646 Journal of Electrical Engineering & Technology Vol. 7, No. 4, pp. 646~651, 2012
http://dx.doi.org/10.5370/JEET.2012.7.4.646

New Watermarking Technique Using Data Matrix and Encryption Keys

Ilhwan Kim*, Chang-Hee Kwon and Wangheon Lee†**

Abstract – Meaningful logos or random sequences have been used in the current digital watermarking techniques of 2D bar code. The meaningful logos can not only be created by copyright holders based on their unique information, but are also very effective when representing their copyrights. The random sequences enhance the security of the watermark for verifying one's copyrights against intentional or unintentional attacks. In this paper, we propose a new watermarking technique taking advantage of Data Matrix as well as encryption keys. The Data Matrix not only recovers the original data by an error checking and correction algorithm, even when its high-density data storage and barcode are damaged, but also encrypts the copyright verification information by randomization of the barcode, including ownership keys. Furthermore, the encryption keys and the patterns are used to localize the watermark, and make the watermark robust against attacks, respectively. Through the comparison experiments of the copyright information extracted from the watermark, we can verify that the proposed method has good quality and is robust to various attacks, such as JPEG compression, filtering and resizing.

Keywords: Data matrix, Encryption keys, Copyright information, Watermarking

1. Introduction

With the latest developments of multimedia, the spread of high-speed communication networks, and the emergence of strong tools to easily manipulate digital data, intellectual rights protection for digital content has become an important issue. Various digital watermarking techniques have been proposed and studied as a solution to these problems. Generally, digital watermarking is inserted into digital content not only to prevent the illegal distribution and display of copyrighted digital content but also to secure one's ownership of digital content.

The watermark is not recognizable by the naked eye or ears [1, 2]. In order to make effective use of digital watermarks, which contain ownership information, they must have the following characteristics [2, 3]. First, they must be invisible to perception and statistics. Second, they must be secure against outer attacks that may cause loss of information. In other words, damaged watermarks must be retrievable after any attack. Third, they must be safely protected from illegal uses. Fourth, they must clearly state ownership. Meaningful logos or random sequences have been used in existing digital watermarking techniques [1-3, 6-9] and [10]. The meaningful logos are created by copyright holders based on their unique information and are very effective when representing their copyright. The random sequence is a signal of a normal distribution with an average of 0 and dispersion of 1 that is widely spread throughout an image spectrum and can enhance security against intentional or unintentional attacks.

However, if these watermarks are damaged by various types of attacks, they would no longer be able to verify one's copyrights. In the case of a meaningful logo, the size of the watermarks becomes larger when a large quantity of data is used to represent a digital signature or copyright [4].

We propose a new watermarking technique using Data Matrix and encryption keys as a solution. Data Matrix is used to recover the original data through an error checking and correction algorithm even when the high-density data storage and barcode are damaged.

Usually, the matrix not only encrypts copyright verification information using a Data Matrix generation algorithm, but also randomizes the barcode using ownership keys, to create an extensive watermark signal. In this paper, encryption keys were used to establish watermark location and patterns to make watermarks stronger against outer attacks.

Watermark insertion is converted with a 512 × 512 image using DCT (Discrete Cosine Transform) and inserted with a 64 × 64 watermark within the given range of frequency. A blind watermarking method is used in watermark detection instead of the original image. In order to evaluate the proposed method, we make use of the watermarked PSNR (Peak Signal to Noise Ratio) as well as NC (Normalized Correlation) that is extracted after several attacks using a 2D barcode scanner.

† Corresponding Author: Dept. of Information Technology, Hansei University, Korea. (whlee@hansei.ac.kr)
* Dept. of Electrical and Electronic Engineering, Kangwon National University, Korea. (ihkim@kanwon.ac.kr)
** Dept. of Information Technology, Hansei University, Korea. (kwonch@hansei.ac.kr)
Received: March 2, 2012; Accepted: May 13, 2012

2. Data Matrix Structure

The Data Matrix of the 2D barcode was established in the mid 1980s to eliminate the data expression limit of the 1D barcode. The Data Matrix code includes high-density data storage and error correction systems which are widely used for 2D barcodes. The Data Matrix is an error checking and correction algorithm, which is classified as ECC00 – 140, that uses the Convolution method and ECC200 that uses Reed-Solomon. In this paper, we use ECC200.

Fig. 1 shows a Data Matrix 2D barcode comprised of a data range that includes square modules in a regular arrangement. The data range is separated by arrangement patterns. It is surrounded by the finder pattern which is surrounded by empty margins. Fig. 1(b) and (c) show a finder pattern which is a module that exists around the data range and has a width of 1.

