International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

A Hybrid Approach with Watermark Encryption for Digital Data Protection.

[1]M.Sri Lakshmi,[2]Vallamkonda Sai Manogna, [3]Ediga Usha Rani
[1]Asst.professor, Dept. of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool.

[2,3]B.Tech Final Year Student, Dept. of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool.

Abstract: *-Now a day's digital technology plays vital role in every segment for ease of data transmission and sharing using internet across the different corners of the universe. Security is a prime concern therefore copyright data protection, tamper proof, data authentication, and facsimile protection to the digital data has to be assured in certain techniques.A digital Watermarking technique has come into social media area to protect image security to ensure this; various security concepts have been introduced. This paper recommends hybrid approach, provides more solid grounds for an effective security of digital images i.e ARC6 (Augmented Rivest Cipher 6) and RDM (Rational dither modulation) technique. A Hybrid approach to provide copyright protection to the digital data. The proposed method uses an encryption algorithm to encrypt the compacted 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.*

Keywords: *Watermark, ARC6, Rational dither modulation (RDM), Copyright protection.*

1. Introduction

The rapid continuous increase in exchange of multimedia data over protected and unprotected networks such as the worldwide available internet and local networks such as shared networks and local area networks etc. has encouraged activities such as unauthorized access, illegal usage, disruption, alteration of transmitted and stored data.[1] This widely spread use of digital media over the internet such as on social media, won cloud storage systems etc. and over other communication medium such as satellite communication systems have increased as applications and need for systems to meet current and future demands evolved over the years[2]. Security concerns with regards to such data transmission. Usually the contents transferred over the network are in the compressed/encrypted format and hence watermarking is the right technique for various applications 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. Cryptography is the fundamental platform in which modern information security, which involves the use of advanced mathematical approaches in solving hard cryptographic issues, has gained its grounds in the digital world [3] Where we use secure crypto graphic system i.e. Symmetric or Asymmetric crypto systems that present Homomorphic property which ensure the copyright protection. The combination of both cryptographic and watermarking techniques can provide some important solutions for securing digital images. This hybrid approach will provide more solid grounds for an effective security of digital images.

In this paper, we proposed a hybrid cryptographic and digital watermarking technique for securing digital images based on a Generated Symmetric Key. The cryptographic encryption technique made use of both digital image pixel displacement and visual cryptographic encryption techniques in securing the digital images engaged in the process.

Digital watermarking procedure mainly classified into three steps

- Embedding
- Distribution
- Extraction or Detection

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Embedding is the process where a secret data i.e. either an image or an audio or video is embedded into a input data which may an image or an audio or video, using a key. Then this embedded data is broadcast or distributed through a lossless or lousy channel, which is known as distribution. The process is shown in figure 1.

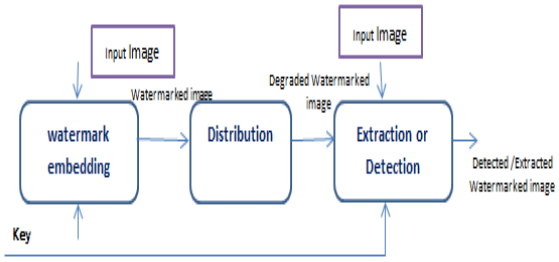

Figure 1. Basic model for Copyright protection using watermarking.

2. System Study

2.1 Presented system

Digital technology plays vital role in every segment for ease of data transmission and sharing using internet across the different corners of the universe. Security is a prime concern consequently copyright data protection, tamper proof, data authentication, and facsimile protection to the digital data has to be assured in certain techniques [4]. While sharing data over internet security is the prime concern as per our presented system. In the presented system watermarking technique has been applied on plain data. Thus there is a risk for digital data which consist lack of copyright data protection, tamper proof, data authentication, and facsimile protection.

2.2 Proposed system

The proposed system is aimed at combining LSB watermarking method with Augmented Version of RC6 (ARC6) encryption scheme to provide content authentication for compressed images. The cover image may be of any image type and is given as input to the JPEG2000 encoder. The JPEG2000 encoder processes the input image by undergoing five stages by dividing the image into rectangular tile that does not overlap and then it undergoes discrete wavelet transformation (DWT) and is quantized and is further divided into different bit planes.

The block diagram of the proposed work is as shown in Figure 1 [5]. The symbols used in the block diagram are described in Table1.

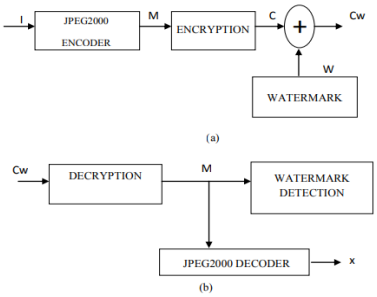

Table 1. Symbol and output image

I	Input Image
M	Compressed Image
C	Encrypted Image
W	Watermark
C_w	Watermarked Image
X	Decoded Image

Figure 2. Block diagram of (a) watermark embedding (b) watermark extraction

JPEG2000 Encoder

In the Proposed 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. First the image is split into non overlapping tiles which are unsigned values and is reduced by a constant value. Then Discrete wavelet Transformation (DWT) is done followed by quantization and further 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

3. Augmented Rivest Cipher 6 (ARC6)

ARC6 (32/18/16) has 32 registers each with 'w' bit words, whereas the working registers is less in numbers in the previous version of RC6. ARC6 has an integer multiplication as an extra 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 ARC6 algorithm has three basic modules.

