International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212553 Volume 9, Issue 3, May – June (2022)

RESEARCH ARTICLE

A Secure Image Encryption and Embedding Approach using MRSA and RC6 with DCT Transformation

Ganavi M
Department of Computer Science & Engineering, Jawaharlal Nehru New College of Engineering, Shivamogga, Karnataka, India.
gaanavi4@jnnce.ac.in

Prabhudeva S
Department of Master of Computer Applications, Jawaharlal Nehru New College of Engineering, Shivamogga, Karnataka, India.
pdshirematt@gmail.com

Sankhya N Nayak
Department of Computer Science & Engineering, Jawaharlal Nehru New College of Engineering, Shivamogga, Karnataka, India.
sankhya.nayak@jnnce.ac.in

Received: 13 February 2022 / Revised: 01 May 2022 / Accepted: 06 May 2022 / Published: 28 June 2022

Abstract – The growing potentialities of recent communications necessitate information security on the computer network. The various fields such as banking, E-commerce, education, and health sectors depend on the online network to communicate. Information security is becoming more significant. Hackers can get the data if it is sent as it is in an unsafe network. Therefore, security challenges like confidentiality, integrity & undetectability are essential to safeguard sensitive data from unauthorized users. To secure communicated information from a third party, it is necessary to convert the information into a scrambled form. Researchers have used various cryptographic and steganographic algorithms. The public key and private key cryptographic algorithms are suitable to scramble the input secret data. Using private key algorithms, key exchange is a challenge. Always two-level of scrambling of data is safe. After scrambling, embed it in cover media by using suitable transform domain techniques to provide higher security. In the proposed method, two-level scrambling of input secret images is carried out by applying faster processing symmetric algorithms such as Rivest Cipher 6 (RC6) & One Time Pad (OTP) to enhance the security of images. As these algorithms use the key on their own, it becomes difficult for any intruder to extract and identify the keys. Also, there is a necessity to safely send keys to the recipient. These two keys are scrambled using a public key cryptographic algorithm such as Modified Rivest-Shamir-Adleman (MRSA) algorithm. This reduces the chances of stealing the keys. Another level of security for the scrambled image is provided by embedding it in cover media using DC coefficients resulting in the stego image. Send the stego image and scrambled keys to the receiver. Simulation outcomes and analysis show that the proposed method provides two-level security for color image mediation and key authentication.

Index Terms – Modified RSA, RC6, DCT, OTP, Encryption, Steganography.

1. INTRODUCTION

The various fields such as banking, telecommunications, E-commerce, web browsers, chat applications, government databases, emails, organizations, education, and health sectors depend on the online transfer of sensitive data [1]. Information security is becoming more significant. There are various online threats to extracting such sensitive data. Therefore, security challenges like confidentiality, integrity & undetectability are essential to safeguard data from unauthorized users [2]. To secure communicated information from a third party, it is necessary to convert the information into a scrambled form. With the digitization of data and the networking of communications, information security over the Internet is becoming more and more crucial. Data transference across various means is the main element to possessing the security of confidential and proprietary information. Cryptography [3, 4, 5, 6, 7], steganography [8, 9], and watermarking [10] are the solution to confidentiality [11] and information security. Based on the requirements of the

RESEARCH ARTICLE

different applications, the steganography technique is used. Steganography is the art of writing secret details in other multimedia data thereby hiding the existence of the communicated information. Cryptography is the process of converting any information to its incomprehensible form and vice versa. It is a process to store and transmit details in a particular way so that only the intended recipient can read and process them.

The most important types of cryptographic techniques are symmetric, asymmetric, and hash functions. Cryptography using symmetric [12, 13] exchanges a single key-value between sender and receiver resulting in the ciphertext and recovering the native message. RC6 cryptographic standard [4, 14, 15] was chosen among the remaining standards to get the new associated AES. OTP applies XOR computations to achieve cipher. OTP is foremost suited for operations where the key is random and never reapplied [16]. No separate key is used in the hash. A hash of the determined length is computed according to plain text. This creates difficulty for anyone to recover the plain text. Operating system passwords are encrypted by using hash values and are stored. Cryptography using the public key considers two different keys. Sender scrambles by utilizing the public key and receiver descramble by utilizing the private key.

Steganography is a computerized image that can be accomplished in domains like spatial and frequency. The secret data is placed straight into the pel of the cover media in spatial, for instance, Least-Significant-Bit (LSB) [8, 17, 18]. Whereas in the frequency domain many transformations are used [25]. For secure message transactions, the current steganography technique is not providing security. To handle the issues of computerized content security menace, a great deal of analysis that mixes embedding and scrambling approach goes on. Encrypt the secret message before it is inserted to get proper security.

The research objectives of the proposed work include:

1. Deploy a two-level scrambling of the input image using fast processing, and less complex private key cryptographic algorithms such as RC6 and OTP. Double scrambling of the input image converts it into still more random so that it is difficult for the attacker to identify the actual input secret image. This is helpful to achieve confidentiality of the input image.
2. Sending private keys safely to the receiver is a big challenge in private key cryptographic algorithms. Therefore, scramble these keys by using complex modified RSA and then send it to the receiver. This is helpful to achieve key authentication.
3. After scrambling the input image, hide it in cover media using transform domain techniques like DCT. This makes the secret data undetectable.
4. Various statistical analyses such as PSNR, MSE, SSIM, NPCR, UACI, Information entropy, Correlation coefficients, & Avalanche effect of the scrambled and stego images are analyzed to show the effectiveness of the proposed work.

