactions respectively.

Only few previous works on BIBD can be found in the field of information science [1, 14, 17, 21, 23, 24, 25, 26, 27, 28, 30]; some of them focus on coding and experimental designs [1, 17, 21, 30]. The works related to data hiding focus on fingerprinting [14, 23, 24, 25, 26, 27], and among these BIBD-related researches on fingerprinting [14, 24, 25, 26], structures of BIBD sets are not the core of the whole work.

In this study, concatenation of the previous proposed BIBD-based watermarks is considered to generate more BIBD-based watermarks. The goal is to obtain a large number of BIBD-based watermarks which still keep the structural information of BIBD. In the proposed method, arbitrary number of BIBD incidence matrices can be concatenated, and the corresponding recognition rules are derived.

The rest of the paper is organized as follows. Section 2 shows the proposed approach, including introduction of BIBD, system overview, and watermark design and recognition. The experimental results and discussions are presented in section 3, and the final conclusions are given in section 4.

Γ	1	1	1	1	1	1	0	0	0	0	0	0	0	0]	
	1	1	0	0	0	0	1	1	1	1	0	0	0	0	
	1	0	1	0	0	0	1	0	0	0	1	1	1	0	
	0	1	0	1	0	0	0	1	0	0	1	1	0	1	
l	0	0	1	0	1	0	0	1	1	0	0	0	1	1	
	0	0	0	1	0	1	0	0	1	1	1	0	1	0	
L	0	0	0	0	1	1	1	0	0	1	0	1	0	1	

FIGURE 1. Incidence matrix of (7, 3, 6, 14, 2)-BIBD.

2. Proposed Approach.

2.1. **BIBD.** The theory of the BIBD belongs to the field of combinatorial mathematics and has applications in codes, computer science, cryptography, etc. [4, 9, 11, 22]. The definition of the BIBD is as follows [9].

Definition 2.1. (definition of BIBD) A BIBD, a (v, b, r, k, λ) -configuration, is a pair (V, B) where V is a v-set and B is a collection of b k-subsets of V (blocks). Every 2-subset of V appears in exactly λ blocks, and each element of V appears in exactly r blocks.

A BIBD set is a structured set, which can be described as a pair (V, β) . The V set consists of v elements, and β is a set of k-subsets of v. The k-subsets are called blocks, and the total number of the blocks is b. The structural information of the BIBD also includes that each element of V is contained exactly in r blocks, and that any of the 2-subsets of V is contained in exactly λ blocks. Therefore, the parameters used to define a BIBD set are v, k, r, b and λ [9]. A BIBD set can be explicitly described by using the corresponding incidence matrix. The incidence matrix is a v by b matrix with each row representing one element in v, and each column one block. A value of one in the incidence matrix denotes the corresponding element in the set V appears in the corresponding block, and a value of zero appears, otherwise. Figure 1 shows one example, which is the incidence matrix of a (7, 3, 6, 14, 2)-BIBD.

The structure of the BIBD can be considered as a set of relations imposed on the v elements in the set V. The structure aims to group the v elements into b blocks, the collection B. The blocks may overlap; however, such overlap is balanced based on the three parameters associated with a BIBD, namely, r, k, and λ . First, all the blocks are of the same size, that is, every block consists of k elements of V. Second, each element of V appears r times in the blocks. Third, every two elements of V can be found λ times in the blocks. Not all k-subsets of V are selected as the blocks, and the selection of blocks into the collection B is subject to the three parameters. That is, the grouping of elements of V into blocks is incomplete since only collection of some k-subsets would fulfil the requirements. Thus, The BIBD can be viewed as an incomplete collection of k-subsets of a set of v elements subject to three criteria concerned with balance.

Balance and incompleteness are two features of how the structure information is spread over a BIBD, and these two features are advantageous to robustness. The property of balance intends to distribute the structure information fairly and equally, so that the same structure can be found all over the data set. Such balanced structures are good properties which can be used to verify correctness of a watermark in which structure information of the BIBD is utilized, and that is the reason why the structure information of the BIBD is considered in this work to be advantageous to a robust watermarking system. For example, the parameter k means to make all the blocks the same size of k, so all undistorted blocks should consists of k elements from the set B. The principle of balance is applied via the parameters k and λ as well: the parameter r requires each element in the set V to appear exactly r times in the whole block set B, thus each undistorted elements in the set V should be found r times in the set B. Furthermore, if two elements from the set V are found to appear together in the set B not exact f times, the structure of the involved blocks is distorted.

