Block Encryption and Static Watermarking for Intellectual Property Protection

[1] Dr. S. J. Jereesha Mary, [2] Dr.S.Sebastin Antony Joe, [3] E.Edwin Jijo
[1] Annai Vailankanni College of Engineering, [2] Gulf College,oman, [3] Military Technological College

Abstract*— The rapid growth in the transmission of information through the internet has given attention on information security for decades. Digital data like text, image, audio and video in the digital form are the major components being transmitted over the internet. In everyday life, images like diagrams, paintings, digital arts constitute the major part of multimedia content. This paper consists of a model for intellectual property protection system that is a combination of Modified Least Significant Bit embedding (MLSB) and Enhanced Modified Rivet Cipher 6 (EMRC6) for encryption. The input data is either text or two dimensional image but this model can be extended to video data too. The MLSB embedding scheme is a static watermarking method which is an improvement of the basic Least Significant Method (LSB) and is suitable for authentication purpose. The EMRC6 encryption scheme is a block cipher which is faster and secure than its predecessors. Since a static watermarking scheme and a block encryption schemes are integrated together, this model provides a high level of security and increases the payload. The output digital image has good visual clarity, since the PSNR value is around 44 dB on an average and the correlation coefficient is near to zero. The encryption time is very low and the throughput is high thus concluding that the working model is very fast.

Index Terms— ***MLSB; EMRC6; watermarking; Encryption; Authentication.***

I. INTRODUCTION

This paper investigates various existing method for the Intellectual property protection. The theory of Intellectual property protection for images were studied by researchers over a decade and as a key to this various watermarking schemes and encryption schemes have been used to protect the digital information that is transmitted over the internet.

Leitao [1] proposed a method with Watermarking and Fingerprinting techniques to protect Intellectual property. The Watermarking technique which is based on signature.

Subramanyam et al. [2] proposed an embedding scheme for JPEG images that are encrypted and partially compressed. The ciphering scheme used is RC4 and embedding is processed by quantizing the DCT- coefficient and then coding is done using VLC technique. Sebastin et al. [3] proposed a model in which Intellectual property protection is achieved by RDM embedding and MRC6 encryption method. RC6 is a block cipher being designed to overcome the downsides of the stream cipher RC4 and block cipher RC5 proposed by Rivest at el[4]. But this block ciphers RC6 undergoes attacks such as differential linear attack, statistical attack, X2 attack with 16 rounds, less than 16 rounds and more than 16 rounds respectively [5,6,7]. Prasad et al. designed a robust watermarking scheme in the compressed encrypted domain using AES encryption and combined DCT-DWT embedding method. As two types of transformation is done, the embedding is more robust. The encryption algorithm used here is prone to differential cryptanalysis and many more [8]. Guo et al. explained a cryptosystem that is homomorphic in nature. After encrypting the input image using PAILLIER cryptosystem, it protects the original images by watermarking them with a combination of DCT-DWT based methods. The visual clarity and robustness of the output is satisfactory. But the computational cost and space occupiedis more [9]. The EMRC6 encryption scheme is a block ciphering method which is faster than other version of RC6. It is better than all block cipher schemes and is not prone to any attack [10]. EMRC6 achieves better results when integrated with CDMA technology to produce a robust model for DRM system [11].

II. PROPOSED SYSTEM

The proposed model gives emphasis on providing Intellectual property protection to digital image with a combination of a faster encryption scheme like EMRC6 and a spatial domain watermarking algorithm like MLSB. As per the literature survey made, EMRC6 is not prone to any kind of attacks and MLSB is suitable for high payloads.

A. Selecting cryptographic Method

Enhanced Modified Rivest Cipher Version 6 (EMRC6) algorithm for encryption and decryption uses 32 registers and has an integer multiplication as an extra basic operation to improve the security. EMRC6 has 16 rotations per round and hence is three times faster than its parent RC6.The throughput of the encryption algorithm is high when compared to its predecessor MRC6. The 16r+32 sub-keys are a great strength to EMRC6 and hence it is robust against all the attacks that are being applied over its predecessor. The various procedures used in this ciphering process are:

1. EMRC6 key generation.
2. EMRC6 Encipherment.
3. EMRC6 Decipherment.

1. *EMRC6 key generation*

The key generation process of EMRC6 is done separately, in which (16r +32) key 'K' is generated from the user supplied key of length 'b', where $0 \leq b \leq 255$. The key generation algorithm is shown in Fig. 1. This process is done prior to encipherment.

```
e=2.718281;
Ø=1.618033;   // is called the golden constant.
Pw = odd ((e -2) 2w);
Qw= odd ((Ø -1) 2w);
T[0] = Pw
for i = 1 to 16r+31 do
   T[i] = T[i-1] + Qw;
   R[i] = R[j] = i = j = 0
   z = 3 * Max (c, 16r+32)
```

```
for y = l to z do
   {
     R1 = T[i] = (T[i] + R1 +R2) <<< 3;
     R2 = V[j] = (V[j] + R1 +R2) <<<(Rl+R2);
     i = (i+1) Mod(16r+31);
     j = (j+l) Mod c;
   }
```

Fig. 1. Key generation Algorithm

2. *EMRC6 Encipherment.*

The steps involved in EMRC6 encryption are Addition (+), Bitwise EX-OR operation, Left Rotation, a<<<b and Integer Multiplication modulo 2n(*). The input to the algorithm is the image bits, stored in 16-word input array R[i] (i=1 to 32), Number of rounds 'r', sub-key set T[i] and 'w' is fixed as 32. The output is ciphered output stored in array Q[j]. Fig. 2 depicts the encipherment process of EMRC6.

```
K=2;
for (i=0; i≤15; i++)
{
      R[k]= R[k]+T[i];
      K=K+2;
}
for (i=1; i≤r; i++)
{
      K=2;
      for (j=0; j≤15; j++)
      {
          a[j]=(R[k]*(2*R[k] +1)) <<< log(w);
          k=k+2;
      }
      x=1;
      for (l=0; l≤15; l++)
      {
           y=l;
           R[x] = ((R[x] a[l]) <<<a[y+1] + T[(16*i)+l]
           x=x+2;
           R[x] = ((R[x] a[l+1]) <<< a[y] +T[(16*i)+(l+l)]
           l=l+1;
           x=x+2;
      }
      Q[31] = R[0];
      for (m=0; m≤30; m++)
      {
          Q[m] = R[m+1];
       }
}
j=1;
k=16; for (y=0; y≤15; y++)
{
Q[j] = Q[j] + T[(16*r)+k];
k=k+1;
j=j+2;
}
```

Fig. 2. Encipherment Algorithm

3. *EMRC6 Decipherment.*

The steps involved in EMRC6 encryption are subtraction (-), Bitwise EX-OR operation, Right Rotation, a>>>b and Integer Multiplication modulo 2n(*). The input to the decipherment process is the cipher bits stored in 16-word array Q[j] (j=1 to 32), Number of rounds 'r', sub-key set T[i] and 'w' is fixed as 32. The deciphered output is stored in array R[j]. Fig. 3 shows deciphering process of EMRC6.

```
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++)
{
     R[0]= Q[31];
     for (m=0; m ≤ 30; m++)
     {
      R[m]=Q[m-1];
      }
      K=32;
       for (j=15; j ≥ 0; j++)
      {
      a[j]=(R[k]*(2*R[k]+1))<<< log(w);
      k=k-2;
      }
      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-z]) a[l];
      l=l-1;
       x=x-2;
       }
 }
 K=32;
for (i=32; i ≥15; i++)
{
   R[k]= R[k]-T[i];
   K=K-2;
}
```

Fig. 3. Decipherment Algorithm

B. Selecting Embedding method

Modified Least Significant Bit (LSB) technique is based on exchanging few characteristics of each pixel last bit with some of the information from the input image. In order to overcome the common disadvantages of LSB embedding, a Pseudo Random Number Generator (PRNG) is used.

1. *MLSB EMBEDDING ALGORITHM*

- 'Ew' is read and is stored as matrix element 'Ew[][]'.
- 'Ij' is normalized and rounded off to the adjacent integer with a bit precision of eight.

- Determine the size of 'Ew' and 'Ij'.
- 'Ij' is split into pixel and stored in 'Ij[][]'.
- Expand 'Ew[][]' such that the size of watermark is same as that of 'Ij'. The Components in 'Ew[][]' are individual bits that represent pixel values of the 'Ew'.
- The pixel in 'Ij[][]' is chosen based on the pseudo random number being generated.
- The LSB of the chosen pixel from 'Ij[][]' is replaced by the matching elements from 'Ew[][]'.
- The resultant matrix is converted into the watermarked image.

