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], Anushree Gawad[2], Jyoti Maurya[3], Rucha S. Raje [4]

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

Abstract

Images have taken an important place in today's Digital world. Image security thus becomes a huge concern in terms of storage and communication. Image cryptography ensures secure storage and transfer of images. Watermarking is mainly used to identify the ownership of the image thus providing authentication. This paper proposes a combination of algorithms: advanced encryption standard (AES), hybrid of DWT and DCT watermarking techniques and residue number system (RNS) for image security. A grayscale image is given as input to AES-128 using a key, its output is watermarked using hybrid discrete wavelet transform and discrete cosine transform. Finally this watermarked image undergoes RNS procedure. Reverse process is carried out for retrieval of original image. The retrieved and original image are compared on the basis of PSNR and MSE values. The entire process is designed in Java.

Keywords:*Encryption,decryption,watermarking, AES,DCT,DWT,RNS*

1. Introduction

Encryption of image is really essential in areas such as confidential transmissions, video surveillance, law enforcement, military operations and medical sciences in order to ensure its authorized access. Encryption refers to encoding of image with some algorithm while decryption is decoding the image with reverse steps. Image encryption not only prevents the encrypted image from being intercepted but also ensures that image can only be decrypted, interpreted and viewed by the intended person. It was performed using algorithms such as DES, RSA in the past. AES has never been used along with DWT-DCT watermarking and RNS for image encryption. This paper intends to use AES encryption on an image. Digital watermarking is another aspect that enhances image security by providing a copyright of the owner. Thus helps detecting fraud images or if your image has been tampered with. Hybrid DCT-DWT has been used for reversible watermarking. RNS has been used with AES previously. In this paper, we propose a combination of AES encryption with hybrid DWT – DCT watermarking and RNS methodology.

The Data Encryption Standard (DES) is a symmetric-key block cipher. It was published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. The block size is 64-bit. It has a limited key size of 56 bits thus only 2^56 keys are possible [4] .These keys can be determined easily. Hardware implementations of DES are very fast. It was not designed for software, so runs relatively slower for software .The most practical attack on it to date is still a brute force attack. Thus DES proved inefficient in image encryption. AES encryption is more secure due to variable key lengths and block sizes.

Watermarking can be done using various techniques, prominent among which are DCT and DWT. Hybrid DWT-DCT overcomes the individual drawbacks of each one and provides a more secure watermark which is difficult for the intruder to extract. RNS methodology breaks a large integer into smaller integer sets for easy computations. Breaking of image data further enhances security.

2. Literature Review

2.1 AES

The AES -Advanced Encryption Standard is a symmetric block cipher. It is used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES has cipher blocks as AES-128, AES-192 and AES-256 based on key length. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys which can be of sizes 128, 192 and 256-bits [4], respectively.

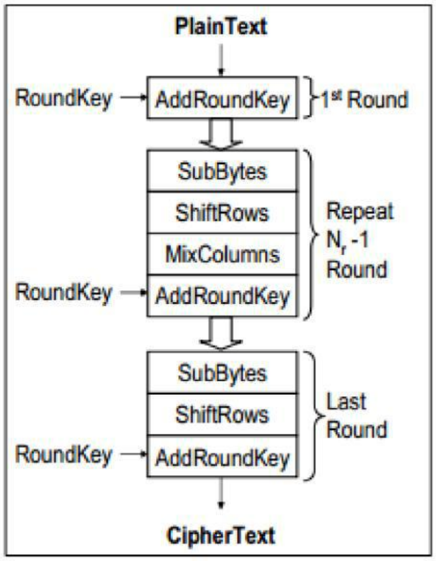


Fig 1 AES encryption algorithm [1]

Decryption of an AES ciphertext is reverse in order to the encryption process.

Table 1 Experimental Analysis of DES and

AES [4]

Parameter	AES	DES
MSE	8149.8396	8185.4343
PSNR	7.5523	7.6057

Above result concludes that AES has less MSE value as compared to DES, which makes AES preferable over DES.

2.2 Blowfish

Blowfish is a symmetric-key block cipher. Bruce Schneier designed it in 1993 and it is included in a large number of cipher suites and encryption products. It provides a good encryption rate in software .Till date no effective cryptanalysis of it has been found. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits [11]. It is a 16-round Feistel cipher and uses large key-dependent S-boxes.

