A SECURED WATERMARKING TECHNIQUE WITH RC5 ENCRYPTION

[1]APARNA SONI, [2]DEEPTY DUBEY

[1]Research Scholar, Deptt. of CSE, CSIT, Durg(Chhattisgarh), [2]Assistant Professor, Deptt. of CSE, CSIT, Durg(Chhattisgarh)
Email: aparna13788soni@gmail.com, deeptydubey@csitdurg.in

Abstract— In the digital world, that is currently evolving at such a rapid pace, intellectual copyright protection is becoming increasingly important. This is due to digital data being particularly simple to copy and resell without any loss of quality. Digital representation and distribution of data has increased the potential for misuse and theft and thus gives rise to problems associated with copyright protection and the enforcement of these rights. The main technical approaches to address the challenge of intellectual copyright protection are digital watermarking techniques. The encryption algorithm is proposed to use a block cipher. While the proposed technique embeds watermark in the encrypted domain, the extraction of watermark can be done in the decrypted domain. Double encryption technique will be used with RC5 symmetric cipher for providing increased level of security to the digital content. Experimental results show the security as well as copyright protection of the proposed algorithm.

Keywords—Decryption, Digital media, Encryption, RC5, Watermarking, etc.

I. INTRODUCTION

Digital rights management (DRM) technologies have been developed to protect digital content items. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. Sometimes the media contents are often need to be carried over as well as distributed in the encrypted domain and for more security watermarking techniques must be adopted.

A. V. Subramanyam et. al., focussed on the robust watermarking technique for JPEG2000 images in which the watermark can be embedded in a predictable manner in compressed-encrypted bytestream. The approaches by them are the bytestream encryption by the symmetric stream cipher RC4 and then embed robust watermark over the images in the compressed-encrypted domain [1] and [4]. One of the other encryption algorithms is the RC5. RC5 provides more security as compared to the RC4 encryption algorithm. *Omar Elkeelany and Adegoke Olabisi*, presented high performance RC5- integrated architecture with variable key registration, enhanced security and improved encryption throughput. The proposed architecture is synthesized to Field Programmable Gate Arrays (FPGA) device similar to the family of related work for comparisons. The proposed architecture shows an improvement in the speed of operation as compared to the conventional architecture and related work. Compared to conventional RC5 encryption throughput, they have shown an 80% increase in the achievable encryption throughput [11]. *Anjan Pal and Snehasish Banerjee* introduced a scheme for watermarking of digital images in which one can embed some secret text in an encrypted manner and a secret image more than once in the host image, starting from different pixel positions based on the key [2]. *Abdullah Bamatraf et. al.,* introduced a new algorithm using Least Significant Bit (LSB) by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of image before embedding the watermark. The algorithm is flexible enough depending on the length of the watermark text [8]. Similarly *Minewa M. Yeung and Fred Mintzer* in [9], *Puneet Kr Sharma and Rajni* in [10], *Preeti Gupta* in [12] introduced various watermarking techniques for providing security to the digital contents.

II. PROPOSED METHODOLOGY

The proposed algorithm attempts to combine and unite the two approaches of image watermarking and text encryption together into one. Encryption is the process of converting a readable plain text into an equivalent unreadable format called cipher text, which cannot be easily understood by all. Symmetric Encryption cores provide security to data by using a secret key both for encryption and decryption processes. RC5 Encryption algorithm will be used for the encryption of texts. After completion of the encryption process the data will be embedded over a JPEG Image using a watermarking scheme i.e. Least Significant Bit Substitution. For protecting the data from copyright protection, tamper detection, etc. This

encrypted-watermarked data will be re-encrypted for providing increased level of security to the data or information.

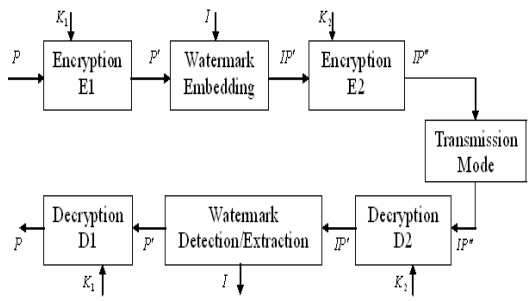

Fig.1. Block diagram of secured Watermarking with Encryption.

RC5 Algorithm

More recently, RC5 algorithm was developed by Ronald Rivest in 1995 as a parameterized symmetric encryption core. RC stands for "Rivest Cipher", or alternatively, "Ron's Code". A novel feature of RC5 is the heavy use of data dependent rotations. RC5 parameters are; a variable block size (w), a variable number of rounds (r) and a variable key size (k). Allowable choices for the block size (w) are 32, 64 and 128 bits. The number of rounds can range from 0 to 255, while the key size can range from 0 bits to 2040 bits in size. RC5 has three modules: key-expansion, encryption and decryption units. Relatively, RC5 is more secure than RC4 but is slower in operation. The choice of r affects both encryption speed and security. The more number of rounds will increase the security but somehow slower down the encryption speed.

