Performance Evaluation of Hybrid Method for Securing and Compressing Images

C.Yoga Anitha[1], P.Prabhu[2]
[1]M.Phil Scholar, Department of Computer Applications, Alagappa University, Karaikudi
[2]Assistant Professor – DDE, Department of Computer Applications, Alagappa University, Karaikudi
Email: yogaa177@gmail.com, pprabhu70@gmail.com

Abstract—Security is a most important field of research work for sending and receiving of data in secret way over the network. Cryptographyis a method for securing transformation like image, audio, video, text without any hacking problem. Encryption and Decryption are two methods used to secure the data. Image compression technique used to reducing the size of an image for effective data communication. There are variety of algorithms has been proposed in the literature for securing images using encryption/decryption techniques and reduce the size of images using image compression techniques. These techniques still need improvement to overcome issues, challenges and its limitations. Hence in this research work a hybrid method which combines securing image using RSA, hill cipher and 2bit rotation and compressing of images using lossless compression algorithm has been proposed. This method compared to execution time of existing method. This method secures the image and reduces the size of the image for data communication over the internet. This method is suitable for various applications uses images like remote sensing, medical and Spatio-temporal.

Keywords—Cryptograph; Image Compression;RSA;Hill Cipher; 2-bit Rotation;

I. INTRODUCTION

Cryptography comes from the Greek word ‘kryptos’. It means hiding information. Information security uses *cryptography* on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored.his method has two types. They are given below:

Public Key Cryptography (Asymmetric)
Private Key Cryptography (Symmetric)

The Public Key Cryptography has two different keys. They are public key for encrypt and private key for decrypt. It is used to transmit image data over a network.

Encrypt-→Key-→Decrypt
Encryption (K_e)
Decryption (K_d)

The Private Key Cryptography otherwise called Secret Key Cryptography. This method using only one key for encrypts 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.

Cryptography method has five purposes. They are given below:

- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity
- ✓ Non-Reputation
- ✓ Access control

Confidentiality: Its means access only the authorized user not anyone else

Authentication: The transmission of data from one computer to another computer has to be accessed only the authorized user. Unauthorized user cannot access the data or information.

Integrity: Modify the transmitted information or data by only the authorized user. Unauthorized use cannot modify.

Non-Reputation: Ensure the messages that sender or receiver.
Access Control: The authorized persons only can able to access the information during the transfer.

A) Technique

Here we are using three techniques for encrypt and one method for compression.

1. Encrypted Techniques:

- RSA
- 2Bit Rotation
- Hill cipher

1.1 RSA:

The RSA is a cryptographic algorithm for encrypt and decrypt the data. This algorithm invented 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. This describes Public Key Cryptosystem. This technique suitable for various applications like e-mail, Banking, e-commerce on the internet

1.2 2Bit Rotation:

In 2Bit rotation, we rotate the pixel values of the image with 2bit. In first step, we select the size of the image. Then generate the key. After that convert key value to binary format. And then apply 2bit rotation.

1.3 Hill cipher:

Hill cipher is a polyalphabetic cipher. It is a generalized version of the affine cipher and the vigenere cipher combined. Invented in 1929 by Lester S.Hill. It's explained by matrix. Numbers are assigned in below format

a=0, b=1, c=2, d=3, e=4, f=5,……………………, z=15.

2. Compression Technique:

Image compression is a type of data compression for images. It's used to reduce the image size. Here we use the technique given below:
LOCO (Low Complexity LOssless COmpression)

2.1 LOCO:

The lossless compression method means reduce the size of image without any loss.
LOCO **(**Low Complexity Lossless Compression**)** has two components.

- Modelling
- Coding

II. RELATED WORKS

Research in any field requires literature review is a written document that presents a logically argued case founded on comprehensive understanding of the current state of knowledge about a topic of study. This case establishes a convincing thesis to answer a study question. It will also give readers the necessary background to understand the research work.

Monika Suhag [1] proposed 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. First RSA encrypt the image with 1-bit rotation and then second, they are applying 2-bit rotation to make it more secured image conversion. In Decryption time they have apply reverse method.

