Compressed Image Authentication using CDMA Watermarking and EMRC6 Encryption

C.Seldev Christopher¹, S.J.,Jereesha Mary²*,S.Sebastian Antony Joe³

¹Department of CSE, St. Xavier’s Catholic College of Engineering, Chunkankadai-629003, India.
²Department of CSE, Loyola Institute of Technology and Science, Thovalai-629302, India
³Department of CSE, Loyola Institute of Technology and Science, Thovalai-629302, India.

*Corresponding author (E-mail: joejerisia@gmail.com)

Abstract

This paper proposes a robust watermarking technique called Code division Multiple Access (CDMA) which is used to provide authentication to medical images. CDMA is more resistant to attack when compared with other spatial domain schemes. The system is made robust by integrating the watermarking method with Enhanced Modified Rivet Cipher 6 (EMRC6) encryption. EMRC6 is a block cipher and is more secure and faster than its predecessor MRC6. The watermarked image and the extracted watermark have no visual impairment. Also the Peak Signal to Noise Ratio (PSNR) value is high and Mean Square Error (MSE) value is low when compared to the previous method where LSB technique is integrated with EMRC6 for image security. This method is targeted to increase the embedding capacity and robustness which are the basic requirement of medical image security.

Keywords: Watermark, Content Authentication, Encryption, Spatial Domain, Block Cipher

1. INTRODUCTION

Due to technological growth threat to the digital data become a great concern for the data owners. For example, work of an individual can be altered and accessed by another thus compromising the security. Hence encryption and watermarking are used together to protect the content. Watermarking is hiding the secret message inside the cover for the purpose of protecting it from illegal detection and attacks. Encryption is a cryptographic process in which the input data is converted into cipher text using a key which is in the non-readable format. Various medical image formats used for watermarking is explained by Michele (Michele, Larobina and Murino, 2016). Rabbani (Rabbani and Joshi, 2002) described a lossless image compression format for storing images of any type that occupies less storage space. Researchers proposed different watermarking methods for data authentication. To overcome the weakness of digital signature methods where explained by Lin (Lin, Podilchuk and Delp, 2000). In digital signature, data modification or tampering can be found out but the location could not be identified which was proposed by Kundur (Kundur and Hatzinakos, 1999).

Many scholars combined watermarking schemes with encryption algorithms to increase the security of the digital content. A symmetric stream cipher named RC4 encryption with homomorphic property was designed to work with watermarking methods which overcomes the weaknesses of other stream cipher was proposed by Subramanyam (Subramanyam, Emmanuel and Kankanahalli, 2010). A symmetric block cipher RC5, that is more secure due to its increased number of rounds and is used with the watermarking schemes was proposed by Gayathri (Gayathri, 2013). RC6 is being used instead of RC5 due to its increased use of registers which was proposed by (Mathew, 2013). Elashry (Elashry, Allah et al., 2009) used LSB method and integrated with RC6 to provide security with good image quality. But RC6 undergoes differential linear attack, statistical attack and X² attack which were explained by Miyaji (Miyaji and Takano, 2007). Enhanced version of RC6 (ERC6) is used which encrypts at about 17.3 MB/sec making it about 1.7 times faster than RC6. But it is prone to X² attack up to 44 rounds was depicted by Ragab (Ragab, Ismail et al., 2001). ERC6 a modified version of RC6 (MRC6) is used which has greater security at fewer rounds thus increasing the throughput with minimum encryption/decryption time was proposed by Fishawy (Fishawy, Danaf and Zaid, 2004). Extended Modified Version of RC6 (EMRC6) attains high security and maximum throughput in less number of rounds than MRC6 which was proved by Khanapur (Khanapur and Patro, 2015). A modified LSB watermarking for authenticating medical images with Huffman compression that finds tampering and recovers from tampering is proposed by Adiwijaya (Adiwijaya, Permana et al., 2013). Even though it can recover up to 98%, it is still prone to few attacks. A CDMA based reversible embedding scheme is proposed that is blind. This has high embedding capacity and is more robust even after embedding in the high PSNR value which was explained by Samee (Samee and Gotze, 2012).
From the literature survey it is concluded that for content authentication application, CDMA watermarking method in spatial domain can be used, since it has high embedding capacity and is fragile too. Also EMRC6 encryption can be chosen for encrypting the watermark as it is not prone to any attack. To reduce the storage and increase the execution speed JPEG2000 compression technique is used for compressing the input image. Hence the input is compressed using JPEG2000 and the watermark is encrypted using EMRC6 algorithm and finally both are watermarked using CDMA technology in spatial domain.

