ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016 April 10(4): pages 184-189

Published BY **AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

A Novel Approach for Watermarking in JPEG 2000 Images using RC4-2S Encryption

[1]C. Kanmani Pappa and [2]Dr.M.Vijayaraj

[1]Assistant Professor, Dept of ECE, National College of Engineering, Tirunelveli, Tamil Nadu, India.
[2]Associate Professor, Dept of ECE, Government College of Engineering, Tirunelveli, Tamil Nadu, India.

Received 25 January 2016; Accepted 18 April 2016; Available 28 April 2016

Address For Correspondence:
C. Kanmani Pappa, Assistant Professor, Dept of ECE, National College of Engineering, Tirunelveli, Tamil Nadu, India
E-mail: kans_262@rediffmail.com

ABSTRACT

It is necessary to watermark media content for tamper proofing, quality assessment and copy control since, in digital multimedia there is an increased ability to create similar and unauthorized data, which can be easily copied, manipulated and distributed, the need for copyright management protection, ownership identification, tamper detection and other security issues is becoming more important. In this paper, we propose a method of embedding with a digital Spread Spectrum Watermarking technique and encrypting with RC4-2S in JPEG 2000 images, which is secure and allows watermarking in the compressed-encrypted domain. The robustness, embedding capacity, perception quality and security of the proposed scheme is to be investigated. The values for the PSNR are also measured.

KEYWORDS: Compressed and encrypted domain watermarking, JPEG 2000, RC4-2S encryption algorithm

INTRODUCTION

There has been phenomenal growth in the creation of content, capturing, processing, and distribution of digital media over the past several years. Digital multi media content is often distributed in compressed and encrypted domain format, and watermarking for detection of violations in copyright, proof of ownership or distributorship and media authentication must at times be carried out in the compressed-encrypted domain. Digital rights management (DRM) systems [10] allow owners to distribute multimedia content in a compressed and encrypted format to consumers through multilevel distributor networks. DRM systems are used for digital content delivery. They distribute the encrypted content and request the license server in the system to distribute the associated license containing the decryption keys to open the encrypted content to the consumers. Each distributor needs to watermark the content to prove the distributorship and media authentication. Watermarking is done in the compressed-encrypted domain.

In this paper, we focus on an efficient approach for compressed and encrypted domain watermarking in JPEG 2000 images. Deng et al. [9] have proposed an efficient buyer-seller watermarking protocol based on composite signal representation in which the content is accessible for watermarking only in encrypted form. Prins et al. [6] propose a robust quantization index modulation (QIM)-based watermarking technique in the encrypted domain where the watermark is embedded. This technique involves the addition or subtraction of a watermark bit to a sample based on the value of a quantized plaintext sample. A content-dependent watermarking technique proposed by Li et al. [5] embeds the watermark in an encrypted format, while the signal is in the plaintext format.

The system proposed in this paper has been developed to overcome the drawbacks of the existing systems. This system uses a novel technique to embed a watermark in the JPEG 2000 compressed-encrypted images. The algorithm is directly performed in the compressed-encrypted domain and does not require decrypting or partial

decompression of the content. The Rivest Cipher 4 with two state tables (RC4-2S) encryption algorithm is used to encrypt the image.

The remaining part of the paper is organized as follows: Section II describes the main stages of the proposed method, Section III shows the experimental results and Section IV provides conclusions and some future work lines.

II. Methodology:

The proposed method consists of the following three modules: the algorithm for encryption, the embedding algorithm, and watermark detection. First, an input image of 512x512 pixels is taken for preprocessing and compression is done using JPEG2000 compression technique. The image is then divided into rectangular tile format which is non-overlapping and the unsigned samples are reduced by a constant to make them symmetrically around zero and finally, a transform which is multi component is performed. The discrete wavelet transform (DWT) is then applied, which is followed by quantization. The co-efficients obtained after quantization are regrouped to provide spatial and resolution access and that will give a multi-resolution image. These resolutions are divided into smaller blocks called code-blocks and each of them will be encoded independently.

The DWT coefficients obtained after quantization are then divided into different bit planes and coded through multiple passes at embedded block coding with optimized truncation (EBCOT) to give a compressed byte stream. It is then possible to select bytes generated from different bit planes of different resolutions for encryption and watermarking. The proposed algorithm uses a stream cipher.

