IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Image Security using AES and RNS with Reversible Watermarking

Prof. Prajakta Bhangale[1], Rucha S. Raje[2], Jyoti Maurya[3], Anushree Gawad[4]

Department of Information Technology, Fr. Conceicao Rodrigues College of Engineering , Bandra (W) , Mumbai, Maharashtra 400050, India

Abstract

Image is a two dimensional representation of an object. Images form an integral part of day-to-day information transfer. Security while storage and transfer of images thus become an important aspect. Image security is applicable in many sectors where confidential information needs to be sent over the network; it includes Defense operations, law enforcement, etc. Various algorithms have been implemented for image security over the past years. Survey from different papers is carried out and the outcomes are described.

Keywords: *Encryption, Decryption, Watermarking*

1. Introduction

Encryption of images for storage and security purposes has been implemented several times over the past few years. Prominent encryption algorithms among several other algorithms are Data Encryption Standard (DES), Blowfish algorithm, Advanced Encryption Standard (AES).

AES, DES and Blowfish are discussed based on previous available literature. Watermarking techniques to hide image contents for security and to declare ownership has been implemented previously through techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Hybrid DWT-DCT. These techniques are discussed and comparison is provided.

2. Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. It Provides security only to software (no hardware) [5].It has a 64-bit block size and a variable key length from 32 bits up to 448 bits [1]. It runs for 16-rounds and uses large key-dependent S-boxes.

In each round r, 4 actions take place : First, XOR the left half (L) of the data with the rth P-array entry, second, use the XORed data as input for Blowfish's F-function, third, XOR the F-function's output with the right half (R) of the data, and last, swap L and R components.

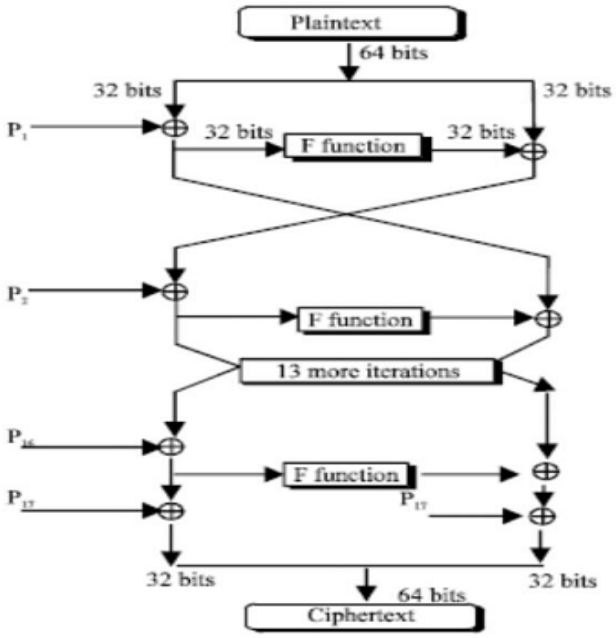

Fig. 1 : The Feistel structure of Blowfish [1]

An attacker needs to try 28r+1 times to breach Blowfish encryption, r being the number of rounds. More rounds thus gives more security [1].Blowfish is one of the fastest block ciphers in general use, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 KB of text. This is very slow compared to other block ciphers [7].

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

3. DES

Data Encryption Standard (DES) is a block cipher method for encrypting information. DES was developed in early 1970.The National Institute of Standards and Technology (NIST) approved the Data Encryption Standard (DES) block cipher. It has a relatively short key length of 56 bits and is symmetric-key block cipher which forms a backdoor. It is vulnerable to brute force attack and hence is not used for secure applications.

4. AES

Advanced Encryption Standard (AES) is a symmetric block cipher with variable key length which was invented in the year 2000.The key can be of 128,192 or 256 bits which is decided by the encoder. Input image is encrypted in rounds. Number of rounds required for encryption depend on size of key which is used. Number of rounds are 10 for 128 bits key, 12 for 192 bits key ,14 for 256 bits key.

Each round consists of four steps viz: Sub byte transformation, Shift rows transformation, Mix Column transformation and Add round key transformation. The order of these stages can be changed.