2. PROPOSED SYSTEM

The proposed system is targeted at merging CDMA watermarking method with extended modified version of RC6 (EMRC6) encryption scheme to provide content authentication for compressed medical images. The cover image ‘I’ may be of any image type and is the input to the JPEG2000 encoder. The encoder undergoes five stages where the image is split into rectangular tile that does not overlap and then it does discrete wavelet transformation (DWT) and is quantized and is further divided into different bit planes. This is then block coded with optimized truncation which results in stream of compressed byte which is packed into different wavelet packets. This JPEG2000 encoded output is represented as ‘Ij’. The watermark image represented as ‘Wm’ is encrypted using EMRC6 encryption using key ‘K’. The input stream undergoes 18 rounds each with 16 rotations to produce the output cipher ‘Ew’. This is encoded using CDMA method to obtain ‘Ce’. The encoded cover image ‘Ij’ and the output ‘Ce’ are given as input to the CDMA watermarking scheme. The CDMA embedding scheme replaces few characteristics of each pixel of the cover image ‘Ij’ with few information from the watermark ‘Wm’. Thus the output of embedding process is the watermarked image ‘We’ which is highly secure and has good image quality. The PSNR value is high and MSE value is low when compared to the previous method where LSB technique is integrated with EMRC6. Figure 1 show the embedding of the watermark in the encrypted domain.

![Figure 1. Embedding of Watermark](image)

2.1 JPEG2000 Encoder

In this algorithm the input is any image and this image is converted into JPEG 2000 compressed code image using JPEG 2000 encoder by undergoing five steps. The image is split into non overlapping tiles which are unsigned values and is reduced by a constant value in the first step. Then Discrete wavelet Transformation (DWT) is done which followed by quantization and then the co-efficient are split into different bit-planes using embedded block coding with optimized truncation (EBCOT) coding method. As a final step compressed stream are packed into different wavelet packages. This was detailed in the paper proposed by Wu (Wu and Ma, 2004). These are given as one of the input to the watermarking scheme.

2.2 Enhanced Modified Rivest Cipher6 (EMRC6)

EMRC6 (32/18/16) has 32 registers each with ‘w’ bit words. It has an integer multiplication as basic operation which increases the diffusion attained per round. This provides high security, increase in number of rounds and greater throughput. It can process 1024 bits as a single block per round. The EMRC6 algorithm has three basic modules.

- EMRC6 key expansion.
- EMRC6 encryption.
EMRC6 decryption.

2.2.1 EMRC6 Key Expansion

In EMRC6, more number of words is extracted from the key supplied by the user. The key of length ‘b’ bytes where 0 ≤ b ≤ 255 is supplied by user. Then enough zeroes are added to make the length of the key equal to non-zero integral values and stored in U[0], U[1]…U[b-1]. Then it is stored in the little endian format as V[0],V[1]…V[c-1] which is expanded and stored in a table T[0],T[1]…T[16r+31], thus making 16r +32 sub keys. Contents of ‘T[]’ is shifted thrice by left barrel shifter. Code 1 show the key expansion algorithm.

\[
T[0] = P_w
\]

For i = 1 to 16r+31 do
\[
T[i] = T[i-1] + Q_w.
\]
R[i] = R[j] = i = j = 0
\[
z = 3 \times \text{Max} (c, 16r+32)
\]
for y = l to z do{
\[
R_1 = T[i] = (T[i] + R_1 + R_2) \ll 3;
\]
\[
R_2 = V[j] = (V[j] + R_1 + R_2) \ll (R_1 + R_2);
\]
i = (i+1) Mod(16r+31);
\[
 j = (j+l) \text{ Mod } c;
\]
}

Where
\[
P_w = \text{odd } ((e - 2) 2^w)
\]
\[
Q_w = \text{odd } ((\emptyset - 1) 2^w).
\]
e = 2.7182818 and
\[
\emptyset = 1.618033 \text{ is called the golden constant.}
\]

Code 1. Key expansion algorithm

2.2.2 EMRC6 Encryption Algorithm

The steps involved in EMRC6 encryption are Addition (+), Bitwise EX-OR operation, Left rotation, a<<<b and Integer Multiplication modulo 2^w (*). Code 2 shows the encryption algorithm for EMRC6.