As for incompleteness, the set B is a chosen subset of the set of all k-subsets of the set V, and then the missing k-subsets can be considered as "holes" in the space of the whole k-subsets space. Thus one such hole found represents distortion happens. Thus, both balance and incompleteness are advantageous to robustness.

2.2. System Overview. Figure 2 shows the proposed watermarking system. First, a key is prepared for each transaction or user. The key is used to select two or more BIBD incidence matrices from the BIBD database. Through the watermark designer, the desired watermark is generated by concatenating these incidence matrices. The generated watermark then is arranged into a binary sequence by row-major order and mapped from the binary value set $\{1, 0\}$ into the value set $\{1, -1\}$ [29].

At the embedder, the wavelet transform is performed on the digital content, and the wavelet coefficients of the digital content are used to embed the watermark. The embedding method is basically follows our previous work [29] as shown in the following equation.

$$C'_{ij} = C_{ij} + \alpha S_k,\tag{1}$$

where C'_{ij} is the modified wavelet coefficient, C_{ij} the original wavelet coefficient, S_k the corresponding kth element of the watermark sequence, and α the watermark strength. Only wavelet coefficients in the median frequencies are selected to improve robustness. More than one copy of the watermark may be embedded in order to utilize all the selected wavelet coefficients. Then the inverse wavelet transform is applied to get the watermarked digital content. Finally, the watermarked digital content is transmitted via the channel.

After the transmission stage, the transmitted watermarked digital content arrives at the receiver site. The extractor is then used to extract the embedded watermark. Notice that the original digital content is available at the extractor and that this is not a blind extraction case here. At the extractor, both the transmitted watermarked digital content and the original digital content are transformed into the wavelet domain. Then the transmitted watermark can be obtained by subtracting the transformed original digital content from the transmitted one. If multiple copies of the watermark are embedded, the value of every bit in the final extracted watermark is obtained by selecting the value with the majority among all individual extracted watermarks [29].

At the watermark recognizer, the transmitted key is used to select the BIBD incidence matrices from the BIBD database to get the corresponding watermark generated at the sender site. Recognition rules are then applied to recognize whether the extracted watermark is the correct watermark, and the matching result is reported as the final answer. The focus of this paper is the watermark designer and the watermark recognizer. The concepts of the key and BIBD database will be discussed briefly in the section of watermark design and recognition, and the methods of embedding and extraction follows the methods proposed in our previous work [8].

2.3. Watermark Design and Recognition. After informed which BIBD sets are selected according to a specific key, the watermark designer generates a binary sequence as the desired watermark based on the corresponding incidence matrices. The basic ideas are to concatenate all the involved incidence matrices, and then to scan each concatenated



FIGURE 2. Proposed watermarking system.

matrices in row major. Suppose that the number of the input BIBD incidence matrices is n, and that the size of the incidence matrix \mathbf{M}_i of the *i*th BIBD set is $v_i \times b_i$, then the watermark length is $\sum_{i=1}^n v_i \times b_i$, and the element at the *p*th row and the *q*th column of the *r*th selected incidence matrix \mathbf{M}_r is located at the $(\sum_{i=1}^{r-1} v_i \times b_i + (p-1) \times b_r + q)$ th bit of the watermark.

Theoretically, a total of 2^N watermarks can be generated, where N is the number of available BIBD sets. Then the watermark design procedure would begin at gathering the BIBD sets with proper sizes according to the application, prepare the set of keys representing different combinations of the gathered BIBD sets for transactions or users, and proceed with key selection, watermark generation, and embedding parts for each transaction or user. Notice that the keys are available at the receiver site; that is, which BIBD sets are involved and the related order information are known when the watermark recognizer works.

