Correlation-Based Watermarking Scheme Using Complete Complementary Code

De Li¹, WenJi Quan¹ and JongWeon Kim²

 ¹ Department of Computer Science, Yanbian University 133002, Yanji, China
 ² Department of Copyright Protection, Sangmyung University 110743, Seoul, Korea

leader1223@ybu.edu.cn, moongill2008@163.com, jwkim@smu.ac.kr *Corresponding author: JongWeon Kim (jwkim@smu.ac.kr)

Abstract

Digital watermarking technologies with spread spectrum sequences (SS) have previously proposed. However, the SS sequences used in previous studies do not necessarily have good correlation properties. The previous studies also have proposed the complete complementary codes (CCC), which have an ideal auto-correlation and cross-correlation properties and methods for the construction and extension of the complete complementary codes. However, some methods in the studies do not have good auto-correlation or cross-correlation properties. In this paper, we used the latest complete complementary code constructor to detect the embedded secret information from the watermarked images. In the experimental results, we successfully detected the secret information from the watermark against various attacks.

Keywords: Digital Watermark, Complete Complementary Codes, Correlation Detection, Spread Sequence

1. Introduction

With the development of social network, more and more digital contents such as text, images, audio and video are being distributed through the Internet. It is easy to illegally copy and upload digital contents without any copyright. To solve these kinds of problems, digital watermarking technologies which embed some secret information into digital contents have been developed and can be an effective method for protecting the right of copyright owners.

In the previous studies, spread spectrum sequences and M-sequences were used as a watermark. But with the length of the sequences and the amount of embedded information, the computational cost of correlation function values is increased [1-2]. In addition, the M-sequence is not having good correlation properties. Among various spread spectrum sequences, complementary codes have ideal correlation properties, which can be considered useful for digital watermarking technologies [3-5].

In the early period, Suehiro [6-7] proposed the complete complementary code, which is defined as a set of finite length complex-valued sequences. Some previous studies have proposed several methods of construction and expansion of complete complementary codes [14-21].

In this paper, we compare the relevant features of the previously proposed complementary codes, and choose an optimal complete complementary code as our watermark.

This paper is organized as follows. In Section 2, we describe the fundamental theory of Complete Complementary codes and compare correlation properties between some CCC construction methods. Section 3 gives Correlation-Based digital watermarking, Section 4 give the experimental results. Finally, we present our brief conclusions in Section 5.

2. Complete Complementary Code

The complete complementary code proposed by Suehiro [6] is defined as a set of finite length complex-valued sequences. The general definition of the (m,n,l)-complete complementary code consists of several auto-complementary codes, any two of which are cross-complementary codes. With the sequence length l, the number of sequences in each auto-complementary code n, and the number of different auto-complementary code m, the (m,n,l)-complete complementary code can be written as:

$$\begin{cases} \{C_0^{(0)} , C_1^{(0)} , ..., C_{n-1}^{(0)}\} \\ \{C_0^{(1)} , C_1^{(1)} , ..., C_{n-1}^{(1)}\} \\ & \dots \\ & \dots \\ \{C_0^{(m-1)}, C_1^{(m-1)}, ..., C_{n-1}^{(m-1)}\} \end{cases}$$
(1)

Where *m* rows represent m auto-complementary codes, any two of which are crosscomplementary codes. The sum of the correlation functions satisfy the property as shown in Equation (2), for any *i*, k=0,1,...,n-1,

$$\sum_{j=0}^{n-1} R_{c_j^{(i)} c_j^{(k)}}(u) = \begin{cases} A & if \ i = k \text{ and } u = 0\\ 0 & otherwise \end{cases}$$
(2)

Where $R_{C_j^{(i)}C_j^{(k)}}(u)$ is the correlation function for the finite length sequences $C_j^{(i)}$ and $C_j^{(k)}$, u

denotes arbitrary shifts between $-(L-1) \le u \le L-1$, and A denotes a constant independent of the indices *i* and *k*. Eq.(2) implies that the sum of the auto-correlation functions included in each sequence set is 0 except u=0 and the sum of the cross-correlation function between the sequences included in any two sequence sets is always 0. Therefore, complete complementary code can be defined as a set of m auto-complementary codes, any pair of which is cross-complementary codes.

