IOSR Journal of Electronics & Communication Engineering (IOSR-JECE)
ISSN(e) : 2278-1684 ISSN(p) : 2320-334X, PP 29-40
www.iosrjournals.org

WATERMARKING OF COMPRESSED AND ENCRYPTED JPEG 2000 IMAGES

Deepika.R[1], Dhanya.S[2]
[1](ECE, Toc-H Institute of Science and Technology,Arakkunnam/ CUSAT, INDIA)
[2](ECE, Toc-H Institute of Science and Technology,Arakkunnam/ CUSAT, INDIA)

ABSTRACT : *In digital rights management (DRM) systems [1]-[4], digital media is often distributed by multiple levels of distributors in a compressed and encrypted format. So it become necessary for distributors to watermark these compressed encrypted media items in the compressed-encrypted domain itself for tamper detection, ownership declaration and for copyright management purposes. But it is a challenge to watermark these compressed encrypted streams as the compression process would pack the raw media into a lower number of bits and encryption would have randomized the compressed bit stream. Hence attempting to watermark such a randomized bit stream can cause degradation of the media quality. Thus it is necessary to choose an encryption scheme that is both secure and will allow watermarking in a predictable manner in the compressed encrypted domain. This paper proposes a watermarking algorithm to watermark JPEG2000 compressed and encrypted images. The encryption algorithm used is RC4 stream cipher. Here the proposed algorithm embeds watermark in the compressed-encrypted domain and the extraction of watermark is done in the decrypted domain*

Keywords - *Compression, DRM Systems, Encryption, JPEG2000, Watermarking*

I. INTRODUCTION

Digital watermarking is the process of embedding information into digital multimedia content such that the information which we call the watermark can later be extracted or detected for a variety of purposes including copy prevention and control. A digital watermark can be visible or invisible. A visible watermark typically consists of a visible message or a company logo indicating the ownership of the image. On the other hand, an invisibly watermarked image appears very similar to the original. The existence of an invisible watermark can only be determined using an appropriate watermark extraction or detection algorithm. This paper deals with a watermarking algorithm to watermark compressed and encrypted JPEG 2000 images.The performance of this watermarking algorithm is evaluated by investigating the watermarked image quality using these watermarking schemes: Spread Spectrum (SS) and Scalar Costa Scheme Quantization Index Modulation (SCS-QIM). This paper is structured in such a way that, introduction section followed by section 2 describes challenges in the Compressed Encrypted domain Watermarking, Section 3 describes proposed watermarking algorithm, and Section 4 deals with performance evaluation of watermarking algorithm using two existing watermarking techniques: Spread Spectrum and Scalar Costas Scheme Quantization Index Modulation.

II. CHALLENGES IN THE PROPOSED TECHNIQUE

1. Compressed Domain Watermarking

A small modification in the compressed data may lead to a significant deterioration in the quality of decoded image. Therefore the position for watermark embedding has to be carefully identified in the compressed data, so that the degradation in the perceptual quality of image is minimum. Hence LSB embedding is done here i.e. watermark is embedded in the LSB of ciphered bytes.

2. Encrypted Domain Watermarking and Watermark Retrieval

In an encrypted data, changing even a single bit may lead to a random decryption; therefore the encryption scheme chosen should be such a way that the distortion due to embedding should be controlled to maintain the

image quality. It should also be possible to detect the watermark correctly even after the content is decrypted. Also, the compression gain should not be lost as encryption may lead to cipher text expansion. There is a tradeoff between security-compression efficiency-payload capacity, which poses a challenge for deciding which cipher scheme to apply Symmetric ciphers with homomorphic property can be applied on a smaller message size, like a byte, without increasing the compressed data size and can achieve a better payload capacity than asymmetric counterparts. There is a tradeoff between security-compression efficiency-payload capacity, which poses a challenge for deciding which cipher scheme to apply. Therefore we use RC4 stream cipher with homomorphic property.

III PROPOSED WATERMARKING ALGORITHM

In the proposed algorithm watermark is embedded on the compressed encrypted image and extraction of watermark is done from both encrypted and decrypted images.The proposed watermarking algorithm has got two stages: Watermark Embedding and Watermark Extraction.

