Image Security using DES and RNS with Reversible Watermarking

Suraj Kumar Singh
Departmentof ECE
National Institute of Technology
Tiruchirappalli, India
ssuraj054@gmail.com

Varun P. Gopi
Departmentof ECE
Government College of Engineering
Wayanad, India
varunpg@gecwyd.ac.in

P. Palanisamy
Departmentof ECE
National Institute of Technology
Tiruchirappalli, India
palan@nitt.edu

Abstract—**In this modern world of Internet and with the development of digital communication and multimedia application, image security has become an important concern in storage and communication. A cryptography technique provides good strength for securing and protecting images essentially in the fields as medical, law enforcement and military. Reversible watermarking provides authentication, in which original image and watermark gets recovered. In this paper, Initially, secrete image is passed through S-DES (Simple-Data Encryption Standard) using a key image, then this encrypted image is watermarked using a watermark image and a position matrix, this watermarked image is passed through RNS (Residue Number System) and finally we get our DES watermarked RNS encoded image. For decoding, we have to go in reverse order, i.e. initially reverse RNS (CRT, Chinese Remainder Theorem) followed by watermark and S-DES encoded image extraction and hence our secrete image back.**

Keywords-Image Security, Encryption, Cryptography, Simple-Data Encryption Standard(S-DES), Watermarking, Residue Number System(RNS), Chinese Remainder Theorem(CRT).

I. INTRODUCTION

With the growing aspect in modern communication system, network security has become essential, especially in the field of computer communication. Also, with increase in the number of connections in Internet, data exchanged over it increases and requires security. Therefore, authentication should be present to protect against unauthorized access. This leads in the growth of data and image hiding methodology in digital medium. Some of theapplication for data hiding includes Digital Watermarking, Cryptography, Steganography and fingerprinting.In digital watermarking or Steganography, an invisible data or signal is added into a digital medium (an image, audio, video data) to protect it from alteration or third party use, so as to provide authentication to the information[1,2,3].

Residue Number System (RNS) is defined by a set of number ($m_1, m_2, \ldots, m_k$) called moduli, which are relatively prime to each other, i.e. two moduli should not have a greatest common divisor greater than 1. Hence, each integer number X can be mapped onto the legitimate range and represented as an N-tuple of residue digits ($R_1, R_2, \ldots, R_n$) [4].Reversible watermarking is data embedding, which is also called as lossless data embedding, embeds data called payload such as image or data in a fashion so that the original image and the payload is recovered without any losses [5,6,7]. Cryptography, a word with Greek origins, means secrete writing. However, it is used to refer as the science and art of transforming messages to make them secure and immune to attack [8]. Cryptography can be of private key (symmetric) or public key (asymmetric) encryption scheme, where DES is under private key encryption method. Here, we have considered Simple-DES (S-DES) is for our proposed method. Ramaiya [9] proposed the method for Security Improvisation in image steganography using DES. This technique is based on DES, which includes the secret key and S-box mapping and then the above DES image is embedded onto the LSB two bit of the cover image that do not make much difference in cover image. Rahman [10] proposed a method of Reversible Watermarking using RNS, where RNS mapping of pixel value of original image is done before embedding the watermark and hence pixels are randomly selected to be watermarked by one bit and the other pixels are changed into residue. Finally, even parity of residue is calculated and appended to the corresponding residues.

The proposed model below combines the features of Simple-DES, watermarking and RNS respectively. This provides security strength to the secrete image, because it requires secrete key, position matrix and RNS moduli. Hence, it is impossible to decrypt, without knowing secrete key, position matrix and RNS moduli. The rest of the paper is arranged as follows: section II describes the proposed method (block diagram, encryption and decryption method for both gray scale image and color image). The efficiency measurement is discussed in section III. Section IV describes the Simulation results and section V gives the conclusion.

II. PROPOSED METHOD

A. Block Diagram Representation:

The block diagram of proposed method is shown in Fig. 1. The proposed model is based on secrete key, S-DES function, position matrix, watermark image and RNS moduli.

