IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Watermarking of Encrypted Image using RC5 for DRM System

Dhatri Verma[1], Yogesh Rathore[2]

M. Tech. Scholar, Computer Science and Engineering, Raipur Institute of Technology, Raipur, India[1]

Asst. Professor, Computer Science and Engineering, Raipur Institute of Technology, Raipur, India[2]

Abstract: Digital image security is an important issue in internet and network application. Digital images are distributed in encrypted format and watermarking of these images for authentication and copyright protection. We need media authentication in encrypted domain to enhance security. So sometime necessary to watermarking in encrypted media for copyright management and authentication. In this paper we use block cipher called RC5 encryption algorithm to encrypt image which gives minimum correlation coefficient and maximum throughput among all block cipher. We use LSB method to watermark the image. In this method we embed watermark in encrypted image and extraction of watermark in decrypted domain.

Keywords: Encryption, watermarking, RC5 encryption algorithm, block cipher, LSB method.

I. INTRODUCTION

Many copyright holders, hardware manufacturers uses digital right management (DRM) access control technology which limit the use of digital content after sale. DRM restrict the use of digital media that are not desired by content provider. Digital media are handled in encrypted format. Therefore sometime we need to watermark in encrypted domain for ownership declaration, temper detection or copyright management purposes. Encryption is the technique that converts the original image into another image that is difficult to understand. Digital watermarking is the act of hiding a message (i.e. an image, song, and video) within the signal.

In [1]-[3] DRM system is represented where multimedia content is distributed in encrypted format by the owner of the content. In [4] joint digital watermarking and encryption are done in MSB plane and watermarking is done on remaining bit plane. Drawback of this method is we need to decide encryption bit plane priori and rest of the bit plane are in plain text format. In [5] commutative encryption and watermarking scheme is presented. In this scheme image is firstly watermarked then encrypted. But our scheme is image is firstly encrypted and then watermarked. In [6] content dependent watermarking scheme is presented. In this scheme watermark is in encrypted format but the original signal is in the plain text format. In [8] A. V. Subramanyam presented Robust watermarking of compressed and encrypted JPEG2000 images. But this scheme is only applicable for JPEG2000 compressed image. Here the watermark embedding position plays a crucial role in deciding the watermarked image quality and only additive homomorphic encryption algorithm can be used.

In our scheme watermark is embedded in encrypted domain and extraction of watermark is in encrypted domain as well as decrypted domain. In section 2 methodology we are describing proposed methodology to be used.

In section 3 we are showing output of the algorithm, comparing encryption quality and watermark quality. In section 4 conclusions is given in which discussion about the result.

II. METHODOLOGY

Figure1 represents the overall block diagram of the proposed technique. The input image to be transmitted is divided into wavelet sub-bands using 1-level dwt decomposition. We encrypt LL sub band by RC5 encryption algorithm and embed binary watermark in LH sub-band by using LSB method. Inverse DWT is used to obtain the Encrypted-Watermarked image which is to be transmitted at the sender side. At the receiver side, watermark recovery and decryption is performed in LL sub-bands and LH sub-band respectively.

A. RC5 Encryption

The input image to be transmitted is first divided into wavelet sub-bands. We choose LL band for encryption since the largest part of the image energy is concentrated at lower frequency sub- bands.

The RC5 algorithm is represented as RC5-w/r/b where r=number of rounds, w=word size in bits, b=number of 8-bit byte in the key.RC5-32/12/16 encryption algorithm is used to encrypt the LL sub-band. To reduce the computation time, particular region of the input image can be selected encryption without doing it for whole image.

RC5 uses following parameters

- A variable block size (w). Block size may be 32, 64, and 128 bits.
- A variable key size (k). Key size can range from 0 bits to 2040 bits in size.
- A variable number of rounds (r). The number of rounds can range from 0 to 255

