Digital Watermarking Using RC5 Encryption On JPEG2000 Images

Gayathri I. K
M.Tech,Communication Engineering, FISAT

Anil Kumar M. N
Assistant Professor, Electronics and Communication Engineering, FISAT

Abstract

For the rapid revolution in digital multimedia and the ease of creating similar and unauthorized data, the digital data can be copied or manipulated or distributed. So it is necessary to watermark the media content for tamper proofing or quality assessment or copy control. In this paper we propose a digital watermarking using RC5 encryption on JPEG2000 images. The compression standard is chosen such that it provides higher compression ratio and the compressed byte stream are randomized by the encryption algorithm. The proposed encryption algorithm used here is a block cipher. In our paper watermarking was done in the compressed – encrypted domain. We use different watermarking techniques for this. The watermarked data can be detected both in the encrypted and decrypted domain. The PSNR values of three watermarking schemes are also measured.

Keywords

JPEG2000, RC5, watermarking, Compressed Domain, Watermark Extraction, Watermark Embedding, Encrypted Domain, PSNR etc.

1. Introduction

Nowadays, the protection and enforcement of intellectual property rights for digital media is becoming increasingly important. In order to prevent the users from unauthorized copying of digital content and to control its use, digital rights management (DRM) technologies were developed.

DRM uses digital watermarking techniques to prevent consumers from unauthorized copying of digital media and to control the use of digital content.

Digital watermarking is the process of embedding information into digital media content. The embedded information can later be extracted or detected for a variety of purposes including copyright protection, transaction tracking etc. This provides an indication of ownership of the digital data. Digital watermarking can be applied to media like text, audio, image, video etc. The watermark might contain additional information including the identity of the purchaser of a particular copy of the object.

In this paper, we propose a digital watermarking on JPEG2000 images in which the watermark can be embedded in a predictable manner. In [1] A.V. Subramanyam et.al proposed a robust digital watermarking on compressed and encrypted domain.

Watermarking in compressed-encrypted domain saves the computational quality and also preserves the confidentiality of the content. In this proposed algorithm we use three watermarking schemes: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

In this paper we use RC5 block cipher as the encryption algorithm. It is a symmetric block cipher. The main features of RC5 are data - dependent rotations, variable block size, variable number of rounds and variable key size.

This paper is organized as follows. Section II describes the methodology. In section III we discuss the security of encryption algorithm. The experimental results are discussed in section IV and the conclusion of the paper is done in Section V.

2. Methodology

In the proposed scheme the image was compressed by using JPEG2000 compression standard. The JPEG2000 encoder provides a set of features that are of importance to many high end and emerging applications by taking advantage of new technologies. The compression standard is divided into five different stages. The first stage is component and tile separation, whose function is to cut the image into manageable chunks and to decorrelate the color components. Huge original images are separated into spatially non overlapping tiles of equal size and finally a multi-component transform is performed. In the second stage the data are first transformed in the wavelet domain followed by quantization in the third stage. After that, the quantized coefficients are regrouped to facilitate localized spatial and resolution access. These resolutions are further divided into smaller blocks known as code-blocks where each code block is encoded independently. In the fourth stage, each code-block is decomposed into number of bit-planes and are then entropy encoded using fractional bit-plane coding and binary arithmetic coding that provides a stream of compressed data. The compressed byte stream is arranged into different wavelet packets based on resolution, precincts and layers in the final stage.

Thus the compressed byte stream is given to the RC5 encryption algorithm. The RC5 is a symmetric block cipher and it also provides better security.

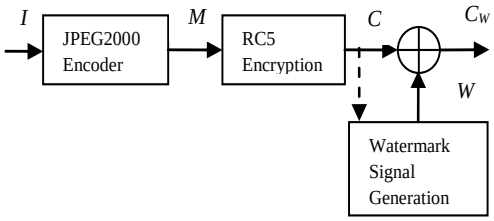


Fig.1 watermark embedding

Fig.1 shows the watermark embedding process. The watermark was embedded in the compressed encrypted domain. For Spread Spectrum watermarking scheme, the watermark signal is generated without using the host signal. In the case of Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM) the watermarked signal is generated using C which is shown as dotted line in the figure.