The RC5 algorithm uses three primitive operations and their inverses.

(1) Addition/subtraction of words modulo 2^w, where w is the word size.
(2) Bit-wise exclusive-or denoted by XOR.
(3) Rotation: the rotation of word m left by n bits is denoted by $m <<< n$. The inverse operation is the rotation of word m right by n bits, denoted by $m >>> n$.

In the key expansion module, the password key K is expanded to a much larger size using an expansion table (T). The size of table T is $2(r+1)$, where r is the number of rounds. The key-expansion process must be performed before encryption or decryption processes.

The encryption process takes a plain text input and produces a cipher text as the output. The decryption process takes a cipher text as the input and produces a plain text as the output. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. Both processes use the expanded key along with segments of the input message to produce their outputs.

1) Encryption

Assume that the input block is given in two w bit registers X and Y. The array $T[0,1,....s-1]$ has been computed and the key expansion has been performed. So the steps in encryption algorithm are as follows:-

Steps:

i. $X = X + T[0];$
ii. $Y = Y + T[1];$
iii. $for\ \ i = 0\ \ to\ \ r\ \ do$
$X = ((X \oplus Y) <<< Y) + T[2*i];$

$Y = ((Y \oplus X) <<< X) + T[2*i+1];$

The output will be in the registers X and Y.

2) Decryption

The Decryption module will be computed or derived from the Encryption module. The steps involved in decryption algorithm are as follows:-

Steps:

i. $for\ i = r\ \ down\ to\ 1\ \ do$
$Y = ((Y - T[2*i+1]) >>> X) \oplus X;$
$X = ((X - T[2*i]) >>> Y) \oplus Y;$
ii. $Y = Y - T[1];$
iii. $X = X - T[0];$

3) Key Expansion

The key expansion routine expands the user's secret key K to fill the expanded key array T, so that T resembles an array of $s = 2(r+1)$ random binary words determined by K. The key expansion algorithm uses two constants and consists of three simple algorithmic parts.

Definition of the Constants: The key expansion algorithm uses two word sized binary constants A_w and B_w. They are defined for arbitrary w as follows:

$$A_w = Odd((e-2)2^w) \qquad (1)$$

$$B_w = Odd((\phi-1)2^w) \qquad (2)$$

where

$e = 2.718281828459....,$ Base of natural logarithms

$\phi = 1.618033988749.....,$ Golden ratio

and where $Odd(m)$ is the odd integer nearest to m (rounded up if m is an even integer).

Converting the Secret Key from Bytes to Words: The first algorithmic step of key expansion is to copy the secret key $K[0....b-1]$ into an array $H[0....h-1]$ of $h=[(b*8)/w]$ words. This operation is done in a natural manner, using $(w/8)$ consecutive key bytes of K to fill up each successive word in H, low-order byte to high-order byte. Any unfilled byte positions of H are zeroed. In the case that $b=h=0$ we reset h to 1 and set $H[0]$ to zero.

$$h=[\max(b,1)/(w/8)]$$
$$for\ i=b-1\ down\ to\ 0\ do$$

$$H[i/(w/8)]=(H[i/(w/8)]<<<8)+K[i];$$

Initializing the Array T : The second algorithmic step of key expansion is to initialize array T to a particular fixed (key-independent) bit pattern, using an arithmetic progression modulo 2^w determined by the constants A^w and B^w. Since B^w is odd, the arithmetic progression has period 2^w.

$$T[0]=A_w;$$
$$for\ i=1\ to\ t-1\ do$$
$$T[i]=T[i-1]+B_w;$$

Mixing in the Secret Key: The third algorithmic step of key expansion is to mix in the user's secret key in three passes over the arrays T and H. Due to the different sizes of T and H, the larger array will be processed three times, and the other may be handled more times.

$$i=j=0;$$
$$X=Y=0;$$
$$do\ 3*\max(s,h)\ times:$$
$$X=T[i]=(T[i]+X+Y)<<<3;$$

$$Y=H[j]=(H[j]+X+Y)<<<(X+Y);$$
$$i=(i+1)\mathrm{mod}(s);$$
$$j=(j+1)\mathrm{mod}(h);$$

The key-expansion function has a certain amount of one-wayness: it is not so easy to determine K from T.