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

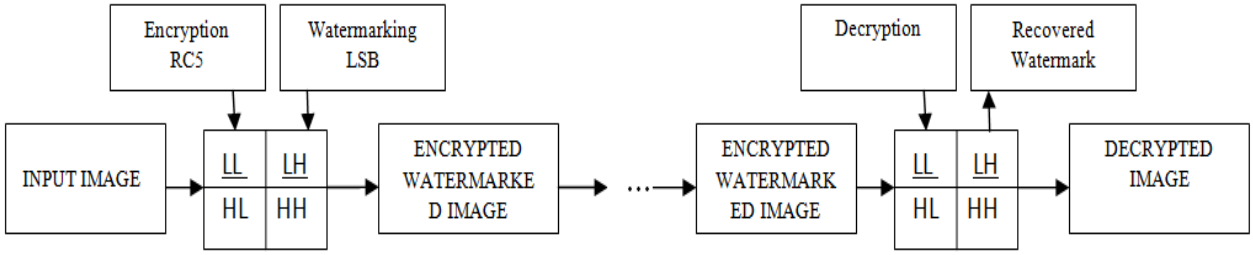


Figure 1: block diagram of encryption, decryption and watermarking Process at sender and receiver side

RC5 has three modules:

1-key-expansion,
2-Encryption
3- Decryption units

The choice of r affects both security and encryption speed. The more number of rounds will increase the security but somehow slower down the encryption speed.

The RC5 algorithm uses three operations and their inverses.

(1) XOR denotes bit-wise exclusive-or.

(2) Addition/subtraction of words modulo 2^w, where w is the word size.

(3) Rotation: the rotation of word p left by q bits is denoted by p<<<q.The inverse operation is the rotation of word p right by q bits, denoted by p>>>q

1) Key Expansion:

In this module, the password key k is expanded. For this expansion table (t) is used. The size of table t is 2(r+1), where r denotes the number of rounds. The key-expansion process must be performed before encryption or decryption processes..

2) Encryption Algorithm:

The two w-bit words inputs are denoted as M and N.

M = M + S[0];

N = N + S[1];

for i = 1 to r do

M = ((M ⊕N) <<< N) + S[2 * i];

N = ((N ⊕M) <<< M) + S[2 * i + 1];

3) Decryption Algorithm:

Decryption is done at receiver side for the same sub-band which is used for encryption. RC5 is a symmetric cipher, so encryption and decryption key are same.

The decryption algorithm is the reverse of encryption algorithm. The two w-bit word inputs are denoted as M and N.

for i = r down to 1 do

N = ((N –S[2 * i + 1]) >>> M) ⊕M;

M = ((M –S[2 * i] >>> N) ⊕N;

N = N -S[1];

M = M -S[0];

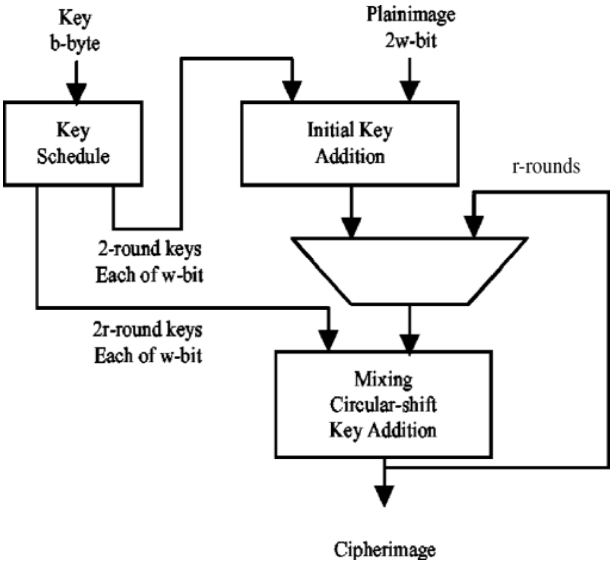


Figure 2: RC5 encryption

B. Watermarking (LSB Method)

The digital watermarking system fundamentally consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark image onto the cover image and the watermark detector detects the presence of watermark image.

1) Watermark embedding:

The largest part of the image energy is concentrated at the lower frequency sub-band .Therefore embedding watermarks in these sub-bands may corrupt the image a lot. Also, changing the high frequency sub-band HH is not sensitive to human eye. So, many DWT based watermarking algorithm uses middle frequency sub-band HL and HL for embedding the watermark where acceptable performance of imperceptibility and robustness could be achieved. In proposed scheme, for embedding the watermark first step is to choose the high frequency sub-bands which is most sensitive to human visual system i.e. LH sub-band and second step is to apply LSB watermarking in LH sub-band. The Watermarking technique LSB (Least Significant Bit) substitution digital watermarking is invisible watermarking technique in which we embed information which is not visible. In digital watermarking, the watermark bits are spread in the image in such a way that they cannot be recognized and show toughness against attempts to remove the hidden data. In a digital image, information can be inserted directly into every bit of cover image or the more busy

DOI 10.17148/IJARCCE.2015.41112

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

areas of an image. We insert information into every bit of cover image.

