A NOVEL COPYRIGHT PROTECTION FOR DIGITAL IMAGES USING EXTRA SCRAMBLED INFORMATION

Jin-Wook Shin, Jucheng Yang, Dong-Sun Park
Dept. of Infor. & Comm. Eng., Chonbuk Nat'l University, Jeonju, Jeonbuk, 561-756, Korea

Sook Yoon
Dept. of EECS, University of California at Berkeley Berkeley, CA 94720

Keywords: Digital content, Copyright protection, Extra scrambled information, Watermarking, Fingerprinting.

Abstract: Both watermarking and fingerprinting techniques can be used for protecting digital contents with different properties. A watermarking system may degrade the fidelity of the digital contents by embedding watermark messages, while a fingerprinting system may have high computational complexity to generate unique features for digital contents. In this paper, we propose a novel copyright protection technique that combines positive features of both techniques. The proposed technique can distribute digital images without embedding messages related with them, and save extra scrambled information on simple fingerprints stored in a certified database. Experimental results show that the proposed method outperforms an existing method for various signal processing attacks. The proposed technique is also flexible and fast so that it can be used for real-time applications.

1 INTRODUCTION

The explosive growth in Internet and its supporting digital technology for the last decade brings the production and spread of huge amount of multimedia data. Since it is very easy to copy, edit, save and/or transmit digital data, illegal operations on digital data, such as illegal copy and distribution, have been frequently conducted without having any charges against those actions. Protection of intellectual property rights, therefore, is one of the major issues in the current Internet era.

Cryptography (Cox, 2002) can be used to protect digital data during transmission through digital networks from network eavesdroppers, but it is not appropriate for cases of illegal copy and distributions. Recently, digital watermarking techniques are focused as the copyright protection technique for those cases. Using this technique, we can embed information of manufacturers or authorized users inside the digital contents to prevent the illegal actions. The basic requirement of a watermarking technique is to minimize the degradation of the original contents when embedding a watermark message and the watermark itself should be unperceivable to other users. Depending on different applications, a watermarking system should have required properties including fidelity, robustness against various signal processing attacks, computational complexity and cost.

Various researches have been performed on developing efficient watermarking systems (Huang, 2004) (Schydel, 1994). Most watermarking systems developed so far one of two types depending on the method of embedding watermark messages : spatial domain and frequency domain methods.

Since watermarking techniques embed watermark messages in the digital contents, slight degradation of quality cannot be avoided. If a digital contents experience many signal processing operations during transmission and distribution, the embedded watermark message may be severely affected and hard to recover.

A fingerprinting technique (ISO/IEC 21000-11, 2004), included in MPEG21 part11, extracts unique features from digital contents using computer vision techniques, saves them in a database, and uses them when there is a need to prove the identification of the digital contents. Since this method distributes the

Shin J., Yang J., Park D. and Yoon S. (2006).
A NOVEL COPYRIGHT PROTECTION FOR DIGITAL IMAGES USING EXTRA SCRAMBLED INFORMATION.
In *Proceedings of the First International Conference on Computer Vision Theory and Applications*, pages 27-32
DOI: 10.5220/0001367100270032

original contents without modifying any values, it may endure more changes during distribution. However, this technique is usually not flexible because it cannot embed external information. Moreover, it is usually time-consuming due to the high computational complexity implementing computer vision techniques.

In this paper, we propose a novel copyright protection technique for digital images using positive features of both watermarking and fingerprinting techniques. The proposed method uses external copyright messages and original digital contents to generate extra scrambled information. Random number generator is used to randomly select the elements of digital contents. The generated extra scrambled information contains the information of both external copyright messages and original digital contents. The generated information can then be stored in a certified database with initial seeds for random number generator. The original digital contents can be distributed without having any changes in element values. If there is a need to identify either the external copyright message or the original contents, the stored extra scrambled information can be used for identification. The proposed technique generates and saves extra scrambled information as a function of external copyright message and original contents, and distributes the original contents. Therefore, there is no degradation in fidelity on the distributed contents. In addition, in generating the extra scrambled information we use a simple and fast spatial domain insertion method so that the proposed technique has a very low computational complexity.

This paper is organized as follows. In section 2, related techniques including watermarking and fingerprinting models briefly described. The proposed technique is explained in detail in Section 3. Experimental results and conclusion are described in Section 4, 5, respectively.

2 RELATED WORKS

2.1 Watermarking

In typical watermarking systems, a watermark message which contains information on manufacturers or authorized users is embedded in the digital contents and distributed to the outside world. The embedded watermark message should not be perceivable not to degrade the quality of the digital contents. The embedded watermark message can be extracted to resolve legal disputes on the digital contents such as illegal copy, modification and distribution.