The rest of the paper is organized as follows: In section 2, previous work carried out by various researchers is included as a literature review. The problem statement is discussed in section 3. A brief explanation about symmetric key algorithms to scramble such as RC6 & OTP, and DCT transformation to embed are included in section 4. The proposed system framework to scramble and embed the input secret image as well the scrambling of keys along with algorithms are explained in detail in section 5. Results and discussions are included in Section 6. Conclusion and future scope are included in section 7.

2. LITERATURE REVIEW

The purpose of the proposed method is to secure the confidentiality of data for images in which symmetric, as well as asymmetric cryptography along with the steganography techniques, are used. With this objective, some of the literature on encryption and embedding techniques of previous work carried out by the researchers will be discussed in this section.

The RC6 algorithm has various benefits over the AES algorithm used for image encryption. This algorithm is combined with various other encryption algorithms to improve the performance and some researchers have implemented RC6 with modifications. The RC6 algorithm with modification has been proposed for image scrambling [4]. A cyclic shift has been combined in the permutation-diffusion system to enhance the mechanism of RC6 for images. Apply the XOR operation on the input data thrice [7] or twice [8] and then embed it in the carrier image using the spatial domain technique resulting in good PSNR. A method by combining Discrete Cosine Transform (DCT) and vernam cipher has been proposed in [9]. Scramble the data by vernam cipher and then embedded it in cover media by DCT. Transform domain steganography acts stronger against attacks.

A method in combination with RSA has been proposed [11] for data scrambling. This method's processing time is lesser compared to basic RSA. RC4, RC5, and RC6 are all symmetric key algorithms used for the fast processing of image encryption. RC4 stream cipher is used for encryption and decryption [12]. Symmetric algorithms with the combination of asymmetric grant a good result. Encryption of images has been carried out by RC6 & blowfish and encryption of keys by RSA [13]. A cryptography system using RC6 and RSA algorithms where the four different keys have been used for the decryption process along with the extra

RESEARCH ARTICLE

shifting of pixels by XOR. The comparison of Rijndael and RC6 cryptography has been discussed [14].

There is a necessity for the safety of patient electronic records in hospitals. The patient records are scrambled using RC6 and then hidden in cover media using shifting of the histogram [15]. A method has been proposed [16] where scramble the images by OTP followed by DCT-DWT. The computational complex RSA algorithm has been used for encryption in the system framework of SMS security in election situations [19]. Hiding the data after scrambling, is very much important in image security. RGB pixel shuffling with steganography has been used by applying hash-least significant Bit (HLSB). Advanced encryption standard and RC5 has been used for scrambling data [20]. The different cryptography and steganography algorithms that have been used by various researchers are summarized in Table 1.

Table 1 Summary of Literature Review

Sl. no.	Authors	Methodology	Observation
1.	Catherine Bhel B. Aguila et al [4]	RC6 algorithm with modification	A cyclic shift operation is additionally added.
2.	Yani Parti Astuti et.al., [7]	Encryption by performing XOR operation three times and using LSB steganography.	A single level of encryption with spatial domain steganography.
3.	Ali Ahmed, and Abdelmotalib Ahmed [8]	The message is encrypted using double XOR operations and used LSB technique.	MSE, PSNR, Entropy, and histogram distribution are evaluated.
4.	De Rosal Ignatius Moses Setiadi and Eko Hari Rachmawanto [9]	Scramble using vernam cipher. DCT is used for embedding.	A single level of encryption with transform domain steganography.
5.	May H Abood [12]	Encryption using an RC4 stream cipher. RGB pixel shuffling with steganography is used by applying hash-least significant Bit (HLSB).	The security evaluations are presented by calculating a peak-signal-to-noise ratio and mean square error.
6.	Vivek Kapoor and Rati Gupta [13]	Scramble using RC6 & RSA.	Two-level encryption is used.
7.	Shabir A. Parah et al [15]	Scramble using RC6 and embedded using histogram shifting.	Used for the security of patients' records.
8.	Wellia Shinta Sari et.al., [16]	OTP Encryption of the image with DCT-DWT Steganography.	A single level of encryption but two transformations are used at embedding.
9.	Dwi Yuny Sylfania et al [19]	Scramble the data using RSA.	Security of SMS messages. Only encryption is used.
10.	Md. Sagar Hossen et al [20]	Scramble using AES & RC5. Hash-least significant bit with RGB pixel shuffling used for the embedding of scrambled data	Two-level encryption with embedding is used.

3. PROBLEM STATEMENT

There is a necessity to implement an approach to enhance the confidentiality of color images. The confidentiality of the sensitive input image can be achieved by converting its pixel value to some other value. This changed value is random when compared between neighboring pixels in the input image. The peak-signal-to-noise ratio among input images and converted scrambled images should be lesser. Encryption algorithms are helpful to achieve random images. A combination of public and private key cryptographic algorithms is helpful to achieve confidentiality of the input secret image and authentication of the private keys. To further

RESEARCH ARTICLE

enhance the security of the input secret data, transform domain steganographic techniques are always suited. Instead of hiding the raw secret data as it is in the cover image, scramble and then hide makes the proposed method a better system.