There are many ways to construct complete complementary codes. JIA Zhi-cheng [20] proposed a complete complementary sequence based on 'generating tree' construction method, which can use a simple method to construct complete complementary code. However, the cross-complementary code of each row is not well. Xing Yang [17] proposed three kinds of new complete complementary code construction methods, but they are too complex and the auto-complementary code of each method is not good enough. Han [18] proposed a Systematic Framework for the construction of complete complementary codes, which has optimal auto-complementary and cross-complementary codes and easy constructed by unitary-like matrix. Figure 1 gives the cross-complementary codes of JIA [18] and Han [20]. In order to compare the cross-complementary codes between JIA [18] and Han [20], we generate the same length of complete complementary codes.



Figure 1. A Denotes the cross- complementary of JIA^[20] and B denotes the cross-complementary of Han^[18]

3. Correlation-Based Watermarking

In this section, we consider the correlation-based digital watermarking technology. We use a pair of IDs to distinguish different groups and different individuals of each group.

GIDs are used to distinguish different groups and UIDs are used to distinguish different persons who belong to each group. In the complete complementary code, a GID is represented by the used sequence and *UID* is represented by the phase shift of sequences. Figure 2 shows the concept of *GID* and *UID* used in this paper.



Figure 2. The concept of GID and UID

3.1. Embedding Method

In the watermark embedding method, we require some secret information such as *GID* and *UID*, secret key. The secret key is used to select frequency domain coefficient. *GID* is used to select a line of *CCC*. *UID* is used to phase shift. The embedding procedure can be explained in the steps as follows:

Step 1. Apply Two layer two-dimensional DWT into the original image.

Step 2. Extract $d_o(i) (0 \le d_o(i) \le n-1)$ with *secret key* in the middle frequency coefficients of two layer two-dimensional DWT.

Step 3. Generate complete complementary code c(i). Use GID to chooses a line.

Step 4. Shift c(i) with the *UID* and sent the shifted sequences to others as a *public key*. The embedding complete complementary code is given below in Equation (3).

$$d'(i) = \alpha c(i) + d_o(i) \tag{3}$$

Where α represents the embedding strength which can improve robustness and c(i) represents the sequences of complete complementary code.

Step 5. Put d'(i) back into the DWT coefficients instead of d(i). Two layer of twodimensional IDWT is performed on it.



Watermarked Image



Figure 3 illustrates the embedding procedure. It is shown that if we choose a different *GID* or *UID* and *key*, it is hard for attackers to know who the owner of the digital content is by simply using the sequences.

3.2. Extracting Method

In the extraction method, we do not need the original image; instead we need some other information such as secret key, public key, watermarked image, *etc.* Figure 4 shows the extraction procedure and it can be explained through the following steps.

Step 1. Transform the watermarked image by two layer two-dimensional DWT.

Step 2. Extract the two layer DWT components by using secret key from the watermarked image, defined as $d_w(i)$.

Step 3. As the UID, extract the shift index $u(0 \le u \le n-1)$ which corresponds to the cross-correlation value $Rd_wp_k(u)$ between *public key* and $d_w(i)$ lager than the given threshold.

watermarked Image2 layer 2D-DWT



Figure 4. The extraction procedure of watermark and UID

4. Experimental Results

In this section we give the experiment results of the embedding and extraction methods and performance of extracting the UID from the watermarked image under some attacks such as adding Gaussian noise, Scale, rotation, Compression etc. In addition, we used four different images to test the extraction performance of UID. Finally, we extracted the UID from the random number covered image.

For the experiment, we used the original image, which is size 512×512 pixels and 24-bit bitmap. We constructed (64,64,128)-complete complementary code using the method that proposed by Han [18-19] and set UID=2000 and GID=1. Figure 5 shows the original image and the watermarked image. Figure 6shows the experimental result of the extraction procedure. The horizontal axis represents the phase shift and the vertical axis represents the correlation function value. Table 1 shows the results of the experiment performed under

Gaussian noise attack and Table 2 shows the experimental results performed under JPEG Compression. Table 3 shows the experimental results under rotation and Table4 shows the result under Scaling. Furthermore, Table 5 shows the extraction results of the UID from the different images. At last, we considered the complete complementary code covered by random sequences.