Every round r consists of 4 actions [12]:
1.XOR the left half (L) of the data with the r th P-array entry [12],
2.give this data as input for Blowfish's F-function [12],
3. XOR the F-function's output with the right half (R) of the data [12], and
4.swap left and right components[12].

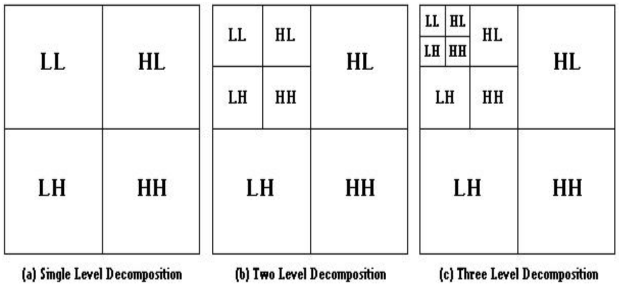
The 32 bit input is split by F function into four quarters of eight bit each .This quarters are given as input to the S-box. The S-boxes accept 8-bit input and produce 32-bit output. Addition modulo 2^32 is performed. These outputs are then XORed to produce the final 32-bit output. Decryption is preformed in reverse order of encryption.

2.3 DWT

A **discrete wavelet transform** (**DWT**) samples wavelets discretely. It has an advantage over Fourier transform. DWT works on temporal resolution which means it captures both frequency and location information (location in time) [6].

It basically divides the image into four non-overlapping blocks LL1, LH1, HL1 and HH1 in one cycle. The coarse-scale DWT coefficients are represented by LL1while the fine-scale DWT coefficients are represented by LH1, HL1 and HH1 [7].

In next cycle, the LL1 component again can be divided into four multi-resolution blocks. Alfred Haar gave the first DWT which is known as the Haar Transform. It stores the difference of pixel values and passes the sum of all pixel values for the next cycle.



(a) Single Level Decomposition
(b) Two Level Decomposition
(c) Three Level Decomposition

Fig. 2 Different levels of DWT

2.4 DCT

There are many transforms most of which are very slow. This is important to consider since video demands real-time encoding and decoding. The use of several different transforms was studied by the JPEG committee. DCT (Discrete Cosine Transform) proved superior among all the transforms that were studied. The **discrete cosine transform (DCT)** separates the image into non-overlapping sub-bands of differing frequency. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain

DCT operates on one block at a time in JPEG. Because there are 64 elements in an 8x8 block, this is called the 64-element or 64-coefficient DCT. The DCT transform operates on this block in a left-to- right, top-to-bottom manner.

Formula for FDCT:

$$S_{ij} = {}^{1}\!/_{4}\, C_j C_i \sum_{x=0}^{7} \sum_{y=0}^{7} P_{xy} \cos\left[(2x+1)j\pi/16\right] \cos\left[(2y+1)i\pi/16\right]$$

$C_i, C_j = 1/\sqrt{2}$ when $i, j = 0$

$C_i, C_j = 1$ otherwise

(1)

The block-based DCT transform divides image into non-overlapping blocks. It then applies DCT to each block. This result in giving three frequency sub bands [2]:
low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on following facts[2]:

1. Most of the signal energy lies in low-frequency sub band. . This band contains the most important visual information of an image.
2. High frequency bands of the image are often removed during compression or noise attacks. The watermark is embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and as shown in fig 2.[2]

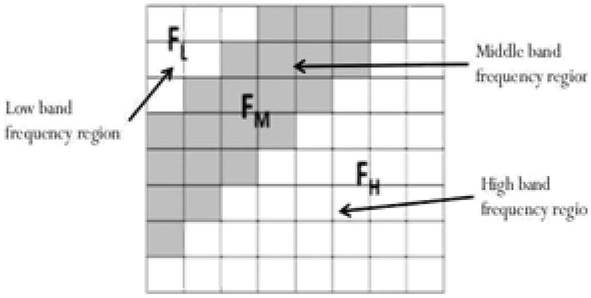

F_L
F_M
F_H
Low band frequency region
Middle band frequency regior
High band frequency regio

Fig. 3 Discrete wavelet transform [2]

2.5 RNS

For RNS procedure, RNS for each of the pixel value using the moduli (7, 9, 10) is calculated. These numbers are combined as a decimal value. The pixel is now represented by its RNS combined value.