4. SCRAMBLE AND EMBED ALGORITHMS

4.1. RC6

RC6 is a symmetric block cipher obtained through RC5. It considers a block of 128 bits and key bits of 128, 192, and 256. It provides better security than AES and provides all the requirements of the AES. An additional multiplication is used in RC6 which is not present in RC5. In a word, every bit is used for rotation along with the least significant bits. The 128-bit is segmented as 32 bits and encryption is carried out for the first 10 rounds by using a symmetric coat and decryption in another 10 rounds [4, 21].

4.2. One Time Pad

One-time pads are used in pairs [9] as shown in Figure 1. Each user holds one of the pairs of the pad and exchanges it via a secure channel. The "pad" is considered by applying XOR operation on every bit of the pad with every other bit of the input data. After the data is encoded with "pad", is directed over the network to the intended beneficiary. On receiving, the same is XORed with another pair of "pads" and the original data is extracted. The random number generator of a seed with a value of 128-bits must be used.

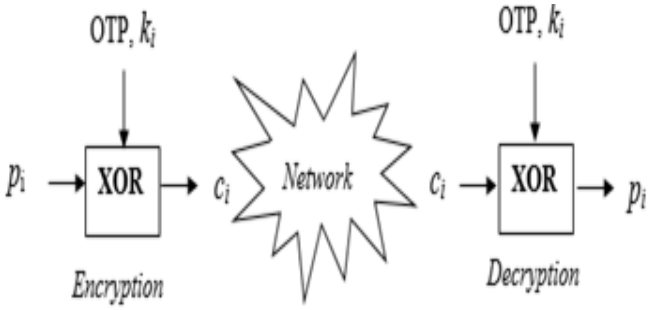

Figure 1 Technique for One Time Pad

Both sender and intended recipient have random OTP. Perform XOR operation between the plaintext "p" and the OTP value loaded in "k"

$$c_i = p_i XOR k_i \quad (1)$$

The ciphertext "C" generated is sent to the receiver at the destination. The receiver knowing the OTP can recover the message by computing the XOR operation between the received ciphertext "C" and the OTP "ki"

$$p_i = c_i XOR k_i \quad (2)$$

4.3. Discrete Cosine Transform (DCT)

The DCT divides the image into spectral sub-bands [9, 16]. This transform divides carrier signal into bands of low, middle, and high frequency. Encrypted data is embedded into one of these three bands. The DCT transforms an input from the spatial to frequency. This can be shown as

$$C(u,v) = \frac{1}{\sqrt{2N}}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2x+1)v\pi}{2N}\right] \quad (3)$$

$$f(x,y) = \frac{1}{2N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)\,C(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2x+1)v\pi}{2N}\right] \quad (4)$$

Where u, v = 0, 1, 2.....N-1 and α (k) is defined as, $\alpha(k) = \begin{cases} \frac{1}{\sqrt{2}}, & for\ k = 0, \\ 1\ , & otherwise. \end{cases}$

Many image compression techniques and embedding algorithms make use of this technique. In equations (3) and (4), f (x, y) represents the input signal and C (u, v) represents its two-dimensional DCT.

5. THE PROPOSED METHOD

The proposed method uses symmetric and asymmetric cryptographic encryption algorithms. Symmetric key algorithms are less time-consuming and suitable for the encryption of images. Asymmetric key algorithms are complex & more time-consuming, suitable for key encryption/decryption & exchange. Therefore, the two symmetric key algorithms such as RC6 and OTP are used for the encryption of input secret images at two layers. RC6 is a symmetric-key block cipher that provides more security, high performance, fast, and flexibility. OTP is another symmetric key algorithm where a pad is generated randomly and maintained as confidential between the two communicating entities. These two symmetric key algorithms are used to enhance the security of images. Two separate keys are randomly generated and are used in RC6 and OTP encryption process. Two layers of encryption with two different algorithms with their keys are used. Here, any third party can understand that the data is scrambled by looking into it, but it is difficult to extract the actual data by guessing the encryption/decryption keys. Therefore, the proposed method is resistant to a brute-force attack. Cryptographic algorithms are helpful to scramble the data. But this scrambled data needs to be made undetectable by embedding it in the cover image. Another level of security for the encrypted image is provided by embedding it in the cover image using DC coefficients, which results in a stego image. These DC coefficients are generated from the DCT transformation of the cover image.