Fig. 1 shows the conceptual block diagram of a typical watermarking system. It consists of a embedder and a detector. The embedder embeds the watermark message to the original content and the watermarked contents are distributed. The watermarked contents can be modified by various signal processing operations or malicious attacks. The watermark detector is to detect a watermark message form the corrupted version of the digital contents. Various techniques have been developed for the better performance depending on the specific applications (Nikolaidis, 2001) (Fazam, 2001).

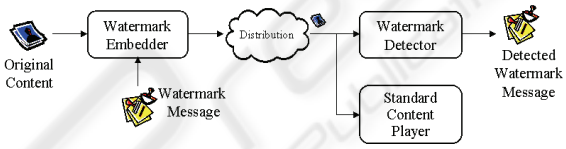

Figure 1 : General watermarking system.

The properties required for a watermarking system can be varied according to the applications. Some properties including fidelity, robustness, computational complexity, and informed/blind detection can be found in (Cox, 2002).

2.2 Fingerprinting

A fingerprinting technique (ISO/IEC 21000-11, 2004) is can be also used to protect digital contents from illegal uses as in the watermarking system. The main difference between two methods in that a fingerprinting system extracts features from digital contents and uses the features for identifying the digital contents while a watermarking system embeds an external watermark message in the digital contents. Therefore, this fingerprinting technique does not embed any information on the digital contents.

The conceptual block diagram of a fingerprinting system is shown in Fig. 2. It consists of two fingerprint generators and a comparison part. The technique usually employs computer vision techniques to generate an invariant fingerprint from the digital contents.

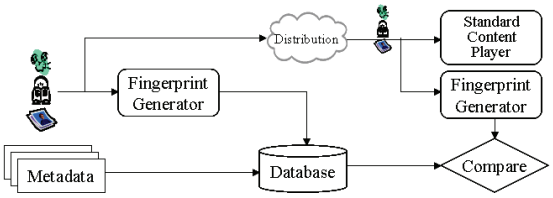

Figure 2: Fingerprinting system.

The generated fingerprint is stored in a database and then it can be used for comparison whenever a legal dispute happens. As in the figure, the fingerprinting technique does not embed any information in the digital contents. The digital contents is not modified and distributed to outside so that there can be no degradation in the contents. Since this technique usually uses time-consuming technique to find unique fingerprint, it is very hard to apply them to real time applications.

3 PROPOSED METHOD

The method proposed in this paper combines the features of watermarking and fingerprinting. The method extracts some simple information such as intensity value from original digital contents and distributes the original contents as in the fingerprinting technique. In the meanwhile, it also generates extra scrambled information with external copyright message and the information extracted from the contents.

Fig. 3 shows the block diagram of the method. In the figure, original digital contents are used to generate extra scrambled information as a function of external copyright message and random number sequences. The resulting extra scrambled information and additional parameters of the generator may be stored in a certified database for later identification purposes. The original contents may then be distributed without changing any temporal or spectral information. The stored information can be used whenever there is a need to prove the identification of the digital contents or the existence of the copyright message in the stored information. The detection process uses the information stored in the database and the same procedure to generate the extra scrambled information for the copyright message. In this method, we used a pseudorandom number generator and a spatial domain to generate to extra scrambled information.

3.1 Extra Scrambled Information

Extra scrambled information is a binary data that combines the information from the external copyright message and the original contents. It represents the copyright message or the original work depending on applications. In other words, it can be used to identify the copyright message or the original digital contents itself.

The extra scrambled information generator can be depicted as in Fig. 4. It consists of a position selection part using three random sequences from the random number generator, and a binary data generator part to combine information from the copyright message and the selected elements in the previous part. In the figure, for simplicity, we used a still image as the original digital contents. In this system, it is defined that original image is X, random sequence value K, and copyright message W.

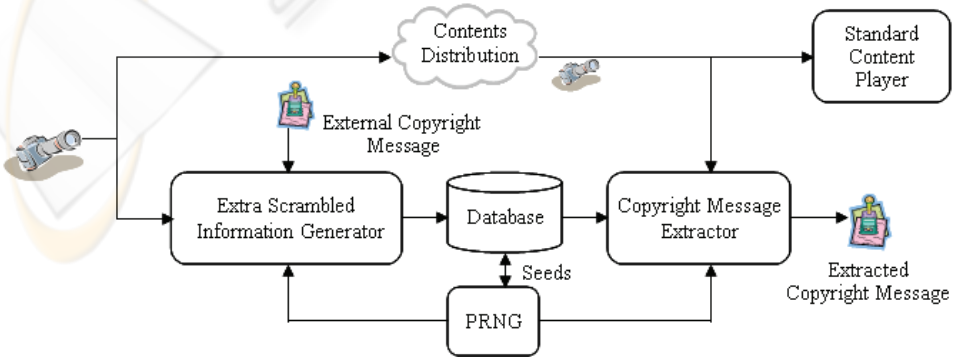

Figure 3: Proposed block diagram.