Devashish Vaghela [2] 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.

Samson chepuri [3] explained image encryption using RSA algorithm for RGB image encryption. First read the input of RGB colour image. After applied RSA algorithm for encrypt and decrypt. The time taken for both encrypt and decrypt together is 12.36 seconds which is less compared to existing methods. Here the image encryption and decryption approaches are highly securable and with less computational time. Sneha ghoradkar [4] proposed AES encrypt and decrypt method. Encrypt have substitute bytes, shift rows, mix columns, add round key. And decrypt have add round key, inverse shift row, inverse substitute bytes, and inverse mix columns. AES process with the data block of 128 bit and cipher key length of 256 bit. The image of 256 bit cipher key to achieve the high security. Because 256 bit cipher key is difficult to break

Monika Suhag [5] 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. Swati Kumari [6] proposed approach used Image encryption and decryption using Sylvester equation and Hankel matrix and another line mapping algorithm used for encryption.

Kirti Sapra [7] 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. S.Anandkumar [8] explained approach said an Image cryptography using RSA method used to protect the confidential image data from unauthorized access. They have explained purpose of cryptography and merits/demerits of cryptography and applications of cryptography.

Zhiqiang Li, et.al [9] proposed approach they are used A Chaotic encryption used digital image compression and encoding technology based on discrete cosine transform and discrete wavelet transform. This compression encryption algorithm is feasible and it decrease the redundant information of the image, it reduces the storage space and improves the efficiency of data transmission. Sunita [10] proposed approach said an Image encryption and decryption using RSA method. They have implemented RSA with bit rotations and hill cipher techniques. In this chapter, various image security algorithms like RSA, AES, 2bit, Hill cipher and its variants proposed by various authors has been studied and analysed for their performance and their limitations. To overcome these limitationsHMSCI method has been proposed.

III. PROPOSED METHOD

In this work, a Hybrid Method for securing and compressing images (HMSCI) has been proposed. In this method three different encryption techniques namely 2bit, RSA and hill cipher algorithms are used to secure the image and an image compression technique is used to reduce the size of an image.

A) SYSTEM DESIGN:

The system design of this proposed encryption method is shown in figure 1 and decryption method is shown in figure 2.

1. **Encryption Process:**

1.1 SENDER:

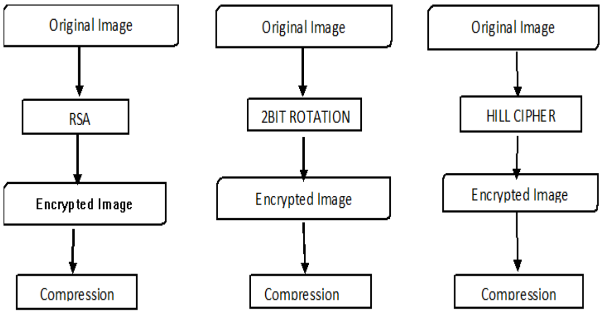


Figure 1 HMSCI Encryption with compression design

1.2 Encryption Process:

Step 1: Begin
Step 2: Select the image from file.
Step 3: Apply RSA/ algorithm for encrypt and compress the image
Step 4: Then apply 2bit rotation technique for second encryption and compress image
Step 5: Finally use hill cipher technique using involuntary matrix and compress the image.
Step 6: Send the image to receiver.
Step 7: End.

2. Decryption Process:

2.1 RECEIVER:

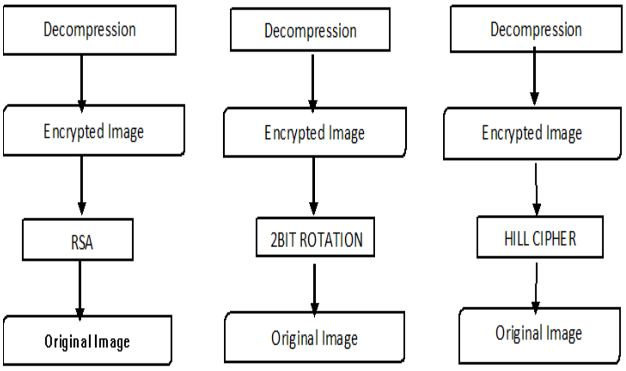


Figure 2 HMSCI Decryption with decompression design

2.2 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 4: Decompress the compress image then decrypted by 2 bit rotation.
Step 5: Decompress the compress image then decrypted by hill cipher.
Step 7: Receive image successfully.
Step 8: End.

