IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Robust & Secure Image Reverse Watermarking using Data Encryption Standard & RNS

J. Jain[1*], A. Singh[2]

[1]Department of Computer Science and Engineering, Chandigarh University, Punjab, India &
[1]Department of Computer Science and Engineering, Uttarakhand Technical University, Dehradun, India
[2]Department of Computer Sciences and Engineering, BTKIT, Dwarahat, Uttarakhand, India

[*]*Corresponding Author: jaishree3112@gmail.com, Tel.: +91-7055455947*

DOI: https://doi.org/10.26438/ijcse/v7i4.1823 | Available online at: www.ijcseonline.org

Accepted: 13/Apr/2019, Published: 30/Apr/2019

***Abstract*—** In the modern field of Internet with the advance development of digital communication, image security is the important concern to store data for communication in various organizations. By the use of cryptography techniques, it provides best strength and reliability to encrypt the images more essentially in the different type of organizations such as criminal law enforcement, Ministry of Defence. Reverse watermarking is used for authentication and to authorize the users of the respective panel where the original image and watermark image gets recover. In this paper, original secrete image is encrypted through S-DES (Simple-Data Encryption Standard) with the use of a key image. This encrypted image is called watermarked image and on this watermarked image, we applied RESIDUE NUMBER SYSTEM and get the DES watermarked RESIDUE NUMBER SYSTEM encoded image. For decoding, we go for reverse process and get the secrete image back.

***Keywords*—** Image Security, Watermark Image, Data Encryption Standard, Residue Number System

I. INTRODUCTION

As the users are increasing day by day and trying to take latest communication service to share the data by standard technique system securely. It is necessity to give more security. It will have to become essential to their respective field with computer communication [1]. Also, with increase in the number of connections using the multiple services of Internet, data exchange and hack that requires security. Therefore, powerful and strong authentication should be required to protect against unauthorized access [2]. It leads to the growth of data and image hiding methodology in digital watermarking medium. Many of the applications are being used for data hiding, like - Digital Image Watermarking, Cryptography, finger printing, Eye Retina, etc. But in digital image watermarking or Steganography, signal add into a digital medium (an image, audio & video clip data) to encrypt it from alteration or third party use, so as to provide authentication to the information[3, 4].

Residue Number System is defined by a set of number (pl, p2, ..., pn) called moduli, which are relatively prime to each other, i.e. two moduli should not have a greatest common divisor greater than 1[5]. Reversible watermarking embeds data called payload such as image or data in a manner so that the original image and the payload is recovered without any losses [6,7]. Cryptography 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 [9]. Here, we have considered Simple-DES (S- DES) is for our proposed method. Ramaiya [10] 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 proposed a method of Reversible Watermarking using RESIDUE NUMBER SYSTEM, where RESIDUE NUMBER SYSTEM 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 [11]. Mamarade proposed a technique in which first the secret image is encrypted using a key image, then encrypted image is watermarked using the watermark image, then it is passed through encryption function [12]. S. Aguru focused on data security with the help of encryption at client side and steganography at server side it provides a highly secure model [13]. S. Bansal emphasized on Steganography for information security through the Internet [14].

The proposed model below combines the features of Simple-DES, watermarking and RESIDUE NUMBER SYSTEM

respectively. This provides security strength to the secrete image, because it requires secrete key, position matrix and RESIDUE NUMBER SYSTEM moduli. The rest of the paper is arranged as follows: Section 2 describes the brief description of various watermarking attack, Section 3 describes proposed method (block diagram, encryption and decryption method for both grey scale image and color image). The efficiency measurement is discussed in section 4, Section 5 describes the Simulation results and section 6 gives the conclusion.

II. Overview & Brief Description Of Various Watermarking Attacks

The attacks to the digital watermarking are categorized. Hence, Brief of watermarking attacks are classified here as geometric, protocol, removal & cryptographic attacks [15, 16, 17, 18, 19, 20].

A. Removal attacks- The intention of this attack is to remove the watermark of the image without having any cognizance of the embedded algorithm or the key generated used for watermark embedding. This includes quantization, re-modulation & de-noising attacks.

B. Geometric attacks- The embedded watermark in these attacks is not critically removed but this attack is to disfigure the watermark detector balance with the embedded watermark. These attacks include scaling rotation, cropping, warping, etc.

C. Cryptographic attacks- These attacks find an approach to banish the embedded watermark. Such attacks include oracle, brute-force search, etc.