2.1 RC5 Algorithm

From the compression standard we get packetized byte stream *M* as its output. The message *M* , should be encrypted using RC5 block cipher. Thus we get *C* as the encrypted output. This *C* is fed to the watermarking module for generating the watermarked data.

RC5 algorithm was developed by Ronald Rivest. This algorithm is a block cipher that converts plain text data blocks of 16, 32 and 64 bits into cipher test blocks of same length. It uses a key of selectable length b byte. The key size can range from 0 bits to 2040 bits. In this algorithm a variable number of rounds(r) is used that takes values in the range 0-255, as illustrated in Fig.2

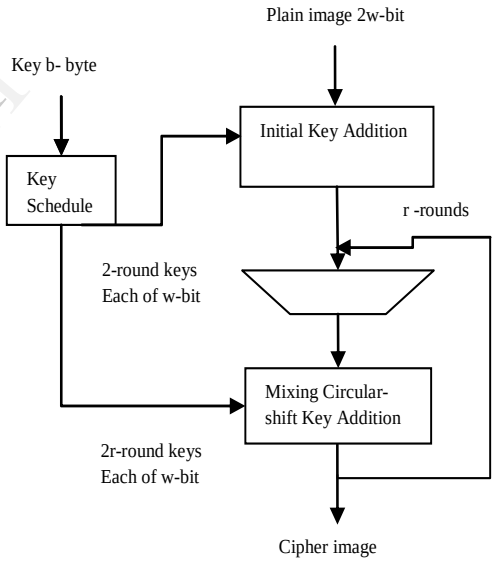


Fig .2 RC5 Encryption Algorithm

The RC5 algorithm uses three primitive operations and their inverses.

(1)Two's complement addition of words, denoted by "+"

(2)Bit-wise exclusive -or(XOR)

(3)A left rotation of words: the cyclic rotation of word x left by y bits is denoted x<<<y. The inverse operation, right rotation is denoted by x>>>y

In the key expansion module, the key K is expanded to a much larger size using an expansion table(S).

The size of the table S is (2r+2), where r is the number of rounds. Before every encryption or decryption processes, the key expansion process should be performed. The encryption process takes a plain text input and produces a cipher text as the output. The reverse operation should be done in the decryption part.

2.1.1 Key Expansion

The key expansion algorithm expands the users secret key to a much larger size using an expansion table(S). The size of the table S is (2r+2). It uses two magic constants and consists of three simple algorithms

Definition of the constants:

The key expansion algorithm uses two word sized binary constants P_w and Q_w. They are defined for arbitrary w as follows

$P_w = Odd((e - 2)2^w)$ →(1)

$Q_w = Odd((\phi - 1)2^w)$ →(2)

where

e=2.718281828…. (base of natural logarithms)

ϕ=1.618033988…. (golden ratio = (1+sqr(5))/2)

Odd(x): odd integer nearest to x

The three algorithms are defined as follows

Step 1: Convert secret key bytes to words

Step 2: Initialize sub key array S (S[0],S[1],…,S(t-1))

Step 3: Mix the secret key into sub key array S

2.1.2 Encryption

The input block is given in two w-bit registers A and B. The output is also placed in the registers A and B. The encryption algorithm is done as follows.

Steps:

i. A=A + S[0]

ii. B=B + S[1]

iii. for i= 1 to r do

$$A = ((A \oplus B) <<< B) + S[2i]$$
$$B = ((B \oplus A) >>> A) + S[2i+1]$$

2.1.3 Decryption

The decryption routine is easily derived from the encryption routine. The decryption is done as follows.

