Biomedical Research 2017; 28 (1): 51-57 *ISSN 0970-938X*
www.biomedres.info

Novel watermarking scheme with watermark encryption for copyright protection.

Sebastin Antony Joe S[1*], Seldev Christopher[2] , Jereesha Mary S J[1]

[1]Anna University Chennai, Tamil Nadu, India

[2]Department of Computer Science, St.Xaviers Catholic College of Engineering, Chunkankadai, Tamil Nadu, India

Abstract

During the digital era as more data are being transferred over internet the need for secure communication arises. Hence copy right protection, tamper proof, content authentication, and copy protection to the digital data has to be assured in some ways. Watermarking has entered in the area of bio medical image processing since it is used to hide the information about the patient. To ensure this, various security concepts has been introduced. This paper proposes a grouping of two algorithms to provide copyright protection to the digital data. The proposed method uses an encryption algorithm to encrypt the compressed input image and the resultant encrypted output is watermarked with a frequency domain watermarking algorithm. The output is the watermarked encrypted image. The experimental results produced, show that the visual clarity of the watermarked image is high and the watermarked image is of more secure. The PSNR value and MSE value of the proposed method is satisfactory when compared to the previous method where Rational Dither Modulation techniques combined with RC4, RC5, RC6 for assuring copyright protection.

Keywords: Watermark, MRC6, Rational dither modulation (RDM), Copyright protection.

Accepted on April 07, 2016

Introduction

Due to the growth of digital data the task of creation, processing and distribution of digital data like medical images over the network become a big task. Usually the contents transferred over the network is in the compressed/encrypted format and hence watermarking this format for various right management application such as copyright protection, content authentication and tamper proof should be done in compressed/ encrypted mode. Encryption is the process in which the digital data like text, image, audio, video etc., is converted into an unreadable format using a key. Encryption methods like Goldwasser-Micali, RSA, Elgamel, and Paillier are asymmetric scheme that exhibit homomorphic property and the downside of it, is the output cipher text has low compression efficiency and decrease in payload for small and large message sizes respectively [1-3].

The above said drawbacks are overcome by using RC4 which is a symmetric stream cipher with homomorphic property and this method ensures copyright protection [4]. Based on the key scheduling algorithm Fluhrer [5] has proved that the probability of data trade-off attacks is increased due to low sampling resistance in RC4. RC5, a block cipher algorithm is said to be better than RC4 as in [6]. The method proposed by Gayathri in [7] exhibits the usage of RC5 along with the watermarking techniques depicted in [4]. RC5 undergoes differential attack when the chosen plaintext is 244 and the number of rounds is less than eighteen [8]. Rivest et al. designed the block cipher RC6 to overcome the drawbacks of RC5 [9].

RC6 along with the watermarking algorithm suggested by [4] was proposed by Kukoo Anna Mathew, since RC6 has more number of registers than RC5 [10]. RC6 is prone to differential linear attack with 16 rounds, statistical attack with less than 16 rounds and x^2 cryptanalysis with more than 16 rounds [8,11,12]. A scheme which is not in a fully compressed and encrypted domain watermarking, which derives the content based features from the plain text, for the purpose of watermarking is proposed in [13]. Encryption is done in chosen low resolution sub bands and watermarking is done on the remaining sub bands of higher resolution as explained in [14,15]. A watermarking technique based on quantization index modulation where the addition/subtraction of a bit from the watermark to a sample is done using the quantized plain text sample [16].

A content dependent technique to watermark is proposed by [17], in which the input signal is in the plain text format and watermark is an encrypted one. Here the distortion over the input signal may be large. In [18] encryption is done on most significant bit plane and the remaining lower significant bit plane are being watermarked. The drawback in this scheme is, if lesser number of sub bands is being encrypted the attacker can extract information from the unencrypted sub bands, else if

more sub bands are encrypted the watermark can be removed without reducing the image quality. Chen proposed a watermarking method for medical image in which the result is limited to JPEG compression [19].Various watermarking algorithms are being compared in [4] of which Rational Dither Modulation has greater capacity than other schemes. It has benefits from the gains afforded by distortion compensation and channel coding.