A. Encryption algorithm:

JPEG 2000 gives out packetized byte stream as its output. RC4-2S algorithm has been chosen for encrypting the message. Using RC4-2S,byte-by-byte encryption is done to get the ciphered signal. RC4 is one of the most important symmetric cryptographic algorithms, a stream cipher that can be applied to many security applications in real-time security. However, the RC4 cipher shows some weaknesses, including correlation problems between the publicly known outputs of the internal state. Therefore, we propose the RC4 stream cipher with two state tables (RC4-2S) as an enhancement to RC4 to solve the correlation problems between the publicly known outputs of the internal state using permutations between state 1 (S1) and state 2 (S2). In addition, the key generation time of the RC4-2S is less than that of the original RC4. This is because fewer operations are required for each key generation and the streams generated by the RC4-2S are more random than those generated by RC4 and also require less time.

The high resistivity provided by the RC4-2S also protects against many attacks to which the RC4 is vulnerable and solves several weaknesses of RC4, that is, it is not able to recognize attacks. The RC4 design avoids the use of Linear Feedback Shift Registers (LFSRs), while many stream cipher algorithms depend on it, especially in the hardware. LFSRs attempt to achieve the highest randomness through swapping elements in arrays. The RC4 algorithm also has variable key lengths that range from 0 to 255 bytes for initializing a 256-byte array in the initial state through elements from S[0] to S [255]. RC4 uses a key that is 128 bytes long. The RC4 stream cipher uses the key scheduling algorithm (KSA) and the pseudo-random generation algorithm (PRGA), which are executed sequentially.

The RC4 key is initialized by the key scheduling algorithm, and the pseudo-random number is produced by the PRGA. This look up table which has the self-modifying capability is simple and has been applied efficiently in software [15]. The output of the PRGA algorithm is a key sequence that will use the XOR (exclusive OR) cipher with plaintext (or ciphertext) to get ciphertext (or plaintext).

B. Attacks on RC4:

Several weaknesses have been identified in the RC4 cipher. Some of these can be solved easily, but others are critical because they can be exploited by attackers. The problems that RC4 has include 1) the weakness of the KSA and 2) the weakness of the relations between the S-boxes at different times. The initial state of the PRGA is efficient in protecting against a number of attempted attacks. However, the RC4 algorithm has the weakness of being vulnerable to exploitation through ciphertext-only attack. Such attacks are limited to broadcast applications involving the use of different keys to encrypt the same plaintext for multiple recipients. There are many other attacks, such as those resulting from guessing subkeys, linear consistency attacks and inversion attacks. Algebraic attacks are also a new type of higher order correlation attack. Since a fairly straightforward approach, such as a brute force attack, identifies the internal state of the PRGA, increased internal state size is recommended; however, this results in increased encryption and decryption times.

C. The RC4 stream cipher with two state tables:

This algorithm is one of the RC4 stream cipher algorithm which can reduce the correlation problem between the publicly known outputs of the internal state and, therefore, improves the speed of encryption and

decryption. This algorithm has an initialization phase (KSA) and output phase (PRGA). All additional operations are carried out by modular numbers. The KSA takes a key, "k", which includes 16 n-bit words. After the setup, the round algorithm is executed once for each word output. In almost all practical applications the developed RC4 is implemented with n = 8, in which case all entries of S along with i and j are bytes. In the first phase of the KSA, S1 is filled from 0 to (N/2)-1 and S2 gets the remaining N/2 numbers from N/2 to N-1. The secret input key, "k", is used as a seed for the two states, S1 and S2, and also to make the permutations and handle the swapping of the elements of S1and S2. Therefore, S1 and S2 are the two secret random inputs for the second phase. S1 and S2 produce two keys in each loop cycle instead of just one as occurs in the second phase of the standard RC4.

In this algorithm, there are more elements to be swapped between S1 and S2, by three pointers: i, j1 = j1 + S1 [i], and j2 = j2 + S2 [i] in the S-box. S1 and S2 in the PRGA are used to produce the sequence of that output stream, which is XOR-ed with plaintext (or ciphertext) to generate ciphertext (or plaintext). The RC4-2S is faster than RC4, since the RC4-2S includes two swaps and five modular functions to generate two bytes of the key per iteration in the PRGA algorithm, while RC4 involves one swap and three modular functions to generate only one byte of the key. Therefore, this technique combines the increasing randomness of the initial internal states with the permutations of the two state tables during key generation to solve the correlation problem between the publicly known outputs of the internal state.