Steps:

i. for i= r down to 1 do

$$B = ((B - S[2i+1]) >>> A) \oplus A$$
$$A = ((A - S[2i]) >>> B) \oplus B$$

ii. B= B - S[1]

iii. A= A- S[0]

2.2 Watermark Embedding Algorithm

The watermark is embedded to the compressed-encrypted domain. The embedding algorithm used here is the additive watermarking technique. The robust additive watermarking technique is the most straightforward method in spatial domain such that the pseudo random noise pattern is added to the intensity of image pixels. For watermark embedding the ciphered bytes from the least significant bit plane of an image were considered. Here we consider the three watermarking techniques and each of one are explained below.

2.2.1 SS

In SS watermarking scheme, a narrow-band signal is transmitted over a much larger bandwidth such that the signal energy presented in any signal frequency is undetectable. In this scheme the embedding process is carried out by first generating the watermark signal W. This W can be generated using information bits b, chip rate r and pseudo noise sequence P ={p_j} where p_j ={1,-1}. The information bits b are spread by r , where b ={1,-1} which gives

$$a_j = b_i, ir \le j < (i+1)r \quad \rightarrow(3)$$

This sequence is multiplied by α > 0 and P, and finally we get the watermark signal W= $\{w_j\}$, where

$$w_j = \alpha a_j p_j \quad \rightarrow(4)$$

The generated watermark signal in (4) is added to the encrypted signal *C*, to give the watermarked signal C_w

$$C_w = C + W = c_i + w_i \quad \text{,for all i= 0,1,…….L-1}$$

→(5)

2.2. 2 SCS-QIM

For SCS-QIM watermarking, the watermark message is encoded into a sequence of watermark letters d, where $d[n] \in \{0,1\}$ .Each of the watermark letters is embedded into the corresponding host elements x[n] . For making the codebook secure a random sequence K can be chosen such that k[n] ϵ (0, 1]. The embedding rule is given by

$$q_n = Q_\Delta(x[n] - \Delta(d[n]/2 + k)) - (x[n] - \Delta(d[n]/2 + k))$$

→(6)

Here $Q_\Delta(.)$ denotes a scalar uniform quantization with step size Δ. This embedding scheme depends on two parameters: the quantizer step size Δ and the scale factor β. The watermark sequence is then given by

$$W = \beta * q_n \quad \rightarrow(7)$$

Finally the watermarked signal is obtained as

$$C_w = C + W \quad \rightarrow(8)$$

2.2.3 RDM

This scheme is based on the quantization of the ratio of host signal to a function.The function is chosen such that the scheme is robust against amplitude scaling attacks and is given by

$$g(c_{wi-1}) = (1/L_m \sum_{j=i-L_m}^{i-1} |c_{wj}|^\gamma)^{1/\gamma}, \gamma \geq 1 \quad \rightarrow(9)$$

The quantizers are given by

$$Q'_\Delta = 2\Delta + w\Delta/2 \quad \rightarrow(10)$$

where *w* ϵ{-1,1} is the watermark information to be embedded in the host element. The embedding rule is then given by

$$c_{wi} = g(c_{wi-1})Q'_\Delta(c_i / g(c_{wi-1})) \quad \rightarrow(11)$$

where c_{wi} and $c_{wi\ -1}$ are the current and previous watermarked samples . Thus the additive nature of watermark is given as

$$w_i = c_{wi} - c_i \quad \rightarrow(12)$$

2.3 Watermark Extraction Algorithm

From the encrypted and decrypted domain the watermark data can be detected. Fig.3 shows the watermark extraction module.

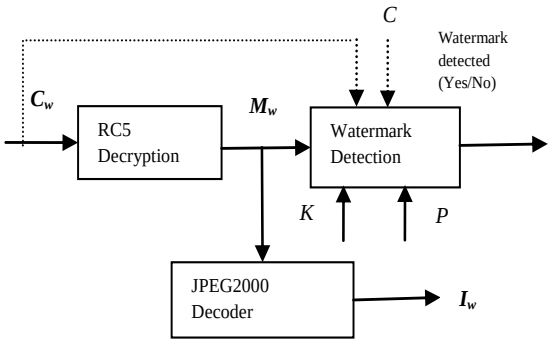


Fig .3 Watermark Extraction

2.3.1 Encrypted Domain Detection

As shown in Fig.3, the C_w is directly fed to the watermark detection module. The watermark detection process is formed using the above three watermarking techniques.