Moderately it is robust to Invariant value metric scaling attack. Watermarking is used to lessen the forgery of data that is being transferred through the internet as well as to the data that is being stored in digital format in any computer system. The watermarking process embeds a watermark inside the input data to produce a watermarked data. Using digital signature forgery can be found but the forged location cannot be found. So watermarking is being used as a solution to this [20-23]. Encryption schemes together with watermarking algorithm make the digital data more reliable and secure. As the technology used for encryption and decryption are complex, cryptographic algorithms become harder to detect. Also the key used for encryption makes it more complex and secure.

The disadvantages of both schemes are overcome by bonding both of them together [24-28] proposed an algorithm in which encryption is done in the JPEG 2000 image with the exception of header and marker segment. Wu and Ma [29] made it clear that JPEG2000 is suitable for encryption / watermarking, because for the same compression ratio decompression of the signal can be done at any ratio. Figure 1 shows the basic model for copyright protection using image encryption and watermarking. The previous studies state that MRC6 encryption algorithm is one of the best blocks ciphering algorithm to be used together with watermarking algorithms due to its robustness against attacks.

Also as compressed images maintain low file size as they are transferred over the network, JPEG2000 is used as the input file format because it supports both loss and lossless compression. Hence the input medical image is converted into JPEG2000 image format. In previous algorithms, watermarking is done in plain text, whereas in the proposed method it is done in the compressed encrypted format since the key for decryption is also unknown. Also Rational Dither Modulation (RDM) is chosen as the watermarking algorithm to watermark the encrypted input image since it withstands many attacks as compared to other frequency domain algorithms.

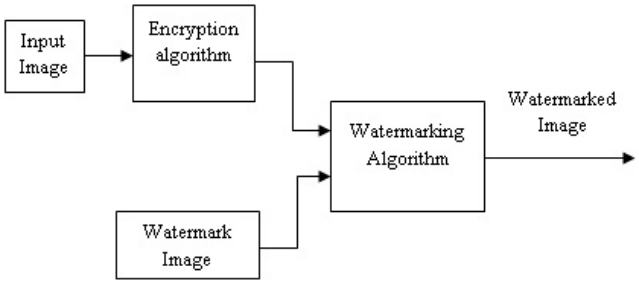

Figure 1. *Basic model for Copyright protection.*

Proposed system

In the proposed algorithm, the input is a JPEG2000 compressed code stream. There are five different stages in the JPEG2000 compressed standard [18]. As a first step the input JEG2000 image is divided into rectangular tiles that are non-overlapping and the unsigned values are being reduced by a fixed value to be symmetric around zero and a multi compound transformation is being done. The Discrete Wavelet Transformation (DWT) is applied as the second step. The third step is to quantize the transformed values. In the fourth step these coefficients are further split up into various bit planes and coded using Embedded Block Coding with Optimized Truncation (EBCOT) coding method.

The output of this step is the compressed byte stream. In the fifth stage the byte stream which is in the compressed format is classified into various wavelet packets based on the number of pixels in an image, precincts, components and layers. Hence for encryption and watermarking the bytes from different bit planes with different resolution can be selected. Also JPEG2000 image supports both loss and lossless compression. Figure 2a shows the proposed model where 'M' is the input image which is given as input to the JPEG2000 encoder. The encoded JPEG2000 bit stream is represented as 'E'. 'C_i' is the encrypted JPEG2000 bit stream. The key for encryption is represented as 'K'. Watermark is indicated as 'W' and the watermarked cipher text is 'W_c'. The input image is given as an input to the JPEG2000 encoder. The encoder undergoes five stages of evaluation of the given input and produces wavelet packets as output. This output is encrypted using MRC6 encryption algorithm.

The MRC6 algorithm uses 16 working registers and undergoes four stages of operation to produce a cipher text that is more secure and robust with an increased throughput value. A copy of the encrypted content is given as input to the watermark signal generator which produces the watermark to be embedded in the encrypted input image. This watermark is added with the cipher text output using Rational Dither Modulation (RDM) Scheme. RDM is being used since it has higher capacity and is more robust than many algorithms. The output is a highly secure watermarked image. This watermark image can be detected using any of the detection algorithms either in encrypted format or decrypted form.