Example [5]:
Encryption

First find the residue of 317 with corresponding moduli:

Rl = 317 mod 7 = 2 R2= 317 mod 9 = 2 R3= 317 mod 10 = 7

Hence, combine the three number as decimal value of 227.

Decryption

Decryption involves the following steps:

- Initially, separate the digit from decimal value 227 as 2, 2, 7 and mark as Rl, R2, R3.
- Then use CRT theorem expression as:

$$X = \sum_{i=1}^{N} (Ai * Ti * Ri) mod\ M$$

(2)

Where, dynamic range (M) = 7*9* l0 = 630, (i.e. we can use decimal number of range [0,1,2,..,629])

Ai = M / Ri, i.e. AI = 630/7 = 90, A2 = 630/9 = 70, A3 = 630/10 = 63.

Multiplicative inverse (Ti) of above Ai as:

TI = 90 mod 7 = 6 and 6*6 mod 7 = 1 so, TI=6.

T2 =70 mod 9 = 7 and 7*4 mod 9 = 1 so, T2=4.

T3 = 63 mod l0=3 and 3*7mod 10=1 so, D=7.

Hence, X = (90*6*2 + 70*4*2 + 63*7*7) mod 630

= 4727 mod 630
= 317

3. Methodology

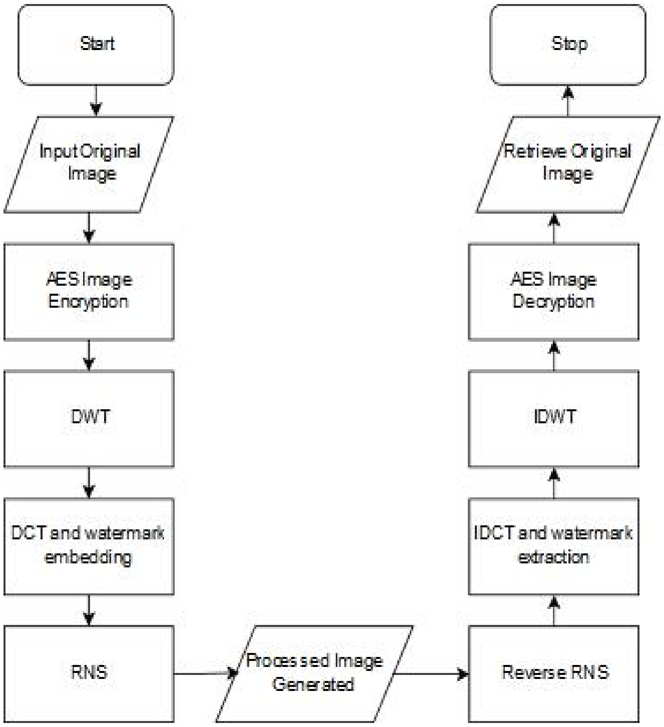


Fig.3 Flow Diagram

Steps of the implementation
Step1: AES Encryption
Step 2: Embedding Watermark

- Apply level-1 DWT technique to segment the cover host image so that it gives four non-overlapping sub-bands: LL1, HL1, LH1, and HH1.
- Divide the sub-band LL1 into 8 x 8 blocks.
- Apply DCT watermarking to each block in the chosen sub-band.
- Take a grey-scale image having pixels equal to the number of 8 x 8 blocks. Re-formulate the grey-scale watermark image into a vector of zeros and ones.
- Generate two uncorrelated pseudorandom sequences. One sequence is used to embed the watermark bit 0 (W0) and the other sequence is used to embed the watermark bit 1 (W1). Element‘s number in each of the two pseudo random pattern sequences must be equal to the number of mid-band elements of the DCT-transformed DWT sub-bands.
- Embed the entire pseudorandom sequence, either W0 or W1, with a gain factor, in the entire DCT transformed 8 x 8 block of the selected DWT sub-band of the host image. Embedding is not applied to all coefficients of the DCT block, but only to the mid-band DCT coefficients. If we denote X as the mid-band coefficients of the DCT transformed block, then embedding is done as given in below equation:

If the watermark bit is 0 then

$$X = X + *W0 \quad (3)$$

If the watermark bit is 1 then

$$X = X + *W1 \quad (4)$$

Repeat this procedure for each the 8 x 8 blocks in the chosen DWT sub-band.