At the receiver site, the recognition rules applied in the watermark recognizer is as follows:

$$S = 100(1 - R)$$

$$= 100 \left[1 - \sum_{i=1}^{n} w_i \left(\frac{w_{iv}}{v_i} \sum_{j=1}^{v_i} R_j^{v_i} + \frac{w_{ib}}{b_i} \sum_{k=1}^{b_i} R_k^{b_i} + \frac{w_{i\lambda}}{C_2^{v_i}} \sum_{l=1}^{C_2^{v_i}} R_l^{\lambda_i} \right) \right]$$
(2)

where S is the score of the watermark gets, R the total error rate of a transmitted watermark, n the number of BIBD sets involved, v_i , b_i , and λ_i the parameters of the *i*th involved BIBD set, w_i the weight of the error rate of the *i*th involved BIBD set with $\sum_{i=1}^{n} w_i = 1$, w_{iv} , w_{ib} , and $w_{i\lambda}$ the weights for the bit error rates of the *i*th BIBD set's structural parameters v, b, and λ with $w_{iv} + w_{ib} + w_{i\lambda} = 1$, $R_j^{v_i}$ the error rate of the *j*th row of the *i*th involved BIBD set, $R_k^{b_i}$ the error rate of the kth column of the *i*th involved BIBD set, and $R_l^{\lambda_i}$ the error rate of the *l*th pair of elements the *i*th involved BIBD set.

As we can see from the above recognition formula, the structural information contained in the proposed watermark is checked by examining each involved BIBD incidence matrix individually. For each BIBD incidence matrix, the structural information is checked through the parameters v, b, and λ , respectively. For each parameter, the bit error rate is evaluated for all corresponding elements. The calculation of the bit error rate follows our previous work [8].

The weight w_i is selected according to the corresponding importance. For example, if the size of the BIBD incidence matrix is the only considered factor, the weight for the *i*th BIBD set would be $\frac{v_i \times b_i}{\sum_{i=1}^n v_i \times b_i}$. Based on the same thoughts, the weights w_{iv} , w_{ib} , and $w_{i\lambda}$ can be imposed.

Overall speaking, the formula looks correlation-based, and the underlying idea is that the structural information is checked by examining the special relations imposed on a set of v elements for the BIBD set.

3. Experimental Results and Discussions. Experiments were conducted to test the true positive and the false positive [6] for both the proposed BIBD watermark and the watermarked real image. The BIBD watermark used was composed of two BIBD sets arbitrarily selected from a total of four BIBD sets with the parameter set (7, 3, 6, 14, 2). The weights w_i for the two selected BIBD sets are both set to 0.5. For each individual BIBD set, the weights, w_{iv} , w_{ib} , and $w_{i\lambda}$, are all equal to $\frac{1}{3}$. Gaussian noise was added; the deviations were set to 0.1, 0.15, 0.2, 0.25, 0.3 and 0.35 for the proposed BIBD watermark, and 0.5, 1, 5, 10, 15, and 20 for the watermarked real image. The embedding strength of the watermark is selected as 4 according to our experimental experiences. A total of 1000 randomly composed BIBD watermark were tested for each data point in Figure 4 and Figure 6, and a total of 200 watermarked real images were testes for each data point in Figure 5 and Figure 7. The image Lena was selected as the real image in the experiments. Some samples of the distorted and watermarked images can be found in Figure 3.

Figure 4 and Figure 6 present the experimental results of true positive. Setting the threshold around eighty, the system can get nearly 100% true positive rate for quite large noise level. It means the proposed recognition rules work successfully for the proposed BIBD-based watermark. Figure 5 and Figure 7 present the experimental results of false positive. We can see the system can get lower false positive rates if the thresholds were set around ninety for middle noise level. Notice that the watermarks used in the experiment of watermarked images are selected from the same BIBD parameter set as the target watermark. That is, the false positive rate is tested under a rather strict condition.

The selection of threshold is suggested depending on the requirements of applications. If recognizing all watermarked works is more important than excluding un-watermarked ones, thresholds are suggested around eighty. Thus, the proposed BIBD watermark can be recognized to be above ninety-five percent under a noise variance of twenty gray levels according to the experimental results. Thresholds smaller than eighty are better for larger noise levels, and thresholds larger than eighty are better for situations not desiring un-watermarked cases or different watermarks. Furthermore, the degree of complex of cover images affects which image processing techniques will be applied, and thus the noise level caused by the corresponding image processing techniques affects the embedded watermark accordingly. For example, high-pass filters are usually used to sharpen details of complex images, and lower thresholds should be adopted to compensate the produced higher level noise.