(A) Original Image



(B) Watermarked Image

Figure 5. Original Image and Watermarked Image

In the experiment, the peak signal to noise ratio (PSNR) was 43 dB. From the pictures above, it would be quite difficult for human eyes to recognize the difference between the original and watermarked image.



Figure 6. Extract the results of the UID

In Figure 6, the correlation value has reached a peak at the 2000, which corresponds to the given UID. This indicates that the complete complementary code is quite effective in the correlation-based digital watermarking.





Table 1 shows the extraction results of UID under Gaussian noise attack when we use the variance 0.005, 0.01, and 0.05 in the experiment. The experimental results present that the UID could be correctly extracted.



Table 2. Extraction of the UID from Compression

Table 2 shows the extraction results of the UID from JPEG Compression, and the results present that the UID could be correctly extracted.



Table 3. Extraction of the UID from Rotation

Table 3 shows the extraction results of the UID from Rotation attack, and the results show that the UID was correctly extracted from the rotated image.



Table 4. Extraction of the UID from Scaling

We performed the experiment by carrying out scaling attack with three rates, 4, 6, and 8, and the experimental results are given in Table 4. The results show that the UID could be correctly extracted.



Table 5. Extraction of the UID from Different Watermarked Image

We conducted the experiment for extracting UID from different images and the experimental results are given in Table 5. We used the pictures of Pepper, Lake, Zelda and Baboon and the results present that the UID could be correctly extracted from these pictures.



Figure 7. Extract UID from random number covered

In the last, w performed the experiment for extracting UID from the random number covered image. Figure 7 shows that the UID could be correctly extracted from the random covered image.

5. Conclusions

In this paper, we have proposed a blind watermark scheme based on optimal complete complementary codes. We compared the cross-correlations of different complete complementary code construction methods, and embedded an optimal complete complementary code as a watermark into the original image. In order to evaluate the performance of the proposed method, we performed the experiments with respect to robustness against several kinds of attacks, such as adding Gaussian noise, Rotation, Scaling and JPEG compression. The experiment results presented that the complete complementary codes have high robustness and can extract UID correctly. In addition, we used a pair of sequences of complete complementary code to distinguish lots of characters, for the watermark technology, which need a high imperceptibility and a small amount of embedding number.

For our further study, we are considering how to reduce the computational complexity and construct a high Auto-complementary, Cross-complementary, and Complete Complementary Codes. It is also interesting to consider some other embedding algorithms. For example, the adaptive algorithm is a good choice.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 61262090)