2.3.1.1 SS

In this scheme, the C_w is fed to the watermark detection module and this will be multiplied by pseudo noise sequence and followed by summation over chip rate, yielding the correlation sum S_i . The sign of S_i gives the watermark information bit.

$$S_i = \sum(c_{wj} p_j) = \sum(c_j + w_j) p_j = b_i \sigma_p{}^2 \alpha r$$

→(13)

2.3.1.2 SCS-QIM

In this method, by quantizing the received signal to the nearest data in the codebook, the watermark data is detected. For this purpose we use the equation

$$\hat{w} = Q_\Delta(c_{wi}) - c_{wi} \quad \rightarrow(14)$$

If $\hat{w} = 0$, then watermark bit zero is extracted and if close to $\pm\Delta/2$, then bit one is retrieved.

2.3.1.3 RDM

By using the minimum distance criteria, the detection of watermark is performed by applying the equation

$$\hat{w} = \arg\min_{1,-1}\left(\frac{c_{wi}}{g(c_{wi-1})} - Q'_{\Delta}\left(\frac{c_{wi}}{g(c_{wi-1})} \right) \right)^2 \quad \rightarrow (15)$$

Here Q'_{Δ} gives two quantizers belonging to bits 1 and -1. From this, the minimum distance gives the watermark bit.

2.3.2 Decrypted Domain Detection

In the decrypted domain watermark bit detection, we use the above three watermarking schemes. Here the C_w is fed to the RC5 decryption module. From that we will obtain the M_w as the output. This M_w is encrypted by using the key and will obtain the C_w. For watermark detection remove C from C_w. The above procedure was done in three watermarking schemes and finally the watermarked data can be obtained. Also the decrypted message will be fed to the JPEG2000 encoder and will generate the original image.

3. Results and Discussions

3.1 Security of Encryption Algorithm

The three routines in RC5 are key expansion, encryption and decryption. In the key expansion, the user provided a secret key, which is expanded to fill a key table whose size depends on the number of rounds. Key table is used in both encryption and decryption. RC5 is a symmetric block cipher, which means the same secret key is used for encryption and decryption. It is suitable for hardware and software. It is adaptable to processors of different word lengths. It is simple to implement, fast and require low memory. The number of rounds is an important parameter in RC5. Choosing large number of rounds provides an increased level of security. The security of RC5 block cipher is estimated for digital images, even under brute-force attack, statistical and differential attacks.

For selecting the word size 32 bits, RC5 allows a maximum of 2040 secret key bits and a maximum of 25(2r+2) expandable key table bits. Thus by choosing large values of r and b can prevent exhaustive attacks. In the case of statistical analysis, the histogram of original and encrypted images is taken. From this we can find that the encrypted image is fairly uniform and different from that of the original one.

The watermarked data is added in the compressed encrypted domain. This provides better security than other schemes because the image is first compressed and after that it is encrypted and then only watermark data is added. Thus the watermarked data's are entirely distributed in the lowest bit plane of an image. For this purpose we use additive watermarking technique. Thus at the receiver side any change or modification in the watermarked data can be found out by decrypting the data with the same key. Thus it is robust against most attacks in the digital world and protects the copyright content and prevents its distribution.