D. Protocol attacks- Invertible watermark works or effect as protocol attack in which the hacker extracts his own watermark from the watermarked content to infect watermarked data. Copy attack calculates the pixels of watermark and copy into other data that is the target of attack. Mosaic attack is also the type of protocol attack.

E. Estimation-based attacks- The effect of this attack is derived from the notion that the original data can be anticipated from the watermarked data visionless. These attacks work as removal and desynchronize attacks.

F. Re-modulation attacks- The effects of this attack are to transmogrify the watermark hostile to that used in embed process.

G. Synchronization removal attacks- The fundamental and effects of this attack is to analyze the synchronize Residue Number System, erase or stamp out of watermark and apply de-synchronization process.

H. Non-geometric attacks- These attacks effect on common image processing attacks like compression, sharpening, brightness, average filtering, noise addition, scanning, gamma correction.

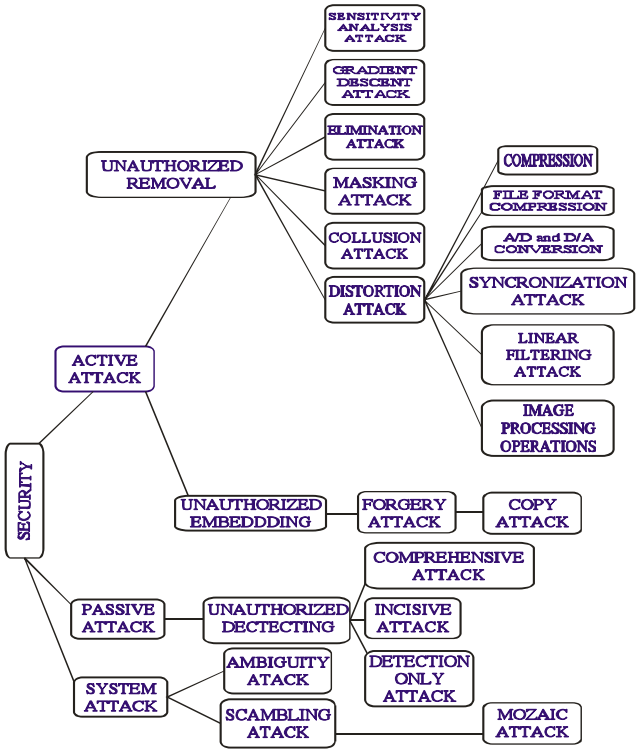


Fig. 1 Processing of Attacks

III. Proposed Method

A. Block Diagram:

The block diagram is focused on Secret key, RESIDUE NUMBER SYSTEM moduli, Position Matrix, S-DES function as shown in Fig. 2.

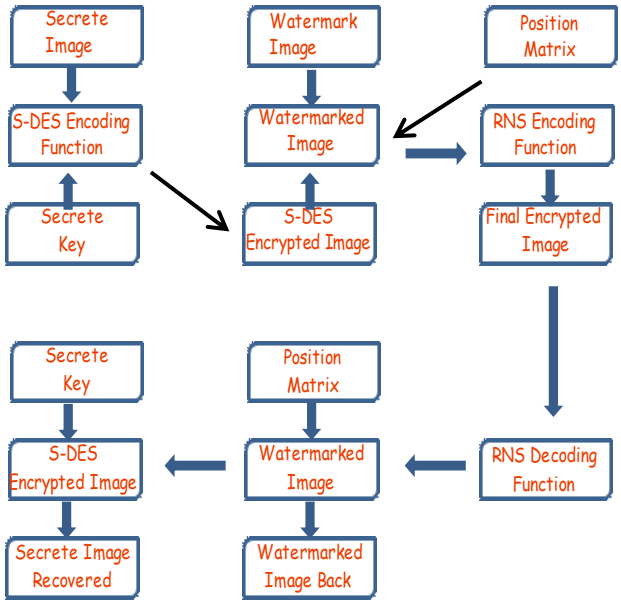


Fig. 2: Proposed Model

B. Encryption Method:

Step1: Take the secrete image of (XxY) size and secrete key of (XxY/2) size, and convert each pixel value into binary value as shown in Fig. 3.

Step2: Now perform the Simple-Data Encryption Standard to each pixel in row-wise and column- wise order respectively as shown in Fig. 5.