References

- [1] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon, "Secure spread spectrumwateramarking for multimedia", IEEE Trans. Image Processing, vol. 6, no. 12, (**1997**) December, pp. 1673-1687.
- [2] A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, N. R. A. Mee and C.F.Osborne, "Electronic watermark", in Proc, 2ndConf, on Digital Imaging Computing Techniques and Applications (DICTA '93), Sydney, Australia, (1993), December, pp. 663-673.
- [3] F. A. Peticolas, R. J. Anderson and M. G. Kuhn, "Information hiding a survey", Proc. IEEE, vol. 87, no. 7, (1999) July, pp. 1062-1078.
- [4] A. Hiroyuki, T. Yoshihiro, M. Takahiro and M. Shinya, "A correlation-based digital watermarking method using two-dimensional complementary Pairs (in Japanese)", Tech. Rep. of IEICE, WBS2003, (2003) October, pp. 73-77.
- [5] N. Hayashi, "On the property of spectrum sequence for the CDMA-based fingerprinting scheme (in Japanese)", Proc, of SITA 2007, Shima, Mie, Japan, (2007) November, pp. 442-447.
- [6] N. Suehiro and M. Hatori, "N-shift cross-orthogonal sequences", IEEE Trans. Inf. Theory, vol. 34, no. 1, (1988) January, pp. 143-146.
- [7] T. Kojima and M. Aono, "Properties of a convoluted-time and code division multiple access communication system based upon complete complementary codes", IEICE Trans. Fundamentals, vol. E91-A, no. 10, (2008) October, pp. 2881-2884.
- [8] T. Kojima, N. Ohitani, T. Matsumoto and U. Parampalli, "A blind digital watermarking scheme based on complete complementary codes", Communications Theory Workshop (AusCTW), (2011) February, pp. 1-6.
- [9] Y. Horii and T. Kojima, "On Digital Watermarks Based on Complete Complementary Codes", Signal Design and its Applications in communications, (2009) October, pp. 126-129.
- [10] N. Suehiro, N. Kuroyanagi, T. Imoto and S.Matstufuji, "Very efficient frequency usage system using convolution spread time signals based on complete complementary code", in Proc. 11th IEEE int. Symp. On Personal, Indoor and Mobile Radio Communications (PIMRC 2000), London, UK, (2000) September, pp. 1567-1572.
- [11] W. Trappe, M. Wu, Z. J. Wang and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia", IEEE Trans. Signal Process, vol. 51, no. 4, (2003) April, pp. 1069-1087.
- [12] Q. Liu, C. Khirallan, L. Stankovic and V. Stankovic, "Image-in-image hiding using complete complementary sequences", Multimedia and Expo, IEEE Trans, (2008) April, pp. 249-252.
- [13] El-khamy, N. O. El-Ganainy and M. A. Mookhtar, "The Twin Image Watermarking Algorithm(TIWA): A new Techniques for Single and Multi-Message Watermarking Based on Optimum Complete Complementary Codes", Computer as a Tool, 2005, EUROCON, (2005) November, pp. 939-942.
- [14] H. Torii, N. Suehiro and M. Nakamura, "General Construction of Periodic Complete Complementary Codes Composed of Expanded Modulatable Orthogonal Sequences", Computers and Communications, 2000, Proceedings, ISCC, (2000), pp.738-743.

- [15] H. Torii, M. Nakamura and N. Suehiro, "Generalized Method for ConstructingModulatable Periodic Complete Complementary Codes", IEEE Signal Processing Workshop on Signal Processing Advances in Wireless Communication, Taiwai, (2001) March, pp. 259-262.
- [16] Z. Chao, H. Chenggao, L. Yiting, L. Xiaokang and H. Mitsutoshi, "Iterative Method for Constructing Complete Complementary Sequences with Lengths of 2^mN", TSIGHUA SCIENCE AND TECHNOLOGY, vol. 10, (2005) October, pp.605-609.
- [17] X. Yang, Y. Mo, D. Li and M. Bian, "New Complete Complementary Codes and Their Analysis", Global Telecommunications Conference 2007, (2007) November, pp. 3899-3904.
- [18] C. Han, N. Suehiro and T. Hashimoto, "A Systematic Framework for the Construction of Optimal Complete Complementary Codes", information Theory, IEEE Transactions, (2011) September, pp. 6033-6042.
- [19] C. Han and T. Hashimoto, "Z-connectablecomplete complementary code and its application in CDMA", in Proc, Int, Symp. Inf. Theory (ISIT2009), (2009) June, pp. 422-438.
- [20] Z. -c. Jia, L. Ge, W. Jing and L. Shu-feng, "Research of Simple Constructing Method of Complete Complementary Sequences", Journal of HeBeiUniversity of Technology, vol. 36, no. 4, (2007) August, pp. 1-5.
- [21] C. Han and N. Suehiro, "A generation method for constructing (N,N,MN/P) complete-complementary sequences", in Proc. Joint IST workshop on Mobile Future and Sym. Trends in Commun. (Sympotic'04), (2004) October 24-26, pp. 70-73.
- [22] A. Kbakchiev, V. Kyovtorov, C. Kabakchiev and A. Lazarov, "Comparison of Communication Signals for Passive Radar Application", Radar Symposium (IRS), (2010), pp. 1-4.

Authors



De Li

He received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.



Wenji Quan

He is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas oftext document copyright protection, text image copyright protection, information security and digital watermarking.



JongWeon Kim

He received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a professor of Dept. of Copyright Protection at Sangmyung University in Korea. He has a lot of practical experiences in the digital signal processing and copyright protection technology in the institutional, the industrial, and academic environments. His research interests are in the areas of copyright protection technology, digital rights management, digital watermarking, and digital forensic marking.

International Journal of Multimedia and Ubiquitous Engineering Vol.8, No.6 (2013)