

Complexity Analysis of Hybrid Method for Securing and Compressing Images

¹C.Yoga Anitha, ²P.Prabhu

¹Research Scholar, ²Assistant Professor - DDE

^{1,2}Department of Computer Applications, Alagappa University, Karaikudi.

Corresponding author email id: yogaa177@gmail.com

Abstract

Security is a most important issue for communication and storing images during image transformation. Protection of image becoming very important. The protection of image done with encryption and decryption. There are various techniques has been proposed to protect the confidential image from unauthorized access. Image compression technique is used to reducing the size of an image. Hence, in this research work a hybrid method, which combines securing image using RSA, hill cipher and 2-bit rotation and compressing of images using lossless image compression method have been proposed. The complexity of algorithm is analysed using execution time and quality of image compression using PSNR and MSE measures. This method secures the image and reduce the size of the image for data communication over the internet.

Keywords: *cryptography, image compression, RSA, hill cipher, 2-bit rotation. encryption, decryption.*

I.INTRODUCTION

Cryptography comes from the Greek word 'kryptos'. Sending information in secret way. This is called cryptography. Crypt – O - Graphy. Hidden + Message. There are two types of cryptography. They are Public Key Cryptography (Asymmetric) and Private Key Cryptography (Symmetric).

In Public Key Cryptosystem (PKC), two keys for encryption and decryption are used. One is public key and another is private key. PKC otherwise called Asymmetric cryptosystem. Encryption (K_e) and Decryption (K_d). The existing algorithms are RSA, Diffie-Hellman, ElGamal and Digital Signature Algorithm (DSA) [10].

The Private Key Cryptography otherwise called Secret Key Cryptography. This method using only one key for encrypt and decrypt. Sender and receiver know the same secret key. Sender is encrypt the message using secret key and receiver decrypt the message using same secret key [5].

The existing algorithms are DES, 3DES, AES and Blowfish.

Image compression

Image compression is one of the data compression for images. It is used to reduce the image size. Here we use LOCO (Low Complexity Lossless Compression) technique for image compression. This technique has two components: Modelling and coding.

The second chapter literature review of various types' image encryption, decryption and compression is discussed. Third chapter deals with the architecture of the proposed HMSCI method, Fourth chapter explains the results about the complexities of HMSCI method.

II.LITRATURE SURVEY

Research in any field needs literature in the related filed. This chapter presents the literature review of image security and compression.

Ako Muhammad Abdullah [1] analysed Hash Least Significant Bit (H-LSB) with affine cipher algorithm proposed for providing more security to data in a network environment. A hash function is used to select the particular position of insertion in LSB bits. This system allow a message sender to select keys to encrypt the secret message before embedding into the image and a receiver is used the keys to decrypt the message .Receiver can be decrypted the encrypt message with incorrect the keys but to a different form from the original message.

Ashwak Mahmood Alabaichi [2] detailed focus on colour image encryption and decryption using 3D chaotic map with AES key dependent S-Boxes. It has four major parts: 3D Logistic Map, 3D Chebyshev map, and 2D Arnold Cat Map, and Dynamic S-box of AES. Here, Exclusive X-or is used for image diffusing. 3D Logistic Map is employed for the generation of secret keys the purpose of scrambling the image. 3D Chebyshev map engaged for the generation secret keys for diffusing the image. 2D Arnold Cat Map is to scramble the coordinate values of AES S-Box to make it secret.

Devashish Vaghela [3] implemented public private key pair in the modified key based image encryption using RSA algorithm for encrypt and decrypt the image which increase the security and also used alphanumeric password secret key pair which is derived from RSA First, they applied Hill Cipher algorithm for image encryption, after that they applied Bit rotation and Bit reversal method for more secured image encryption and decryption.

Dijana TRALIC [4] developed a new method for digital image encryption, based on a 2D cellular automaton and pixel separation. Novelty in the proposed method lies in the application of the balanced 2D cellular automata with extended more neighbourhood separately on each level of pseudorandom key-image. This process extends key space several times when compared to the previous methods. Furthermore, pixel separation is introduced to define operation for each pixel of the source image.