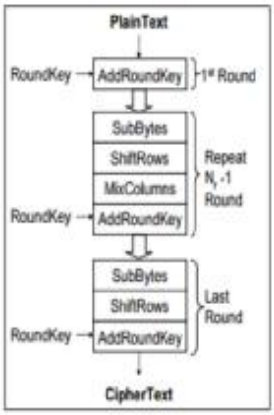

Fig. 2 AES Encryption algorithm [6]

4.1 Sub byte transformation

In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; b (i,j) = S(a(i,j)).

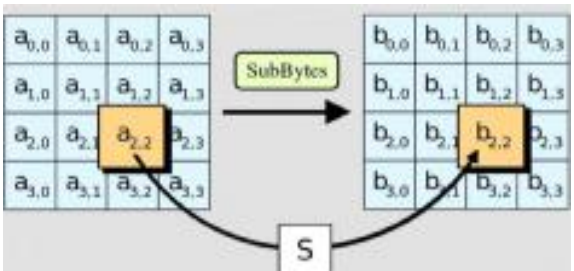

Fig. 3 SubBytes operation for AES [3]

4.2 Shift rows transformation

In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left [6]. For each row ,number of places by which each byte is shifted is different.

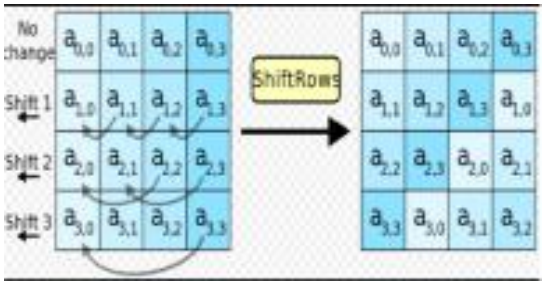

Figure 4 ShiftRows operation for AES [3]

4.3 Mix Columns transformation

In the MixColumns step, c(x), a fixed polynomial is multiplied with each column of the state [6].

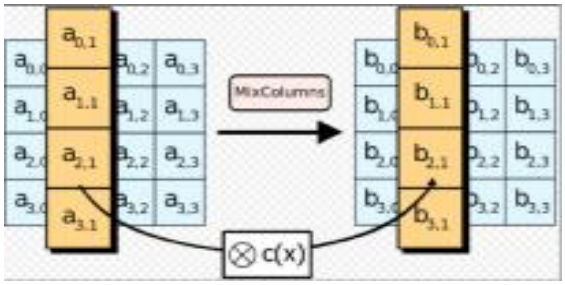

Fig. 5 MixColumns operation for AES [3]

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 5, May 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

4.4 Add Round key transformation

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation.

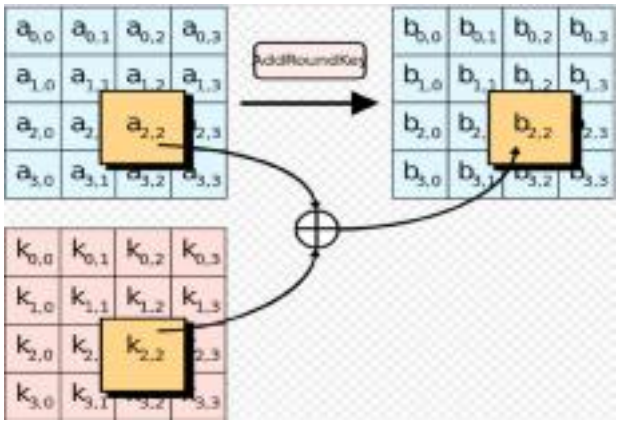

Fig. 6 AddRoundKeys operation for AES [3]

At the end of last round, we get an AES-encrypted image. The process of decryption of an AES cipher text is reverse in order of the encryption.

Advantages of AES are:

- It is faster and more secure as compared to DES [5].
- It has variable key length and so is difficult to intrude.

5. Watermarking

Watermarking is done on an image to copyright it with the owner's identity. This ensures that the image is authentic and safe .It can be done in Spatial domain and Transform domain. Under spatial domain, LSB is modified. But it is too vulnerable due to its simplicity .Under Transform domain there are various transforms used. Here we study Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and their combination– hybrid DWT-DCT.