B. Encryption Method:

Step1: Take the secrete image of (N×N) size and the secrete key of (N×N/2) size, and convert each pixel value into corresponding binary value as shown in Fig. 2.

Step2: Now perform the S-DES (Simple-Data Encryption Standard) function, pixel by pixel in row-wise and column-wise order respectively as shown in Fig. 4.

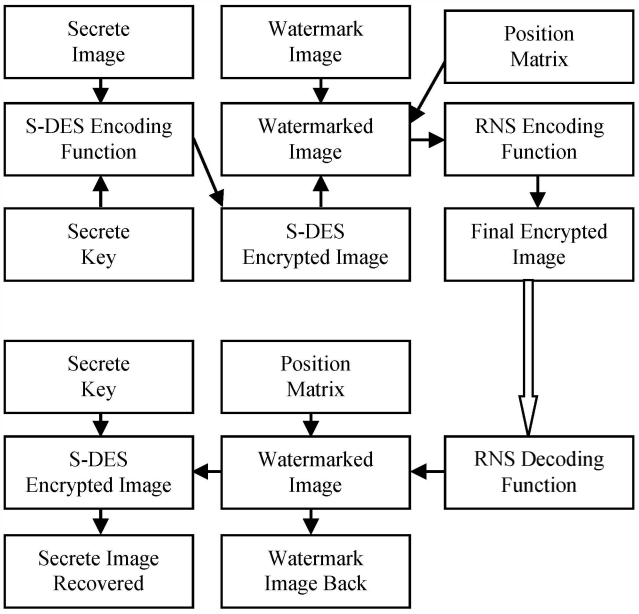

Fig 1: Proposed Model

215	142	58	94	--	--	--	244
220	211	185	--	--			219
159	160	227	--	--			172
144	--	--	--				114
--	--	--					--
--							--
--						--	--
98	131	154	183	--	--	--	160

Say 256 x 256 Secrete Image

1	1	0	1	0	1	1	1

Fig 2: Conversion of pixel to binary

R\C	1	2	3	4
1	5	9	11	1
2	6	15	8	12
3	2	7	13	0
4	3	10	4	14

Fig 3: S-box mapping

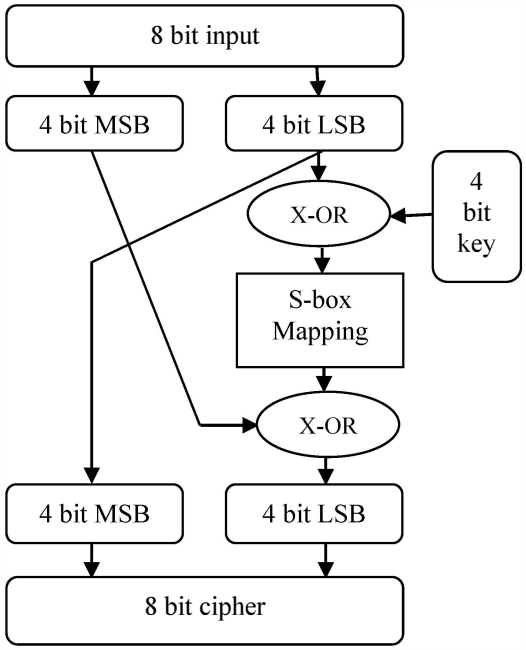

Fig 4: S-DES encoding function

Here, first 8-bit of secrete image is taken and divided as 4-bit MSB and 4-bit LSB, then 4-bit LSB is XOR with first 4-bit of key image and output is passed to S-box mapping, where first 2-bit (converted to decimal) is considered for row position and last 2-bit bit (converted to decimal) is considered for column position, and hence we get a new value from S-box mapping. The S-box mapping is shown in Fig. 3. Now this is passed to XOR with 4-bit MSB input and hence we get our 4-bit LSB cipher. Finally, 4-bit MSB cipher is taken from 4-bit LSB input image, 8-bit cipher is found as shown in Fig. 4.

