International Journal of Computer Applications Technology and Research
Volume 2– Issue 3, 245 - 249, 2013, ISSN: 2319–8656

Watermarking of JPEG2000 Compressed Images with Improved Encryption

Kukoo Anna Mathew
Viswajyothi College of
Engineering and Technology,
Muvattupuzha, Kerala, India.

Abstract: The need for copyright protection, ownership verification, and other issues for digital data are getting more and more interest nowadays. Among the solutions for these issues, digital watermarking techniques are used. A range of watermarking methods has been projected. Compression plays a foremost role in the design of watermarking algorithms. For a digital watermarking method to be effective, it is vital that an embedded watermark should be robust against compression. JPEG2000 is a new standard for image compression and transmission. JPEG2000 offers both lossy and lossless compression. The projected approach is used to execute a robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images. For encryption it uses RC6 block cipher. The method embeds watermark in the compressed- encrypted domain and extraction is done in the decrypted domain. The proposal also preserves the confidentiality of substance as the embedding is done on encrypted data. On the whole 3 watermarking schemes are used: Spread Spectrum, Scalar Costa Scheme Quantization Index Modulation, and Rational Dither Modulation.

Keywords: JPEG2000, compression, encryption, watermarking, spread spectrum, scalar costa scheme.

1. INTRODUCTION

The two active areas in academia and industry are multimedia communication and information security. These play a vital cause in the information era. Secure delivery of multimedia data will be possible if we merge these two aspects. Security of data can be achieved by maintaining confidentiality, authenticity and integrity. As a part of assuring these constraints, techniques such as watermarking have been introduced. Encryption is also an important tool in defending digital contents, e.g. in digital rights management (DRM) systems [1]-[4]. While encryption is used to look after the contents from unauthorized access, watermarking can be deployed to serve various other purposes.

Watermarking is a procedure for reducing counterfeiting. Also the multimedia data will be scattered in compressed and encrypted format, so watermarking this content will be a difficult process which is very much necessary for ownership, copyright and authentication purposes. In a DRM system there may be multiple levels of consumers and distributors. The distributors don't have access to the unencrypted data content. Basically distributors are those who issue compressed encrypted content, but at times the distributors will have to watermark the content, and so have to watermark in the compressed encrypted domain.

In this paper we present an approach for watermarking of compressed and encrypted images. A range of watermarking methods has been proposed. Compression plays a key part in the design of watermarking algorithms. For a digital watermarking scheme to be effective, it is vital that an embedded watermark should be robust against compression. JPEG2000 is a new standard for image compression and transmission. JPEG2000 offer both lossy and lossless compression. For encryption it uses RC4 stream cipher. The technique embed watermark in the compressed-encrypted domain and extraction is through the decrypted domain. Watermarking in compressed-encrypted content saves the computational complexity as it does not have need of decompression or decryption, and also conserve the confidentiality of the content.

There have been several related image watermarking techniques proposed to date. In [5], Deng *et al.* projected an efficient buyer-seller watermarking protocol based on composite signal representation specified in [6]. In [7] and [8], a few sub-bands of lower resolutions are preferred for encryption while watermarking the rest of higher resolution sub-bands. In [9], the encryption is performed on most significant bit planes despite the fact of watermarking the rest of lower significant bit planes. Prins *et al.* in [10] projected a robust quantization index modulation (QIM) based watermarking technique, which embeds the watermark in the encrypted domain. In [11] Li *et al.* projected a content-dependent watermarking technique, which embeds the watermark in an encrypted format, although the host signal is still in the plain text format.

2. PROPOSED SCHEME

The projected algorithm works on JPEG2000 compressed code stream. There are five different stages for JPEG2000 compression [12].