Algorithm 1. KSA FOR RC4 – 2S

$INPUT: K[k, m]$

$OUTPUT: S1, S21.$

$For\ i \leftarrow 0 to \frac{N}{2} - 1\ Do$

$S1[i] \leftarrow i$

$For\ i \leftarrow \frac{N}{2}\ to\ N - 1\ Do$

$S2\left[i - \frac{N}{2}\right] \leftarrow i$

$j \leftarrow 0$

$For\ i \leftarrow 0\ to \frac{N}{2} - 1\ Do\{$

$j \leftarrow (j + S1\left[i + k[imodL]mod\frac{N}{2}\right] + k[imod\ L]mod\frac{N}{2}$

$Swap\ S1[i]withS1[j]\ \}$

$j \leftarrow 0$

$For\ i \leftarrow 0 to \frac{N}{2} - 1\ Do\{\ j \leftarrow (j + S2[i] + k[imod\ L])mod\frac{N}{2}$

Swap S2[i]with S2[j]

Return S1 and S2

Algorithm 1. PRGA FOR RC4 – 2S

$INPUT: K[k, m]$

$OUTPUT: Key\ Sequence\ Kseq$

$i, j, j2 \leftarrow 0$

$While\ not\ end\ of\ half\ sequence\ Do$

$i \leftarrow (i + 1)modN/2$

$j1 \leftarrow (j1 + S1[i])modN/$

$Swap\ S1[i]with\ S2[j1]$

$t1 \leftarrow S1\{(S1[i] + S1[j1])mod\ N/2$

$j2 = j2 + S2[i]mod\ N/2$

$Swap\ S2[i]withS2[j2]\ \}$

$t2 = S2[(S2[i] + S2[j2])mod\ N/2$

$Kseq = [t1, t2$

Return(Kseq)

D. Embedding algorithm:

The RC42S encryption algorithm used is an additive privacy, using a robust additive watermarking technique the watermark embedding is performed . Since the embedding is done in the compressed ciphered byte stream, the watermarked image quality is decided by the embedding position. Hence, for watermarking, ciphered bytes from most significant bit planes degrades the image quality to a greater extent so we choose inserting watermark in the ciphered bytes from the less significant bit planes of the middle resolutions. Also, the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, whose modification leads to loss of quality. Study of impact on quality of watermarking in this compressed-encrypted domain is done using this experiment. Here how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much is shown. Now we can explain the embedding process.

Spread Spectrum Watermarking:

Different watermarking methods for images have been proposed. Most of them are based on ideas known from spread spectrum radio communications, namely watermark recovery and additive embedding of a pseudo-noise watermark pattern by correlation.Here the embedding process used is spread spectrum watermarking scheme. For embedding process the watermark signal W are generated by using watermarking information bits b ,chip rate r and PN sequence P .The watermark information bits $b = \{b_i\}$, where $b_i = \{1, -1\}$, are spread by r ,can be given as

$$a_j = b_i, \qquad ir \le j < (i+1) \tag{1}$$

The a_j sequence is multiplied by $\alpha > 0$ and P. Then the watermark signal $W = \{w_j\}$, where

$$w_j = \alpha a_j p_j \tag{2}$$

Now the watermark signal generated is added to the encrypted signal C, to give the watermarked signal C_w

$$C_w = C + W = c_{w_i} = c_i + w_i \qquad \forall = 0,1 \ldots \tag{3}$$

D. Detection of Watermark:

Final stage is the detection of watermark. Either in encrypted or decrypted compressed domain the watermark can be detected. Now we can explain the detection in encrypted domain followed by decrypted domain.

i) Encrypted Detection Domain:

In the encrypted domain C_w is directly given to the extraction module for watermark detection.

SS Watermarking:

The encrypted-watermarked signal which is received from the previous section $C_w = C + W$ is applied to the correlator detector .Then it is multiplied by PN sequence used for embedding, summation over chip-rate window , yielding the correlation sum .

$$S_i = \sum_r (c_{w_j} p_j) = \sum_r (c_j + w_j) p_j = b_i \sigma_p^2 \alpha \tag{4}$$

Here $c_j p_j$ is zero if C and P are uncorrelated. This cannot be applied always for real compressed data. We can subtract away C from $C_w$to remove the correlation effect completely to get a better watermark detection rate. The watermark information bit is given by sign S_i

$$sign\,(S_i) = sign\left(b_i \sigma_p^2 \alpha r\right) = sign(b_i) = b_i \tag{5}$$

ii) Decrypted Detection Domain:

The received compressed- encrypted watermarked image is passed through the decryption module, which defines the corresponding byte by byte decryption for the encryption defined .Thus the key stream can be generated. The received signal is decrypted to give as

$$\begin{aligned} M_w = D\,(C_w, k) = \left(c_{w_i} - k_i\right) mod 255 \;\; \forall = 0,1 \ldots L-1 \\ = (c_i + w_i - k_i) mod 255 \\ = m_i + w_i \\ = m_{w_i} \end{aligned} \tag{6}$$