Er. Jyoti Sharma [12] analysed a hybridization technique of cryptography is proposed for the better security of the data. The message was initially encrypted with DES and the keys of DES are encrypted with RSA then the hybrid of both DES-RSA is embedded inside the speech with help of genetic algorithm. Results of the technique provide a stronger security. The encryption time is also faster than the previous techniques as well as brute force attack to this technique is almost not possible.

Fausto Meneses [7] proposed optimize the RSA encryption algorithm and thus improve the security, integrity and availability of information. The results show the efficiency and functionality of the RSA algorithm in terms of information security. Presented deal with time,

memory, processor and network performance when performing encryption and decryption are lower than other RSA solutions, because calculations are performed on the client and server.

Karrar Dheiaa Mohammed AlSabti [8] a particular strategy in the public key cryptosystem called RSA Cryptosystem is presented and to be applied over gray and color images with the help of MATLAB Program. Since the RSA cryptosystem is a well-known secure cryptosystem, they used MATLAB to apply public key cryptosystem over gray and color images. Moreover, that would be generating two algorithms for the encryption and decryption procedures. However, the image is partitioned into blocks that are $n \times m$ matrices.

Kirti Sapra [9] explained approach said an Image encryption and decryption using RSA method used to protect the confidential image data from unauthorized access. They have implemented RSA with bit rotations and Extended hill cipher techniques.

Komal D Patel [13] detailed survey on existing work, which is used different techniques for image encryption, and we give general introduction about cryptography.

Monika Suhag [11] analyzed approach said an Image encryption and Decryption using RSA algorithm and 2 bit rotation method makes more securable transaction. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

III. PROPOSED METHOD

In this Hybrid Method (HMSCI), various types of images are secured and compressed. This method works in two phases; Image encryption, decryption and image compression. In first phase, selected image is encrypted and decrypted using RSA, 2-bit rotation and hill cipher algorithm. In second phase, images is compressed using LOCO algorithm.

3.1. HMSCI Encryption Process:

Encryption process is convert the original image to coded or encrypted image.

1. SENDER

Figure 1 shows the encryption process of HMSCI method.

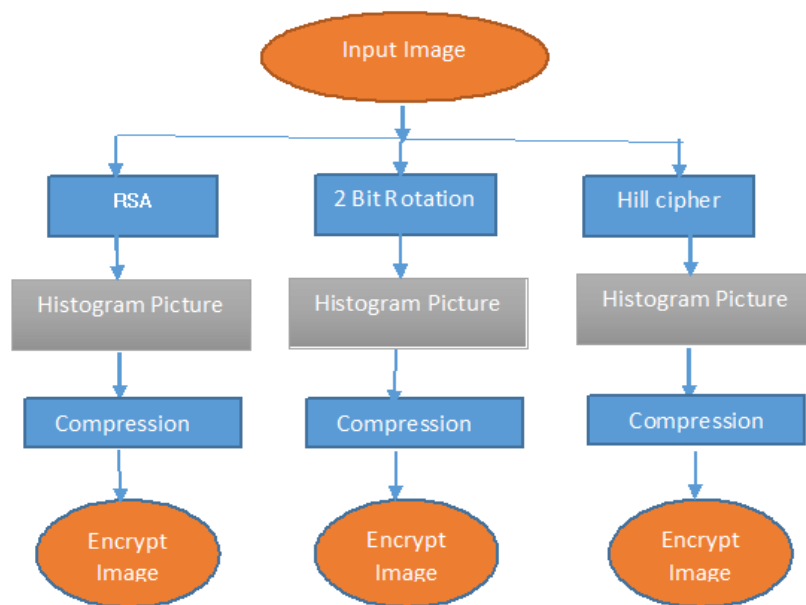


Figure 1: HMSCI Encryption diagram

2. HMSCI Encryption Process:

- Step 1: Begin
- Step 2: Select the image.
- Step 3: Apply RSA algorithm for encrypt and compress the selected image
- Step 4: Generate the histogram picture.
- Step 5: Apply 2-bit rotation technique for second encryption and compress image
- Step 6: Generate the histogram picture.
- Step 7: Finally use hill cipher technique using involuntary matrix and compress the image.
- Step 8: Generate the histogram picture.
- Step 9: Send the image to receiver.
- Step 10: End.