A module is a cell used to encrypt a bit of data within the Data Matrix. The L-shaped left part of Fig. 1(b) and the boundary on the bottom are drawn in a black line. These are usually used to decide the actual shape, direction, and symbol distortion. Fig. 1(c) consists of an alternating arrangement of black and white modules. These are used to define the cell structure of symbols and may help in setting the actual size, as well as the distortion, of barcodes.

The empty margin in Fig. 1(d) is the space that surrounds the recognition pattern and must be at least as wide as a module. The data region shown in Fig. 1(a) indicates a code word from input data including an error correction code word. A barcode has 10 even numbers and 10 lines. This is a square that ranges from 10 x 10 to 144 x 144 with no empty spaces.

The Data Matrix can contain up to 2334 characters including letters and numbers. Error correction can be recovered even if about 30% of the barcode is damaged [5]. In Data Matrix, data is encrypted using six encryption schemes [5]. Table 1 lists the six encryption schemes. The process of encryption to generate Data Matrix barcodes is classified into the following three steps described below:

Step 1: Data Encryption

The input data for an encryption is analyzed. The highest encryption scheme of the input data group may not be one scheme with at least one bit of number per letter. A Data Matrix barcode basically uses various encryption schemes that can convert the input data into a code word more efficiently than a scheme.

Step 2: Error Checking and Correction Code Word

An error correction code word is generated using the Reed-Solomon algorithm and is overwritten onto the encrypted row of data.

Step 3: Module Arrangement in Matrix

A code word module is arranged using symbol letter arrangement.

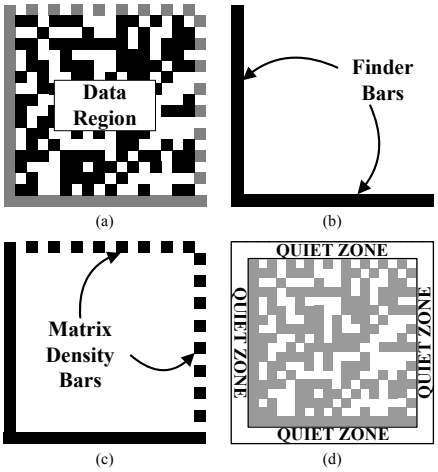

Fig. 1. Data Matrix barcode structure

Table 1. Data Matrix Encryption schemes

Encryption schemes	Characters
ASCII	Double digit numerics ASCII values 0~127 Extended ASCII values 128-255
C40	Primarily upper-case alphanumeric
Text	Primarily lower-case alphanumeric
X12	ANSI X12 EDI data set
EDIFACT	ASCII values 32-94
Base256	All byte values 0-255

3. New Watermarking Technique

This paper uses a method to insert and extract watermarks by applying insertion weight factor, α, which changes the size of the DCT coefficient based on the absolute average deviation of the DCT block. Also, an encryption key is used to establish the location and pattern of the watermark.

3.1 Watermark insertion

The watermark insertion algorithm in this paper can be roughly divided into watermark generation and watermark insertion. Fig. 2 shows the overall watermark insertion algorithm. The watermark generation takes advantage of the input information to finally generate a randomized watermark signal, as shown in the following four steps.

Step 1: Input the creator's name, signature, and date of creation.
Step 2: The input data generates a Data Matrix 2D Barcode through Data Matrix encryption.
Step 3: Generate a watermark using the Data Matrix 2D barcode from Step 2.
Step 4: Use the owner's key to convert the watermark image from Step 3 into a randomized watermark signal.

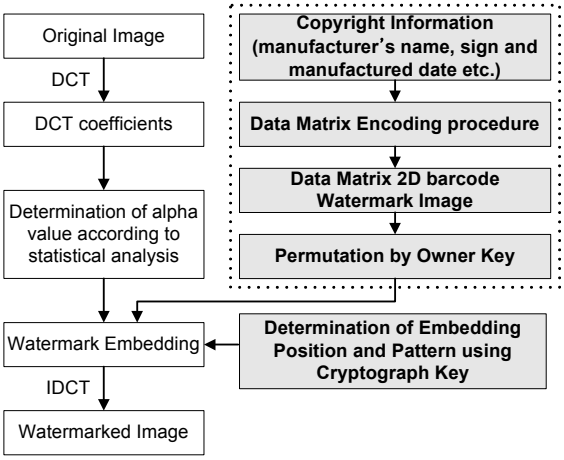

Fig. 2. Watermark insertion algorithm

The watermark is inserted onto the original image as shown in the following four steps.