3.1)Watermark Embedding

In the proposed watermarking algorithm we are embedding watermark on the compressed-encrypted image. For embedding the watermark first image is compressed, then it is encrypted and finally the watermark signal generated is added to the image

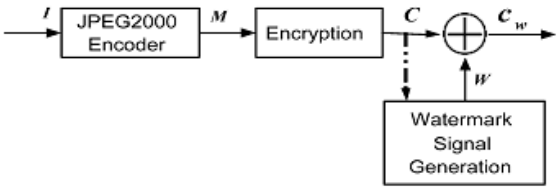


Fig 1 WATERMARK EMBEDDING

Three steps are there in Watermark Embedding

3.1.1) ***Compression***

The compression scheme used here is JPEG 2000. JPEG 2000[11] is a new compression standard for still images intended to overcome the shortcomings of the existing JPEG standard. JPEG2000 makes use of wavelet and sub band technologies. This standard is commonly used in Internet, digital photography, remote sensing, mobile, digital libraries and E-commerce.

JPEG 2000 Compression is divided into five different stages

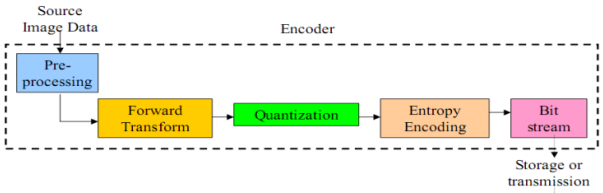


Fig2- JPEG 2000 Encoder

1.Pre-Processing

In the first stage the input image is preprocessed by dividing it into non-overlapping rectangular tiles, the unsigned samples are then reduced by a constant to make it symmetric around zero and finally a multi-component transform is performed from RGB to YCbCr format.

2.Forward transform

In JPEG 2000 Discrete Wavelet Transform (DWT) is used to decompose each tile component into different sub-bands. The transform is in the form of dyadic decomposition and use biorthogonal wavelets. Multiple levels of DWT give a multi-resolution image. The lowest resolution contains the low-pass image while the higher resolution contains the high-pass image.

3.Quantization

After transformation, all coefficients are quantized using scalar quantization. Quantization reduces coefficients in precision. Quantization, involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible.

Quantization process is done by following formula:

$$q_b(u,v) - sign\left(a_b(u,v)\right)\frac{\|a_b(u,v)\|}{\Delta_b} \qquad (1)$$

$q_b(u,v) - Quantized\ value$

$a_b(u,v) - Transform\ coefficcient\ of\ sub - band\ b$b

$\Delta_b \quad - Quantization\ StepSize$

4.Entropy Encoding

Entropy encoding is a lossless data compression scheme that is independent of the specific characteristics of the medium. One of the main types of entropy coding creates and assigns a unique prefix-free code to each unique symbol that occurs in the input. These entropy encoders then compress data by replacing each fixed-length input symbol with the corresponding variable-length prefix-free output codeword.

In JPEG 2000 Huffman Encoding is used for encoding the quantized coefficients. Huffman coding is based on the frequency of occurrence of pixel in images. The principle is to use a lower number of bits to encode the data that occurs more frequently and larger number of bits to encode data that occur less frequently.

This compressed byte stream is arranged into different wavelet packets based on resolution, precincts, components and layers in the fifth and final stage. Thus, it is possible to select bytes generated from different bit planes of different resolutions for encryption and watermarking.

3.1.2) Encryption

A secure symmetric stream cipher with homomorphic property is used for encryption here. It is mainly due to the following two reasons. Symmetric ciphers with homomorphism can be applied on a smaller message size, like a byte, without increasing the compressed data size and achieving a better payload capacity than asymmetric counterparts. So there is a tradeoff between security-compression efficiency-payload capacity, which poses a challenge for deciding which cipher scheme to apply. Therefore we use the RC4 stream cipher [10] with homomorphism property.

Here the encryption algorithm used is RC4 stream cipher. RC4 is used in a number of applications currently. One of its most important uses is in Secure Sockets Layer (SSL), which is used to secure most of the world's electronic commerce over the World Wide Web. It is also used in WEP, the IEEE 802.11 wireless networking security standard. It is also used in other applications like email encryption products.

RC4 is a binary additive stream cipher. It uses a variable sized key that can range between 8 and 2048 bits in multiples of 8 bits (1 byte). Since it is a stream cipher Byte by Byte encryption is done.

RC4 algorithm has got 2 stages

- **Key scheduling algorithm**
- **Key stream generation algorithm**

3.1.2.1)Key Scheduling Algorithm

The major part of the algorithm is the initialization function, n which accepts a key of variable size and uses it to create the initial state of the key stream generator. This is known as the key schedule algorithm. RC4 is actually a class of algorithms parameterized on the size of its block. This parameter, n, is the word size for the algorithm. This is recommended n = 8, but for analysis purposes it can be convenient to reduce this. Also, for extra security it is possible to increase this value. So in this project we have chosen n=8. The internal state of RC4 consists of a table of size 2n words and two word sized counters. The table is known as the S-box, and will be known as S. It always contains a permutation of the possible 2n values of a word. The two counters are known as i and j.