3.2 HMSCI Decryption Process:

Decryption Process is converted encrypted image into original image.

1 RECEIVER

Figure 2 shows the decryption process of HMSCI method.

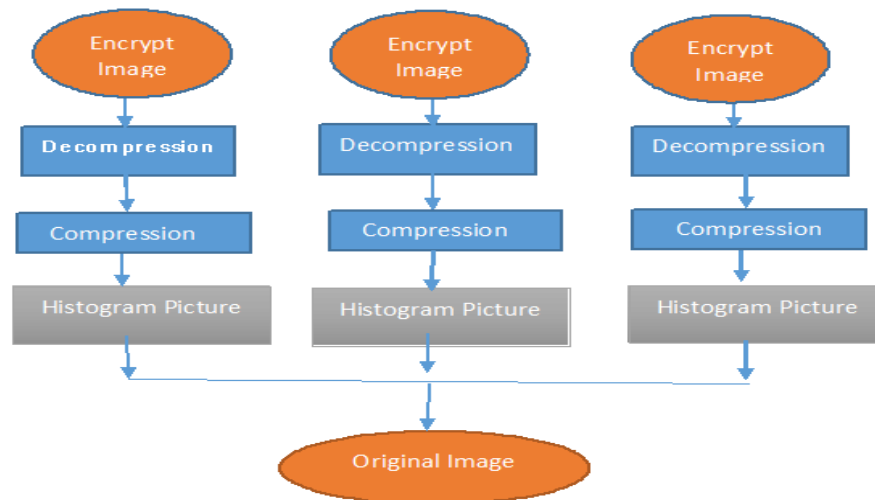


Figure 2: HMSCI Decryption Process

2 HMSCI Decryption Process

Step 1: Begin

Step 2: Select the compressed image.

Step 3: First decompress the compressed image and then image decrypted by RSA algorithm.

Step 8: Generate the histogram picture.

Step 4: Decompress the compress image then decrypted by 2-bit rotation.

Step 8: Generate the histogram picture.

Step 5: Decompress the compress image then decrypted by hill cipher.

Step 8: Generate the histogram picture.

Step 7: Receive image successfully.

Step 8: End.

This algorithm has been implemented and tested using various images for analyzing its complexities.

IV RESULT AND DISCUSSION:

In this chapter, the complexity of proposed HMSCI method has been analyzed. Various kinds of images are selected to test the complexity of algorithm. The results of various images for data transmission and compression calculated using execution time and image quality measures PSNR and MSE is tabulated. The figure 3 shows the original, encrypted and decrypted images using HMSCI method.

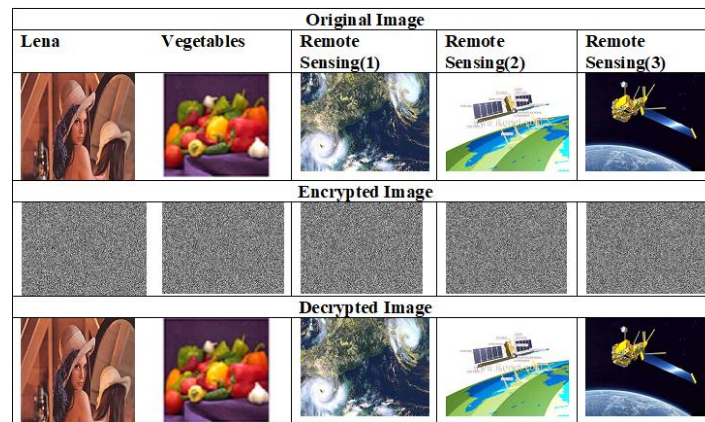


Figure 3. Original, encrypted and decrypted image using HMSCI algorithm

The table 1 shows the encryption and decryption time calculated for HMSCI method for various images.