RESEARCH ARTICLE

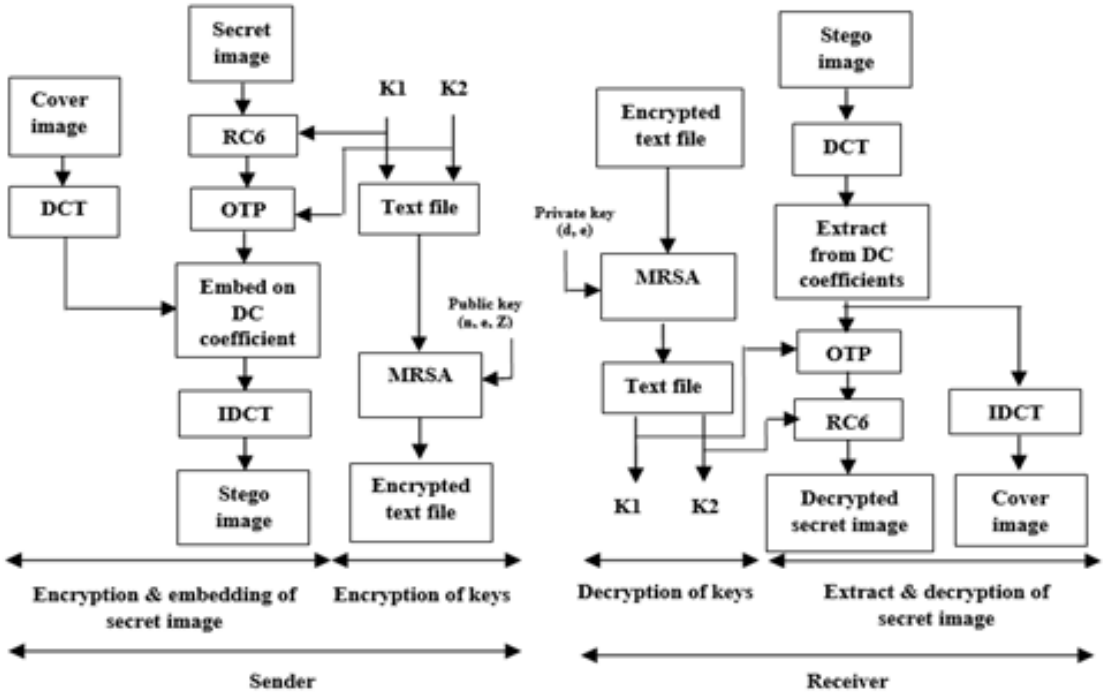

Figure 2 Proposed System Framework at Sender & Receiver

There is a necessity to safely send keys to the recipient. Instead of sending the keys as it is to the recipient, it is always safe and secure to encrypt them and then send them. Therefore, an asymmetric key algorithm such as modified RSA [22] is used to encrypt the text file containing the keys using the public key of the receiver. Now, send the stego image and encrypted keys to the receiver as shown in Figure 2. At the receiver, the extraction process is carried out on the stego image in reverse order. First, extract the embedded image from stego using DCT. Then, decrypt the text file using the private key of the receiver by applying modified RSA. By using these keys, decrypt the extracted scrambled image using OTP & RC6 algorithms.

The proposed method is divided into three parts, encryption & embedding process of an input secret image, extraction & decryption process for an input secret image, and encryption & decryption of keys using MRSA.

5.1. Encryption & Embedding Process of an Input Secret Image

This process involves the encryption of a secret image and hiding it in the cover image as shown in Figure 3. Two-level encryption is carried out using RC6 and OTP. Then DCT is used to produce the stego. The steps involved in encryption & embedding the secret image in the cover are shown in Algorithm 1.

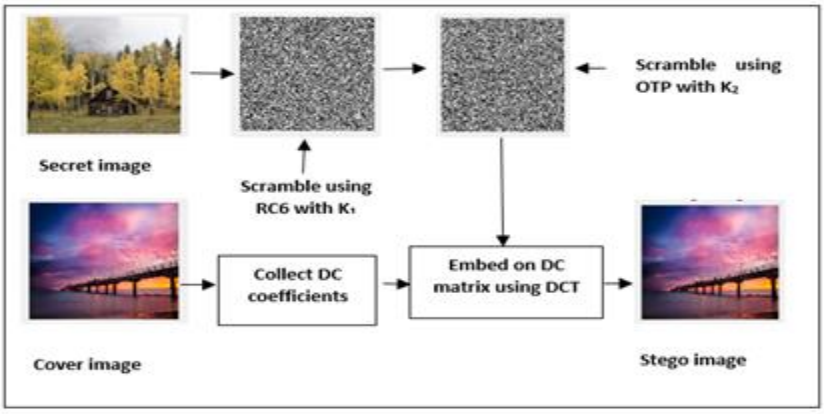

Figure 3 Encrypt and Embed Secret Image

RESEARCH ARTICLE

Input: Cover image '*Icm'*, Secret image *'Iim'*, keys *K1 & K2*

Output: Encrypted text file *'S'*

1 Read cover image *'Icm'*, and divided it as a 16x16 sub-block.

2 Develop DC Coefficients *(Dcm)* out of each sub-block to create a DC matrix.

3 At the same time, read the input secret color image *'Iim'* from the dataset.

4 Encrypt the secret image using RC6 by applying the key *K1*, resulting in *RCout*.

5 Generate random key matrix K2 to the size of RCout and apply to scramble it is using OTP

$$OTPout = RCoutXORK2 \quad (5)$$

6 Embed two-level encrypted image *OTPout* by using DC coefficients of the cover image using

$$Dsm = Dcm + (a * OTPout) \quad (6)$$

where, *Dcm*=DC coefficients of carrier image, *a*=embedding factor, *OTPout*=Encrypted output, *Dsm*=DC array of stego.

7 The modified DC coefficients are replaced in the subblocks. Generate stego image *(Dsm)* by performing inverse DCT (IDCT).

8 Send stego image *(Dsm)* to the receiver.

Algorithm 1 Secret Image Encrypt & Embed

5.2. Extraction & Decryption Process for an Input Secret Image

The extraction process involves the reverse procedure to recover back the secret image as shown in Figure 4. This process involves the extraction of the encrypted image from the stego image, and it is carried out using DCT. Decryption is carried out first by using OTP and then by using RC6. The steps involved in the extraction & decryption of the secret image from the cover are shown in Algorithm 2.

Input: Stego image *'Ism'*, Cover image *'Icm'*

Output: Decrypted Secret image '*RCout'*

1 On receiving the stego image *'Ism'*, divided it as a 16x16 subblock.

2 Collect DC Coefficients *'Dsm'* out of each sub-block to create a DC matrix.

3 Extract secret image from DC matrix using:

$$EXTout = (Dsm - Dcm) / a \quad (7)$$

where, *Dsm* = DC matrix of stego, *a* = embedding factor, *Dcm* = DC matrix of Cover image, *EXTout* = extracted output.