Step 3: Take the S-DES encoded image (N×N), Watermark image (N×N/8) and Position matrix (1×N). Convert watermark image pixel value into binary value, then watermark image becomes (N×N). Now with respect to value in position matrix, insert the watermark bit into the pixel value of the encoded image by shifting the LSB bits which are less than and equal to the position value, as below:

Say, pixel value of image = 157, Watermark bit = 1, position value = 4.

1	2	3	4	5	6	7	8
1	0	0	1	1	1	0	1

=157

(a)

1	2	3	**4**	5	6	7	8	9
1	0	0	**1**	1	1	1	0	1

=317

(b)

Fig 5: (a) Before insertion of watermark bit (b) After insertion of watermark bit

This is done for whole encoded image. Hence, we get S-DES Watermarked image.

Step 4: Take the above image and find the RNS for each of the pixel value using the moduli (7, 9, 10) as: Here, we have to find the residue of 317 with corresponding moduli:

R1= 317 mod 7 = 2
R2= 317 mod 9 = 2
R3= 317 mod 10 = 7

Hence, combine the three number as decimal value of 227. After finding RNS to every pixel value, we will get our S-DES watermarked RNS encoded image.

C. Decryption Method:

Step 5: Take the encoded image and perform the reverse RNS (CRT, Chinese Remainder Theorem) using the same moduli (7, 9, 10) as shown below:

Initially, separate the digit from decimal value 227 as 2, 2, 7 and mark as R1, R2, R3. Then use CRT theorem expression as:

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

Where, dynamic range (M) = 7*9*10 = 630, (i.e. we can use decimal number of range [0,1,2, ….,629])

A_i = M / R_i, i.e. A_1 = 630/7 = 90, A_2 = 630/9 = 70,
A_3 = 630/10 = 63.

Multiplicative inverse (T_i) of above A_i as:

T_1=90 mod 7=6 and 6***6**mod 7=1 so, T_1=6.

T_2=70 mod 9=7 and 7***4**mod 9=1 so, T_2=4.

T_3=63 mod 10=3 and 3***7**mod 10=1 so, T_3=7.

Hence, X = (90*6*2 + 70*4*2 + 63*7*7) mod 630
= 4727 mod 630 = **317**

Follow this operation for all the pixel value of image.

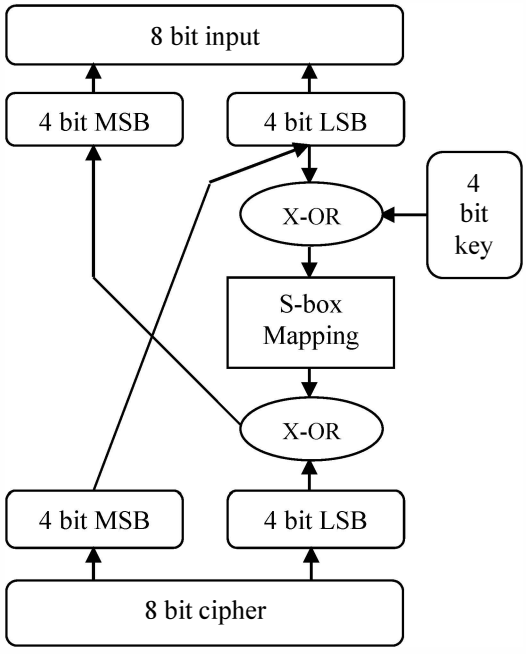

Fig 6: S-DES decoding function

Step 6: After doing reverse RNS to every pixel value, extract the watermark image from above image using position matrix, and compare this watermark image with original watermark image, if both are the same, then we can say that image is authenticated. Hence, extract the S-DES encoded image form the above watermarked image, else, discard it.

Step 7: Then perform S-DES decryption function to the above image in pixel by pixel form, both in column-wise and row-wise order respectively using key image as shown in Fig. 6. Hence, we obtain our final secret image back.

D. Encryption Method for Color Image:

The same algorithm as stated above must be applied, but the difference between is Gray scale image and RGB image.