Table 1. Encryption and Decryption Time (time/s)

Time	Lena	vegetables	Remote sensing(1)	Remote sensing(2)	Remote sensing(3)
Encryption	2	1.09	1.05	1.00	1.67
Decryption	1.21	2.08	2.00	1.30	1.88

The table 2 shows the image compression quality is calculated for HMSCI method using PSNR and MSE for various images[14,15].

Table 2.PSNR and MSE values of images

Quality	Lena	Vegetables	Remote Sensing(1)	Remote Sensing(2)	Remote Sensing(3)
PSNR	56.93	50.35	47.59	47.06	62.91
MSE	57.56	50.46	52.75	48.45	63.72

The figure 4 shows the encryption time calculated using HMSCI method of various images.

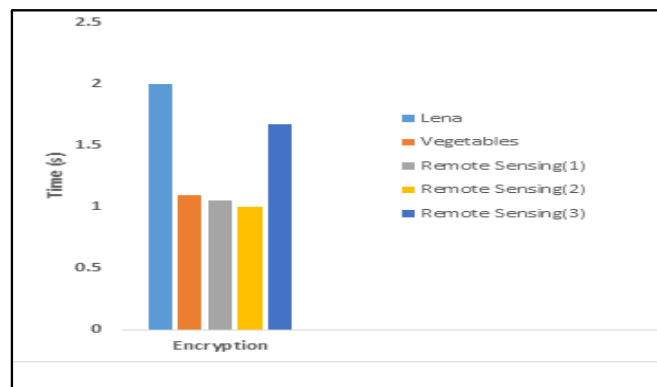


Figure 4 Encryption time of proposed HMSCI method.

The Figure 5 shows the Decryption time calculated using HMSCI method of various images.

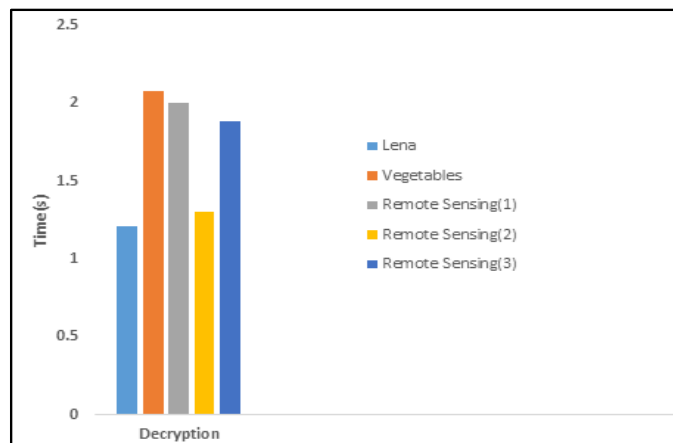


Figure 5 shows decryption time of proposed method.

The Figure 6 shows the PSNR values of HMSCI method of various images.

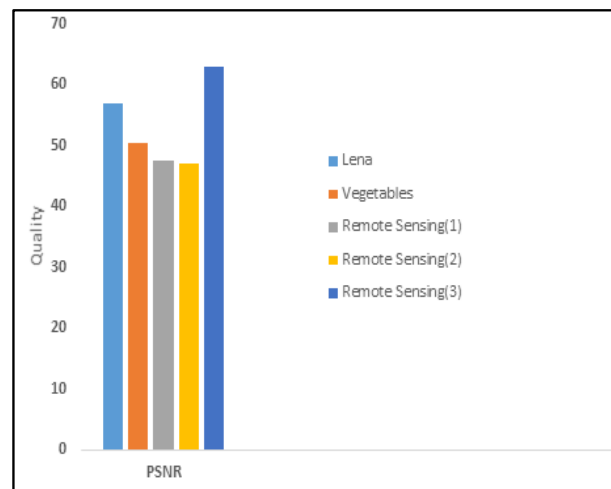


Figure 6 shows the PSNR value of proposed method.