Step 3: RNS Encryption

Step 4: RNS decryption

Step 5: Watermark Extraction

- Regenerate the two different pseudo random sequences (W0 and W1) using the same seed used in the previous watermark embedding procedure.

- For each block in the sub-band, calculate the correlation between the mid-band coefficients and the two generated pseudorandom sequences (W0 and W1). If the correlation with the W0 was higher as compared to the correlation with W1, then the extracted watermark bit is considered as 0, otherwise the extracted watermark is considered as 1.

- Reconstruct the watermark using the extracted watermark bits, and compute the similarity between the original image and extracted watermarks [7].

Step 6: AES Decryption

3. Results

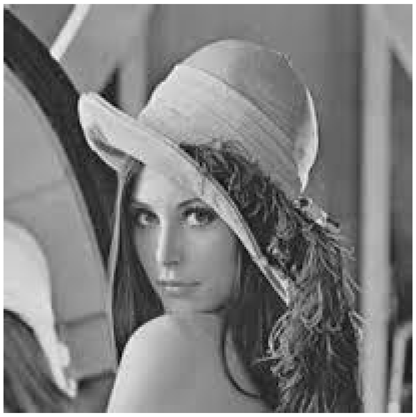


Fig.4 Original Image: 204 x 204: 5.85kb

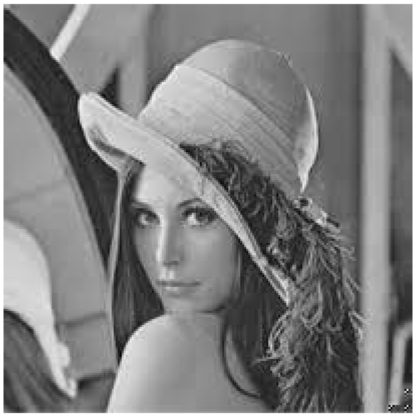


Fig. 5 Decrypted Image: 204 x 204: 7.62kb

We get the following results:

Table 2 Comparison of AES and Blowfish

Algorithm	MSE	PSNR
AES	3.3591	42.8685
Blowfish	5188.690176	10.980

Since AES gives better MSE and PSNR values than blowfish, we use it further to implement hybrid DWT-DCT watermarking and RNS.

We get the following results:

Table 3 MSE and PSNR values of the

proposed combination

PSNR	MSE	Algorithm
36.3934	14.9188	AES + DWT + DCT + RNS

3. Conclusion

In this project we have implemented AES image encryption along with hybrid DWT –DCT watermarking and RNS methodology. The above model of image security requires secret key, pseudorandom seed and RNS moduli to recover the original image. Also, applying hybrid of DWT and DCT transforms helps to overcome the drawbacks of individual methods and helps in effective watermarking. For the test image used the PSNR and MSE values for the proposed combination are 36.3934 dB and 14.9188 respectively. Hence we conclude that proposed combination is highly efficient as it enhances image security and provides authentication.

4. Future work

The proposed combination has been applied for grayscale images only. For increasing the scope of project and to facilitate wide scale application, we aim to implement the proposed combination for color images as well.

References

[1] P. Radhadevi , P. Kalpana "SECURE IMAGE ENCRYPTION USING AES "IJRET:International Journal of Research in Engineering and Technology ,ISSN: 2319-1163**.**

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

[3]https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node231.html

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

[5] 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.*

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

[7] 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

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

[9] 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.

[10] 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.*

[11] 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.

[12] Page Name: Blowfish (cipher) https://en.wikipedia.org/w/index.php?title=Blowfish_(cipher)&oldid=782001280

[13] Ghoradkar, Sneha and Shinde, Aparna, "Review on Image Encryption and Decryp*tion 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 wat*ermarking 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.

[16] Page Title: Advanced Encryption Standard.https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[17] 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

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.