To extract the watermark in the decrypted domain, the watermarked/encrypted image is decrypted and then given to the detection module. To extract the watermark in encrypted mode, the watermarked/encrypted image is directly fed to the detection module. Even after making alterations to the content, if it is possible to retrieve the watermark correctly, then the watermarking algorithm is said to be robust. A small change in the image may result in the failure of the extraction process which indicates that the algorithm is fragile. In the Figure 2b, the dotted 'C_i' input to the watermarking detection module indicates that the watermarking detection is not blind and this detection is optional. Here 'W_E' is the decrypted watermark

image. 'W_M' represents decoded watermarked image. The Pseudo noise sequence is represented by 'P'.

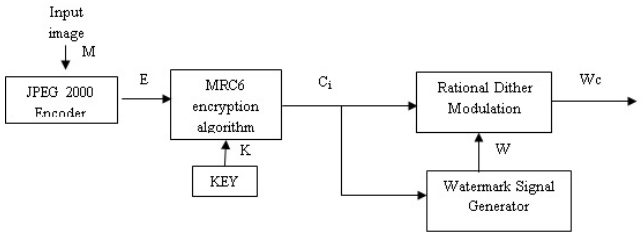

Figure 2a. *Watermark embedding.*

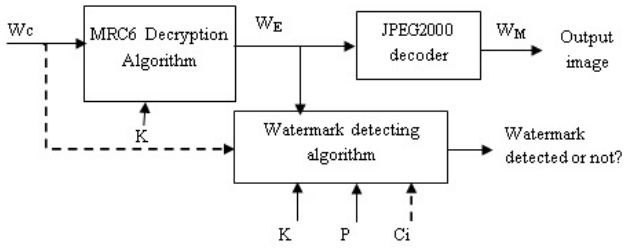

Figure 2b. *Watermark detection.*

Modified rivest cipher 6 (MRC6)

A modified version of RC6 is MRC6 which is a block cipher and it has 16 working registers instead of 8 working registers in RC6. Also the input and output block size of MRC6 is 512 bits. The parameterized family (w, r and b) is used in MRC6 as used by its predecessor. Also the basic operations are also same as other block ciphers like RC5, RC6, and AES. The four basic Operations of MRC6 algorithm is

Addition, denoted by '+' and its inverse operation subtraction, signed by (-1).

Bit-wise exclusive-OR operation, denoted by (Θ).

A left rotation of words: x<<<y. Here y is taken as modulo w and the log (w) low-order bits of y determines the rotation amount when w is a power of two. The inverse operation is, x>>>y.

Integer multiplication modulo 2n, denoted by (*)

MRC6 has a key table K_t [0, t-1] which is expandable that has key value as t= 8r+16 'w' bit words that depends on the number of rounds 'r'. The number of bytes in the secret key 'b' is K [0], K [1]……. K [b-1], and b can range between 0 <=b<= 255. Thus MRC6 has the advantage of having more number of rotations per round and uses huge bits of data to find rotation amounts in each round. MRC6 uses Integer multiplication as a "diffusion primitive" to calculate the rotation amounts. Various steps in MRC6 ciphering method are

1. Key expansion algorithm
2. Encryption Algorithm
3. Decryption

Key expansion algorithm:

Key expansion algorithm of MRC6has two magic constants P_w and Q_w which is defined as

P_w = odd ((e -2) 2^w) → (1) and

Q_w = odd ((Ø-1) 2^w) → (2)

Where

e=2.7182818 and

Ø=1.618033.

