A Novel Public Watermarking System based on Advanced Encryption System

Ko-Ming Chan and Long-Wen Chang
Department of Computer Science
National Tsing Hua University
Hsinchu, Taiwan, 300
lchang@cs.nthu.edu.tw

Abstract

A lot of digital watermarking techniques have been proposed to resolve the issues of copyright protection. However, almost proposed watermarking methods keep the watermarking algorithm private to ensure the embedded watermark secret. If the watermarking technique needs to be widespread applied to realistic multimedia environment, the algorithm used by watermarking techniques should be public.

In this paper, a novel watermarking scheme which can be public is presented. The proposed watermarking technique is developed based on the following criterions: (1) the watermarking algorithm is open; (2) the embedded watermark can be extracted and embedded by the people who own the secret key. The watermarking scheme employs the advance encryption standard (AES) and the Reed-Solomon code, to make the watermarking algorithm public. Simulation shows that the proposed algorithm can be very robust to resolve the ownership of the digital image.

1. Introduction

Digital watermarking technique can provides copyright protection for digital data [1-3]. Almost all watermarking methods, which have been proposed today, can provide robust and secret watermark and against various attacks such as A/D or D/A converting, data compression, etc. The watermark is robust and secret due to the owner keeps the algorithm private. If the owner reveals the watermarking algorithm, this is equivalent to tell the location for watermarking, and the malicious attack can easily eradicate or destroy the embedded watermark. Generally speaking, a serviceable watermarking technique should reveal the algorithm to allow all people to manipulate and still provide a robust and secret watermark.

Cryptography is well known to make message secre[6-7] and can be applied to the watermarking system to help to reveal the watermarking algorithm without disclosing the location for embedding the watermark. The Rijndael block cipher is the next generation of advanced encryption standard for 21 century [8]. We use it to encrypt the positions for watermarking. Error-Correcting code is capable of providing reconstruction when some of the transmitted codes are lost. Reed-Solomon code [9-11] is adopted for the proposed watermarking method to generate fragile watermark and to correct the damaged image.

2. The proposed watermarking Algorithm

2.1 The watermark embedding Algorithm

The proposed watermarking system embeds two different watermarks into the spatial and the frequency domain, separately. In the frequency domain, a robust watermark is embedded first. Then, a fragile watermark is embedded into the LSB plane in the spatial domain. Figure 1 illustrates the watermark embedding procedure. The robust watermark embedding algorithm is stated below:

1. W_{RS} = RS_Encode (W_0),
2. I_Z = Set_LSB_Zero (I_0),
3. CS_0 = DWT (I_z),
4. MSCPS = Order_of_Significant_Coefficients (CS_0, k, $\|W_{RS}\|$),
   C-MSCPS = Rijndael_Encrypt (MSCPS, K),
   WMPS = Select_Watermark_Positions (C-MSCPS, $\|W_{RS}\|$),
5. CS_W = Embed_Robust_Watermark (CS_0, WMPS, W_{RS}),
6. I_{wf} = IDWT (CS_W).

In step 1, the original watermark W_O is first encoded with a Reed-Solomon encoder to generate W_{RS}, where "o" indicates original, "RS" means the Reed-Solomon code is encoded. In step 2, the LSB bit of every pixel of the original image I_O is set to zero to obtain a new image I_Z, where "z" means that the least significant bit is zero. In step 3, I_Z is processed by Discrete Wavelet Transformed to obtain four wavelet sub-bands coefficients LL, HL, LH and HH. CS_0 is the wavelet coefficient sequence, which records the LL, HL, LH, HH coefficients in raster scan order, respectively. In step 4, major significant coefficients (MCS) are first selected according to the length of encoded watermark,, $\|W_{RS}\|$

Proceedings of the 18th International Conference on Advanced Information Networking and Application (AINA'04)
0-7695-2051-0/04 $ 20.00 © 2004 IEEE

and selection factor *k*, i.e. $k\|W_{RS}\|$ most significant coefficients of the LL band of CS_0. Usually *k* > 1, this can ensure the locations, which are selected to embed the robust watermark, to be secret. The order of these major significant coefficients is recorded in the descending order of magnitude to be MSCPS. Each byte records one position. After MSCPS is generated, MSCPS is encrypted with a key K by the Rijndael block cipher to obtain Cipher-MSCPS (C-MSCPS). That is, $\|W_{RS}\|$ significant bytes of C-MSCPS are selected as the embedding positions. The position, which corresponds to the most significant byte of C-MSCPS, embeds the first bit of encoded watermark, W_{RS}. The above 6 steps embed robust watermark into the original image in the frequency domain. The watermark is added to the significant coefficients of the LL band of the original image to ensure its robustness.