Step 1: Divide the original image into 8 × 8 blocks to run a DCT.
Step 2: Consider the invisibility and durability of each 8 x 8 DCT block to select 22 insertion locations. Then, use the encryption key to decide 15 watermark insertion locations out of 22 preselected ones and the insertion pattern.
Step 3: Use the preselect location coefficients from each 8 × 8 DCT block to calculate the insertion strength, α, which is proportionate to the absolute average deviation.
Step 4: Insert each bit of watermark into the 15 8 × 8 DCT blocks based on the α value, the insertion pattern as shown in the Eq. (1).

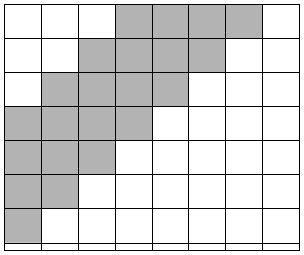

Fig. 3. Watermark insertion position

$$W_i = I_i + \mathrm{sgn}(I_i)\alpha E_i^j \ , \ i = i, 2, \cdots, 15 \ , \ j = 0,1$$
$$where \ \alpha = C * \sigma \ , \ E_i^j \in [\, E_i^0 \, , E_i^1 \,] \tag{1}$$

The Eq. (1) considers watermark insertion, where I_i is the DCT coefficient of the original image, W_i is the DCT coefficient after watermark insertion, C is the proportional constant, σ is the absolute average deviation of the 15 coefficients within 8×8 DCT blocks, and E_i^0 and E_i^1 are watermark bits' insertion pattern based on 0 and 1.

The most important element of the watermark insertion algorithm is the watermark generation algorithm which converts not only copyright information to the Data Matrix 2D barcode, but also decides the insertion pattern as well as the location using the encryption key

3.2 Watermark etraction

Fig. 4 explains a watermark extraction algorithm. We use a blind watermarking technique because it does not require the original image. The overall process of the algorithm is described as follows:

Step 1: Divide the watermark insertion image into 8 × 8 blocks to run the DCT.
Step 2: Use the encryption key to decide the location and pattern of insertion.
Step 3: Use the Eq. (2) to derive out the correlation between the coefficient value of insertion location and the insertion pattern for each 8 × 8 DCT block and to extract the watermark

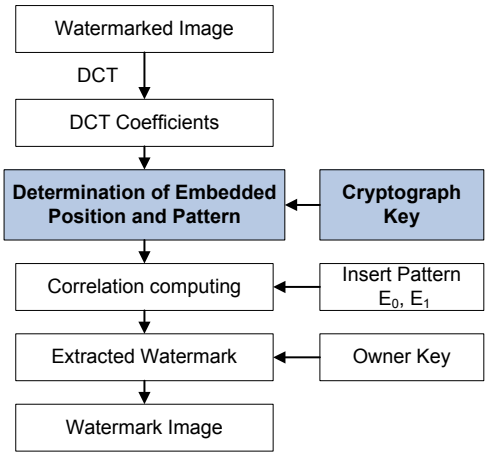

Fig. 4. Watermark extraction algorithm

$$D_0 = \sum |W_i| E_i^0 \ , \ \ D_1 = \sum |W_i| E_i^1$$
$$if \begin{pmatrix} D_0 \geq D_1 \ , \ bit = 0 \\ D_0 \langle D_1 \ , \ bit = 1 \end{pmatrix} \tag{2}$$

4. Experimental Results

We inserted a watermark to evaluate the performance of the proposed method and used the PSNR to measure the loss of image and the NC to compare the similarity of the original and the extracted watermarks. Eq. (3) shows the PSNR, where $I(x,y)$ and $\hat{I}(x,y)$ denote the original image and the image with a watermark, respectively.

$$PSNR(dB) = 10 \log_{10} \frac{MN \max I(x,y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [\hat{I}(x,y) - I(x,y)]^2} \tag{3}$$

Eq. (4) measures the similarity between the original and the extracted watermarks. $w(i,j)$ and $\hat{w}(i,j)$ indicate the original watermark and the extracted watermark, respectively.

$$NC = \frac{\sum_i \sum_j w(i,j)\hat{w}(i,j)}{\sum_i \sum_j w(i,j)^2} \quad (4)$$

In this experiment, three standard experimental images, including a 512 × 512 Boat image are used. We take advantage of the binary Data Matrix barcode of "1234567890" as a watermark based on the proposed method. Fig. 5 shows the 64 × 64 Data Matrix of a 2D barcode image that represents "1234567 890". For testing robustness, JPEG compression, filtering, and variable sizes of attacks were used. The extracted watermark is read using a 2D barcode scanner to verify the results.