The Key Schedule Algorithm of RC4 is shown below. It accepts as input the key stored in K, and is l bytes long. It starts with the identity permutation in S and, using the key, continually swapping value to produce a new unknown key-dependent permutation. Since the only action on S is to swap two values, the fact that S contains a permutation is always maintained.

Initialization:

For i = 0 to 2^n - 1

S[i] = i

j = 0

Scrambling:

For i = 0 to 2^n - 1

j = j + S[i] + K [i mod l]

Swap(S[i]; S[j])

3.1.2.2)Key Stream Generation Algorithm

The RC4 key stream generator algorithm is shown below. It works by continually shuffling the permutation stored in S as time goes on, each time picking a different value from the S permutation as output. One round of RC4 outputs an n bit word as key stream, which can then be XOR'ed with the plaintext to produce the cipher text.

Initialization:

i = 0

j = 0

Generation Loop:

i = i + 1

j = j + S[i]

Swap(S[i]; S[j])

Output z = S[S[i] + S[j]]

WATERMARKING OF COMPRESSED AND ENCRYPTED JPEG 2000 IMAGES

After JPEG2000 compression we get packetized byte stream as its output. In order to encrypt the message, we choose, a randomly generated key-stream using RC4. Then the encryption is done byte by byte as given in following equation to get the ciphered signal.

$$C = E(M, K) = c_i$$

$$= (m_i + k_i) mod\ 255\ \forall i = 0,1, \ldots L - 1 \qquad (2)$$

The watermarking technique used is an additive one, so the encryption algorithm must have privacy homomorphism property with addition. The privacy homomorphism property will make it possible to detect the watermark from the decrypted content and also help us to control the watermarked image quality easily.

Additive homomorphic property of RC4 Stream cipher,

$$C_1 = E(M_1, K_1)\ and\ C_2 = E(M_2, K_2)$$

Additive homomorphic property gives,

$$D(C_1 + C_2, K) = M_1 + M_2$$

3.1.3) Watermark Signal Generation

Distributors in the distribution chain are given the compressed encrypted byte stream, C to distribute. They do not have access to the original image. So distributors need to watermark C, to prove their distributorship to the recipient or copyright violation detection purposes.

The encryption algorithm used is an additive privacy homomorphic one, so the watermark embedding is performed by using a robust additive watermarking technique. Since the embedding is done in the compressed ciphered byte stream, the embedding position plays a crucial role in deciding the watermarked image quality. Hence, for watermarking, we consider the ciphered bytes from the less significant bit planes of the middle resolutions, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent.

In this paper we are generating the watermark signal that is to be embedded into message using two methods: Spread Spectrum [12] and Scalar Costas Scheme Quantization Index Modulation [13].

3.1.3.1. Spread Spectrum (SS)

In Spread spectrum Communication the transmitted signal is spread over a wide frequency band so that signal energy present in any one frequency bin is essentially small and is undetectable. Similar principle is used here. In Spread Spectrum Watermarking watermark signal is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable.

In Spread spectrum watermarking scheme, the embedding process is carried out by first generating the watermark signal W, by using watermark information bits b, chip rate r, and PN sequence P.

Watermark signal generation: The watermark information bits, $b= \{b_i\}$, where bi ε {-1, 1} are spread by chip rate r. This gives a new sequence a_j, where

$a_j = b_i, \quad ir \leq j \leq (i+1)r$

This spread sequence is then modulated with a binary pseudo-random sequence p_j, p_j ε {-1,1} and amplified by a factor α, yielding the watermark sequence w_j.

Watermark sequence, $w_j = \alpha a_j p_j$

where α-amplificationfactor,0<α<3

This watermark signal generated in is added to the encrypted signal C, to give the watermarked signal Cw. Here LSB embedding is done that is to the LSB's of ciphered bytes watermark is added.

$$C_w = C + W = c_{wi} + w_i \forall i = 0,1, \ldots L-1, \quad (3)$$

3.1.3.2. ***Scalar Costas Scheme-Quantization Index Modulation***

This is a quantization based watermarking technique. In this scheme watermark strength β will be given. Then depending upon the watermark information bit w ε {0, 1} we have to choose a quantizer. The quantizer can be chosen as,

$$U = (l + k_{qim})\beta\Delta + \frac{w\Delta\beta}{2} \quad (4)$$

Where w introduces a shift in the quantizer and l gives the different sets of quantizers. For making the codebook secure

a random sequence Kqim can be chosen.