Experiments of more attacks are conducted as well in this study, some samples can be found in Figure 8, including image stretching, median filtering, histogram equalization, and JPEG compression. According to the experimental results, quite good scores are obtained for distortions such as image stretching, median filtering, and histogram equalization; the reasons could be that the degree of distortions of individual pixels are compensated by the structure checking during the recognition stage. As for JPEG compression, lower scores are obtained since high frequencies are filtered by JPEG compression. Extension of Structural Watermarks Based on Balanced Incomplete Block Designs



(A) Original image.



(B) Watermarked image.



FIGURE 3. Samples of watermarked Lena images distorted by Gaussian noise with different deviations 0.5, 1.0, 5, 10, 15, and 20, respectively.

Comparisons of robustness between BIBD watermarks and random patterns is the main discussion in our previous work[29]. The experimental results in [29] show that BIBD watermarks are more robust than random patterns under Gaussian noise with various deviations. How to impose a structure on a random pattern is the motivation of our original thoughts of designing BIBD watermarks, and such a BIBD structure achieves a more



FIGURE 4. True positive of proposed watermark. Horizontal axis indicates threshold of score with value range from 0 to 100, and vertical axis indicates the number of images with scores above threshold. A total of 1000 images are tested.



FIGURE 5. False positive of proposed watermark. Horizontal axis indicates threshold of score with value range from 0 to 100, and vertical axis indicates the number of images with scores above threshold. A total of 1000 images are tested.

robust watermark pattern fits the intuition as well. In this study, the proposed watermark is composed of more than one individual BIBD sets, thus the quality of robustness is inherited through individual BIBD components as well.

Finally, it is suggested to adopt a suitable watermark embedding method for the proposed watermark to facilitate blind extraction in the future. For example, periodic watermarking with autocorrelation properties and informative watermarking embedded with synchronization information may be two possible choices[5]. While the structure among watermark components is the focus of the above two watermark embedding candidates,



FIGURE 6. True positive of real image (Lena). Horizontal axis indicates threshold of score with value range from 0 to 100, and vertical axis indicates the number of images with scores above threshold. A total of 200 images are tested.



FIGURE 7. False positive of real image (Lena). Horizontal axis indicates threshold of score with value range from 0 to 100, and vertical axis indicates the number of images with scores above threshold. A total of 200 images are tested.

the structure inside a watermark component is emphasized in this study. Thus, blind extraction would be a rather interesting extension of this study since the structures will be considered for both inside the watermark component and among the watermark components.



(A) Original image.



(B) Watermarked image.



(C) Image stretching; score = 100.



(D) Median filter; score = 100.



(E) Histogram equalization; score = 100.



(F) JPEG quality = 98; score = 100.



(G) JPEG quality = 95; score = 93.6.



(H) JPEG quality = 85; score = 85.2.

FIGURE 8. Different attacks imposed on watermarked images.

4. **Conclusions.** A new approach to enlarging the BIBD-based watermark set has been proposed. The corresponding recognition rules have also been designed, and the experiments under Gaussian noise have been conducted as well. According to the experimental results, future works are suggested to improve the false positive rate by designing more complicated combination rules of watermark design and the corresponding recognition rules as well.