4 Decrypt the *EXTout* by applying key K2 using OTP

$$OTPout = EXToutXORK2 \quad (8)$$

5 Again, descramble using RC6 by applying *K1* to recover the original secret image '*RCout'*.

Algorithm 2 Secret Image Extraction & Decryption

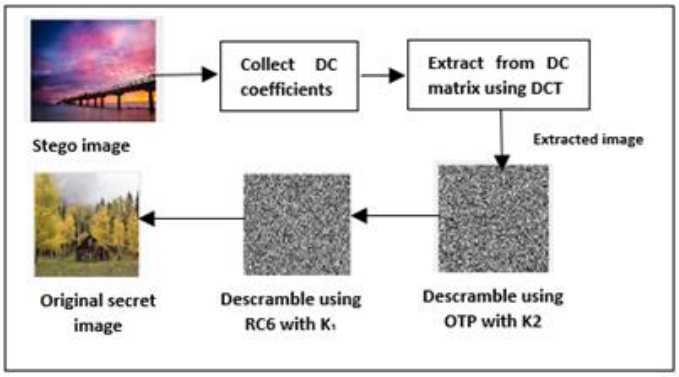

Figure 4 Extract and Decrypt the Secret Image

5.3. Encryption and Decryption of Keys using Modified RSA

RSA is best suited for secure key exchange, scrambling of data & achieving digital signatures. In this paper, a modified RSA [22] is used to encrypt the keys *K1 & K2* and to get a natural number *Z*. The process of modified RSA used for the proposed method is presented in Figure 5. The steps involved in encryption & decryption of keys are shown in Algorithms 3 & 4.

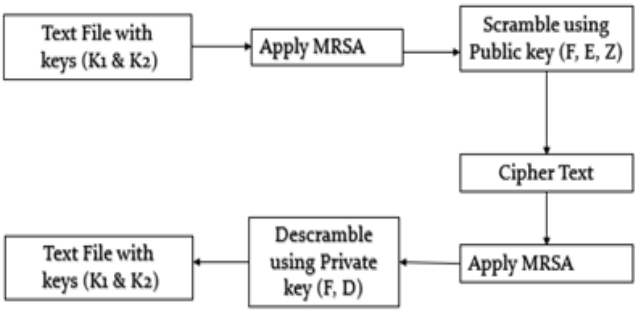

Figure 5 Modified RSA

Input: Prime numbers *P, Q & R*, Text file '*T'*.

Output: Encrypted text file '*S'*.

1 Store the keys *K1 & K2* in a text file *'T'*.

2 Choose three large prime numbers *P, Q & R*.

RESEARCH ARTICLE

3 Generate a natural number '*Z'* by multiplying *R & S*

where *R < (Φ(F) – 1), Φ(F) < S < R and Φ(F) = (P-1) (Q-1) (R-1).*

4 Choose '*E'* such that gcd of *E & Φ(F)* is equal to 1.

5 Compute '*D'* in such a way that *(E*D mod Φ(F)) =1*

6 At the sender, encrypt the text file *'T'* and a natural number '*Z'* using MRSA.

$$S1 = T \wedge E \bmod F \quad (9)$$

$$S2 = Z \wedge E \bmod F \quad (10)$$

$$S = (S1 + S2) = (T \wedge E \bmod F) + (Z \wedge E \bmod F) \quad (11)$$

7 Where *'E'* is the public key exponent, *'F'* is a modulus function.

8 Send the encrypted text file *'S'* to the receiver.

Algorithm 3 Encrypt the Keys using MRSA

Input: Scrambled text file *'S'*

Output: Decrypted text file *'T'*

1 At the receiver, on receiving *'S'*, segment the scrambled text S1 and a natural number S2.

2 Decrypt them separately to get the actual text and a natural number

$$T = S1 \wedge D \bmod F \quad (12)$$

$$Z = S2 \wedge D \bmod F \quad (13)$$

where *'D'* is the private key exponent, and *'F'* is a modulus function.

3 Verify the natural number *'Z'*. If its value remains the same, then encrypted keys are not modified by any intruder.

4 The decrypted text file is *'T'*, containing keys.

Algorithm 4 Decrypt the Keys using MRSA

6. RESULTS AND DISCUSSIONS

The aim is to enhance the confidentiality of secret images by combining double encryption with embedding. Simulation is carried out using MATLAB 9.7 version. This method uses symmetric algorithms like RC6 and OTP for scrambling/descrambling input secret images. Also uses an asymmetric algorithm like MRSA to encrypt the keys which are required for RC6 and OTP. The scrambled secret is hidden in the cover using DCT. The cover image (2048X2048) and the input secret image (128X128) are used. Cover, input secret, RC6 & OTP encrypted, stego, extracted, OTP decrypted & RC6 decrypted images are presented in Figure 6. It is observed that histograms of the cover & stego image and original secret & final extracted image are almost similar as shown in Figure 7. Nobody can identify the presence of a secret image in the cover image. It is very much difficult for an attacker to identify the hidden image and try to extract it. Also, keys used for double encryption are difficult to identify by the attacker. So, this is a more secure system. The proposed method gives double encryption along with key authentication thereby enhancing information security. MRSA is applied for the key which is used in this system. The results for the encryption of a key and a natural number using MRSA are shown in Table 2.