2. MLSB EXTRACTION ALGORITHM

- 'We' is read and is stored as matrix element 'We[][]'.
- Find the size of 'We'.
- An expansion matrix is formed by extracting the MLSB of each pixels from 'We[][]' based on the values generated from the PRNG.
- The bits per pixel of 'We' are determined and the bits are clustered based on it. The expansion matrix consists of repeated pattern of bits at constant intervals.
- Thus multiple watermarks are recovered inside the expansion matrix.

C. Working DRM system model

The cover image 'I' may be of any image type and is given as input to the JPEG2000 encoder. This JPEG2000 encoded output is represented as 'Ij'. The watermark image represented as 'Wm' is encrypted using Extended Modified version of RC6 (EMRC6) with the help of the key 'K' to produce the output cipher text 'Ew'.

The Encoded cover image 'Ij' and the output cipher 'Ew' are given as input to the MLSB watermarking scheme. The MLSB embedding scheme replaces few characteristics of the last bit of each pixel of the cover image 'Ij' with few information from the watermark image 'Wm'. A pseudo Random Number generator (PRNG) that produces a seed value is used with the LSB embedding in order to overcome the attacks on LSB embedding since it is a fragile scheme. Thus the output of the embedding process is the watermarked image 'We' which is highly secure and has good image quality. The reverse process of watermark embedding is the watermark extraction process in which the watermark is retrieved without any visual difference. The insertion process and the extraction process are shown in Fig. 4.

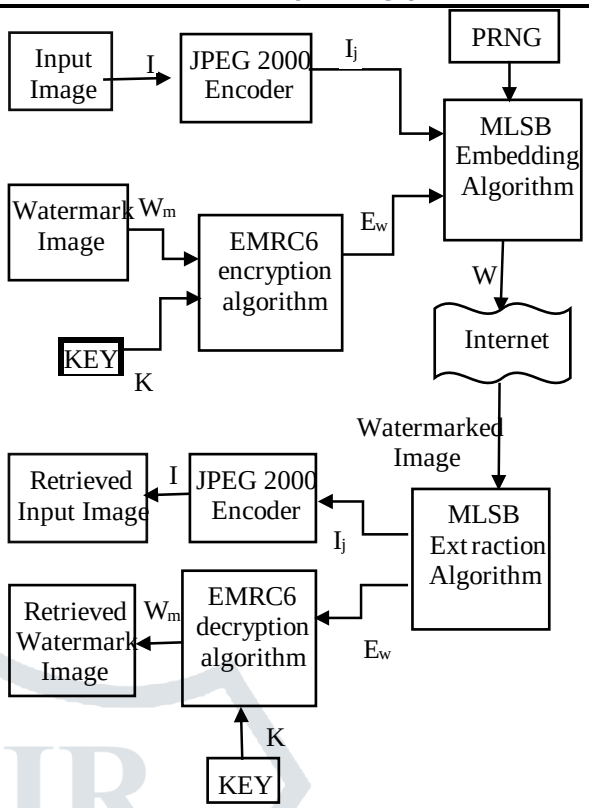

Fig. 4. Model for Intellectual property protection

III. RESULT ANALYSIS

A. Analysis of proposed model

The performance is measured using a variety of measuring metric named encryption time, throughput, correlation coefficient and PSNR. Encryption time, throughput, are used to calculate the working effectiveness of the ciphering method, which is shown in Fig. 5 and Fig. 6 respectively. The correlation coefficient is found for the encrypted input and PSNR is calculated for the watermarked output and is listed in TABLE I and TABLE II respectively.

The encryption time is increased with increase in the size of the input data blocks which is shown in Fig. 5.

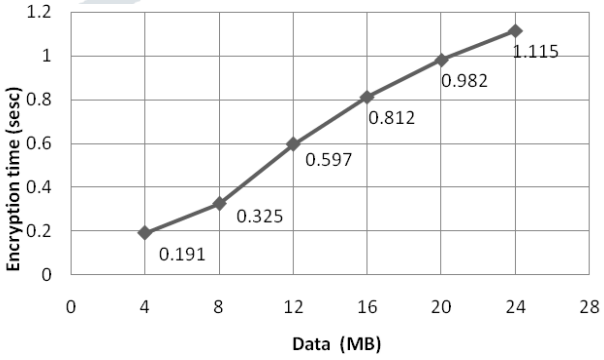

Fig. 5. Encyption time for ciphering the input

The throughput of any system is inversely proportional to the security of any system. From the values in the graph below it is shown that the increase in the number of rounds decreases

the throughput and hence it is concluded that the system is robust.