The embedded watermark information W can be estimated from M_w using correlation detector without the knowledge of originals M or C in SS detection. Here M and P may not always be uncorrelated and hence the noise due to M may not be completely eliminated. In order to obtain better detection results, we can encrypt $M_w$with K which gives C_w and removing C is given as follows

$$S_i = \sum_r (c_{w_j} p_j) = \sum_r \alpha a_j p_j p_j = b_i \sigma_p^2 \alpha r \tag{7}$$

Thus, the watermark information bit is given by the sign as

$$sign\,(S_i) = sign\left(b_i \sigma_p^2 \alpha r\right) = sign(b_i) = b_i \tag{8}$$

E) Decompressed Detection Domain:

In the decompressed detection domain I_{DW} is the decompressed-watermarked image, I_{DU} is the decompressed original image, and I_{DWA} is the decompressed-watermarked-attacked image. The watermark signal in decompressed domain can be computed as $\widehat{W} = I_{DU} - I_{DW}$ and in case of attack, $\widehat{W} = I_{DU} - I_{DWA}$. For decompressed detection, a correlation measure between embedded and attacked watermark signal is computed as

$$corr\left(\widehat{W}_i, \widetilde{W}\right) = \frac{E\left[\left(\widehat{w}_i - \mu_{\widehat{w}_i}\right)\left(\widetilde{w} - \mu_{\widetilde{w}}\right)\right]}{\sigma_{\widehat{w}_i} \sigma_{\widetilde{w}}} \qquad \forall_i = 1,2 \ldots N_w \tag{9}$$

Where E [.]- correlation measure which denotes the expectation operator,

μ - mean

σ^2- variance.

III. Experimental Results:

To evaluate the performance of the binarization techniques several performance metrics are available. We use the MSE,BER and PSNR to analyse the performance.

Peak Signal-to-Noise-Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the attacked image and the original image. The PSNR formula is written as

$$PSNR = 10\,X\,log_{10}\frac{255\ X\ 255}{\frac{1}{H\,X\,W}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}[f(x,y)-g(x,y)]^2}\ dB \qquad (10)$$

Where W -width of the image and H - height of the image

f(x, y) - the grey levels located at coordinate (x, y) of the original image

g(x, y)- the grey levels located at coordinate (x, y) of the attacked image

Output Images: Spread Spectrum Watermarking Technique:

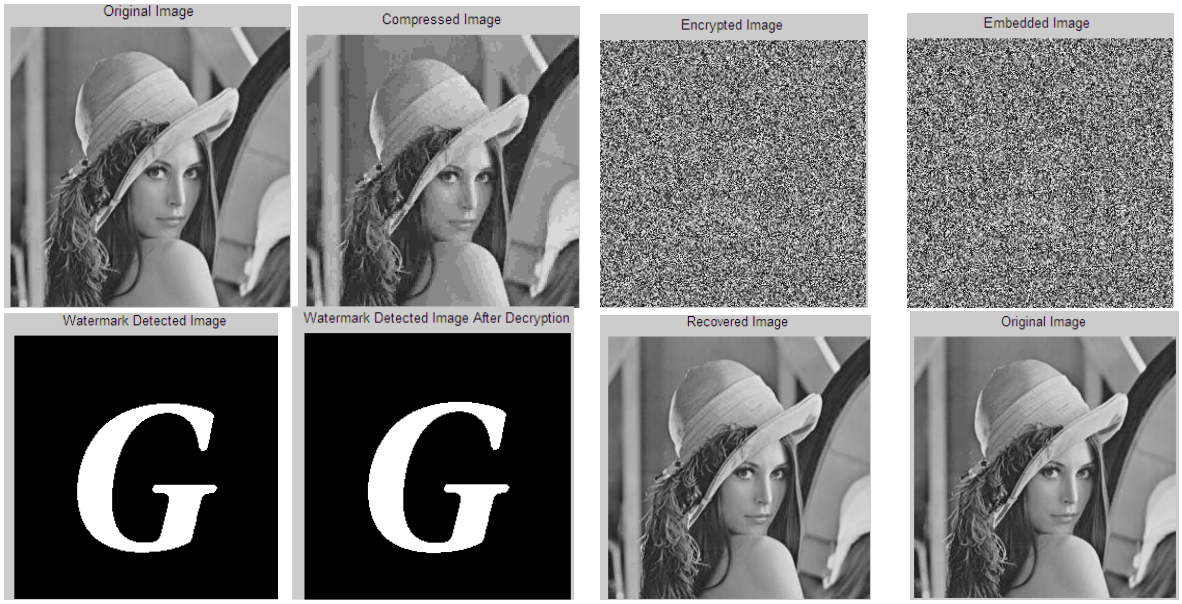

Table : Results for various images

IMAGES PARAMETERS	LENA	CAMERAMAN	BOAT
Encryption PSNR Value	3.3858	1.0563	3.7499
Encryption MSE Value	14.6727	15.5526	14.5397
Encryption Bit error ratio	0.0415	0.0912	0.0261
Embedding PSNR Value	21.2924	19.3511	21.5958
Embedding MSE Value	9.3776	9.8439	9.3067
Embedding Bit Error ratio	0.0398	0.0898	0.0281

Conclusion:

In this paper we proposed an efficient approach for compressed and encrypted domain watermarking in JPEG 2000 images using spread spectrum watermarking technique. The RC4-2S algorithm is easy to analyse and for implementation. This algorithm is directly performed in the compressed-encrypted domain. There is no partial decompression or decrypting of the content are required. Our schemes preserves the confidentiality of content as the embedding is done on encrypted data. It helps to detect the watermark after decryption and control the image quality. In compressed or decompressed domain the detection is carried out. Using experimental results we analysed the relations between MSE, BER and PSNR for different resolutions.

Future work aims at extending the proposed method to JPEG and JPEG-LS Images.

REFERENCES

1. Robust Watermarking of Compressedand Encrypted JPEG2000 Images A.V. Subramanyam, 2012. Sabu Emmanuel, *Member, IEEE*, and Mohan S. Kankanhalli, *SeniorMember, IEEE* IEEE Transactions On Multimedia, 14(3): 703.
2. An Efficient Novel Approach for Compressed and Encrypted Domain Watermarking in JPEG2000 Images L.S.Shibil Jeyanthi Prasad, C. Kanmani Pappa, M.Subbulakshmi Dr.M.Vijayaraj, 2014. International Journal of Recent Development in Engineering and Technology, 2: 3.
3. Mohanty, S.P., K.R. Ramakrishnan, M.S. Kanakanhalli, 1999. "A dual watermarking technique for images, Proceedings of the 7th ACM International Multimedia Conference" (ACMMM), Florida, USA, 2: 49-51.
4. Wu and D.Ma, 2004. "Efficient and secure encryption schemes for JPEG2000," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 5: 869-872.
5. Castelluccia, E. Mykletun, and G. Tsudik, 2005. "Efficient aggregation of encrypted data in wireless sensor networks," in *Proc. 2nd Annu. Int. Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005)*, pp: 109-117.
6. Abrardo, M. Barni, F. Pérez-González and C. Mosquera, 2006. "Improving the performance of RDM watermarking by means of trellis coded quantisation," *IEEE Proc. Inf. Security*, 153(3): 107-114.
7. Lian, S., Z. Liu, R. Zhen and H. Wang, 2006. "Commutative watermarking and encryption for media data," *Opt. Eng*., 45: 1-3.
8. Prins, J., Z. Erkin and R. Lagendijk, 2007. "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP J. Inf. Security.
9. Schaefer, G. and M. Stich, 2000. "UCID—An uncompressed colour image database," *Multimedia Syst.*, 15(4): 243-270.
10. Langelaar, Emir Ganic Ahmet M. Eskicioglu, 2009. "Reversible Watermarking approach for JPEG and MPEG Stream", Proceedings of the 7th ACM International Multimedia Conference (ACMMM), Florida, USA, 2: 49-51.
11. Deng, M., T. Bianchi, A. Piva and B. Preneel, 2009. "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, pp: 9-18.
12. Subramanyam, S. Emmanuel and M. Kankanhalli, 2010. "Compressed encrypted domain JPEG2000 image watermarking," in *Proc. IEEE Int. Conf. Multimedia and Expo*, pp: 1315-1320.
13. Emir Ganic Ahmet M. Eskicioglu, 2010. "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", IEEE Signal Process Lett., 17(6): 567-570.
14. Bianchi, A. Piva and M. Barni, 2010. "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans. Inf. Forensics* Security, 5(1): 180-187.
15. RC4-2S: RC4 Stream Cipher with Two State Tables Maytham M. Hammood, Kenji Yoshigoe and Ali M.Sagheer