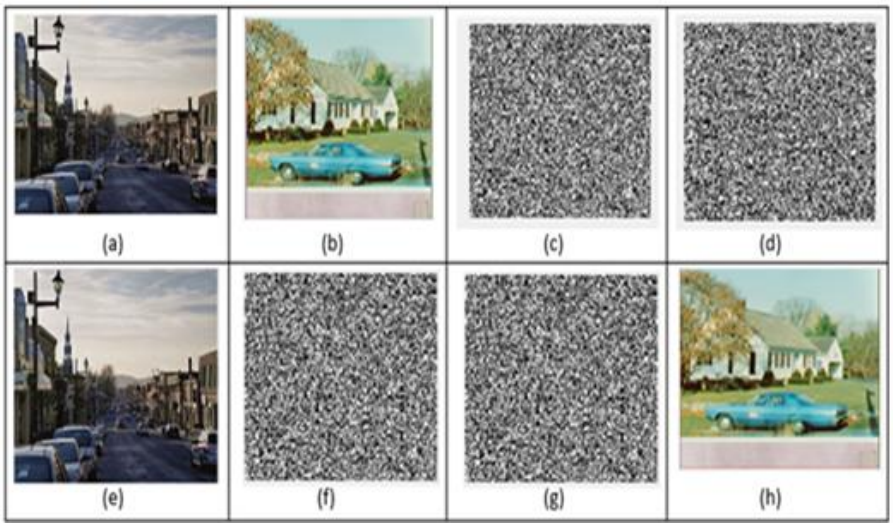

Figure 6. Images of (a). Cover, (b). Secret, (c). RC6 Encrypted Image, (d). OTP Encrypted Image, (e). Stego, (f). Extracted, (g). OTP Decrypted, & (h). Secret Decrypted using RC6

RESEARCH ARTICLE

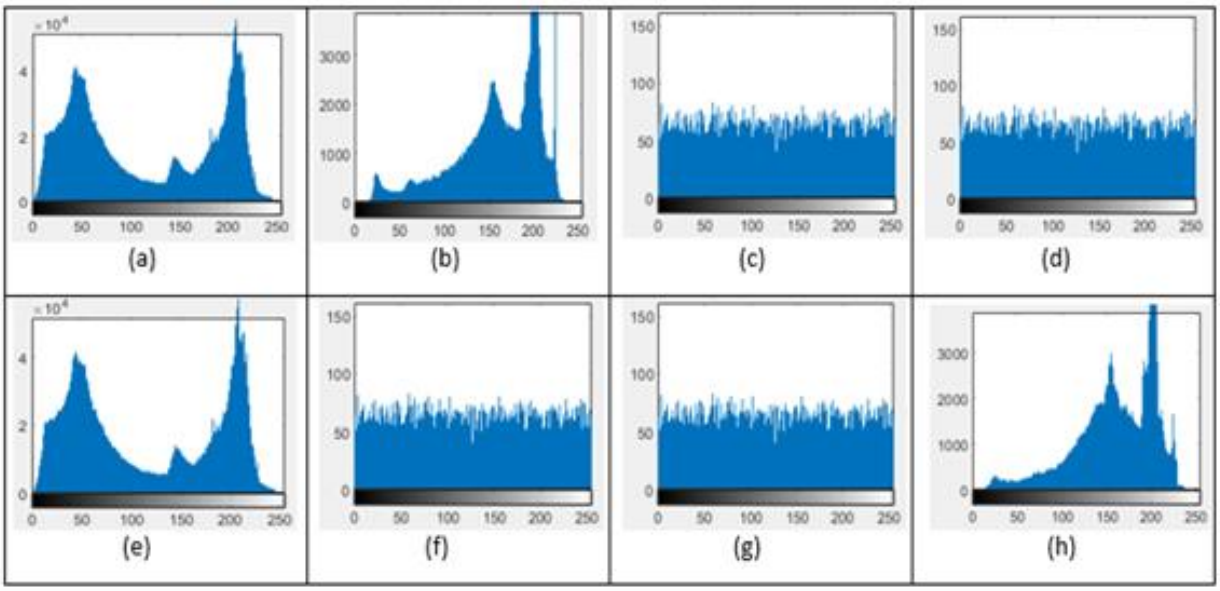

Figure 7 Histograms of (a). Cover, (b). Secret, (c). RC6 Encrypted Image, (d). OTP Encrypted Image, (e). Stego, (f). Extracted, (g). OTP Decrypted, & (g). Secret Decrypted using RC6

Table 2 Outputs from MRSA Algorithm

<table>
<tr><td>(a). Values assigned in MRSA
P=31, Q= 43, R=19, F=25327, Phi= 22680,
E= 11, D= 12371, R= 5, S= 6</td><td>(b). Generated natural number
Z= 30</td></tr>
<tr><td>(c). Text file ‘T’ containing Keys K_1 & K_2 as input to MRSA
192851311 3848191706.00000
4113777100.00000 3284701467.00000
4204514689.00000 3429042687.00000
1697341039.00000 53411267
189 207 150 237
97 227 157 158
253 56 236 34
67 231 96 134</td><td>(d). Encrypted file containing keys
34499 39375 23879 32895
39375 34499 33242 33594
34499 34499 37408 34323
19324 32895 34499 39375
33242 37408 37408 35105
33594 33594 33594 33594
35105 19324 34499 34499
33594 33594 35105 34323</td></tr>
<tr><td>(e). Encrypted natural number
14941</td><td>(f). Decrypted natural number
Z=30</td></tr>
<tr><td>(g). Decrypted text file ‘T’ containing keys K_1 & K_2
Decrypted Message is: 192851311 3848191706.00000
189 207 150 237 224 160 166 89 29 80 57 55 146
226 204 86 179 73 146 173 29 93 108 158 39 211
201 131 128 76 96 116 120 90 23 29 9 193 86</td><td>(h). Time taken
Encryption time: 332.813678 seconds
Decryption time: 239.042921 seconds</td></tr>
</table>