B. The Watermarking Technique- Least Significant Bit Substitution

Digital watermarking is a technique where bits of information are embedded in such a way that is completely invisible. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data. The digital watermarking system essentially consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark onto the cover signal and the watermark detector detects the presence of watermark signal. In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image.

By using three consecutive pixels to embed a single character and from each of those three pixels, here replacing the two least significant bits by the two ASCII bits of the character. No embedding of the two most significant bits of any of the characters will be done because for all characters (A-Z, a-z), the two MSBs are always 01. Embedding of A (01**000001**) into three pixels: 10101010 11001101 11111001. After embedding those pixels will be modified as follows: 10101**00 11001100 11111001**. This text can be the encrypted name of the company or the person who owns the image. For every character, three pixels will be required. So, to embed a text of n characters, only 3n pixels will be required, call them victim pixels. The robustness of the algorithm can be further increased by embedding the text more than once, each time on different set of victim pixels and substitution. The extraction of watermarking process will also be followed performing the opposite concept of the above sequences.

III. DISCUSSION

The technologies proposed to be used for the security of Multimedia Data are Cryptography and Watermarking. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It has two phases- Encryption and Decryption. In the proposed work, Symmetric-Key Cryptography will be used, where the same key is used both for encryption and decryption. RC5 encryption algorithm is proposed to be used for encrypting the text or files which will be the most important digital content. Watermarking is defined as adding (embedding) a watermark signal to the host signal. The watermark can be detected or extracted later. The technique is basically adopted for the copyright protection of the digital media. The technique of invisible watermarking is being adopted with the Least Significant Bit of the compressed-encrypted images. The Watermarking Technique which is proposed to use is on the Least Significant bit of the digital images. A secret image is superimposed on the original data through pixel bit manipulation. For LSB, the least significant bits of the original image are substituted by the most significant bits of the watermark image. It is based on the

substitution of LSB plane of the cover image with the given watermark. The concept of Re-encryption will be proposed to be included for providing increased level of security to the digital content. This will also be performed using RC5 symmetric cipher. The advantage of using RC5 encryption over RC4 is that it is using the block cipher process for encryption rather than stream cipher. The overall method adopted here is for the purpose of providing copyright protection, as well as security to the multimedia data. The process of re-encryption will be the advantageous feature of the concept applied here with watermarking and encryption of digital contents.

CONCLUSION

The increasing amount of digital exchangeable data generates new information security needs. Multimedia documents and specifically images are also affected. Users expect that robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. In the current state of research, it is difficult to affirm which watermarking approach seems most suitable to ensure an integrity service adapted to images and more general way to multimedia documents.

In this proposed work a method of Watermarking is being introduced for providing more security and protecting the digital media from the unauthorized users. The method has Encryption with RC5 symmetric algorithm and then the secret text in the form of watermark is proposed to be embedded at the least significant bit of the digital content. Digital representation and distribution of data becomes easier with copyright protection of the digital media. The application area consists of Military Purposes, Business Applications etc.

REFERENCES

[1] A. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images", IEEE Transactions on Multimedia, Vol. 14, no. 3, pp. 703-716, June 2012.

[2] Anjan Pal and Snehasish Banerjee, "Embedment of Encrypted Text and Secret Images for Digital Image Watermarking," World Applied Programming, Vol .1, no. 3, pp. 132-137 ,August 2011.

[3] S. Hwang, K. Yoon, K. Jun, and K. Lee, "Modeling and implementation of digital rights," J. Syst. Softw., vol. 73, no. 3, pp. 533–549, 2004.

[4] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressed decrypted domain JPEG2000 image watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, pp. 1315–1320, 2010.

[5] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative Watermarking and encryption for media data," Opt. Eng., vol. 45, pp. 1–3, 2006.

[6] Ricardo L. de Queiroz, " Processing JPEG-Compressed Images and Documents," IEEE Transactions on Image Processing, vol. 7, no. 12, pp. 1661-1672, Dec 1998.

[7] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems," International Journal of Information and Communication Engineering, 3:8, pp. 537-542, 2007.

[8] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, "Journal of Computing, vol. 3, Issue 4, ISSN 2151-9617, pp. 1-8, , April 2011.

[9] Minewa **M.** Yeung and Fred Mintzer, "An Invisible Watermarking Technique for Image Verification," 0-8186-8183-7/97 $10.00 *0* IEEE, pp. 680-683, 1997.

[10] Puneet Kr Sharma and Rajni, "Analysis of Image Watermarking using Least Significant Bit Algorithm" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, pp. 95-101, July 2012.

[11] Omar Elkeelany and Adegoke Olabisi, "Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" Journal of Computers, vol. 3, no. 3, pp. 48-55, March 2008.

[12] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, ISSN 2229-5518, pp. 1-4, September 2012.

★★★