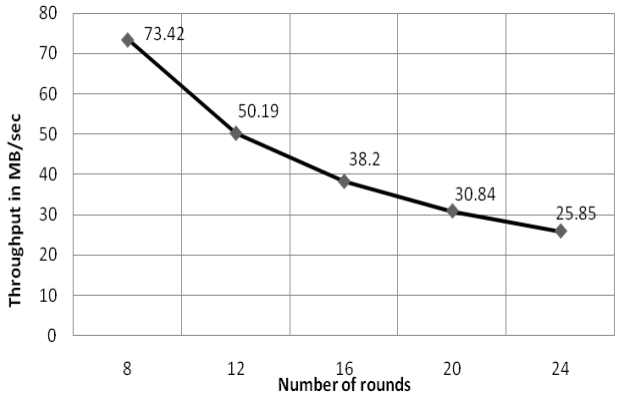

Fig. 6. Throughput for ciphering the input

The values calculated using equation (1), (2) and (3), show that the correlation coefficient of the enciphered blocks with respect to the original data are near to zero, thus indicating that there is no similarity between the input data block and the enciphered data block. As there is no similarity between the two, it concludes that the cipher text is highly secure.

$$\gamma_{IC} = \frac{E\left((W_m - E(W_m))(E_w - E(E_w))\right)}{\sqrt{D(W_m)D(E_w)}} \quad (1)$$

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

$$E(W_m) = \frac{1}{n}\sum_{i=1}^{N}(W_{m_i}) \quad (3)$$

TABLE I. CORRELATION COEFFICIENT OF CIPHER TEXT

Image	Image 1	Image 2	Image 3
Correlation coefficient	0.00180	0.00149	0.00132

Theoretically, it is said that the image has good perceptibility when the PSNR value is more than 40 dB, and the values calculated using equation (5) show that the PSNR value obtained using this proposed model is around 40 dB and hence the output watermarked image has good image quality and lesser distortion.

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

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}\left(I_j(x,y) - W_e(x,y)\right)^2 \quad (5)$$

TABLE II. PSNR VALUES FOR WATERMARKED OUTPUT

Image	Image 1	Image 2	Image 3
PSNR	43.91	44.36	47.7

B. Comparison with other model robust

A comparison of the proposed model was made with the model designed by Sebastin et al. [5] and it is concluded that the proposed model overcomes it, in terms of speed of execution, robustness, security and visual perceptibility.

From Fig.6 it is proven that the encryption time of EMRC6 is less than the encryption time of MRC6. Hence it is proved that the former encryption scheme is much faster than the latter one.

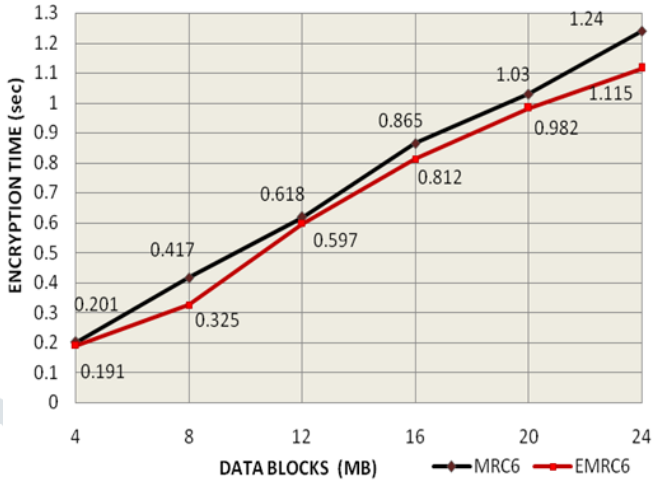

Fig. 7. Comparison of Encryption time

From Fig.7 it is concluded that the proposed system with EMRC6 ciphering scheme has more throughput than the previous system with MRC6 ciphering scheme for the same number of rounds.