Step 1: Initially, we will divide the color secrete image and the secrete key into their corresponding three image as R (Red) image, G (Green) image, B (Blue) image.

Step 2: Now we conditionally apply the above algorithm to all the image components, i.e. RGB as:

- DES Encoding Function, here additional security can be given by using different combination of secrete image and secrete key (RGB) component as (RR, GG, BB), (RG, GB, BR), (RB, GR, BG).
- Watermark embedding, with respect to the position matrix.
- RNS Mapping, of the Intensity value of above image.

Step 3: Hence combine all the image components into a single RGB (color) image.

E. Decryption Method for Color Image:

Step 4: Here also we will separate the embedded color (RGB) image into R, G, B image component.

Step 5: Now conditionally apply the above decryption method to all of the image components, i.e. R, G, B component and correspondingly extract watermark from all RGB images.

Step 6: Finally combine R, G, B image component into single RGB (color) image, and then we will check the efficiency of proposed method, i.e. PSNR (Peak Signal to Noise Ratio) is calculated.

III. EFFICIENCY MEASUREMENT

PSNR (Peak Signal to Noise Ratio): It checks how much distortion takes place after embedding Secrete image to that of the Original image.

$$PSNR = 10 * \log \frac{255^2}{MSE} \qquad (2)$$

$$MSE = \sum_{i=1}^{N}\sum_{j=1}^{N}(f(i,j) - g(i,j))^2/N^2 \qquad (3)$$

Here MSE is Mean Square Error, where f(i,j) and g(i,j) represents the pixel value with respect to position (i,j) in the original image and embedded image respectively. The PSNR represents the quality of image, i.e. higher the PSNR, lower

will be the variation between the above two images and vice-versa. The PSNR is expressed in dB scale.

IV. SIMULATION RESULTS

The proposed model is simulated in MATLAB R2009a. Fig. 7 shows the secrete image and secrete key. Fig. 8 shows encoded S-DES image of green component and watermark image. Fig. 9 shows watermarked image of green component and final RNS Encoded image. There are possibilities that the encoded image may get disturbed or distorted by third party, then the recovered watermark image will not be same as of original watermark image and hence image is not authentic.

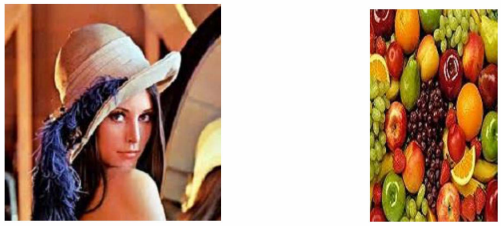

Fig 7: Secrete Image and Secrete Key

Fig 8: S-DES Encoded Green Image and Watermark Image

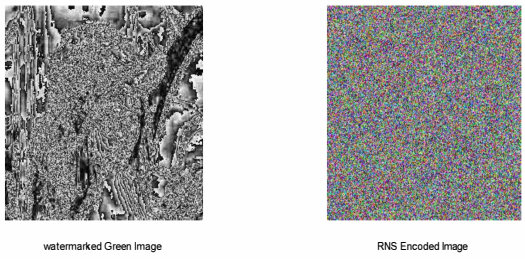

Fig 9: Watermarked Green Image and RNS Encoded Image

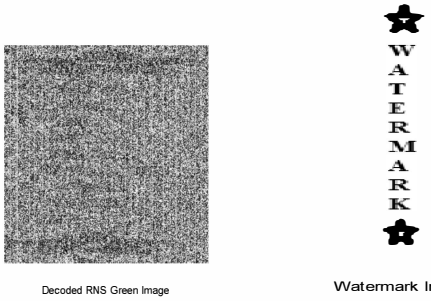

Fig 10: Decoded RNS Image (G) and Watermark Image

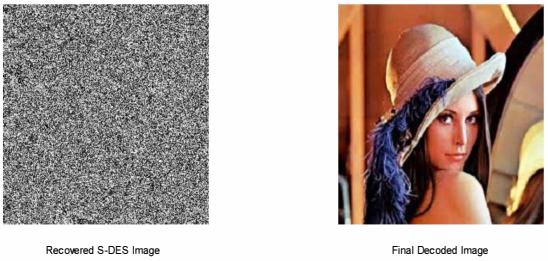

Fig 11: Extracted S-DES Image (G) and Final Decoded Image.