The original image is selected and preprocessed for applying image encryption/decryption. The preprocessed image is encrypted using RSA, 2Bit Rotation and Hill cipher algorithm.

B) RSA Algorithm:

1. Choose two prime p and q and find public modulus
   $N=pq$
2. Choose public exponent
   $e=(p-1)(q-1) \quad 1<e<(p-1)(q-1);$
3. The pair (n,e) is a public key.
4. PrivateKey is an umique integer
   $1<d<(p-1)(q-1);$
   Such $ed=1 \bmod (p-1)(q-1)$

Encryption:

Split a message into m_1, m2, mt.

$0 \le m_i \le n$

$C=E(M)$

$\Rightarrow M^e \pmod n);$

Decryption:

$D(C)=C^d \pmod n);$

M=Message
C=Cipher text
E=Encrypt
D=Decrypt.

So encryption pair of integer (e;n), decryption pair of integer(d;n).

C) 2Bit Rotation:

In bit rotation technique we will first converted images into grayscale images. Each pixel of images will have 8 bits as having intensity from 0 to 255 so each pixel represents 8 bits.

Shift=code mod 7.

Procedure:

Step 1: Select the size of the image.
Step 2: Generate the key by using pixel value of image.
Step 3: Convert key value into binary format.
Step 4: Then apply 2bit rotation.

We apply this method our image will be more secure.

D) Hill Cipher:

Encryption mathematical statement is

$$Y=AX$$

Decryption mathematical statement is

$$X=A^{-1}Y$$

E) LOCO Technique:

Low Complexity Lossless Compression is used to reduce the size of image without any loss and low complexity. It has two components: modeling and coding.

IV . RESULT AND DISCUSSION

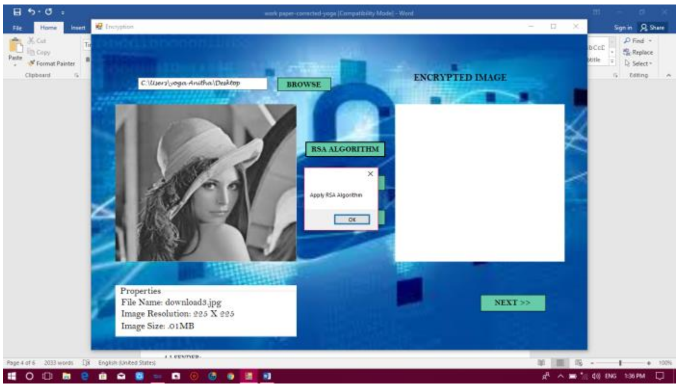
This HMSCI Method has been implemented and evaluated for efficient using various images. Time complexity is tested for the performance of this method.

A) Experimental setup:

This method has been implemented in AMD Processor with speed 2.0 GHz,RAM 4GB and coded using C# in Visual Studio 2010.

4.1 SENDER:

The home page of our work has two buttons like sender and receiver. Sender is going to encryption and compression. Receiver is going to decryption and decompression. The figure 3. Shows the encryption of lena image using RSA algorithm.