S [0] = P_w

For i = I to 2r+3 do

S [i] = S [i-1] + Q_w

R1=R2=i=j=0

V=3* Max (c, 8r+16)

For S = l tovdo

{R1 = S[i] = (S[i] + R1 +R2) <<< 3

R2 = [j] = (L[j] + RI +R2) <<< (Rl+R2)

I = (i+1) Mod (8r+16)

j = (j + l) Mod c}

Figure 2c. *Key expansion algorithm.*

Encryption algorithm

The initial inputs for the encryption process are stored in the sixteen working registers. It also contains the final output data at the end of the encryption process. The least significant bit of the working register R1 contains first byte of the plain text and the last byte of the input is placed in the most significant bit of R16. The values from right registers are transferred to left registers by parallel assignment. Figure 2d show the MRC6 encryption algorithm.

Figure 2c show the key expansion algorithm.

Decryption algorithm

The input to the decryption process and the final output after the decryption process are stored in the sixteen working registers. The least significant bit of the working register R1 contains the first byte of the cipher text and the last byte of the output is placed in the most significant bit of the register R16. Figure 2e show the MRC6 Decryption algorithm.

Rational dither modulation (RDM)

RDM is a modification of Dither Modulation (DM) which overcomes the vulnerability of scaling attack. It is a quantization based data hiding method. It does not require estimating the step-size, as most existing methods do. It does not focus on the step-size of the quantizer and hence avoids the usage of pilot-sequence. It is used for carrying out scalar operation and hence avoids the construction of spherical codes.

R2 = R2+S [0]

R4 = R4+S [1]

R6 = R6+S [2]

R8 = R8+S [3]

R10 = R10+S [4]

R12 = R12+S [5]

R14 = R14+S [6]

R16 = R16+S [7]

For i = 1 to r do

{k = (R2 * (2R2+1)) <<<log w

l = (R4 * (2R4+1)) <<<log w

m = (R6 * (2R6+1)) <<<log w

n = (R8 * (2R8+1)) <<<log w

t = (R10 * (2R10+1)) <<<log w

u = (R12 * (2R12 +1)) <<<log w

v = (R14 * (2R14+1)) <<<log w

z = (R16 * (2R16+1)) <<<log w

R1 = ((R1 ⊕ k) <<<1) + S [8i]

R3 = ((R3 ⊕ l) <<<1) + S [8i+1]

R5 = ((R5 ⊕ m) <<<1) + S [8i+2]

R7 = ((R7 ⊕ n) <<<1) + S [8i+3]

R9 = ((R9 ⊕ t) <<<1) + S [8i+4]

R11 = ((R11⊕u) <<<1) + S [8i+5]

R13 = ((R13⊕v) <<<1) + S [8i+6]

R15 = ((R15⊕ z) <<<1) + S [8i+7]

(R1, R2... R15, R16) = (R2, R3…R16, R1)}

R1 = R1+S [8r+8]

R3 = R4+S [8r+9]

R5 = R5+S [8r+10]

R7 = R7+S [8r+11]

R9 = R9+S [8r+12]

R11 = R11+S [8r+13]

R13=R13+S [8r+14]

R15=R15+S [8r+15]

Figure 2d. *Encryption algorithm.*

R15 = R15 - S [8r+15]

R13 = R13 - S [8r+14]

R11 = R11 - S [8r+13]

R9 = R9 - S [8r+12]

R7 = R7 - S [8r+11]

R5 = R5 - S [8r+10]

R3 = R3 - S [8r+9]

R1 = R1 - S [8r+8]

For i = r down to 1 do

{(R1, R2... R15, R16) = (R16, R1.... R15)

z = (R16 * 92R16 + 1)) <<< log w

v = (R14 * 92R14 + 1)) <<< log w

u = (R12 * 921R2 + 1)) <<< log w

t = (R10 * 92R10 + 1)) <<< log w

n = (R8 * 92R8 + 1)) <<< log w

m = (R6 * 92R6 + 1)) <<< log w

l = (R4 * 92R4 + 1)) <<< log w

k = (R2 * (2R2 + 1)) <<< log w

R15 = ((R15) - S [8i+7] >>>v) ⊕z

R13 = ((R13) - S [8i+6] >>> z) ⊕v

R11 = ((R11) - S [8i+5] >>> t) ⊕u

R9 = ((R9) - S [8i+4] >>>u) ⊕t

R7 = ((R7) - S [8i+3] >>>m) ⊕n

R5 = ((R5) - S [8i+2] >>>n) ⊕m

R3 = ((R3) - S [8i+1] >>>k) ⊕l

R1 = ((R1) - S [8i] >>>1) ⊕k}

R16 = R16 - S [7]