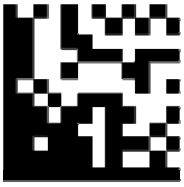

Fig. 5. Data matrix 2D barcode image that represents "1234567890"

Fig. 6 shows the experimental results. Resizing (BO) is an attack that doubles the size of the watermark image and reduces it down to the original size; and Resizing (SO) is an attack that halves the size and expands it up to the original.

Table 2 shows the measurement of image loss under attacks and the similarity of the extracted watermark to the original using a barcode scanner.

Table 2. Experimental results

Test Images	PSNR (dB)	Attacks	NC	Retrieved Data
Barbara	39.34	No attack	1.0	1234567890
		JPEG (Quality 80)	0.98	
		Sharpening	0.98	
		Blurring	0.98	
		Resizing(BO)	0.98	
		Resizing(SO)	0.97	
Boat	40.31	No attack	1.0	
		JPEG (Quality 80)	0.96	
		Sharpening	0.98	
		Blurring	0.98	
		Resizing(BO)	0.97	
		Resizing(SO)	0.95	
Pepper	42.44	No attack	1.0	
		JPEG (Quality 80)	0.96	
		Sharpening	0.97	
		Blurring	0.98	
		Resizing(BO)	0.98	
		Resizing(SO)	0.97	

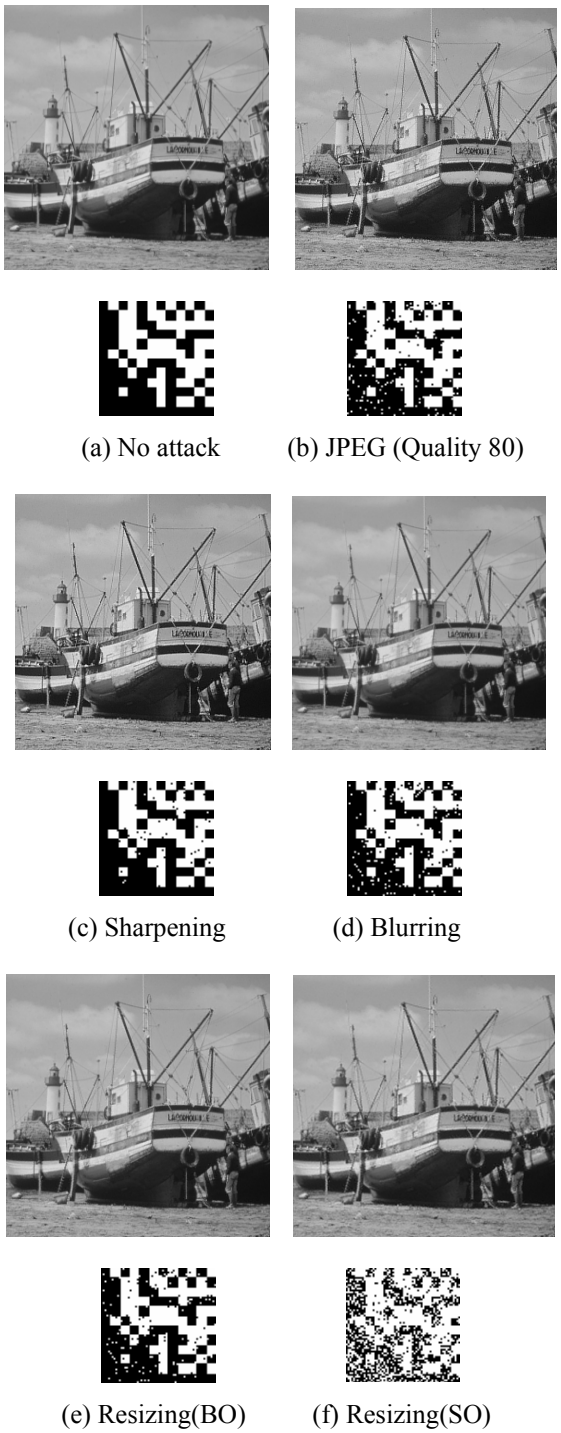

Fig. 6. Results of the robustness test for the boat image

Table 3 shows the comparison results of the proposed technique with the existing watermarking methods.