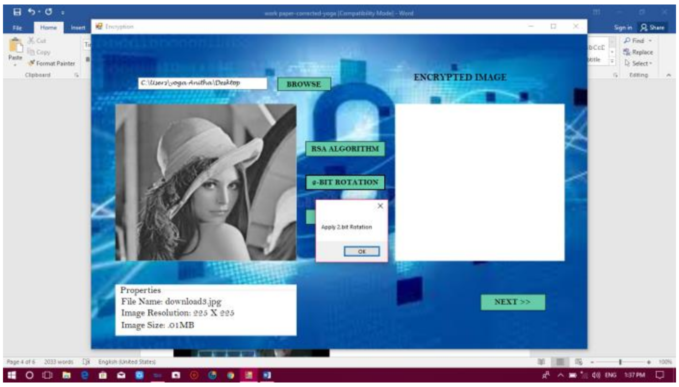
C:\Users\yoga-Anitha\Desktop

Apply RSA Algorithm

Properties
File Name: download3.jpg
Image Resolution: 225 X 225
Image Size: .01MB

Fig 3: Encryption by RSA algorithm

The figure 4. Shows the encryption of lena image using 2bit rotation algorithm.

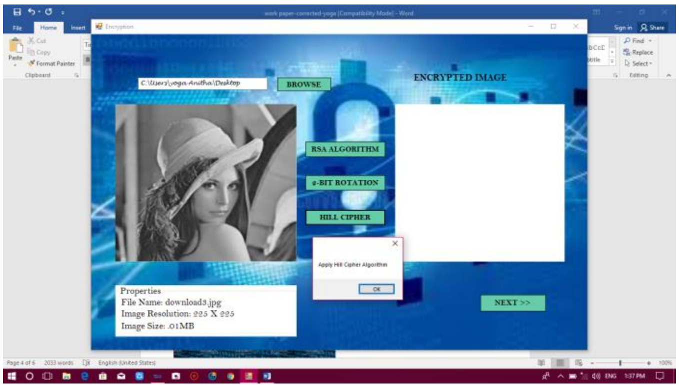


Apply 2 bit Rotation

Properties
File Name: download3.jpg
Image Resolution: 225 X 225
Image Size: .01MB

Fig 4: Encrypted by 2 bit rotation

The figure 5. Shows the encryption of lena image using Hill cipher algorithm

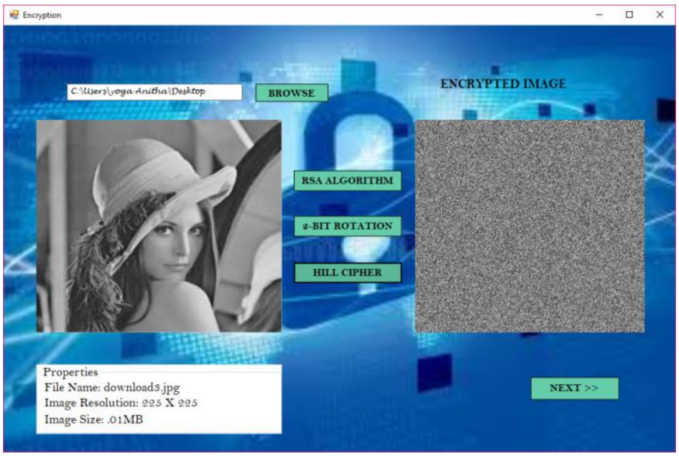


Apply Hill Cipher Algorithm

Properties
File Name: download3.jpg
Image Resolution: 225 X 225
Image Size: .01MB

Fig 5: Encrypted by hill cipher algorithm

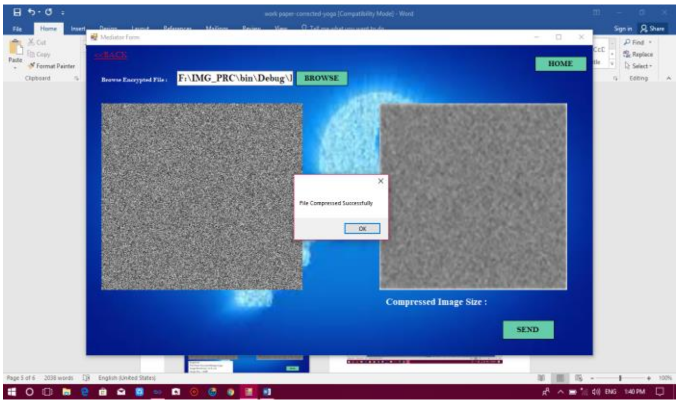
The image is encrypted successfully using three encryption techniques like RSA, 2 bit, hill cipher. Thefigure 6 shows the encrypted lena image using proposed algorithm.