5.1 DWT

Discrete Wavelet Transform discretely samples wavelets [9].It divides the image into four sub-bands of equal size (depending on number of levels). Four components are named as LL1, HL1, HH1, LH1.

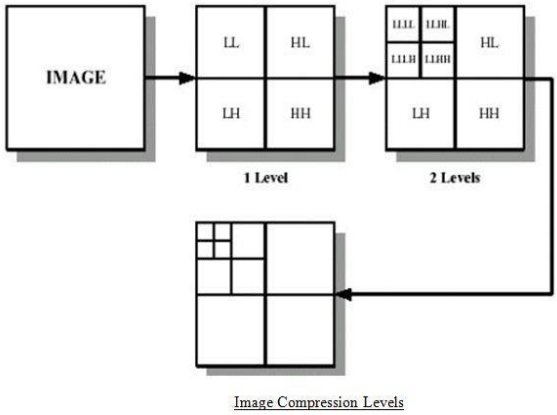

Fig. 7 DWT

5.2 DCT

Discrete Cosine Transform divides the image into frequency components.The block-based DCT transform decomposes image into non-overlapping blocks. It then applies DCT to each block [2].

We get three frequency sub-bands: low frequency, mid-frequency and high frequency sub-band. DCT-based watermarking is based on two facts [2].

1. The signal energy lies at low-frequency sub-band.
2. The high frequency components of the image are usually removed through

   compression and noise attacks. The watermark is embedded on the mid-frequency sub-band.

5.3 Hybrid DWT-DCT

Initially image is divided into four components by DWT algorithm .Then LL component of this DWT performed image is selected for performing DCT. After DCT is performed, watermark image is embedded on it.

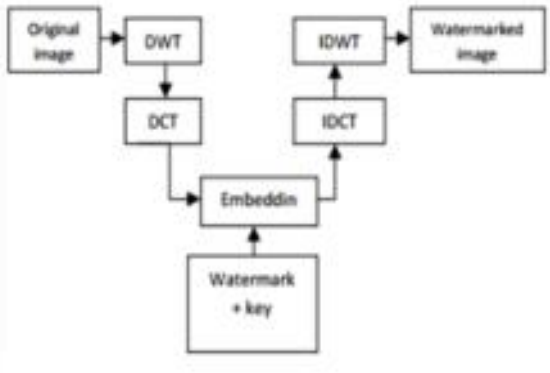

Fig. 8 Watermarking using Hybrid DCT – DWT [4]

6. RNS

Residue Number System (RNS) intends to breakdown large integers into small ones for the ease of computational purposes. RNS for each of the pixel value using the moduli (7, 9, 10) is calculated. Three numbers are combined as a decimal value. Now the pixel is represented by its RNS combined value. Decryption is based on Chinese Remainder Theorem (CRT).

7. PSNR and MSE

PSNR is the ratio between the maximum pixel value and MSE. PSNR is expressed in logarithmic decibel (dB) scale.

$$PSNR = 1\text{og}\left[\frac{MAX^2}{MSE}\right] \quad (1)$$

Where E is Mean Square Error (MSE), f(i,j) is pixel value of original image f(i,j) of watermarked image . MSE is given by formula:

$$E = \frac{1}{MXN}\sum_{i=1}^{N}\sum_{j=1}^{M}[f(i,j) - f'(i,j)]^2 \quad (2)$$

8. Results

Table 1: Comparison of AES and DES based on PSNR and MSE [8]

Algorithm	PSNR	MSE
AES	7.5523	8149.8396
DES	7.6057	8185.4343

Table 2: Comparison of DCT and DWT based on PSNR and MSE [10]

Algorithm	PSNR	MSE
DCT	62.26	0.0389
DWT	52.6024	0.3599

Table 3: Comparison of DWT and Hybrid DWT-DCT based on PSNR [2]

Algorithm	PSNR
DWT	51.466942dB
DCT-DWT	58.392598dB

9. Conclusion

It has been studied that although DES gives more PSNR than AES, MSE value is lesser in case of AES. So for efficient encryption of an image, AES should be used over DES. In terms of transforms, conclusion is that using Hybrid DWT-DCT is better for image watermarking than DCT or DWT alone [4].RNS enhances security by calculating modulus.