Figure 2 shows how to generate C-MSCPS and determine the embedded wavelet coefficient positions. After the C-MSCPS is produced, WMPS is generated according to C_MSCPS and $\|W_{RS}\|$. The embedding watermark positions are recorded in the watermark position sequence WMPS. Figure 3 shows how to generate C-MSCPS. MSCPS is encrypted with a secret key K by the Rijndael block cipher to produce C-MSCPS. The fourth block of C-MSCPS with value 66 is the most significant block. Then, the position 3 with wavelet coefficient value 220 of LL band, is chosen to embed the first watermark bit. Block 7 of C-MSCPS is the second significant block, and position 73 of LL is chosen to embed the second watermark bit. According to C-MSCPS, position 33, 42 of LL are chosen to embed third and fourth watermark bits, respectively. In step 5, modify the wavelet coefficients of CS_0 according to WMPS and encoded watermark W_{RS} to obtain new wavelet coefficients sequence CS_W. The watermark embedding is illustrated as follows [4, 5]:

(1) If $W_{RS}(i) = 0$, then $v_i' = v_i(1 + \alpha * (-1))$,

(2) If $W_{RS}(i) = 1$, then $v_i' = v_i(1 + \alpha * (1))$,

where $W_{RS}(i)$ is the i[th] watermark bit, v_i is wavelet coefficient value of CS_0, and α is a scalar factor and it determines the embedded watermark strength. In step 6, inverse discrete wavelet transformed with the modified wavelet coefficients CS_w to obtain the image I_{wf}, which contains the robust watermark W_{RS}.

The embedding algorithm of fragile watermark is described below:

7. I_{wfz} = Set_LSB_Zero (I_{wf}),

8 RS-ECC = Generate_RS_ECC (I_{wfz}),

9: C-RS-ECC = Rijndael_Encrypt (RS-ECC, K),

10: I_w = Embed_Fragile_Watermark (I_{wfz}, C-RS-ECC).

In step 7, all LSB of I_{wf} are reset to zero to obtain I_{wfz}. We add the fragile watermark C-RS-ECC in the LSB plane of I_{wf}. In step 8, I_{wfz} is encoded by Reed-Solomon encoder to obtain the fragile watermark RS-ECC. The RS-ECC contains all the parity check bits of encoded Reed-Solomon code. In step 9, RS-ECC is encrypted with a secret key K and the Rijndae block cipher to obtain the fragile watermark C-RS-ECC. In step 10, all the LSB of I_{wf} are replaced with C-RS-ECC in a raster scan order and the final watermarked image I_W is obtained.

After above 10 steps, I_W contain two watermarks: a robust watermark W_{RS} and a fragile watermark C-RS-ECC. The robust watermark W_{RS} is used to carry the copyright information and the fragile watermark C-RS-ECC is used to verify the image integrity and capable of providing the ability to recover altered image.

2.2 Watermark Extraction Procedure

There are two phases in watermark extraction procedure: the inspecting phase and the extracting phase. In the inspecting phase, the test image I_W' is inspected whether I_W' is altered or not. In the extracting phase, the watermark W_{RS}' is extracted by comparing to the original image I_0. Figure 4 demonstrates the watermark extraction procedure. The extracting algorithm is described below:

The Inspecting phase:

1:(I_{wz}', C-RS-ECC') =

Extract_Fragile_Watermark_and_Set_LSB_Zero (I_w'),

2: RS-ECC' = Rijndael_Decrypt (C-RS-ECC', K),

RS-ECC = Generate_RS_ECC (I_{wz}'),

3: If RS-ECC' == RS-ECC, jump to Extracting phase.

If RS-ECC' # RS-ECC, jump to step 4,

4: Fix_Image (I_{wz}', RS-ECC'),

The Extracting phase:

1. CS_0' = DWT (I_{wz}'),

2. CS_0 = DWT (I_z),

3. MSCPS = Order_of_Significant_Coefficients (CS_0 , *k*, $\|W_{RS}\|$),

C-MSCPS = Rijndael_Encrypt (MSCPS, K),
WMPS = Select_Watermark_Positions (C-MSCPS, $\|W_{RS}\|$),

4. W_R' = Extract_Robust_Watermark (CS_0', CS_0 , WMPS),

5. W' = RS_Decode (W_{RS}')

The extracting algorithm is explained below:

Inspecting phase:

1. All least significant bits of test image I_W' is collected in a raster scan order to form extracted fragile watermark C-RS-ECC'. After the fragile watermark is extracted, I_{wz}' is obtained by setting all the least significant bits of I_w' to zero.

2. The extracted fragile watermark C-RS-ECC' is decrypted with key K by the Rijndael block cipher to obtain RS-ECC'. The new examining fragile watermark RS-ECC is generated from I_{wz}' with the Reed-Solomon encoder.