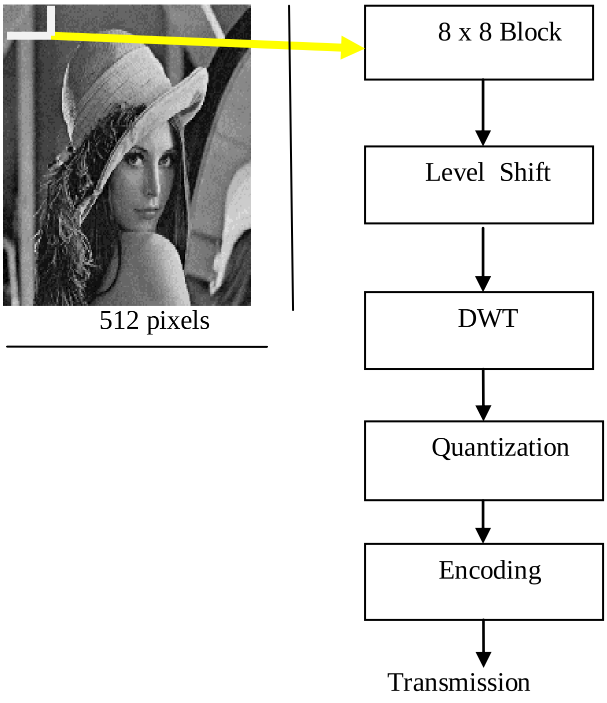

Figure 1. JPEG Algorithm block diagram

In JPEG2000 compression, the complete image is considered as a two-dimensional matrix. In this case, the ‘lenna’ image is a 512x512 pixels image. The intention of this algorithm is to reduce the number of bits used to signify the image. The procedure for compression is:

Step 1: Divide the entire image into several sub matrices of equal dimensions (8x8 blocks).

Step 2: Level shift the entire image. The image is a grayscale image with each pixel represented by 8 bits. Therefore image is level shifted by 128. Subtracting each element of the entire image by 128. Level shift is done to change the range from [0,255] to [-128,127].

Step 3: Perform DWT transform. The input signal X(n) is decomposed into 2 sets of coefficients cA and cD.

Step 4: Perform quantization or normalization to the matrix. This is done with the help of normalization matrix.

Step 5: Encoding is the final process. This arranges the pattern of coefficients of a block in descending order. The block is transformed from a 2-D matrix to a 1-D array of elements.

Thus, it is likely to select bytes generated from different bit planes of different resolutions for encryption and watermarking. The projected algorithm uses a symmetric stream cipher with additive homomorphic properties for encryption. In actuality the distributors get JPEG2000 compressed stream cipher encrypted images for distribution. The distributors can then pertain any robust additive watermarking technique to this compressed encrypted stream.

2.1 Encryption Algorithm

JPEG2000 gives out M, a packetized byte stream as output. In order to encrypt the message M, we use RC6 encryption scheme. RC6 algorithm has a modified Feistel structure and presented symbolically as RC6-w/r/b. w means 32 bits as the size of word, r denotes the number of round. If the size of block is 128 bits, then r, the number, is 20, b means 16 byte as the number of a key. The operations used in RC6 are defined as followings.

- A+B integer addition modulo 2w
- A-B integer subtraction modulo 2w
- A⊕B bitwise exclusive-or of w-bit words
- A× B integer multiplication modulo 2w
- A≪B rotation of the w-bit word A to the left by the amount given by the least significant log w bits of B
- A≫B rotation of the w-bit word A to the right by the amount given by the least significant log w bits of B
- (A,B,C,D)=(B,C,D,A) parallel assignment

The encryption and decryption of RC6 makes cipher text and plain text after carrying out twenty rounds continually with cipher text and plain text in the four storages (A, B, C, and D) per 32bit word.

After doing four words round function, it operates left / right rotate per word with parallel operation as shown in the pseudo code. Furthermore, before and after executing the round functions, it executes round key and add / subtract operations. The foremost security in the round functions is kept by data dependent rotate operation, and the amount of this rotate operation is formed by the fixed 5bit left rotate operation of the quadric, f(x) = x(2x+1).

In decryption operation, the round key of encryption is used with the inverse order. Thus, RC6 has a Feistel structure, however the operation between encryption and decryption is diverse. RC6 does not have a non-linear transformation s-box.

```
Input: Plain text stored in four w-bit input registers A,
       B, C, D
       Number of r rounds
       w-bit round keys S[0,…,2r + 3]
Output: Cipher text stored in A, B, C, D
Procedure: $B = B + S[0]$;
           $D = D + S[1]$;
       For (i=1; i<r; i++)
       {
               $t = (B \times (2B + 1)) \lll \log w$;
               $u = (D \times (2D + 1)) \lll \log w$;
               $A = ((A \oplus t) \lll u) + S[2i]$;
               $C = ((C \oplus u) \lll t) + S[2i+1]$;
```

```
                (A, B, C, D) = (B, C, D, A);
        }
        A = A + S [2r+2];
        C = C + S [2r+3];
```