This embedding scheme is then,

$$q_i = Q_\Delta\left(c_i - \Delta\left(\frac{w_i}{2} + k_{qimi}\right)\right) - \left(c_i - \Delta\left(\frac{w_i}{2} + k_{qimi}\right)\right) \quad (5)$$

Where Q_Δ denotes scalar uniform quantization with stepsize Δ,

The watermark sequence is then given by,

$$W = \beta q$$

Here also LSB embedding is done that is to the LSB's of ciphered bytes watermark is added.

$$C_w = C + W = c_{wi} = c_i + w_i \forall i = 0,1, \ldots L-1$$

The power of quantization error is given as $Exp(q^2) = \Delta^2/12$, considering a uniform distribution for q. So for a given watermark power σ_w^2,

Watermark signal strength,

$$\beta = \sqrt{\frac{\sigma_w^2}{\mathrm{Exp}(q^2)}} = \sqrt{\frac{12\sigma_w^2}{\Delta^2}}. \quad (6)$$

3.2. Watermark Extraction

The watermark detection is done in decrypted domain.

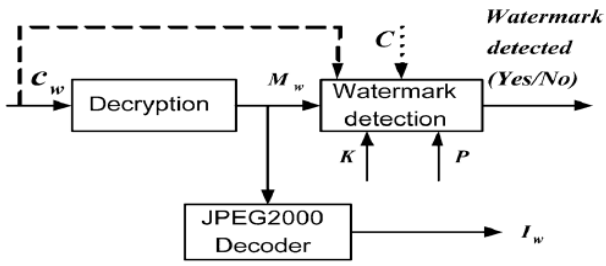


Fig 3 – Watermark Extraction

3.2.1Decrypted Domain Detection

The received compressed encrypted watermarked image is first passed through the decryption module, and is decrypted using equation given below, which defines the corresponding byte by byte decryption for the encryption. Here the same key stream K that is used for encryption is generated for decryption.

The received signal C_W is decrypted to give M_w as,

$$M_w = D(C_w + k_i) mod 255 \; \forall i = 0,1,..L-1$$

$$= (c_i + w_i + k_i) mod 255$$

$$= m_i + w_i = m_{wi} \qquad (7)$$

3.2.1.1 Spread Spectrum Detection

For Spread Spectrum detection, the embedded watermark information W can be estimated from M_w using correlation detector even without the knowledge of the corresponding originals M or C. However, M and P may not always be uncorrelated and hence the noise due to M may not be completely eliminated. Therefore to obtain better detection results, we can encrypt M_w with K which gives C_w and removing C gives,

$$S_i = \sum_r (w_j p_j) = \sum_r \alpha a_j p_j p_j = b_i \sigma_p^2 \alpha r. \qquad (8)$$

Thus, the sign of S_i gives the watermark information bit,

$$\text{sign}(S_i) = \text{sign}\left(b_i \sigma_p^2 \alpha r\right) = \text{sign}(b_i) = b_i \qquad (9)$$

3.2.1.2) Scalar Costas Scheme-Quantization Index Modulation Detection

In SCS-QIM, the decrypted message along with cipher key K is fed to the watermark extraction module. The signal is encrypted with the key to get the ciphered watermarked signal C_w and the watermark is detected using the following equation,

$$\hat{w} = Q_{\Delta}\left(c_{w_i}\right) - c_{w_i} \quad \forall i = 0, 1, \ldots, L-1. \tag{10}$$

If $\tilde{w}$ is close to zero, then watermark bit 0 is extracted and if close to $\Delta/2$, then watermark bit 1 is retrieved.

IV PERFORMANCE EVALUATION

The performance of the watermarking algorithm is evaluated by determining the watermarked image quality. The watermarked image quality is determined by a parameter called Peak signal to noise ratio (PSNR).

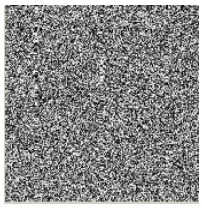
For simulation gray scale image of dimension 256*256 is used

(a)

Original image

(b)

Encoded Image



(c)

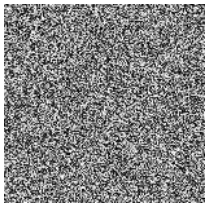
Encrypted Image

1)Watermark Embedding

a) Using Spread Spectrum technique

(c)

Original image with watermark



(d)

Encrypted image with Watermark

b) Using Scs-qim technique

(e)

Original image with watermark

(f)

Encrypted image with *watermark*

2)Watermark Extraction

a) In Spread Spectrum technique

(g)

Decrypted Image

(h)

Unwatermarked Decompressed Image(PSNR=47.08dB)

b) In Scs-qim technique

(i)

Decrypted Image

(j)

Unwatermarked Decompressed Image(PSNR=45.8dB)

In case of Spread Spectrum watermarking, non-blind detection technique (requires original image to extract watermark) is used while in case of SCS-QIM watermarking blind detection technique (does not require original image) is used for detecting the watermark.