3. The embedded fragile watermark RS-ECC' and the new generated fragile watermark RS-ECC are compared. If RS-ECC' is equal to RS-ECC, this means that the received watermarked image I_w' is not altered, i.e. I_w' = I_w. Then, jump to extracting phase. If RS-ECC' is not equal to RS-ECC, i.e. the received watermarked image is altered. Then, jump to step 4.

4. The RS-ECC', which contains the parity check bits of Reed-Solomon code, can help to recover the altered watermarked image.

The **Extracting** phase:

1. Decompose the watermarked image I_{wz}' to obtain the wavelet coefficient sequence CS_0'.

2. Decompose the original I_z to obtain the wavelet coefficient sequence CS_0.

3. Use the same procedure described in the embedding phase step 4 to obtain the embedded watermark position sequence WMPS.

4. Compare the wavelet coefficients of CS_0' with CS_0 according to watermarking position sequence WMPS.

5. $(1)\ W_{RS}'(i) = 1, \quad \text{if } v_i' > v_i$
   $(2)\ W_{RS}'(i) = 0, \quad \text{if } v_i' \le v_i$

6. Decode W_{RS}' by using the Reed-Solomon decoder to obtain the embedded watermark W'.

3. The simulation Results

.The Tsing Hua University logo of 64 * 64 is used to be the watermark. In order to inspect the extracted watermark, we define a similarity measure to decide whether the watermark exists or not. We define the similarity value between W and W^* as:

$$\mathrm{Sim}(\mathrm{W}, \mathrm{W}^*) = \frac{\sum_i \overline{W_i \oplus W_i^*}}{\sum_i \overline{W_i \oplus W_i}},$$

where $\overline{\oplus}$ is the Exclusive-NOR operator, $1 \le i \le N * N$, and the similarity value is calculated from total image bits between W and W^*. Figure 5 shows the original image and the similarity measures of the extracted watermarks for the watermarked images under various attacks. It shows that the proposed algorithm is very robust.

4. Conclusion

A novel watermarking technique that can be public is proposed. The robust watermark is embedded in the wavelet coefficients of LL band of the image to strengthen the watermark and against various attacks such image processing, data compressing, and other malicious modification etc. Advanced encryption standard, the Rijndael block cipher, is adopted to hide the embedded robust watermark positions of the image. The candidate embedded positions are known by the users, who have the secret key to embed/extract the embedded watermark. A fragile watermark is also added in the least significant bit plane of the watermarked image. The fragile watermark, which is encoded with the Reed-Solomon code and the Rijndael block cipher, is capable of providing verification and error correcting abilities.

5. References

[1] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in Proceedings, IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 4, May 1996, pp. 2168-2171.

[2] Houng-Jyh Wang and C.-C. Jay Kuo, "Image Protection via Watermarking on Perceptually Significant Wavelet Coefficients." IEEE 1998 Workshop on Multimedia Signal Processing, Redondo Beach, CA., Dec. 7-9, 1998.

[3] S. Craver, N. Memon, B. L and M. M Yeung "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," IEEE Journal on Selected Areas in Communications, Vol. 16 Issue: 4, May 1998, pp. 573 –586.

[4] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, " Secure Spread Spectrum Watermarking for Multimedia", IEEE Transaction on Image Processing, vol. 6, pp. 1673-1687, Dec. 1997.
[5] C.-T. Hsu and J.-L. Wu, "Hidden Digital Watermarks in Images, "IEEE Transactions on Image Processing, Vol. 8,No. 1, pp.58-68, Jan. 1999.
[6] Wenjun Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images" Image Processing, IEEE Transactions on, Volume: 8 no. 11, Nov. 1999, pp. 1534 –1548
[7] W. Stallings, "Cryptography and network security: principles and practice, 2nd Edition." Prentice Hall, 1999.
[8] Bruce Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, 1996.
[9] J. Daemen, V. Rijmen, "The Rijndael Block Cipher: AES Proposal"
[10] S.G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 11, pp. 674-693, July 1989.
[11] S. B. Wicker and V. K. Bhargava (eds.), Reed-Solomon Codes and Their Applications, IEEE Press, 1994.