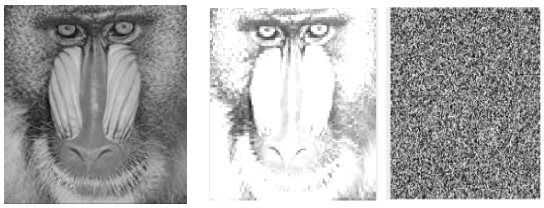
3.2 Experimental Results

The experimental results shall be carried out in the images of baboon, cameraman, boat and goldhill. For this purpose we measure the PSNR of three watermarking schemes. The PSNR is calculated using the following equation.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I(i,j) - I_w(i,j))^2 \quad \rightarrow (16)$$

$$PSNR = 10\log_{10}(255^2 / MSE) \quad \rightarrow (17)$$

The figure shows the image of a baboon. In this first the image was compressed and after that encryption algorithm was applied. Then watermark should be applied with the help of additive watermarking technique. In this process the watermark data should be placed in the least significant bit plane of the image.



(a) (b) (c)

(d)

Fig.4. (a) original image, (b) compressed image, (c)encrypted image and

The performance analysis was done by measuring the PSNR values of various images. From this analysis we observe that the RDM has better PSNR value. In the compressed domain SS technique use the non-blind detection method while other two methods use the blind detection method for estimating the watermarked data. In the decompressed domain all the three techniques use the non-blind detection method. The table I shows the PSNR values of all the three methods in different images.

Table I. PSNR measurements of SS, SCS-QIM

IMAGES / SCHEMES	CAMERAMAN	BABOON	GOLDHILL	BOAT
1)SPREAD SPECTRUM	42.1107	40.4238	41.4744	41.6915
2)SCS-QIM	47.4697	45.7847	46.7699	47.0027
3)RDM	48.1312	46.444	47.4582	47.7478

4. CONCLUSION

In this paper we proposed a digital watermarking on JPEG2000 compressed encrypted images. For the watermark embedding we use three watermarking techniques. The additive watermarking technique is used here. In this technique we embed the watermark in the least significant bit plane of an image. The watermark in the compressed encrypted domain provides the unauthorized distribution of digital data and also provides security. The RC5 used here is one of the major encryption schemes in cryptography and it also preserves the confidentiality of the content. The security of RC5 is also discussed. We analyze the PSNR values of each scheme and found that RDM provides better PSNR values than other schemes. Thus by analysis, the digital distribution of data becomes easier and it also protect the copyright of the digital content. The application area consists of broadcast monitoring, owner identification, transaction tracking, copy control etc.

The future scope aims at extending the proposed work to other compression standard like JPEG-LS. JPEG-LS is significantly less complex than JPEG2000. It is reasonable to use JPEG-LS for lossless compression.

5. REFERENCES

[1] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Trans. on Multimedia, vol.14,no.3*, June 2012.

[2] M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," *Signal Process: Image Commun.*, vol .17, no.4,pp.469-472. .

[3] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no.2.

[4] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems," *International Journal of Information and Communication Engineering*, 3:8, pp. 537-542.

[5] S. Hwang, K. Yoon, K. Jun, and K. Lee, "Modeling and implementation of digital rights," *J. Syst. Softw.* , vol. 73, no.3, pp. 533-549, 2004.

[6] F. Hartung, J. Su, and B. Girod, "Spread Spectrum watermarking: Malicious attacks and counterattacks," *Security and Watermarking of Multimedia Contents*, pp. 147-158.

[7] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Trans. Signal Process*., vol. 51, no.4, pp. 1003-1019, Apr.2003

[8] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrado, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," *IEEE Trans.Signal Process.*, vol. 53, no. 10, Oct.2005.

[9] B. Schneier, Applied Cryptography. New York: Wiley , 1996.

[10] Omar Elkeelany, Adegoke Olabisi, "Performance comparisons, design and implementation of RC5 symmetric encryption core using reconfigurable hardware," *Journal of Computers, vol.3*, no. 3. Mar.2008.

[11] D. Engel, T. Stutz, and A. Uhl, "A survey on JPEG2000 encryption," *Multimedia Syst*., vol. 15, no. 4, pp. 243-270, 2009.

[12] W. Stallings, "Cryptography and Network Security: principles and practices," *Prentice-Hall*, New Jersey,1999.