Input: The watermark bits are stored in 16 word bit input array R[i] (i=1 to 32), Number of rounds ‘r’ and sub key set T[i] and ‘w’ is fixed as 32.

Output: ciphered watermark in array Q[j].

\[
/* \text{ contents in even locations are added with the key */}
K=2;
\]
for (i=0; i≤ 15;i++){
\[
R[k]= R[k]+T[i];
K=K+2;
\]
}
for (i=1; i≤r;i++){
\[
// \text{ Bits in even locations are manipulated}
K=2;
\]
For (j=0; j≤15;j++){\[
a[j]=(R[k] * (2 * R[k] +1)) \ll \text{log}(w);
k=k+2;
\]
}
// Bits in odd locations are manipulated
x=1;
For (i=0; i≤ 15;i++){
\[
y=i;
R[x] = ((R[x] \oplus a[i]) \ll a[y+1] + T[16*i]+l
x=x+2;
R[x] = ((R[x] \oplus a[i+1]) \ll a[y] + T[16*i]+(l+1])
\]
(l=l+1;
  x=x+2;
}) /*The entire 32 bit words are right shifted and stored in a temporary array */
Q[31] = R[0];
For (m=0; m≤30;m++){
  Q[m] = R[m+1];
}
/* contents in odd locations are added with key */
j=1 ; k=16;
For (y=0; y≤15;y++) {
  Q[j] = Q[j] + T[(16*r)+k];
  k=k+1;
  j=j+2;
}

Code 2. Encryption of EMRC6

2.2.3 EMRC6 Decryption Algorithm

The EMRC6 decryption process reproduces the original content from the cipher using the sub key. This is the inverse operation of EMRC6 encryption. Code 3 represents the EMRC6 decryption process. Various steps involved in decryption process are Integer subtraction (-), Bit wise EX-OR, Integer multiplication and Right shift (a>>>b).

/* contents in odd locations are removed from key */
j=31 ; k=31;
for (y=15; y≥0;y--)
{
  Q[j] = Q[j] - T[(16*r)+k];
  k=k-1;
  j=j-2;
}
For(i = r; i≥ 1; i++)
{
  /* The entire 32 bit words are left shifted and stored in another array temporarily */
  R[0] = Q[31];
  For (m=0; m≤30;m++)
  {
    R[m] = Q[m-1];
  }
  // Bits in even locations are manipulated
  K=32;
  For (j=15; j≥0;j+)
  {
    a[j]=(R[k] * (2 * R[k] +1)) <<< log(w);
    k=k-2;
  }
  // Bits in odd locations are manipulated
  x=31;
  For (l=15; l≥0;l--)
  {
    y=l;
    R[x] = ((R[x] -T[(16*i)+l])>>>a[y]) ⊕a[l-1];
    x=x-2;
    R[x] = ((R[x] -T[(16*i)+(l-1)])>>>a[y-1]) ⊕a[l];
    l=l-1;
  }
x=x-2;
}
} /* contents in even locations are removed from key */
K=32;
for (i=32; i≥15;i++){
   R[k]= R[k]-T[i];
   K=K-2;
}

Code 3. EMRC6 Decryption algorithm

2.3 Collision Detection Multiple Access (CDMA)

Collision Detection Multiple Access (CDMA) has greater capacity than other spatial domain schemes. In this method, the watermark is primarily structured as a lengthy string instead of a 2D image. Then a PN sequence using an independent seed is formed for every value of the watermark. The watermark is represented by grouping all of these PN sequences. This grouped watermark is then scaled and appended to the cover image. The Watermark is encoded to obtain the sequence denoted by ‘C_e’ as shown in equation (1)

\[ C_e = \{W_k(i)\} = \{\sum_n w_n g_n(x)\}; \ k = 1,2,3,... 512 \] (1)

The vector ‘w’ which has the collection of watermark bit stream is represented as shown in equation (2)

\[ w \in \{w_1, w_2, .... w_n\} \] (2)

Where
\[ w_i \in \{-1, +1\} \rightarrow i^{th} \text{ bit of the watermark bit stream.} \]
\[ g_n(x) = \{-1, +1\} \rightarrow x^{th} \text{ bit of the n^{th} sequence of the orthogonal gold sequence.} \]

The gold code sequence ‘g_n(k)’ is assigned to each watermark identifier. After encoding, the binary watermark data \( W_k(i) \) is embedded into the input image.