R14 = R14 - S [6]

R12 = R12 - S [5]

R10 = R10 - S [4]

R8 = R8 - S [3]

R6 = R6 - S [2]

R4 = R4 – S [1]

R2 = R2 – S [0]

Figure 2e. *Decryption algorithm.*

RDM uses gain-invariant adaptive quantization step-size at both embedder and decoder which makes the watermarked signal being asymptotically constant. The embedding rule is

$$V_y = g\left(V_{y-1}\right) Q_{bk}\left(\frac{x_k}{g\left(V_{y-1}\right)}\right) \rightarrow (3)$$

Where

V_y- vector with 'L' past samples of vector 'y', i.e. current and previous watermarked samples.

g(.)- is a function that satisfies $g: y^L \rightarrow R$

With >0, $g(V_y)=g(V_y)$ and is robust that it with stands amplitude scaling attacks.

Q_{bk}- Quantizer, where $Q_{bk} = 2\Delta + w\,\Delta/2$ and $\Delta \rightarrow$step size.

Rational Dither Modulation has higher capacity than other frequency domain watermarking algorithms like Spread Spectrum and Scalar Costa Scheme. RDM has benefits from the gains afforded by distortion compensation and channel coding. Moderately it is robust to Invariant Value Metric Scaling attack. The RDM poorly models the human perceptual system and a function that models the properties of perception should be considered. RDM can achieve much higher rates for the same bit error probability.

Detection algorithm

Detection also called the extraction process is an algorithm which attempts to extracts the watermark from the watermarked output. If the watermark is present in the content, then it can be extracted which means the signal was not modified. If the watermark is not present to be extracted, then it makes clear that the watermark has been tampered. In the proposed scheme detection or extraction of the watermark is done in two ways, detected either in encrypted form or decrypted/compressed domain. They are

1. Detection of encrypted output.
2. Detection of decrypted output.

Detection of encrypted output: To detect the watermark from the encrypted form, as shown in Figure 2b, the cipher text, W_c is directly fed to the module. The calculations used for detection is the Least Distance Measure which is listed below,

$$\widetilde{\mathcal{W}} = arg\min_{1-1}\left(\frac{W_c}{g\left(W_{c-1}\right)} - Q_{bk}\left(\frac{W_c}{g\left(W_{c-1}\right)}\right)\right)^2 \rightarrow (4)$$

$_i = 1,\ldots..,\ L - 1$

In the above equation, the two quantizers that belong to the bits 1 and -1 are given by Q_{bk}. The distance equivalent to both the quantizer is calculated. The quantizer that has the least distance produces the watermark bit.

Detection of decrypted output: To detect the watermark in the decrypted form, the encrypted/ watermarked image is formerly decrypted using the following decryption algorithm. Then the decrypted output is just a byte stream that is compressed and watermarked. The message that is decrypted, W_E and Key, K is given as input to the watermark detection module. Then using equation (4) the watermark is being extracted.

Security Issues

Security of MRC6

The diffusion process of MRC6 is very fast when compared with other block cipher algorithm [30]. The expansion availability of the number of rounds makes it more secure. Also the increase in key size increases the complexity thus increasing the security of MRC6 when compared with RC4, RC5, and RC6 [31]. MRC6 is robust against differential linear attack, Statistical attack and with increase in number of rounds it is robust against X^2 cryptanalysis also [32].

Security of RDM

Rational Dither Modulation has higher capacity than spread spectrum and scalar costa scheme. The gains provided by Channel coding and Distortion compensation has benefitted RDM. It is extremely robust to amplitude scaling attacks and reasonably robust against Invariant value metric scaling attack. RDM makes the collusion attack ineffective by using codes that are resistant to collusion [4].