References

[1]Mrs. Smita Desai, Chetan A. Mudholkar,Rohan Khade,Prashant Chilwant, "Image Encryption and Decryption Using Blowfish Algorithm," International Journal of *Electrical and Electronics Engineers ISSN- 2321-2055 (E) IJEEE, vol. 7Jan- June* 2015.

[2] Navnidhi Chaturvedi,Dr.S.J.Basha,"Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR" International Journal of Innovative Research in Science, Engineering and Technology*Vol. 1, Issue 2, December 2012* Copyright to IJIRSET www.ijirset.com 147

[3]Page Title: Advanced Encryption Standard.https://en.wikipedia.org/wiki/Advanced _Encryption_Standard.

[4]Digvijaysinh Vaghela, Ram Kishan Bairwa, "Digital Image Watermarking Using *DWT Based DCT Technique," International Journal of Recent Research and Re*view, dec.2014.

[5]Aarti Devi, Ankush Sharma, Anamika Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 3034-3036

[6] P. Radhadevi , P. Kalpana "Secure Image Encryption using AES "IJRET:International Journal of Research in Engineering and Technology ,ISSN: 2319-1163.

[7]https://www.ukessays.com/essays/computer-science/blowfish-algorithm-history-and-background-computer-science-essay.php

[8]Soni, Shraddha and Agrawal, H and Sharma, M, "Modeling data-centric routing in *wireless sensor networks," Analysis and comparison between AES and DES Crypto*graphic Algorithm, vol. 2, pp. 362–365, 2012.

[9] Page Title: Discrete wavelet transform https://en.wikipedia.org/w/index.php?title=Discrete_wavelet_transform&action=info .

[10] Rashmi Dewangan, Yojana Yadav," Comparison of Watermarking techniques DWT, DWT-DCT & DWT-DCT-PSO on the basis of PSNR & MSE", 2nd International Conference on Recent Innovations in Science, Engineering and Management (ICRISEM-15) ISBN:978-81-931039-9-9. JNU Convention Center, Jawaharlal Nehru University, New Delhi.22 November 2015 www.conferenceworld.in.

[11] M. I. Youssef, A. E. Emam, S. M. Saafan and M. ABD Elghany, "Secured Image Encryption Scheme Using both Residue Number System and DNA Sequence,"*The Online Journal on Electronics and Electrical Engineering (OJEEE), vol. 6.*

[12] Suraj Kumar Singh and Gopi, Varun P and Palanisamy, P, "Image security using DES and RNS with reversible watermarking," IEEE Electronics and Communication*Systems (ICECS), 2014 International Conference on, 2014.*

[13] Ghoradkar, Sneha and Shinde, Aparna, "Review on Image Encryption and Decrypt*ion using AES Algorithm," International Journal of Computer Applications (0975–8887), National Conference on EmergingTrends in Advanced Communication Tech*nologies, (NCETACT-2015).

[14] Dabas, Pooja and Khanna, Kavita, "A study on spatial and transform domain wa*termarking techniques," International Journal of Computer Applications, vol. 71, no.* 14,2013.

[15] Dr. Harsh Vikram Singh," Digital Image Watermarking Algorithm Based on DCT and Spread Spectrum",UACEE International Journal of Advances in Electronics EngineeringVol:1 Issue:1 ISSN 2278 - 215X.

Prof. Prajakta Bhangale received her BE Degree and ME degree in Computers from University of Mumbai. She is currently working as Assistant professor,Department of Information Technology, Fr.CRCE,Mumbai.

Rucha S. Raje is a student, currently pursuing BE Degree in Information Technology from Fr.CRCE, Mumbai.

Jyoti Maurya is a student, currently pursuing BE Degree in Information Technology from Fr.CRCE, Mumbai.

Anushree Gawad is a student, currently pursuing BE Degree in Information Technology from Fr.CRCE, Mumbai.