Example of least significant bit watermarking :-

Image:
10001010 01110100 00011011 01000001 ...

Watermark:
1 0 0 1 ...

Watermarked Image:
10001011 01110100 00011010 01000001…

2) Watermark Extraction :

The extraction of watermarking process will be reverse of embedding. We retrieve watermark bit by extracting LSB of watermarked image.

Algorithm for LSB (n bit):-

1: For each pixel in image.

2: Converting the image pixel into binary.

3: Selection of the last n bits from the binary converted code and replacing it with the secret image binary sequence.

4: End.

III. RESULT

In this section, we present experimental results after encryption and watermark embedding on transmitter side and watermark extraction and decryption on receiver side for various standard test images.

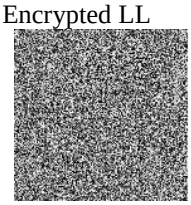
A. Encryption

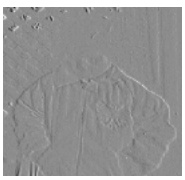
At the transmitter side, the original image is encrypted using RC5-32/12/16 block cipher. It uses 32 bit word size, 16 byte key and 12 rounds for encryption. Here LL sub-band is chosen for encryption to improve the overall security of the image as shown in Figure 3.

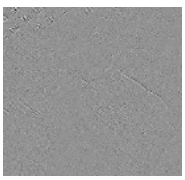
(a)original image

(b) Original Watermark

Encrypted LL Watermarked LH

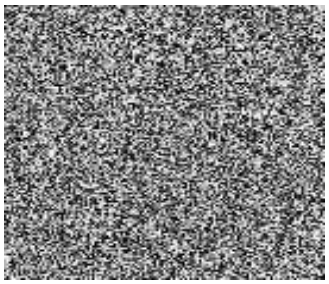






HL HH

(c) Encrypting(LL) & Watermarking(LH)



(d) Encrypted watermarked image

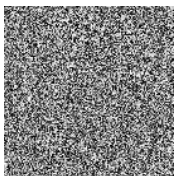
Figure 3. Encryption: (a) Input Image (b) Original Watermark c) Encrypting(LL) & Watermarking(LH) (d) Encrypted watermarked image

B. Watermark Embedding

We embed binary watermark into the incoming image which is greater in size than the size of watermark. We encrypted low frequency sub-band LL and watermarking is to be done in middle frequency sub-bands which gives robustness. The input image is divided into 4-subbands LL, LH, HL, and HH using 1-level Haar Wavelet transform and watermark is inserted using LSB(least significant bit) algorithm in LH sub-bands to improve robustness as shown in Figure 3.

C. Watermark Extraction

At receiver side, watermark is recovered from LH sub-band by retrieving LSB of LH sub-band. Watermark extraction in encrypted domain is shown in figure 4.



(a)encrypted watermarked image

(b) extracted watermark

Figure 4: watermark extraction in encrypted domain

D. Decryption

Decryption is at the receiver side from LL sub-band because encryption is done in LL sub-band. Decrypted image and watermark extraction in decrypted domain is shown in figure 5.

(a) Decrypted image

(b) extracted watermark

Figure 5: watermark extraction in decrypted domain

E. PSNR Calculation

PSNR (Peak Signal-to-Noise Ratio) is the ratio between maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [12].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

PSNR between original watermark and retrieved watermark at receiver side is calculated as 48.18. Imperceptibility of watermarked image are analyzed by calculating PSNR values between original and watermarked image by considering various test images as shown in Table I

Table I: PSNR between Original and Watermarked image

IMAGE	PSNR(db) Value
Peppers.png	42.20
Lena.bmp	42.31
Cameraman.tif	41.82
Rice.png	41.90
Circuit.tif	45.06
Pout.tif	50.06
Coins.png	42.43

Imperceptibility of overall encrypted-watermarked image is analyzed by calculating PSNR between original and encrypted watermarked image as shown in Table II. Less PSNR values indicates that encryption quality is good enough to protect the transmitted images.

Table II: PSNR between Original and Encrypted-Watermarked images

IMAGE	PSNR(db) Value
Peppers.png	8.30
Lena.bmp	9.43
Cameraman.tif	8.55
Rice.png	9.36
Circuit.tif	8.10
Pout.tif	10.07
Coins.png	8.05

PSNR between original and decrypted images is shown in Table III. More PSNR shows that decryption quality is good that means original image and decrypted image is almost same. Decryption is almost perfect because we have high Peak Signal-to-Noise ratio.