Experimental Results

Analysis of compressed domain

As the digital content is often distributed, the watermarking process is done in the compressed/encrypted form. Hence the format in which encryption is done is of great impact, since there is a relationship between efficiency of compression and security of the watermarked content. Different schemes about the domain in which the encryption is being done for JPEG2000 is proposed by [33]. Figure 3a shows the measured PSNR value between the original and decrypted images. When the compression rate increases the quality of the image is lost. But the proposed MRC6 encryption scheme does not have any negative impact over the image quality and hence is used for copyright protection [33].

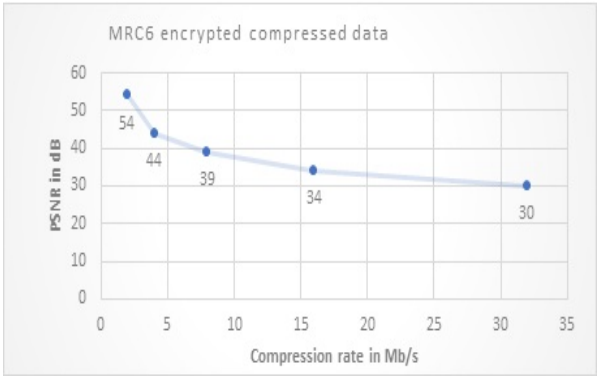

Figure 3a. *PSNR performance in compressed domain.*

Analysing MRC6 encryption

The time taken for encryption and decryption of data block is less when compared with other block ciphers [30]. The encryption time for MRC6 with w=32, b=16 and r=20 is shown in Figure 3b. The encryption time for different input block of varying size using MRC6 is low when compared with other block ciphers and hence the algorithm is the fastest one. The throughput of the MRC6 algorithm is increased with less number of rounds. Throughput and security are inversely proportional. The effect in the increase of secret key length towards the throughput and security is shown in Figure 3c.

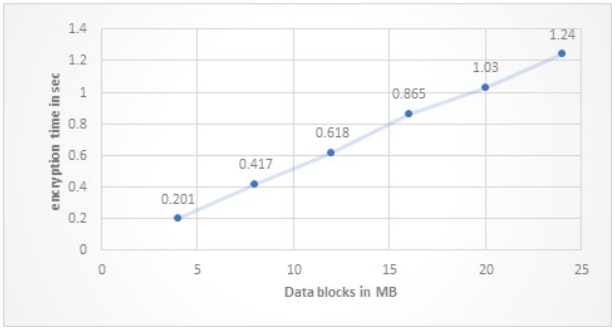

Figure 3b. *Performance of Encryption time.*

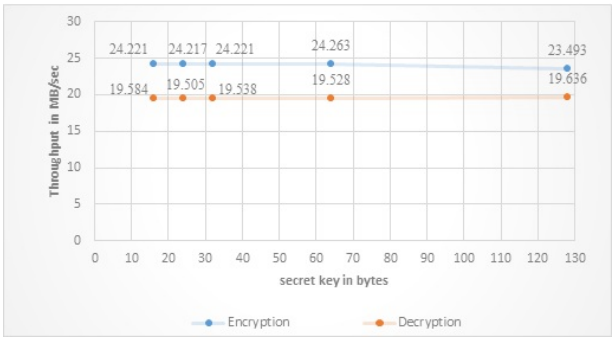

Figure 3c. *Performance of key length.*

Analysis of RDM embedding

The quality of the watermark image is found using two measuring metrics. They are listed below

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(E(i,j) - C_w(i,j)\right)^2 \rightarrow (5)$$

Where

m, n is the row and column values of the images.

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \rightarrow (6)$$

Usually when the embedding capacity is high PSNR will become low. But even though the embedding capacity is high PSNR is increased because degradation is high for low resolution bit plane watermarking. Thus the quality of image is high when embedding is done in low level bit plane which is shown in Figure 3d.