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

Secrete Image 256 x256

1	**1**	**0**	**1**	**0**	**1**	**1**	**1**

Fig. 3: 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 4: Mapping (S-Box)

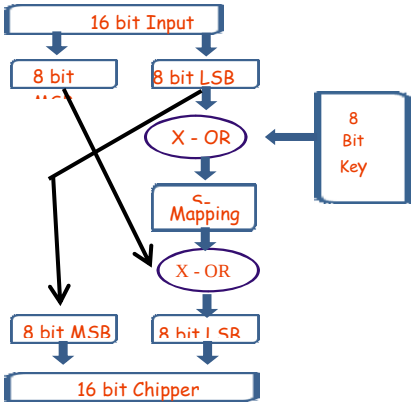


Fig 5: Encoding Function of S-DES

Here, first 16-bit of secrete image is taken and divided as 8-bit MSB and 8-bit LSB, then 8-bit LSB is XOR with first 8-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. 4. Now this is passed to XOR with 8-bit MSB input and hence we get our 8-bit LSB cipher. Finally, 8-bit MSB cipher is taken from 8-bit LSB input image, 16-bit cipher is found as shown in Fig. 5.

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

Say, pixel value of image = 160, Watermark bit = 1, position value = 6.

(a)

1	0	1	0	0	0	0	0

(b)

1	0	1	1	0	0	0	0	0

Fig. 6 (a) & (b)

Fig. 6(a) Before Insertion of Watermark Bit

Fig. 6(b) After Insertion of Watermark Bit

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

Step 4: After taking the above image and get RESIDUE NUMBER SYSTEM for every pixel value using the moduli (5, 6, 7) as: Here, we have to find the residue of 352 with corresponding moduli:

p1 = 352 mod 5 = 2

p2= 352 mod 6 = 4

p3= 352 mod 7 = 2

Hence, combination of the three numbers as decimal value of 242. After getting RESIDUE NUMBER SYSTEM to every pixel value, it will get us S-DES watermarked encoded image.

C . Decryption Method:

Step 1: Take the encoded image and perform the reverse RESIDUE NUMBER SYSTEM (CRT, Chinese Remainder Theorem) using the same moduli (5, 6, 7) as shown below:

Initially, separate the digit from decimal value 124 as 1, 2, 4 and mark as pl, p2, p3. Then use CRT theorem expression as:

$$M = \sum_{i=1}^{X} (Si * Vi * Li) \bmod N \qquad (1)$$

Where, dynamic range (N) = 5*6*7 = 210, (i.e. we can use decimal number of range [0,1,2, ...209])

Si = N / Li, i.e. S1 = 210/5 = 42, S2 = 210/6 = 35, S3 = 210/7= 30.

Multiplicative inverse (Vi) of above Si as:

VI=42 mod 5= 2 and 2*3 mod 5=1 so, VI=3.

V2=35 mod 6= 5 and 5*5 mod 6=1 so, V2=5.

V3=30 mod 7= 2 and 2*11 mod 7=1so, V3=11.

Hence, X = (42*3*5 + 35*5*6 + 30*11*7) mod 210 = 3990 mod 210 = 0.
Follow this operation for all the pixel value of image.

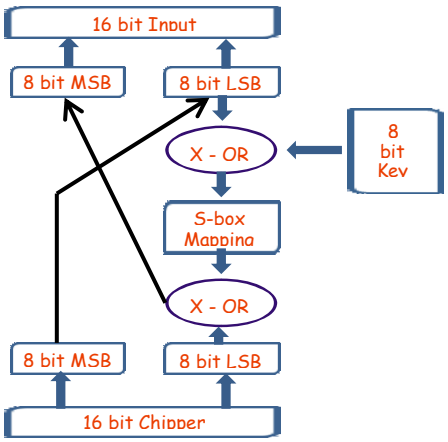


Fig 7: S-DES Decoding Function

Step 2: After the reverse process by RESIDUE NUMBER SYSTEM to every pixel value, then extract the watermark image from encoded image (Fig. 6) using position matrix and compare with original watermark image, if the result comes same, then It would we ensured that watermarked image is authenticated. Else it would be discarded.
Step 3: After performing Simple DES decryption function to the decoding function (Fig. 8) in pixel by pixel form. Both in column and row wise order will use respectively key image. Hence, the final secret image would be back.