Table III: PSNR between Original and Decrypted image

IMAGE	PSNR(db) Value
Peppers.png	42.17
Lena.bmp	42.28
Cameraman.tif	41.80
Rice.png	41.87
Circuit.tif	45.01
Pout.tif	49.92
Coins.png	42.41

F. Information Entropy Analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [11]. Modern information theory is concerned with error correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy H(m) of a source m , we have:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad \text{bits}.....(1)$$

Where $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, $m = \{m_1, m_2, ..., m_2{}^8\}$.

After evaluating Eq. (1), we obtain its entropy H(m) = 8 , corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Let us consider the ciphertext of image encryption using the RC5, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed.

The entropy is shown in Table IV. The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

Table IV: Entropy Calculation For Encrypted Image

IMAGE	ENTROPY
Pepper.png	7.68
Lena.bmp	7.73
Cameraman.tif	7.73
Rice.png	7.70
Circuit.tif	7.70
Pout.tif	7.68
Coins.png	7.65

IV. CONCLUSION

In this paper, watermarking algorithm is proposed to insert the watermark in encrypted image. RC5 algorithm improves the security of system even though it is symmetric .RC5 encryption algorithm has minimum correlation coefficient among all symmetric block cipher. We can improve security of this algorithm simply by increasing rounds into it at the cost of increase in computation time. Since encryption is combined with watermarking the proposed method provides the confidentiality of content. Decryption after watermark extraction was done which is very challenging since the embedded watermark could change the pixel values. Experimental results for decryption after watermarking gives good results.

Future work

We can use more than one sub-band for encryption to improve security. Watermark capacity usually depends on both size of watermark and size of the image. We can increase capacity of watermark by embedding different watermarks in both HL and LH sub-bands

DOI 10.17148/IJARCCE.2015.41112

REFERENCES

[1] S**.O. Hwang**, K.S. Yoon, K.P. Jun, and K.H. Lee, "Modeling and implementation of digital rights,"The Journal of Systems & Software vol. 73, no. 3, pp. 533–549, 2004.

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preserving multiparty multilevel drm architecture," in6th IEEE Consumer Communications and Networking Conference,Workshop on Digital Rights Management, 2009., 2009, pp. 1–5

[3] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli,"Joint watermarking scheme for multiparty multilevel DRM architecture,"IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 758–767,Dec. 2009.

[4] M. Cancellaro, F. Battisti, M. Carli, G. Boato, FGB De Natale, and A. Neri, "A joint digital watermarking and encryption method," in Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Edited by Delp, Edward J., IIIWong, Ping Wah; Dittmann, Jana; Memon, Nasir D. Proceedings of the SPIE, 2008, vol. 6819, pp. 68191C–68191C.

[5] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data,"Optical Engineering,vol. 45, pp. 080510.1–080510.3, 2006

[6] Z. Li, X. Zhu, Y. Lian, and Q. Sun, "Constructing Secure Content-Dependent Watermarking Scheme using Homomorphic Encryption," in IEEE International Conference on Multimedia and Expo, pp. 627–630, 2007.

[7] Q. Sun, S.F. Chang, M. Kurato, and M. Suto, "A quantitive semi-fragile JPEG2000 image authentication system," in Proc. of In-ternational Conference on Image Processing (ICIP02), 2002

[8]. A. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images", IEEE Transactions on Multimedia, Vol. 14, no. 3,pp. 703-716,June 2012

[9] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems"World Academy of Science, Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:8, 2007

[10] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video,"Signal Process., vol. 66, no. 3, pp. 283–301, 1998

[11] Shannon, C. E. (1949). Communication theory of secrecy system. Bell System Technical Journal, 28, 656–715.

[12] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

BIOGRAPHIES

Dhatri Verma received the B.E. degree in computer science and engineering from government engineering college Raipur (c.g.), in 2008. She is a M. Tech. scholar in department of Computer Science and Engineering, Raipur Institute of Technology, Raipur (c.g.) . Her area of interest include digital image encryption and watermarking.

Yogesh Rathore is a lecturer in department of Computer Science and Engineering, Raipur Institute of Technology, Raipur (c.g.) . His area of interest include Digital image processing & Computer Graphics.

DOI 10.17148/IJARCCE.2015.41112