Using MRSA along with key encryption/decryption, the message integrity is also verified to check whether the input is modified or not. Additional natural number ‘Z’ is used to verify at the receiver. If it remains the same as the original, then the input message (keys) is not modified by any intruder i.e., the encrypted keys are not modified in the communication channel.

6.1. Performance Analysis

Various analysis has been conducted to determine the efficacy

RESEARCH ARTICLE

of the method used to place a secret in the cover image.

6.1.1. PSNR & MSE

MSE is a parameter used to find the signal loss among estimated and actual values. Higher MSE gives better image security for the scrambled image and less MSE gives better picture quality in the stego image. MSE can be calculated by the Eq. (18)

$$MSE = \frac{1}{M * N} \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} [\, f(p,q) - g(p,q)]^2 \qquad (14)$$

Where M, N = total rows & columns in picture, $f(p, q)$ = input picture, $g(p, q)$ = output picture

PSNR is for estimating the imperceptibility of the reconstruction of an image. Lower PSNR represents more randomness in the scrambled image and higher PSNR represents higher quality reconstruction from the stego image. The PSNR can be given by the Eq. (19)

$$PSNR_{dB} = 10 \log_{10} \left(\frac{255^2}{\sqrt{MSE}} \right) \qquad (15)$$

Tables 3 and 4 present PSNR & MSE at different stages for the set of input secret images. Input secret images are taken from different datasets. Datasets used here are USC-SIPI (aerials & miscellaneous) [23], Kodak [24] and FAU_orig [25]. It is observed that using OTP after RC6 encryption, PSNR & MSE for the cipher are decreasing & increasing respectively. The cover image is of size 2048X2048. PSNR & MSE are calculated for cipher, stego & decrypted images. Table 5 presents the values of PSNR & MSE for different datasets. For cipher, lesser the PSNR & more MSE gives more scrambling of pixels which represents better the encryption algorithm. For proposed method, PSNR & MSE for cipher are 14.0145 & 2.62e+03, respectively. For stego, more PSNR & less MSE represents the cover image is embedded with minimum distortion. The proposed method achieved a good PSNR & minimal MSE for stego with 64.68(dB) & 0.02. The decrypted image has infinite PSNR and zero MSE. So, the proposed method combining cryptography with steganography gives two-level security for the input image.

Table 3 Values of PSNR at Different Stages for the Set of Input Secret Images

Sl. No.	Input Secret images	PSNR			
		Using RC6	Using OTP	Stego image	Extracted image
1.	Mandril.tiff	15.0227	14.9445	64.6637	Infinite
2.	4.1.05.tiff	15.1889	15.1803	64.6176	Infinite
3.	CT scan.tiff	15.5101	15.4466	64.7448	Infinite
4.	Peppers.tiff	14.5799	14.5314	64.6825	Infinite
5.	House.tiff	15.4065	15.3973	64.6544	Infinite

Table 4 Values of MSE at Different Stages for the Set of Input Secret Images

Sl. No.	Input Secret images	PSNR			
		Using RC6	Using OTP	Stego image	Extracted image
1.	Mandril.tiff	2.0456e+03	2.078e+03	0.0218	0
2.	4.1.05.tiff	1.9687e+03	1.9726e+03	0.0225	0
3.	CT scan.tiff	1.8284e+03	1.8553e+03	0.0218	0
4.	Peppers.tiff	2.2651e+03	2.2906e+03	0.0221	0
5.	House.tiff	1.8725e+03	1.8765e+03	0.0223	0

RESEARCH ARTICLE

Table 5 The Values of PSNR & MSE for Different Datasets

Datasets		Cipher image		Stego image		Decrypted image	
		PSNR (db)	MSE	PSNR (db)	MSE	PSNR (db)	MSE
USC-SIPI	Aerials	14.71	2.21e+03	64.68	0.022	Infinity	0
	Miscellaneous	13.81	2.75e+03	64.68	0.022	Infinity	0
Kodak		13.84	2.70e+03	64.67	0.022	Infinity	0
FAU_orig		13.71	2.81e+03	64.68	0.022	Infinity	0
Average of all datasets used.		14.01	2.62e+03	64.68	0.022	Infinity	0

Table 6 Comparison of PSNR & MSE of Stego Images with Other Existing Methods

Other existing methods	PSNR (dB)	MSE
May H Abood et.al., [12]	63.2499	0.0308
Md. Sagar Hossen et.al., [20]	58.9566	0.3933
Proposed method	64.6810	0.0221