D. Encryption Method for RGB Color Image:
The same algorithm would be applied as stated above, but the difference between is Grey scale image and color image in RGB.
Step 1: Initially, the color secrete image and the secrete key will be divided into their respective RGB images as: R (Red), G (Green), B (Blue).
Step 2: Now we conditionally apply the Simple DES algorithm to all the RGB image components.
•DES Encoding Function provide additional security by using different combination of secrete image and secrete key in (RGB) component as (RR, GG, BB), (RG, GB, BR), (RB, GR, BG).
•Watermark will be embedded according to the value of the position matrix.
Step 3: RESIDUE NUMBER SYSTEM mapped the Intensity value of RGB image.

E. Decryption Method for RGB Color Image:
Step 1: Here we will divide the embedded RGB color image into separate RGB image component.
Step 2: Now applied the Simple DES decryption method to RGB image components and extract watermark from all RGB images.
Step 3: Finally, combine RGB image component into single RGB image component, and then the efficiency would be checked of the proposed method, by the calculation of PSNR (Peak Signal to Noise Ratio).

IV. EFFICIENCY MEASUREMENT

PSNR (Peak Signal to Noise Ratio): It calculates the distortion occurs between the Watermarked image and image.

$$\text{PSNR} = 10 * \log \frac{255*255}{MSE} \quad (2)$$

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

Here MSE is Mean Square Error, where f(i,j) represents the pixel value of original image and g(i,j) represents the pixel value embedded image. If the PSNR value comes high, it means that watermarked is more robust or it goes down that means robustness of watermarked image is less. The PSNR value should be higher for better robustness and the PSNR is expressed in dB scale.

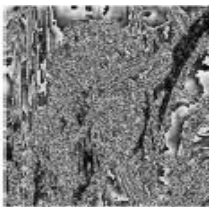
V. SIMULATION RESULTS

The proposed model is implemented using MATLAB R2017a. Fig. 7 shows the secrete image and secrete key. Fig. 9 shows encoded Simple DES image of green component and watermark image. Fig. 10 shows watermarked image of green component and final RESIDUE NUMBER SYSTEM 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.


(a)Secrete Image

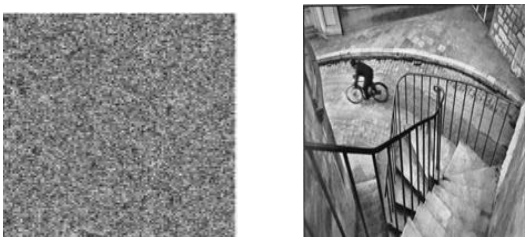

(b) Secrete Key

Fig. 8 (a) Secrete Image and (b) Secrete Key


(a) S-DES Encoded Green Image


(b) Watermarked Image

Fig 9: (a) S-DES Encoded Green Image and (b) Watermarked Image



(a) Watermark Green Image (b) RNS Encoded Image

Fig 10: (a) Watermarked Green Image and (b) RNS Encoded Image

(a)Decoded RNS Image (b) Watermark Image

Fig 11: (a) Decoded RNS Image Green and (b) Watermark Image

(a) Recovered S-DES Image (b) Final Decode Image

Fig 12: (a) Recovered S-DES Image and (b) Final Decode Image

Finally, It has been analysed the efficiency of the grey scale image and RGB Color image as shown in Table 1.

Table 1: MSE and PSNR values

Images	MSE	PSNR
Grey Scale Image	$5.08e^{-002}$	48.452
Color Image (R Image)	$3.157e^{-003}$	30.25
Color Image (G Image)	$2.516e^{-003}$	32.52
Color Image (B Image)	$1.23e^{-003}$	27.23

VI. CONCLUSION AND FUTURE SCOPE

This paper focused to recover or prevent our secrete image with the use of RESIDUE NUMBER SYSTEM moduli, Secrete Key , Position Matrix, and S-box Mapping techniques in sequential order, if the hacker uses attacks to destroy. Here, we recovered secrete image. The model is based on Color image, with the combination RGB of secrete image and secrete key with the combination of Red and Green image components of Color secrete key respectively. We have applied DES and Residue number system technique to provide the security for Color watermark image, which enhance the option for more combination between secrete image, secrete key and watermark image.

REFERENCES

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

[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, pp. 252-255, 2011.

[3] 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, pp. 314-318, 2009.

[4] B. Madhu, G. Holi, S. Murthy, "*An Overview of Image Security Techiques*" International Journal of Computer Applications Vol. 154, No.6, pp. 37-46, 2016.