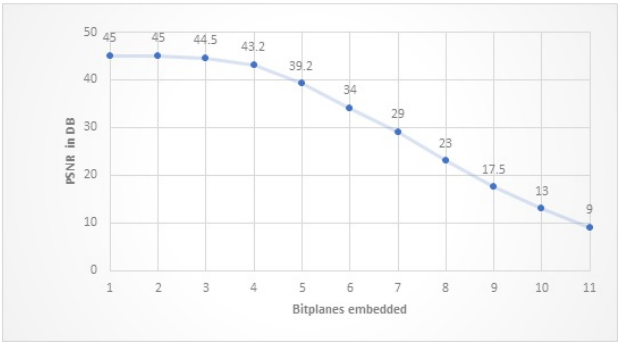

Figure 3d. *Performance of embedding capacity.*

Two sample images are taken for analysis and the details are listed below for all resolution in Figures 3e and 3f.

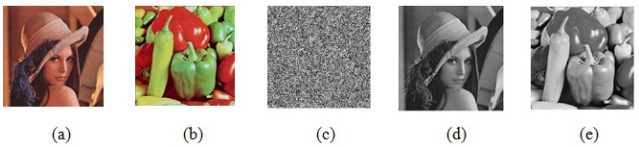

Figure 3e. *(a) Original image (41 KB) (b) Watermark (9 KB) (c) encrypted image (d) Watermarked image (43.2 DB) (e) Extracted watermark image.*

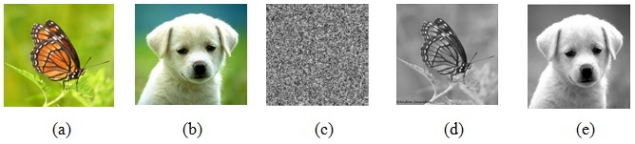

Figure 3f. *(a) Original image (46.1 KB) (b) Watermark (5.58 KB) (c) encrypted image (d) Watermarked image (44.5DB) (e) Extracted watermark image.*

Conclusion

This proposed method is suitable for copy right protection of biomedical images using MRC6 encryption algorithm and RDM watermarking method. The input medical image is in any image format and it is converted into the JPEG2000 compressed format and the encryption is done in a bit stream that makes the watermarking algorithm simple, as it was done in compressed/encrypted domain. Since the watermarking is done on the encrypted data, copyright protection is preserved. The PSNR values of the image before watermarking declare that the MRC6 encryption in the compressed domain proved that the image quality is good. The analysis between the effect of increasing data block size and encryption time proved that MRC6 is faster. Also the analysis between the throughput and increase in the key length shows that MRC6 is more secure than other block ciphers. While considering the performance of embedding capacity of RDM, it shows that RDM has low MSE values and high PSNR value thus proving the image quality is high when watermarking is done in the lowest significant level bit plane. The proposed architecture results in a highly secured output and has minimum encryption time. Also the embedding process is very fast and the watermarked image is of high quality. Future task is intended to work with spatial domain

watermarking algorithms to provide content authentication for medical images. Other encryption schemes may be integrated to make it more robust with less encryption time and maximum throughput.