The Figure 7 shows the MSE values of HMSCI method of various images.

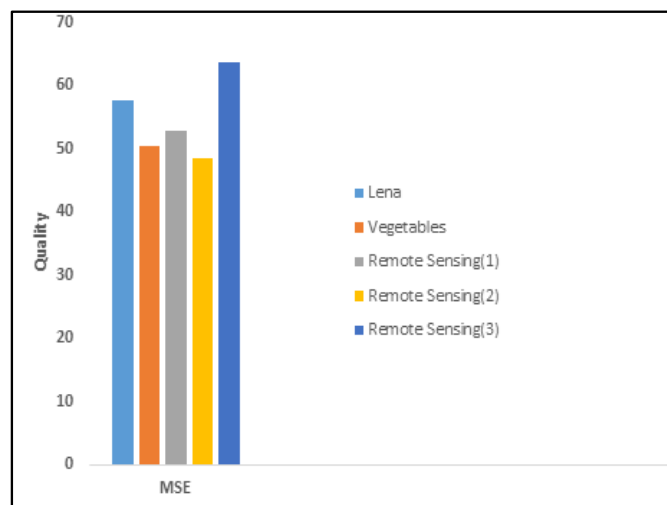


Figure 7 shows the MSE value of proposed method.

V CONCLUSION

In this work, "Complexity Analysis of Hybrid Method of Securing and Compression Images" have been presented. This method combines RSA, 2-Bit rotation and Hill cipher to propose novel hybrid method for image security. It also included LOCO image compression technique to compress the images. The complexity of algorithm for analysis using various measures. This method outperforms conventional methods when tested using various kinds of images. This algorithm is suitable for various applications like medical, crime and remote sensing image processing. Other optimization techniques can be applied to improve the quality of securing and compressing images as a future work.

REFERENCES

- [1] Ako Muhammad Abdullah, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm" Volume 143 – No.4, June 2016.
- [2] Ashwak Mahmood Alabaichi, "Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box" VOL.16 No.10, October 2016.
- [3] Devashish Vaghela, "Modified Key Based Image Encryption Using Rsa Algorithm" May 2016 | IJIRT | Volume 2 Issue 12 | ISSN: 2349-6002.
- [4] Dijana TRALIC, Sonja GRGIC, "Robust Image Encryption Based on Balanced Cellular Automaton and Pixel Separation" March 10, 2016.
- [5] Shankar, K., and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.
- [6] Er. Maninder Kaur, "A Research Paper On A Secure Image Encryption-Then Compression System Using Wavelet Via Prediction Error Clustering And Random Permutation" ISSN: 2277-9655 September, 2015.
- [7] Fausto Meneses, Walter Fuertes, "RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages" VOL.16 No.8, August 2016.
- [8] Karrar Dheiaa Mohammed AlSabti, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB" ISSN 0973-1768 Volume 12, Number 4 (2016), pp. 3631-3640..
- [9] Kirti Sapra, "Modified Image Encryption Technique" volume1 issue6 August 2014.
- [10] Shankar, K., and P. Eswaran. "Sharing a secret image with encapsulated shares in visual cryptography." Procedia Computer Science 70 (2015): 462-468.
- [11] Monika Suhag, "Review On Protection Of Data In Rsa Technique" June-2016 Volume 3, Issue-6.
- [12] Er. Jyoti Sharma, "An Efficient Hybrid Approach for Secure Speech Cryptography" IJCSMC, Vol. 6, Issue. 1, January 2017, pg.23 – 29 .
- [13] Komal D Patel, Sonal Belani, "Image Encryption Using Different Techniques: A Review" Volume 1, Issue 1, November 2011.
- [14] Shankar, K., and P. Eswaran. "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography." China Communications 14.2 (2017): 118-130.
- [15] Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique." Journal of Circuits, Systems and Computers 25.11 (2016): 1650138.