[5] B.D. Parameshachari, K. M. S. Soyjaudah, M.V. Chaaitanyakumar, "*A Study on Different Techniques for Security of an Image*", International Journal of Recent Technology and Engineering, ISSE: 2277-3878, Vol.- 1, Issue-6, pp. 14-19, 2013.

[6] P. Bhangale, A. Gawad, J. Maurya, R.S. Raje, "*Image Security using AES and RNS with Reversible Watermarking*", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4, Issue 5, pp. 350-355, 2017.

[7] 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, pp. 468-472, 2013.

[8] H.K. Maitya, S.P. Maity, "*Joint Robust and Reversible Watermarking for Medical Images*", 2nd International Conference on Communication, Computing & Security, Procedia Technology pp. 275 – 282, 2012.

[9] 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, pp. 235-240, 2013.

[10] M. K. Ramaiya, N. Hemarajani, and A. K. Saxena, "*Security Improvisation in Image Steganography using DES*", 3'd IEEE International Advance Computing Conference, pp. 1094-1099, 2013.

[11] A. Rahman, M. T. Naseem, 1. M. Qureshi, M. Z. Muzaffar, "*Reversible Watermarking using Residue Number System*", IEEE Trans., 7th International Conference on Information Assurance and Security (lAS), pp. 162-166, 2011.

[12] S.S. Mamarde, S.A. Ladhake, "*A Review on Secret Image Protection using Reversible Watermarking*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 1, pp. 188-190, 2017.

[13] S. Aguru , B.M. Rao, "*Data Security In Cloud Computing Using RC6 Encryption and Steganography Algorithms*", International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.1, pp.6-9, 2019.

[14] S. Bansal, "*Data Security by Steganography: A Review",* International Journal of Scintific Research in Network Security and Communication, Vol.7, Issue-1 pp. 10-12, 2019.

[15] M. Mundher, D. Muhamad, A. Rehman, T. Sab and F. Kausar, "*Digital Watermarking for Images Security using Discrete Slantlet Transform*", Applied Mathematics & Information Sciences, An

International Journal, Appl. Math. Inf. Sci. Vol. 8, No. 6, pp. 2823-2830, 2014.
[16] P. Parmar, N. Jindal, "*Image Security with Integrated Watermarking and Encryption*", IOSR Journal of Electronics and Communication Engineering, Vol. 9, Issue 3, pp. 24-29, 2014.
[17] N. Chandra, J. Bagga, "*Performance Comparison of Digital Image Watermarking Techniques: A Survey*", International Journal of Computer Application Technology and Research, Vol. 2, lssue 2, pp. 126-130, 2013.
[18] M. Mangtani, N. Limbad, "*A Survey on Various Watermarking and Cryptography Techniques for Data Hiding in Medical Images*", IJSRD - International Journal for Scientific Research & Development, Vol. 3, Issue 09 , pp. 633-637, 2015.
[19] 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), pp. 41-44, 2010.
[20] A. Al-Haj, N. Hussein and G. Abandah, "Combining cryptography and digital watermarking for secured transmission of medical images," 2nd International Conference on Information Management (ICIM), London, pp. 40-46, 2016.

Authors Profile

Jaishree Jain is an Assistant Professor Department of Computer Science Engineering Department, Chandigarh University, Punjab, INDIA. She has 8.10 years teaching experience in CSE/IT Department as an Assistant Professor since July 2010. She is a Ph.D. scholar of Uttarakhand Technical University, Dehradun, INDIA with her profession. She received the master's degree in Software Engineering from MNNIT, Allahabad. Her research interests include Image Processing, Cloud Security, and Steganography. She had been published one patent in 2018 and about 24 papers in International/National Journals and Conferences. She is the member of 4 professional bodies i.e life time member of (ISTE) International Society for Technical Education, lifetime member of ICSES, member of ECI (Engineering Council of India) as an Professional Engineer by ECI, INDIA and Life time member of SCINAPSE.

Ajit Singh had completed his Ph.D. in Computer Science & Engineering. He is an Associate Professor & HOD of Computer Science & Engineering Department at BTKIT, Dwarahat, affiliated to Uttarakhand Technical University, Dehradun, INDIA. He has 12 years teaching experience. He has published 2 papers in SCI Journals. His research interests include Artificial Intelligence, Genetic Algorithms and Data Mining.