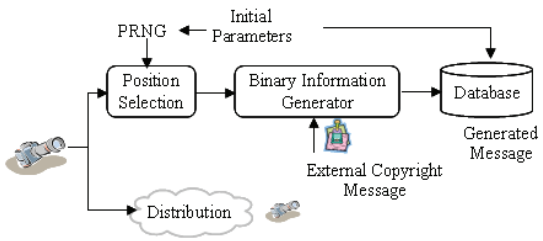

Figure 4: Generation of extra scrambled information.

The elements of original image, $X(X_H, X_W)$, are N-bit gray values and the elements of copyright message, $W(W_H, W_W)$, are assumed to be binary image. Three random number sequences are generated using initial seeds. Two are used to select position of pixels in the input image and the last one is used as a temporary gray value.

The pixel position selector receives two random sequences as the coordinates of a pixel and outputs the pixel pointed by these coordinates. The binary data generator receives the pixels from the pixel position selector, and the temporary gray sequences, g_k from the random sequence generator. Using these values, it computes temporary binary image T as in the Eq. 1.

$$T=\left\{ t_k = \begin{cases} 1 & if\ X(x_k, y_k) \geq g_k \\ 0 & if\ X(x_k, y_k) < g_k \end{cases} \mid k = 0,1,...,n-1 \right\} \quad (1)$$

In the equation, $0 \leq g_k \leq 2^8 - 1$, $k = W_H \times W_W$

Finally, the temporary binary image T is exclusive-*OR*ed with a binary copyright image to generate extra scrambled information(*ESI*) as in Eq. 2.

$$ESI(x,y) = W(x,y) \oplus T(x,y) \quad (2)$$

The generated binary extra scrambled information, *ESI*, is stored in a certified database with the random number seed values for later extracting the copyright image.

3.2 Extraction of Copyright Message

A digital contents received from Internet can be degraded by noise or malicious attacks. Due to the degradation of digital contents, a copyright message embedded in extra scrambled information can also be affected. Fig. 5 shows the extraction process.

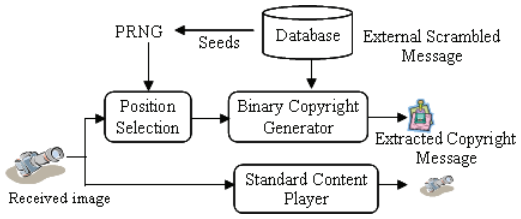

Figure 5: Extraction of copyright message.

The method is very similar to the extra scrambled information generator process. It generates two random numbers using the initial seeds from the database and uses the sequences to select positions of pixels in the input image. It also uses one random sequence as temporary gray values to calculate a temporary binary image as in Eq. 1. Using the temporary binary image and extra scrambled information from database, we can compute the received external copyright message W' as in Eq. 3.

$$W' = ESI(x,y) \oplus T(x,y) \quad (3)$$

In this equation, the received image is X', temporary image, T', and extracted copyright message, W'.

4 EXPERIMENTAL RESULTS

Performance measures in watermarking or fingerprinting systems can be varied dependently on the types of applications. To evaluate the performance of the proposed method, we used a popular benchmark test called Stirmark (Nikolaidis, 2004) (Website). This algorithm generates various spatial signal processing images such as rotation, cropping, median filter, adding noise, and etc. Bit Correct Ratio (*BCR*) is mostly used in this paper to show the correctness of the extracted copyright message and it is defined in Eq. 4 (Chang, 2004).

$$BCR = \left(1 - \frac{\sum_{i=0}^{W_H} \sum_{j=0}^{W_W} \overline{w_{i,j} \oplus w'_{i,j}}}{W_H \text{ X } W_W} \right) \times 100\ \% \quad (4)$$

In this equation, w and w' are the original watermark and the extracted watermark at the detector side, respectively and $\oplus$ denotes the *EX-OR* operator.

In the experiment, we used the 512×512 Lena image with 8-bit gray scale as the original digital content and a 64 × 64 binary image as the copyright message. Total attacked 108 images generated using Stirmark algorithm are used to verify the proposed method. Fig. 6 shows the original Lena, binary copyright message and its generated extra scrambled information, respectively.