REFERENCES

- [1] B. Ammar and B. Honary, Construction of low density parity check codes: BIBD and vandermonde, Proc. of Conference on Mobile Future and the Symposium on Trends in Communications, 2004.
- [2] H. Al-Qaheri, A. Mustafi, and S. Banerjee, Digital watermarking using ant colony optimization in fractional fourier domain, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 3, pp. 179-189, 2010.
- [3] W. Buhse and J. van der Meer, The open mobile alliance digital rights management, *IEEE Signal Processing Magazine*, vol. 24, no. 1, pp. 140-143, 2007.
- [4] C. J. Colbourn and J. H. Dinitz, The CRC Handbook of Combinatorial Designs, Boca Raton, CRC, 1996.
- [5] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*, Boston, Morgan Kaufmann, 2001.
- [6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.
- [7] I. J. Cox, M. L. Miller, and A. L. McKellips, Secure spread spectrum watermarking for multimedia, *Proceedings of IEEE*, vol. 87, no. 7, pp. 1127-1141, 1999.
- [8] D. Delannay and B. Macq, Watermarking relying on cover signal content to hide synchronization marks, *IEEE Trans. Information forensics and security*, vol. 1, no. 1, pp. 87-101, 2006.
- J. H. Dinitz and D. R. Stinson, A Brief Introduction to Design Theory, Contemporary Design Theory: A Collection of Surveys, New York, Wiley, pp. 1-12, 1992.
- [10] E. W. Felten and J. A. Halderman, Digital rights management, spyware, and security, *IEEE Security & Privacy Magazine*, vol. 4, no. 1, pp. 18-23, 2006.
- [11] J. L. Gersting, Mathematical Structures for Computer Science, Computer Science Press, 6th edition, New York, W. H. Freeman, 2006.
- [12] H. C. Huang, Y. H. Chen, and A. Abraham, Optimized Watermarking Using Swarm-Based Bacterial Foraging, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 51-58, 2010.
- [13] D. Kundur and K. Karthik, Video fingerprinting and encryption principles for digital rights management, *Proceedings of IEEE*, vol. 92, no. 6, pp. 918-932, 2004.
- [14] I. K. Kang, C. H. Lee, H. Y. Lee, J. T. Kim, and H. K. Lee, Averaging attack resilient video fingerprinting, Proc. of IEEE International Conference on Circuits and Systems, vol. 6, pp. 5529-5532, 2005.
- [15] V. Licks and R. Jordan, Geometric attacks on image watermarking systems, *IEEE Multimedia*, pp. 68-78, 2005.
- [16] C. Y. Lin et al., Rotation, Scale, and translation resilient watermarking of images, *IEEE Trans. Image Processing*, vol. 10, no. 5, pp. 767-782, 2001.
- [17] Zhichu Lin, Zhixing Yang, and C. Y. Pan, A new design method of multi-rate quasi-cyclic LDPC codes, Proc. of IEEE International Conference on Communications, Circuits and Systems, vol. 2, pp. 707-711, 2006.
- [18] C. H. Lin and C. Y. Yang, Multipurpose watermarking based on blind vector quantization, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 239-246, 2011.
- [19] C. C. Lin and P. F. Shiu, High capacity data hiding scheme for DCT-based images, Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 3, pp. 220-240, 2010.
- [20] D. S. Malik, J. N. Mordeson, and M. K. Sen, Abstract Algebra, Singapore, MacGraw-Hill, 1997.
- [21] M. Rahman. and I. Blake, Majority logic decoding using combinatorial designs, IEEE Trans. Information Theory, vol. 21, pp. 585-587, 1975.
- [22] H. J. Ryser, Combinatorial Mathematics, Buffalo, Mathematical Association of America, New York, 1963.
- [23] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, Anti-collusion fingerprinting for multimedia, *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 1069–1087, 2003.
- [24] Jie Yang, Ping Liu, and GuoZhen Tan, The digital fingerprint coding based on LDPC, Proc. of International Conference on Signal Processing, vol. 3, pp. 2600–2603, 2004.
- [25] Jie Yang, Xiaoxia Xu, A Robust Anti-collusion coding in digital fingerprinting system, Proc. of International Conference on Signal Processing, vol. 4, pp. 16–20, 2006.
- [26] Jie Yang, Xiaoxia Xu, A robust anti-collusion coding in digital fingerprinting system, Proc. of IEEE Conference on Circuits and Systems, pp. 996-999, 2006.
- [27] Z. F. Yang, Anti-collusion Fingerprinting for digital rights protection, Proc. of International Symposium on Wireless Personal Multimedia Communications, 2006.

- [28] Z. F. Yang, Watermarking based on balanced incomplete block designs, *Proc. of International Computer Symposium*, 2006.
- [29] Z. F. Yang and M. S. Wu, Robustness of structure-based watermark by using balanced incomplete block designs, Proc. of International Swaps and Derivatives Association, 2008.
- [30] Fan Zhang, Ying Xu, Xuehong Mao, and Wuyang Zhou, High girth LDPC codes construction based on combinatorial design, Proc. of IEEE International Conference on Vehicular Technology, vol. 1, pp. 591-594, 2005.