Properties
File Name: download3.jpg
Image Resolution: 225 X 225
Image Size: .01MB

Fig 6: Encrypted image

The figure 7 shows the image compressed using LOCO method.



Browse Encrypted File : F:\IMG_PRC\bin\Debug\

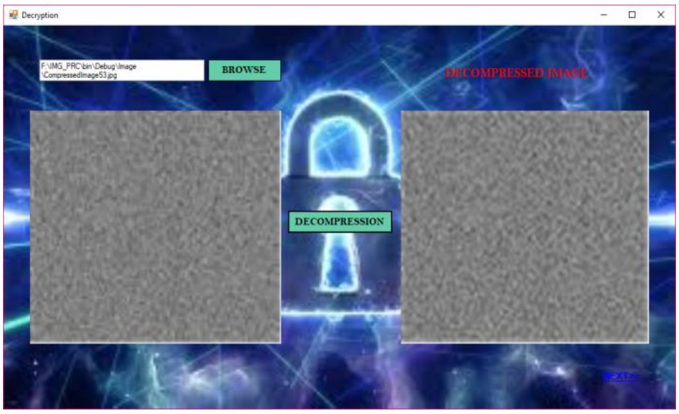
File Compressed Successfully

Compressed Image Size :

Fig 7: Compressed Image

4.2 RECEIVER:

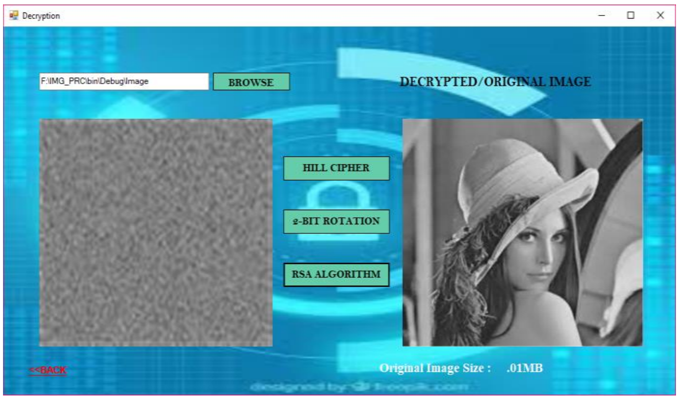
The encrypted image has been decrypted using HMSCI method. Then the decrypted image is compressed using LOCO method. The figure 8 shows the decompressed image using LOCO method.



F:\IMG_PRC\bin\Debug\Image \CompressedImage53.jpg

Fig 8: Decompressed image

The figure 9 shows the decrypted image obtained using HMSCI method.



F:\IMG_PRC\bin\Debug\Image

Original Image Size : .01MB

Fig 9 : Decrypted image

B) Performance Evaluation:

This algorithm has been evaluated using time and size metrics.The table 1 shows the comparison time complexity of the conventional method with proposed model. The table show the proposed method outperform with conventional method in terms of security and time complexity.

Table 1 shows the comparison of time complexity of the conventional model with proposed model.

Encryption (time /s)			**Decryption (time /s)**		
Conventional Method					
RSA [2]	2 BIT [6]	HILL CIPHER [6]	RSA [2]	2 BIT [6]	HILL CIPHER [6]
2	2.1	2.0	2.2	2.0	1.5
HMSCI Model					
1.2	1.0	1.0	1.3	1.0	1.0

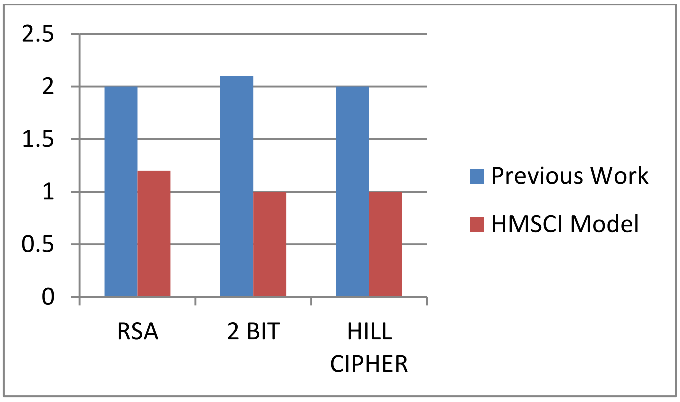


Figure 10 shows comparison of encryption execution time conventional vs proposed method