The comparison results show that the proposed method is more robust than others in PSNR(dB) not lower than 40dB, as well as having the average similarity of about 0.97 of the extracted watermark to the original after various

attacks. And copyright information was accurately traced back even when the watermark was damaged. The proposed technique is robust against various attacks. The robustness is achieved by not only encrypting the copyright verification information using the Data Matrix generation algorithm, but also by randomizing the barcode using ownership keys to create an extensive watermark signal.

Table 3. Comparison results of the robustness to other watermarking method

Comparison Items	Proposed	Choi [9]	Lee [11]
Info(bits)	4096	4096	4096
PSNR(dB)	40	40	38
JPEG	0.90 (Quality 60)	0.91 (20% by Photoshop)	0.85 (Quality 60)
Blurring	0.98	0.94	0.66
Sharpening	0.97	0.98	0.59
Resize	0.97	X	0.57

5. Conclusion

This paper proposed a new hybrid watermarking technique using Data Matrix not only to prevent losing information under attack or damage but also to solve the problem of the size limitation of watermarks. The generated barcode was inserted and extracted using encryption keys.

The copyright information was encrypted using the Data Matrix generation algorithm to create barcodes as well as accurately trace back even when the watermark was damaged. Also, encryption keys were used to decide the insertion pattern and extract the watermark without the original image.

Acknowledgement

This work was supported by the Kangwon National University.

References

[1] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," *Proceeding of Int. Conf. Image Processing*, pp.243-246, 1996.

[2] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Transactions on Image Processing*, pp.1534-1548, 1999.

[3] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," *Proceeding of Int. Conf. Acoustics Speech and Signal Processing*, pp.2168-2171, 1996.

[4] Ji-Hong Chang and Long-Wen Chang, "A new image copyright protection using digital signature of trading message and bar codewatermark," *Proceeding of Image and Vision computing* , pp.205-209, 2003.

[5] J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," *Proceedings of the SPIE : Storage and Retrieval for Image and Video Databases VI 3312*, pp.308-317, 1998 .

[6] M. Barni, F. Bartolini, A. De Rasa and A. Piva, "Capacity of full frame DCT image watermarks," *IEEE Transactions on Image Processing*, vol.9, pp.1450-1455, 2000.

[7] J. O. Ruanaidh, H. Petersen, A. Herrigel, S. Pereira, and T. Pun, "Cryptographic copyright protection for digital images based on watermarking techniques," *Theoretical Computer Science*,vol.226, pp.117-142, 1999.

[8] Tomokazu Onuki, Takeharu Adachi, Madoka Hasegawa, and Shigeo Kato, "A study on a digital watermarking method for still images," *International Technical Conference on Circuits/Systems, Computers and Communications* , pp.19-22, 2000.

[9] Yong C. Kim, Byeong C. Choi, "Two-Step Detection Algorithm in a HVS-Based Blind Watermarking of Still Images," *Lecture Notes on Computer Science*, vol. 2613, pp. 235-248, 2002.

[10] Jong-Eun Ha, "A New Method for Detecting Data Matrix under Similarity Transform for Machine Vision Application," *IJCAS*, vol. 9, no. 4, pp.737-741, 2011.

[11] Kyung-Hun Lee, "Wavelet-Based Digital Watermarking Method," *Journal of The Korea Computer Industry Education Society*, vol.3, no.7, pp. 871-880, 2002.

Ilhwan Kim He received BS and MS degree in Control and Instrument Engineering from Seoul National University in 1982 and 1985 respectively and Ph.D. at the Tohoku University in 1993. In 1995, he joined the Department of Electrical and Electronic Engineering at the Kangwon National University and is currently a professor. His research interests include control, mechatronics, and human interfaces.

Chang-Hee Kwon He received MS and Ph.D. degree in Urban Science from Tokyo Metropolitan University in 1988 and 2003 after B.S from the Konkuk University in 1991, respectively. In 2003, he joined the Division of Information Technology at the Hansei University and is currently an assistant professor. His research interests include U-City, GIS, ITS,U-Healthcare.

Wangheon Lee He received his B.S. degree in Control and Instrumentation from Seoul National University in 1985, his M.S. and Ph.D. degrees in Automation and Design Engineering from Korea Advanced Institute of Science and Technology in 1992, 2001,respectively. In 2006, he joined the Department of Information Technology at the Hansei University, now an assistant professor and became a chairman of technical committee of Machine Vision from 2011 of ICROS. His research interests include computer vision, mobile robotics, and embedded control.