1) ARC6 key expansion.

2) ARC6 encryption.

3) ARC6 decryption

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

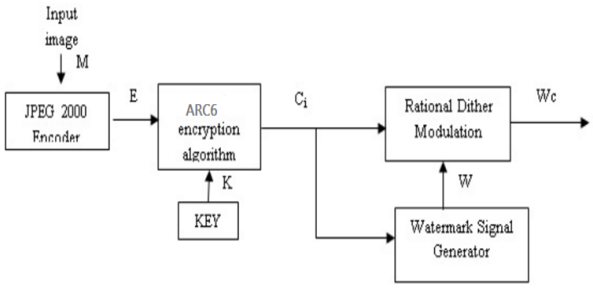

Figure 3(a). Watermark embedding.

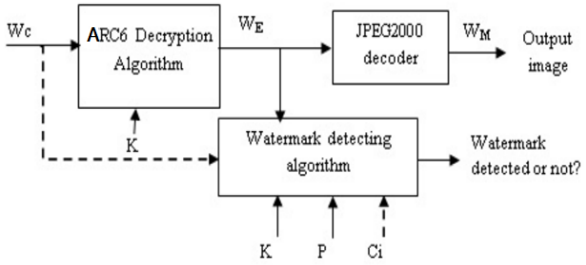

Figure 3(b). Watermark detection.

3.1 Key expansion algorithm

The key expansion algorithm of ARC6 is almost similar to the one in the previous version of RC6. But the main difference in ARC6 is, more number of words are extracted from the key supplied by the user. The key of length "b" bytes where $0 \leq b \leq 255$ is supplied by the user.

Input: An array V[0,1,2,…,c-1] that contains 'b' bytes of user supplied key converted to 'c' words and 'r' number of rounds.
Output: An array S[0,1,2,…,16r+31] that has w-bit round keys
Procedure:

```
T[0] = Pw                    // Pw value is defined in equation (1).
For i = 1 to 16r+31 do
T[i] = T[i-1] + Qw           // Qw value is defined in equation (2).
R1 = R2 = i = j = 0
z= 3 * Max (c, 16r+32)
for y = 1 to z do
{
R1 = T[i] = (T[i] + R1 + R2) <<< 3
R2 = V[j] = (V[j] + R1+ R2) <<< (R1+R2)
i = (i + 1) Mod(16r+31)
j = (j + 1) Mod c
}
```

Key expansion algorithm of ARC6has two magic constants Pw and Qw which is defined as

$Pw = odd((e - 2)2^w) \rightarrow (1)$ and

$Qw = odd((Ø - 1)2^w) \rightarrow (2)$

e=2.7182818 and Ø=1.618033.

3.2 Encryption algorithm:

ARC6 encryption module converts the input into the cipher output using the generated sub key. 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 [5].

EMRC6 encryption is

1. Addition (+)
2. Bitwise EX-OR operation
3. Left rotation, a <<< b.
4. Integer Multiplication modulo 2n (*)

3.3 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.

Detection algorithm:

The ARC6 decryption process reproduces the original content from the cipher using the sub key. This is the inverse operation of ARC6 encryption. The following algorithm represents the ARC6 decryption process. Various steps involved in decryption process are

1. Integer subtraction (−)
2. Bit wise EX-OR
3. Integer multiplication
4. Right shift, a >>> b.

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.

4. Security Issues

Security of ARC6 The diffusion process of ARC6 is very fast when compared with other block cipher algorithm [6]. 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 ARC6 when compared with RC4, RC5, and RC6 [7]. ARC6 is robust against differential linear attack, Statistical attack and with increase in number of rounds it is robust against X2 cryptanalysis also [8].

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].

5. Results

Two sample images are taken for analysis and the details are listed below for all resolution in

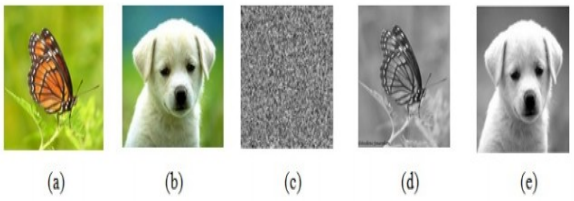

Figure 4(a) Original image (31.1 KB) (b) Watermark (4.52 KB) (c) encrypted image (d) Watermarked image (41.3 KB) (e) Extracted watermark image.

6. Conclusion

This proposed method is suitable for copy right protection of DIGITAL images using ARC6 encryption algorithm and RDM watermarking method. The input 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. ARC6 provides high security since it withstands almost all attacks which was imposed on previous RC6 version. The security level of watermark is increased by this encryption and the watermark embedding capacity also improved 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.

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.

6. 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.

7. 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.

8.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.