(a) Original Lena

(b) Copyright message (c) Extra scrambled information.

Figure 6: Extraction of copyright message.

After degrading the original contents with some signal processing attacks such as histogram equalization, median filtering and scaling, we evaluate the performance using the *BCR*. Fig. 7 shows the results extracted copyright message with *BCR*s. For these typical attacks, it still shows very high *BCR* under those attacks.

(a) Histogram equ. : 90.6% (b) Median(3×3) : 93.7%

(c) Rotation(2°) : 88.0% (d) Rotation(0.5°) : 93.1%

(e) Noise(20%) : 75.4% (f) Scaling(90%) : 94.2%

Figure 7: Extracting results.

The performance of the proposed method is compared to one of the leading research results as in Table 1. C. Chang (Chang, 2004) proposed a wavelet transform-based watermarking system using artificial neural networks. As seen in the table, the proposed method shows much higher *BCR* comparing to the method in the reference.

Table 1: The comparison of *BCR* under various attacks.

Attack Types	Proposed Method	C. Chang
Histogram Equ.	90.67%	-
Median Filter	93.7%	89.25%
JPEG	94.5%	88.43%
Scaling	94.8%	78.58%

We summarize several properties of the propose method as follows:

① Fidelity : Embedding a watermark message to other watermark system requires the modification of pixel values in the spatial domain or frequency components in the frequency domain. This degrades the fidelity of the digital contents. On the contrary, the proposed method is not directly change the original contents as in the fingerprinting technique, so that it keeps the fidelity to 100%.

② Required space : The proposed method requires to have a space to store a binary scrambled information in a certified database. The extra scrambled information has the same size of the copyright message.

③ Computational complexity : The computations in the proposed method are the magnitude comparison and the exclusive-OR operation. The processing time for these operations is less than 10 ㎳ and should be very short so that the method can be used to a real time application

④ Robustness : Most watermarking systems require to have robustness against various signal processing attacks. Various experiments are performed to evaluate the proposed method. It has high *BCR*s for histogram equalization, compress, scaling, and small amount of rotation. On the other hand, the *BCR*s are rather low for high noise and cropping of the original image.

5 CONCLUSION

We propose a novel copyright protection technique by combining features of a watermarking system and a fingerprinting system. The proposed system generates extra scrambled information as a function of original contents and copyright message and stores it in a certified database for later use. The generated extra scrambled information in trusted certification center or database can be used in case of copyright dispute. The stored extra scrambled information can be used to identify the copyright message in many applications.

Since the proposed system can distribute the original contents without changing any of its values, no degradation on the contents is introduced. The experimental results show that the proposed method performs better than the existing leading method for various signal processing attacks. In addition, the computational complexity of the proposed method is very low so that it can be used for some real time applications.

We will further study about the extra scrambled information search algorithms according to increasing contents and robustness algorithms to geometric attacks.

REFERENCES

Cox, Ingemar J., 2002. *Digital Watermarking(Multimedia Information and System)* .Morgan-Kaufmann.

H. Huang, H. Hang, and J. Pan. 2004. "An Introduction to Watermarking Techniques," *Series on Innovative Intelligence*, Vol. 7, pp.3-39, World Scientific Publishing Co. Pte. Ltd.

R.G.V. Schydel, A.Z. Tirkel, and C.F.Osborne. 1994. ”A Digital Watermark”, In *Proceeding of the International Conf. on Image Processing*. pp. 86-90, Austin, IEEE Press.

ISO/IEC 21000-11. *Information technology-Multimedia framework(MPEG-21)-Part11*:Evaluation Tools for Persistent Association Technologies. 2004.

A. Nikolaidis and I. Pitas. 2001. " Region-Based Image Watermarking," *IEEE Trans. on Image Processing*, Vol. 10, No. 11, pp. 1726 – 1740.

M. Fazam and S. Shahram Shirani. 2001. " A robust multimedia watermarking technique using Zernike transform,"in *Proc. IEEE Int. Workshop Multimedia Signal Processing*, pp. 529-534.

N. Nikolaidis and I. Pitas. 2004. “Benchmarking of Watermarking Algorithms”, *Series on Innovative Intelligence*. Vol. 7, pp.315-347, World Scientific Publishing Co. Pte. Ltd.

http://www.petitcolas.net/fabien/watermarking/stirmark/

C. Chang and I. Lin. 2004. "Robust Image Watermarking Systems Using Neural Networks," *Series on Innovative Intelligence*, Vol. 7, pp.395-427, World Scientific Publishing Co. Pte. Ltd.