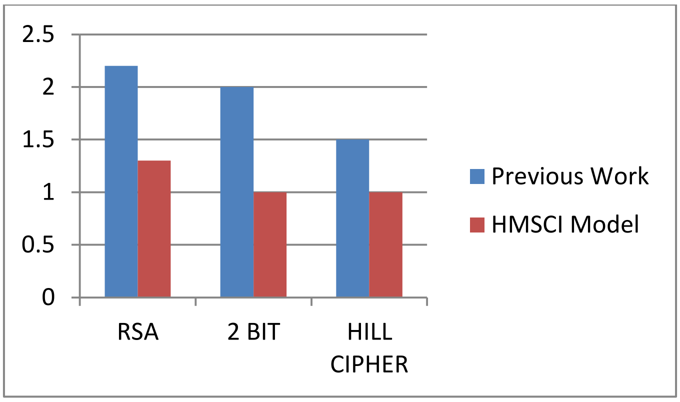


Figure 11 shows comparison of decryption execution time of conventional vs proposed method

Table 2 shows the comparison of image size of the conventional model with proposed model.

	Lena Image	Baboon
Original image	01 MB	6.61 KB
Wavelet Transform	36 KB	3.0 KB
LOCO	2.32 KB	1.5 KB

Fig 10 shows the comparison of encryption execution time of conventional and proposed method. Fig 11 shows the comparison of decryption execution time of conventional and proposed method. The table 2 shows the comparison image size of the conventional method with proposed model. The table show the proposed method outperform with conventional method in terms of reduce the image size. From the table 1 and table 2, it is observed that the HMSCI model outperform in terms of time and size complexity.

V . CONCLUSION

In this Paper "Performance analysis of Hybrid Method for Securing and Compressing Images" has been analyzed. This system is mainly developed to improve the Secure and efficiency of image transmission and decrease the image transmission time. This method use design developed, and tested for efficiency. This method HMSCI out performed in terms of security and reducing the size of image when compared with traditional methods. Optimization techniques may also be used for further improvement.

References

[1] Monika Suhag," Improvement Protection In Rsa Algorithm Using 2 Bit Rotations" June-2016 Volume 3, Issue-6.

[2] Devashish Vaghela," Modified Key Based Image Encryption Using Rsa Algorithm" May 2016 | IJIRT | Volume 2 Issue 12 | ISSN: 2349-6002.

[3] Samson chepuri,"An RGB image encryption using RSA algorithm" e-ISSN 2455–1392 Volume 3 Issue 3, March 2017 pp. 1 – 7.

[4] Sneha ghoradkar ,"image encryption and decryption using AES algorithm" NCETACT-2015.

[5] Monika Suhag ," Review On Protection Of Data In Rsa Technique" June-2016 Volume 3, Issue-6.

[6] Swati Kumari," Encryption and Decryption Techniques: A Review" Volume: 03 Issue: 09 | Sep-2016 .

[7] Kirti Sapra," Modified Image Encryption Technique" volume1 issue6 august 2014.

[8] Anandakumar,"Image Cryptography using RSA algorithm in network security" Vol.5 Issue. 5, May- 2017, pg. 1-14.

[9] Zhiqiang Li, Xiaoxin Sun, and Qun Ding," Design and Implementation in Image Compression Encryption of Digital Chaos Based on MATLAB" Volume 2,DOI: 10.1007/978-3-319-07773-4_50, c Springer International Publishing Switzerland 2014.

[10] Sunita," Image Encryption/Decryption Using RSA Algorithm" Vol.5 Issue. 5, May- 2017.