Figure 2. RC6 Encryption Algorithm

```
Input: Cipher text stored in four w-bit input registers
        A, B, C, D
        Number of r rounds
        w-bit round keys S[0,…,2r + 3]
Output: Plain text stored in A, B, C, D
Procedure: C = C + S[2r+3];
        A = A + S[2r+2];
        for(i=r; i>=1; i--)
        {
                (A, B, C, D) = (D, A, B, C);
                u = (D × (2D + 1)) ⋘ log w;
                t = (B × (2B + 1)) ⋘ log w;
                C = ((C – S [2i+1]) ⋙ t) ⊕u;
                A = ((A – S [2i]) ⋙ u) ⊕ t;
        }
        D = D - S[1];

        B = B - S[0];
```

Figure 3. RC6 Decryption Algorithm

2.2 Embedding Algorithm

The watermark embedding is performed using a robust additive watermarking technique. As the embedding is done in the compressed ciphered byte stream, the embedding position plays a vital role in deciding the watermarked image quality. Hence, for watermarking, we deem 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 larger extent. Also, the higher resolutions are exposed to transcoding operations and lower resolution contains a lot of information, whose amendment leads to loss of quality.

2.2.1 SS

Hartung et al. in [13] proposed a spread spectrum watermarking scheme. The embedding process is carried out by first generating the watermark signal **W**, by using watermark information bits, chip rate and PN sequence P. For watermarking, an a_j sequence of watermarking bits has to be embedded into the image, $a_j = \{-1, 1\}$. The signal is spread by a factor called chip rate, to obtain the spread sequence, $b_{i=} a_j$ where $b_i = \{1,-1\}$. The spread sequence is amplified with a locally adjustable amplitude factor and then modulated by a pseudo-noise sequence, Pi. The modulated signal (SS watermark signal)

$$Wi = \alpha * a_j * Pi. \qquad (1)$$

The watermark signal generated is added to the encrypted signal.

2.2.2 SCS-QIM

In [14], Eggers et al. projected SCS scheme for watermark embedding. In this method, given a watermark strength, we choose a quantizer from an group of quantizers to embed the watermark. The quantizer is chosen by:

$$U = (l+ k_{qimi})\, \beta\Delta + w\, \beta\Delta/2 \qquad (2)$$

where w= {0,1} and l is different sets of quantizers . For making the codebook secure a random sequence k_{qimi} can be chosen. The embedding is done by:

$$q_i= Q_\Delta(c_i – \Delta(w_i/2 \ +k_{qimi})) – (ci\text{-}\Delta(w_i/2 \ +k_{qimi})) \ , \qquad (3)$$

where Q_Δ (.) denotes scalar uniform quantization with step size Δ.

The watermark sequence is given by

$$W=\beta q. \qquad (4)$$

The watermark signal generated is added to the encrypted signal.

2.2.3 RDM

It is based on the quantization of the ratio of the host signal to a function g (.). This scheme was proposed by *Gonzalez et al [15]*. The quantizer is given by

$$Q'\Delta = 2\Delta + w\Delta/2 \qquad (5)$$

w= {-1, 1} is the information that is to be embedded into the host element.

The embedding is done by:

$$c_{wi} = g(c_{wi-1})\, Q'\Delta\, (ci/ g(c_{wi-1})) \qquad (6)$$

where c_{wi} and c_{wi-1} are the current and previous watermarked samples. c_{wi} is an amplitude enhanced version of scaled-quantized . Thus we can write

$$w_i = c_{wi} \text{-} c_i \qquad (7)$$

gives the additive nature of watermark. The function g (.) is chosen such that the scheme is robust against amplitude scaling attacks. We scale g (.) by a constant factor S_c known at both encoder and decoder to control the amount of watermark added.

2.3 Watermark Detection

The watermark can be detected either in encrypted or decrypted compressed domain.

2.3.1 SS

The received signal is applied to a detector and then multiplied by the PN sequence, P used for embedding and summing it with chip rate, r.

$$S_{i\,=}\,b_i * r* \alpha*\sigma_p{}^2 \qquad (8)$$

$$\text{Sign } (S_i) = b_{i,} \qquad (9)$$

resulting in extraction of watermark information bits.

2.3.2 SCS-QIM

The watermark is estimated by quantizing the received signal to the in close proximity data in the code book.

$$\dot{w} = Q_\Delta\,(c_{wi}) - c_{wi} \qquad (10)$$

2.3.3 RDM

The watermark is detected by performing minimum distance criterion by means of

$$\dot{w} = \text{argmin}_{(1,-1)}\,[c_{wi}/g(c_{wi-1}) - Q'\Delta\,(c_{wi}\,/\,g(c_{wi-1}))]^{\,2} \qquad (11)$$

Q'Δ give the 2 quantizers belonging to bits 1 and -1. The distance is computed consequent to both the quantizers and the one which gives minimum distance gives the watermark bit.