3. ANALYSING AND EVALUATING THE PERFORMANCE

The performance evaluation of the proposed system with the existing one is done in this module.

3.1 Analysing EMRC6 Encryption

EMRC6 is better than any other version of RC6 due to its increased complexity, low throughput and high security.

3.1.1 Security Issues

Figure 2 shows that the encryption time is increased with increase in the size of the data block. But when compared with the previous version of RC6 it has got better encryption time.

Figure 2. Result of encryption time over varied data size
Figure 3 shows that throughput decreases with increased number of rounds which gives the conclusion that the security is high with more number of rounds since security and throughput are inversely proportional.

![Graph for Throughput](image)

**Figure 3.** Consequence of number of rounds on throughput

### 3.1.2 Correlation Coefficient

Correlation Coefficient is used to measure the image quality between the pixels in the original image and watermarked cipher image at a particular location. Table 1 shows the correlation coefficient of three sample images which concludes that the correlation coefficient is low when compared with other encryption. Coefficient Correlation $\gamma(I, C)$ is found using equation (3). The Expectation and variant value to be substituted in equation (3) is found using equation (4) and equation (5).

$$
\gamma_{IC} = \frac{E[(W_m - E(W_m))(E_w - E(E_w))]}{\sqrt{D(W_m)D(E_w)}} \quad (3)
$$

$$
D(W_m) = \frac{1}{n} \sum_{i=1}^{N}(W_{mi} - E(W_m))^2 \quad (4)
$$

$$
E(W_m) = \frac{1}{n} \sum_{i=1}^{N}(W_{mi}) \quad (5)
$$

<table>
<thead>
<tr>
<th>Image</th>
<th>Nike</th>
<th>Lena</th>
<th>Girls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlation coefficient</td>
<td>0.00016</td>
<td>0.0021</td>
<td>0.00002</td>
</tr>
</tbody>
</table>

### 3.2 Analysis of CDMA Embedding

The image quality of the output watermarked cipher image ‘$W_c$’ is found using the PSNR calculation. Equation (6) depicts the PSNR calculation in which the MSE value is calculated using equation (7).

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

$$
\text{MSE} = \frac{1}{mn} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} (I(x,y) - W_c(x,y))^2 \quad (7)
$$

Where,

- $m, n$ is the row and column values of the images.
- $x, y$ is the pixel values of the images.
The PSNR value from table 2 predicts that the PSNR value of the sample images is high and hence the quality of the watermarked cipher image is of good quality.

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>Nike.png</th>
<th>Lena.bmp</th>
<th>Girls.jpg</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>43.6</td>
<td>44.1</td>
<td>47.2</td>
</tr>
</tbody>
</table>

### 3.3 Test Results

The working model under study is discussed and their overall results are being mentioned in table 3.

<table>
<thead>
<tr>
<th>Input Image</th>
<th>Watermark</th>
<th>Encrypted watermark</th>
<th>Watermarked cipher output</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Size of the Original Image</th>
<th>45Kb</th>
<th>657Kb</th>
<th>68Kb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of Watermark Image</td>
<td>6 Kb</td>
<td>18 Kb</td>
<td>10 Kb</td>
</tr>
<tr>
<td>PSNR of Watermarked cipher image</td>
<td>43.6</td>
<td>44.1</td>
<td>47.2</td>
</tr>
<tr>
<td>Correlation coefficient of encrypted watermark</td>
<td>0.00016</td>
<td>0.0021</td>
<td>0.00002</td>
</tr>
</tbody>
</table>

### 4. Conclusion

The combination of EMRC6 Scheme with CDMA watermarking technique is a proper method for medical image authentication. The input image is converted into JPEG2000 image to make encryption and embedding scheme simple. EMRC6 provides high security since it withstands almost all attacks which was imposed on previous RC6 version. Even though CDMA is a spatial domain watermarking scheme, it is best suited for content authentication. The Encryption speed of EMRC6 is high and the throughput is high when compared with its predecessor. The correlation coefficient is very low proving that the image quality is good. After embedding the PSNR value is high and MSE value is low when compared with other algorithm. The future work is aimed to provide copyright production using a frequency domain algorithm and EMRC6 encryption scheme.

### REFERENCES