Fig. 10 shows Decoded RNS image of green component and recovered watermark image, which is exactly same as of original watermark. Fig. 11 shows the recovered S-DES image of green component and recovered secrete image.

Finally, we check the efficiency of the above method for both gray scale image and color image, i.e. for all R (Red), G (Green) and B (Blue) component of the color Image as shown in Table 1.

Table 1: MSE and PSNR values

Images	MSE	PSNR
Gray Scale Image	0	∞
Color Image (R Image)	0	∞
Color Image (G Image)	0	∞
Color Image (B Image)	0	∞

V. CONCLUSION

The proposed model of image security requires RNS moduli, position matrix, secrete key and S-box mapping in sequential order, otherwise, it is impossible to recover our secrete image. Here we recovered our secrete image with MSE value of zero and PSNR value of infinite, i.e. exact recovery of original image. This model is also done with color image, with (RG,GB,BR) combination of secrete image and secrete key respectively, where RG (Red and Green) represents red and green image component of color secrete image and color secrete key respectively. We can also go for color watermark image, which increases the option for more (RGB)

combination between secrete image, secrete key and watermark image as (RRR, GGG, BBB), (RRG, GGB, BBR) etc.

REFERENCES

[1] S. Samanta, S. Dutta, G. Sanyal, "An Enhancement of Security of Image using Permutation of RGB-Components", IEEE 3rd International Conference on Electronics Computer Technology (ICECT), Vol: 2, Apr. 2011, pp. 404-408.

[2] G. Huayong, H. Mingsheng, W. Qian, "Steganography and Steganalysis Based on Digital Image", IEEE 4th International Congress on Image and Signal Processing (CISP), Vol: 1, Oct. 2011, pp. 252-255.

[3] Parameshachari B. D., K. M. S. Soyjaudah, Chaaitanyakumar M. V., "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (IJRTE), ISSE: 2277-3878, Vol.-I, Issue-6, Jan. 2013, pp. 14-19.

[4] D. Younes, P. Steffan, "Efficient Image Processing Application using Residue Number System", 20th International Conference on Mixed Design of Integrated Circuits and Systems (MIXDES), Gdynia, Poland, Jun. 2013, pp. 468-472.

[5] M. abdullatif, A. M. Zeki, J. Chebil, T.S. Gunawan, "Properties of Digital Image Watermarking", IEEE 9th International Colloquium on Signal Processing and its Application (CSPA), Kuala Lumpur, Malaysia, Mar. 2013, pp. 235-240.

[6] P. Bandyopadhyay, S.Das, S. Paul, A. Chaudhuri, M. Banerjee, "A Dynamic Watermarking Scheme for color Image Authentication", IEEE Trans., International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 2009, pp. 314-318.

[7] N. Chandra, J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Application Technology and Research, Vol. 2-Issue 2, Jun. 2013, pp. 126-130.

[8] L. Bin, L. Lichen, Z. Jan, "Image Encryption Algorithm based on Chaotic Map and S-DES, IEEE 2nd International Conference on Advanced Computer Control (ICACC), Vol: 5, Mar. 2010, pp. 41-44.

[9] M. K. Ramaiya, N. Hemarajani, and A. K. Saxena, "Security Improvisation in Image Steganography using DES", 3rd IEEE International Advance Computing Conference (IACC), Feb. 2013 , pp. 1094-1099.

[10] A. Rahman, M. T. Naseem, I. M. Qureshi, M. Z. Muzaffar, "Reversible Watermarking using Residue Number System", IEEE Trans., 7th International Conference on Information Assurance and Security (IAS), Dec. 2011, pp. 162-166.