3. DISCUSSION

3.1 Security of Watermarking Algorithm

The watermarking algorithm is as robust as basic watermarking schemes, i.e., SS, SCS-QIM, and RDM. The attacks can be performed either in encrypted or decrypted compressed domain to regain or wipe out the watermark. The attacks are considered in compressed domain since watermark detection for ownership verification, traitor tracing, or copyright violation detection can straightforwardly be done as the content is often derivative and distributed in compressed layout. The robustness, for SS scheme, against filtering, such as 1 × 5 median filter and scaling attack can be enhanced by increasing the chip rate and estimating the scale factor [14], respectively. However in case of mean and Gaussian filtering, when the watermarked samples are replaced by the prediction made from the neighboring samples, the replaced samples may be very different compared to the unfiltered watermarked samples. This is due to the fact that the watermarked samples are uncorrelated and the calculation from the neighboring samples may not be a good approximation of the unfiltered watermarked samples. Thus, it leads to the addition of vast amount of noise to the watermarked samples which may be complex to eliminate and the detection performance is not effective. Further, SCS-QIM and RDM are not robust against filtering attack.

3.2 Effect of Scaling in RDM Detection

In case of watermarking by means of RDM, the quantity of watermark power embedded varies to a vast level due to varying quantization step size. Towards this, Abrardo et al. projected a watermarking design using trellis coded quantization [16]. Though, it still uses the function g (.) which might not perk up the watermarked quality when g (.) itself varies vastly. To prevail over this downside, we scale the step size or the function g (.), to suppress this high variation. Also, the watermark power can be controlled using the preferred scale. On the other hand, we are concerned in dealing with the impact of scaling on detection performance. The quantization of signal c_i with the quantizer Q'Δ can be written as Q'Δ (ci. Δ). When message c_i is scaled with a constant Sc, then we have

$$Q'\Delta(ci,\Delta\,/\,Sc\,) = 1/Sc\ Q'\Delta(Sc\ ci\,,\,\Delta\,) \qquad (12)$$

Consequently the properties of both the quantizers alter equivalently and as S_c is known, it does not impact the detection performance.

3.3 Security of Encryption Algorithm

A main objective of RC6 is simplicity. By keeping the cipher structure simple, it becomes accessible to a larger set of people for evaluation. The simplistic structure also plays a part in performance and security. The security of the cipher is amplified by the simple structure. For instance, the rate of diffusion is improved by several simple steps in the round: integer multiplication, the quadratic equation, and fixed bit shifting. The data-dependent rotations are improved, as the rotation amounts are determined from the high-order bits in *f(x)*, which in turn are dependent on the register bits. RC6 security has been evaluated to possess an "adequate security margin"; this rating is given with familiarity of theoretical attacks, which were devised out of the multiple evaluations. The AES-specific security evaluations provide ample breadth and depth to how RC6 security is affected by the simplicity of the cipher.

4. CONCLUSION

In this paper we propose a fresh technique to embed a robust watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes. The algorithm is simple to put into service as it is directly performed in the compressed-encrypted domain, i.e., it does not involve decrypting or partial decompression of the content. Our proposal also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem is exploited, which allows us to detect the watermark after decryption and manage the image quality as well. The detection is carried out in compressed or decompressed domain. In case of decompressed domain, the non-blind detection is used. The research highlights are:

- The paper proposes a better compression method.

- The method uses three watermarking techniques.
- The paper uses RC6 encryption technique.
- The method can be extended to video with modifiying the method.

5. 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 DRM architecture," 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] 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.

[5] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[6] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[7] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," Opt. Eng., vol. 45, pp. 1–3, 2006.

[8] F. Battisti, M. Cancellaro, G. Boato, M. Carli, and A. Neri, "Joint watermarking and encryption of color images in the Fibonacci-Haar domain," EURASIP J. Adv. Signal Process., vol. 2009.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

[15] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp. 3960–3975, Oct. 2005.

[16] A. Abrardo, M. Barni, F. Pérez-González, and C. Mosquera, "Improving the performance of RDM watermarking by means of trellis coded quantisation," IEE Proc. Inf. Security, vol. 153, no. 3, pp. 107–114, 2006.