The performance of algorithm is evaluated by determining watermarked image quality. The image quality is determined by a parameter called Peak signal to noise ratio (PSNR).

$$PSNR = 20\log_{10}\left(\frac{S}{RMSE}\right) \quad (11)$$

Where S is the maximum pixel value and RMSE is the Root Mean Square Error of the image. RMSE is the sum of squares of difference between the value of pixels in the original image and watermarked image.

In the proposed watermarking algorithm Spread Spectrum (SS) and Scalar Costas Scheme Quantization Index Modulation (SCS-QIM) is used for watermarking the compressed-encrypted images. The disadvantage of SS technique is that original image is required to extract the watermark. While in SCS-QIM technique original image is not required. Hence SCS-QIM is preferred. But disadvantage of this technique is that it uses fixed quantization step size (Δ).The stepsize Δ, used for embedding the watermark is derived from original image. So if any attack occurs to the image (eg:awgn attack) ,the watermark cannot be extracted correctly. So the step size Δ, should be made adaptive. Adaptive SCS-QIM is based on this method.

In adaptive SCS-QIM technique the stepsize Δ is determined from the original image and it is used for watermark embedding. While for extracting the watermark from the attacked watermarked image Δ , is estimated and is used for watermark extraction.

This adaptive SCS-QIM watermarking technique can be used in our watemarking algorithm to reduce the probability of error while extracting the watermark.

V IDENTATIONS

L – Length in bytes

I - Original Image

M - Compressed image

C - Encrypted image

W - Watermark Signal generated

Cw - Compressed Encrypted Watermarked Image

Mw – Decrypted Image with watermark

C – Encrypted Image

K – Key used For Generating Watermark

P – Pseudo random Sequence For Generating Watermark

Iw – Decompressed Image with watermark

b – Watermark information bits

D(.)-Decryption function

α – watermark strength factor in Spread Spectrum

β – scale parameter in SCS-QIM

VI CONCLUSION

This paper proposes a robust watermarking technique to watermark compressed and encrypted JPEG 2000 images. This watermarking algorithm is simple to implement as there is no need for doing any decryption or decompression. Since we are not doing any decompression or decryption confidentiality of the content is preserved. The homomorphic property of the encryption algorithm helps us to detect the watermark from the decrypted content. The performance of the watermarking algorithm is evaluated by determining the watermarked image quality using the existing two watermarking schemes: Spread Spectrum(SS) and Scalar Costas Scheme-Quantization Index Modulation Detection.

VII FUTURE WORK

In future this work may extend to use with other image compression schemes like JPEG

REFERENCES

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

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preserving multiparty multilevel DRMarchitecture," in Proc. *6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management*, 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] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Opt. Eng.*, vol. 45, pp. 1–3, 2006.

[5] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale, and A Neri, "A joint digital watermarking and encryption method," in Proc *SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents* X, 2008, vol. 6819, pp. 68 191C–68 191C.

[6] J. Prins, Z. Erkin, and R. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," *EURASIP J. Inf. Security*, vol.2007.

[7] Z. Li, X. Zhu, Y. Lian, and Q. Sun, "Constructing secure content-dependent watermarking scheme using homomorphic encryption," in *Proc. IEEE Int. Conf. Multimedia and Expo*, 2007, pp. 627–630.

[8] Q. Sun, S. Chang, M. Kurato, and M. Suto, "A quantitive semi-fragile JPEG2000 image authentication system," in *Proc. Int. Conf. Image Processing*, 2002, vol. 2, pp. 921–924.

[9] A.Subramanyam,S.Emmanuel, and M. Kankanhalli, "Compressed-encrypted domain JPEG2000 image watermarking," in *Proc. IEEE Int.Conf. Multimedia and Expo*, 2010, pp. 1315–1320.

[10] H.WuandD.Ma,"Efficient and secure encryption schemes for JPEG 2000," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 2004, vol. 5, pp. 869–872.

[11] M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," *Signal Process.: Image Commun.*, vol. 17, no.1, pp. 3–48, 2002.

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

[13] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," IEEE Trans. Signal Process., vol. 51, no.

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