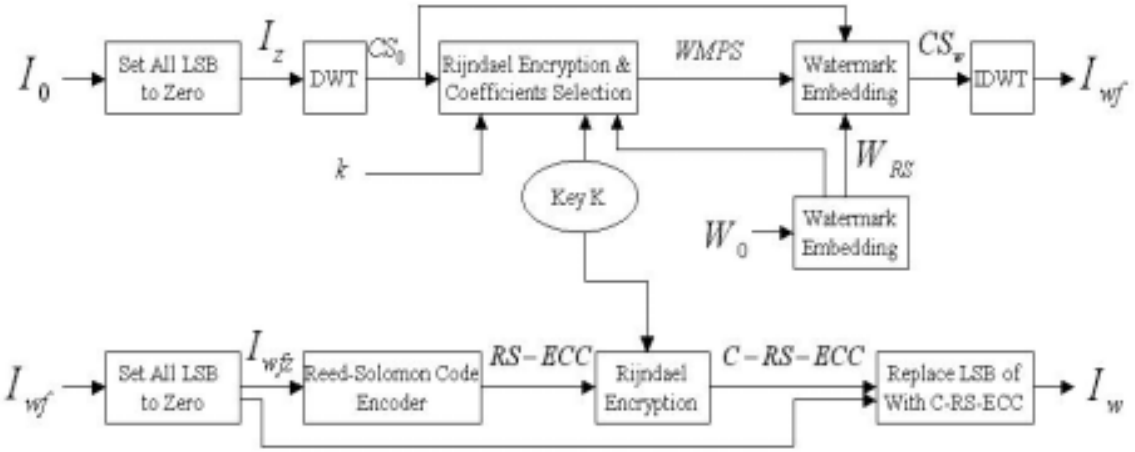

Figure 1: Flowchart for watermark embedding

Wavelet Coefficient Value	252	231	224	220	154	140	132	131
Position in LL band	10	33	42	3	65	20	73	41
MSCPS	7^{th}	5^{th}	3^{rd}	8^{th}	2^{nd}	6^{th}	1^{st}	4^{th}

Figure 2: An example that demonstrates how to generate MSCPS.

Rijndael	Key	K						
	MSCPS	7	5	3	8	2	6	1	4
		↑	↑	↑	↑	↑	↑	↑	↑
	C-MSCPS	21	45 3^{rd}	37 4^{th}	66 1^{st}	12	3	50 2^{nd}	36

Figure 3: An example that demonstrates how to generate C-MSCPS.

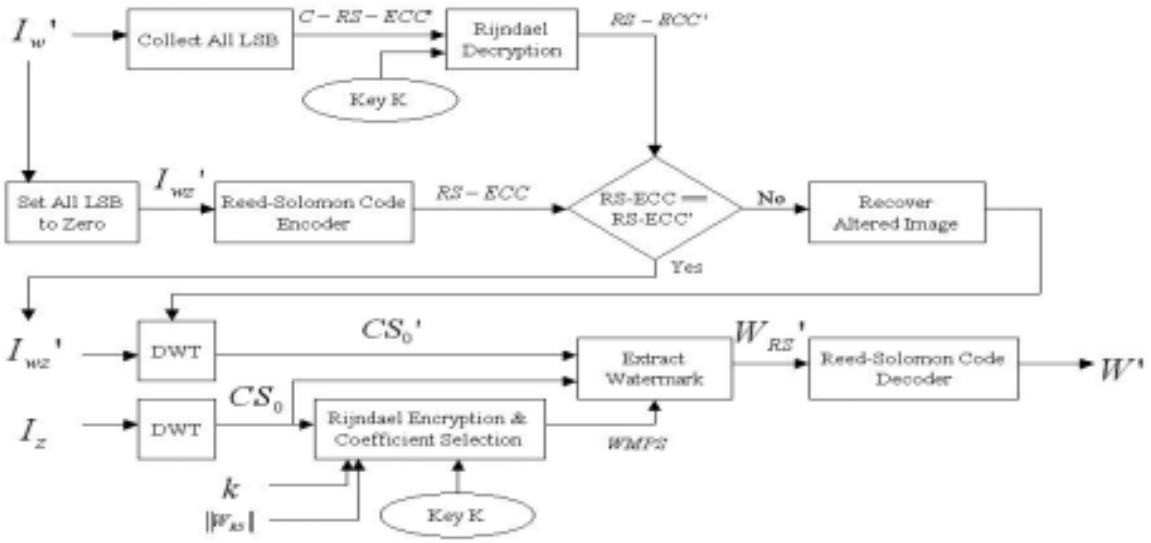

Figure 4: Flowchart for Watermark extraction

(a)

(b) PSNR = 8.527535, Sim = 0.900391

(c) PSNR = 26.734325 Sim = 0.888916

Fig 5 (a) watermarked image without any attacked
(b) Attacked by cropping (c) attacked by sharpening

(d) PSNR = 24.422025 Sim = 0.728271

(e) PSNR = 34.29522 Sim = 0.928223

(f) PSNR = 31.989688 Sim =0.744385

Fig 5 (d) attacked by uniform noise corruption (e) attacked by blurring (f) attacked by JPEG compression