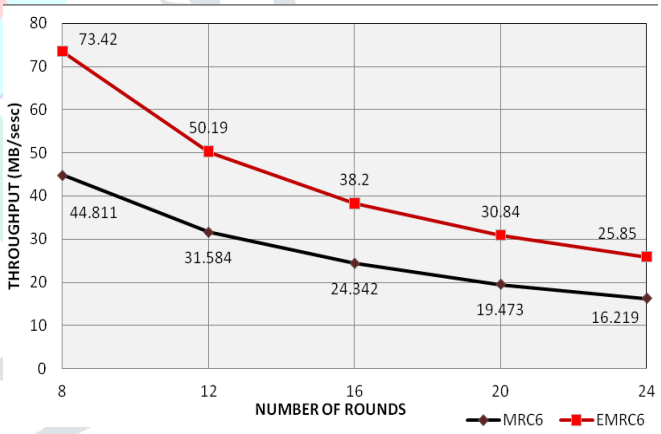

Fig. 8. Comparison of Throughput

From TABLE III it is concluded there is no similarity between the input image and cipher image, since the correlation coefficient is near to zero. TABLE IV concludes that the visual perceptibility is more for the output obtained using MLSB than LSB.

TABLE III. COMPARISION OF CORRELATION COEFFICIENT

Image	Image 1	Image 2	Image 3
EMRC6	0.00180	0.00149	0.00132
MRC6	0. 0001527	0.0029	0.00012

TABLE IV. COMPARISION OF PSNR VALUES

Image	Image 1	Image 2	Image 3
LSB	43.6	44.1	47.2
MLSB	43.91	44.36	47.7

CONCLUSION

The proposed model which is modeled using EMRC6 ciphering algorithm and MLSB watermarking scheme is more robust than the existing models. This model has low encryption time hence the algorithm works faster. Also it has high throughput than other ciphering schemes and it is not prone to X2 attack which is applied on its predecessor. The perceptibility and robustness are also comparatively good with MLSB system and this model withstands all watermarking attacks like JPEG compression attack, scaling attacks, removal and geometrical attack. Hence this model is best suitable for Intellectual property protection of image data.

REFERENCES

[1] F. Leitao, "Intellectual property (IP) protection using Watermarking and Fingerprinting techniques," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, Bangalore,pp. 433-438. doi: 10.1109/ICATCCT.2016. 7912038.

[2] Subramanyam AV & Sabu Emmanuel, 2014, 'Partially compressed-encrypted domain robust JPEG image watermarking', Multimedia tools and applications, 71.3:1311-1331.http://dx.doi.org/10.1007/s11042-012-1272-0

[3] Sebastin Antony Joe S, Jereesha Mary S. J & Seldev Christopher C, 2016, Biomedical Research; vol. 27, no. 4, 'Novel watermarking scheme with watermark encryption for copyright protection'.

[4] Rivest RL, Robshaw MJB, Sidney R, Yin YL. The RC6 block cipher, AES-The First Advanced encryption standard candidate conference, 1998.

[5] Johan B, Bart P, Joos V, Leuven KU. Linear Cryptanalysis of RC5 and RC6, FSE 1999. Lect Note Comp Sci 1999.

[6] Gilbert H, Handschuh H, Joux A, Vaudenay S. Statistical Attack on RC6, FSE2000. LNCS 2000; 2365: 64-74.

[7] Miyaji A, Takano T. Evaluation of the security of RC6 against the x2-attack. IEICE Trans Fundamental 2007; 90:22-28.

[8] Prasad V, Chandra & Maheswari S, 2013, 'Robust watermarking of AES encrypted images for DRM systems', International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), IEEE, http://dx.doi.org/10.1109/ice-ccn.6528490.

[9] Guo, Jianting, Peijia Zheng & Jiwu Huang, 2015, 'Secure watermarking scheme against watermark attacks in the encrypted domain', Journal of Visual Communication and Image Representation, http: //dx. doi. org/ 10.1016/j.jvcir, pp. 125-135.

[10] Nanda Hanamant Khanapur and Arun Patro, 2015, 'Design and Implementation of Enhanced version of MRC6 algorithm for data security', International Journal of Advanced Computer Research, Volume-5,Issue-19,June,pp.225-232.

[11] Jereesha Mary S J, SeldevChristopher & Sebastin Antony Joe S, 2016, Technical Journal of the Faculty of Engineering, TJFE, (64): 'Novel scheme for compressed image authentication using CDMA watermarkingand EMRC6 encryption'.