References

1. Goldwasser S, Micali S. Probabilistic encryption. J Comput Syst Sci 1984; 28: 270-299.
2. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 1985; 31: 469-472.
3. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. Lecture Notes Comput Sci 1999; 1952: 223-238.
4. Subramanyam A, Emmanuel S, Kankanhalli M. Compressed encrypted domain JPEG2000 image watermarking. IEEE Int Conf Multimedia Expo 2010; 4: 1315-1320.
5. Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4, in Selected Areas in Cryptography. Lect Note Comp Sci 2001; 2259: 1-24.
6. Eldean AH, Kalash HM, Faragallah OS. Implementation of RC5 block cipher algorithm for image cryptosystem. Int J Inf Tech 2004; 3: 245-250, 2004.
7. Gayathri IK. Digital watermarking using rc5 encryption on JPEG2000 images. Int J Eng Res Tech 2013.
8. Johan B, Bart P, Joos V, Leuven KU. Linear Cryptanalysis of RC5 and RC6, FSE 1999. Lect Note Comp Sci 1999.
9. Rivest RL, Robshaw MJB, Sidney R, Yin YL. The RC6block cipher, AES-The First Advanced encryption standard candidate conference, 1998.
10. Mathew KA. Watermarking of JPEG2000 Compressed Images with Improved Encryption. Int J Comp Apps Tech Res 2013; 2: 245-249.
11. Gilbert H, Handschuh H, Joux A, Vaudenay S. Statistical Attack on RC6, FSE2000. LNCS 2000; 2365: 64-74.
12. Miyaji A, Takano T. Evaluation of the security of RC6 against the x2-attack. IEICE Trans Fundamental 2007; 90: 22-28.
13. Sun Q, Chang S, Kurato M, Suto M. A quantitive semi-fragile JPEG2000 image authentication system. Int Conf Image Process 2002; 2: 921-924.
14. Lian S, Liu Z, Zhen R, Wang H. Commutative watermarking and encryption for media data. Opt Eng 2006; 45: 1-3.
15. Battisti F, Cancellaro M, Boato G, Carli M, Neri A. Joint watermarking and encryption of color images in the Fibonacci-Haar domain. EURASIP J Adv Signal Process 2009.
16. Prins J, Erkin Z, Lagendijk R. Anonymous fingerprinting with robust QIM watermarking techniques. EURASIP J Inf Security 2007.
17. Li Z, Zhu X, Lian Y, Sun Q. Constructing secure content dependent watermarking scheme using homomorphic encryption. IEEE Int Conf Multimedia Expo 2007.
18. Cancellaro M, Battisti F, Carli M, Boato G, De Natale F, Neri A. A joint digital watermarking and encryption method. SPIE Security Forensic Steganograph Watermark Multimedia Cont X 2008; 6819: 68191C.
19. Zhigang C. A Novel Lossless Robust Watermarking Method for Copyright Protection of Biomedical Image. J Sci Nano 2013; 13: 2108-2116.
20. Wang MS, Chen WC. A majority-voting based watermarking scheme for colour image tamper detection and recovery. Comput Stand Interface 2007; 29: 561-570.
21. Eggers JJ, Girod B. Blind watermarking applied to image authentication. Proceed IEEE Int Conf Acoust Speech Signal Process, 2001.
22. Lin ET, Podilchuk CI, Delp EJ. Detection of image alterations using semi-fragile watermarks. Proceedings of SPIE conference on security and watermarking of multimedia contents II, 2000.
23. Kundur D, Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication. Proceed IEEE Identific Protect Multimedia Info 1999.
24. Nadeem. A performance comparison of data encryption algorithms. IEEE Info Commun Technol 2006.
25. Cox I, Doërr G, Furon T. Watermarking is not cryptography. In: Digital Watermarking, 2006; 4283: 1-15.
26. Farah T, Hermassi H, Rhoouma R, Belghith S. Watermarking and encryption scheme to secure multimedia information. Comput Info Technol 2013.
27. Bouslimi D, Coatrieux G, Roux Ch. A joint watermarking/ encryption algorithm for verifying medical image integrity and authenticity in both encrypted and spatial domains, Proc of Int Conf IEEE-EMBC, 2011; 8066-8069.
28. Wu H, Ma D. Efficient and secure encryption schemes for JPEG 2000, in Proc. IEEE Int Conf Acoustics Speech Signal Process 2004; 5: 869-872.
29. Rabbani M, Joshi R. An overview of the JPEG 2000 still image compression standard, Signal Process.: Image Commun 2002; 17: 3-48.
30. Fishawy NE, Danaf TE, zaid OA. A Modification of RC6 Block Cipher Algorithm for Data Security (MRC6). Proceed Int Conf Electrical Electronic Comput Eng 2004.
31. Nawal EF, Osama MAZ. Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms. Int J Network Security 2007; 5: 241-251.
32. Jorge N Jr, Gautham S, Daniel SF, Chang C, Ramon HDS, Bart P. A New Approach to $\chi 2$ cryptanalysis of block ciphers. Lect Note Comput Sci 2009; 5735: 1-16.
33. Engel D, Stutz T, Uhl A. A survey on JPEG2000 encryption. Multimedia Syst 2009; 15: 243-270.

*Correspondence to

Sebastin Antony Joe S
Anna University
Tamil Nadu
India