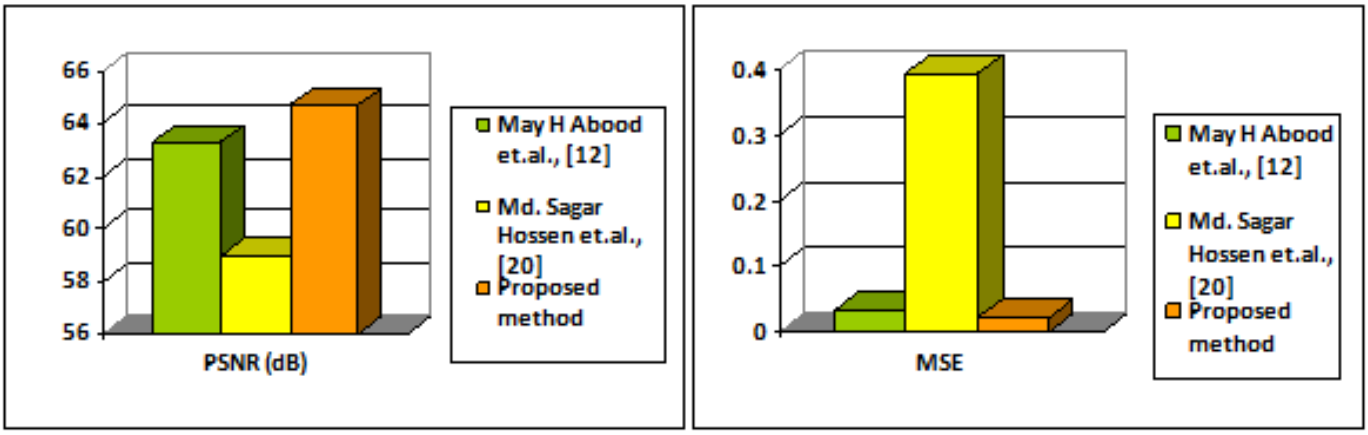

Figure 8 Comparison Plot of PSNR & MSE of the Proposed Method with Other Existing Methods

Table 5 presents the PSNR & MSE values of stego images for the proposed approach with other existing encryption methods and the same is plotted as shown in Figure 8. The proposed approach gives more PSNR (64.6810 dB) and less MSE (0.0221) values compared with other existing methods [12, 20].

6.1.2. Structural Similarity Index (SSIM), Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI)

SSIM is used to indicate the similarity between two images. The range is from 0 to 1. In a scrambled image the SSIM value should be nearer to zero and it should be 1 for the stego image [26]. It can be given by Eq. (20).

$$SSIM = \frac{\left(2\mu_{ci}\mu_{si} + a_1\right)\left(\sigma_{cisi} + a_2\right)}{\left(\mu_{ci}^{\ 2} + \mu_{si}^{\ 2} + a_1\right)\left(\sigma_{ci}^{\ 2} + \sigma_{si}^{\ 2} + a_2\right)} \quad (16)$$

Where a_1 *and* a_2 are constants. *ci* and *si* are input or cover & cipher or stego images. Then, μ & σ is the average & standard deviation. Table 7 presents the values of SSIM for cipher at the outputs of RC6 & OTP, and stego image, achieved by the proposed method. Always SSIM for cipher should be nearer to zero and stego should be approximate to one. So, the proposed method gives good SSIM values as 0.9998 for the stego image.

RESEARCH ARTICLE

NPCR is useful in computing the percent of pixel variation in cipher or stego concerning pixel variation in plain or cover images [26]. NPCR should be nearer to 100 for cipher and should be nearer to zero for stego images. It can be given by the Eq. (17)

$$NPCR = \frac{1}{M_1 * M_2} \sum_{p,q} D(p,q) * 100\% \quad (17)$$

Where, $D(p,q) = \begin{Bmatrix} 1, if & IM_1(p,q) \neq IM_2(p,q) \\ 0, if & IM_1(p,q) = IM_2(p,q) \end{Bmatrix}$,

M_1 *and* M_2 give image size, $IM_1(p,q)$ and $IM_2(p,q)$ is the cipher or stego with pel values before and after image variation.

UACI determines the average intensity variation among two images. The ideal value for UACI is 33 [21]. It can be given by the Eq. (18)

$$UACI = \frac{1}{255 * M_1 * M_2} \sum_{p,q} [IM_1(p,q) - IM_2(p,q)] * 100\% \quad (18)$$

Table 8 presents NPCR for cipher after applying RC6 & OTP, and for decrypted images. It is observed that the NPCR values are above 99% and nearer to 100%. Therefore, the proposed approach is immune to differential attack [26]. Table 9 presents SSIM, NPCR, and UACI for different datasets. On the average, SSIM is 0.9998, NPCR is 99.6145% & UACI is 33.4635. A comparison of the proposed method with the other methods [4, 15] is shown in Table 10 and the same is plotted in Figure 9. Better results are achieved when compared with other methods.

Table 8 Values of NPCR at Different Stages for the Set of Input Secret Images

Sl. No.	Input Secret images	NPCR		
		Using RC6	Using OTP	Decrypted image
1.	Mandril.tiff	99.5178	99.6033	0
2.	4.1.05.tiff	99.4995	99.6216	0
3.	CT scan.tiff	99.4995	99.6948	0
4.	Peppers.tiff	99.4751	99.7009	0
5.	House.tiff	99.5239	99.6277	0

Table 9 The Values of SSIM, NPCR & UACI for Datasets

Datasets		Stego	Cipher	
		SSIM	NPCR (%)	UACI (%)
USC-SIPI	Aerials	0.9998	99.6221	33.4635
	Miscellaneous	0.9998	99.6081	33.4635
Kodak		0.9998	99.6193	33.4635
FAU_orig		0.9998	99.6086	33.4635
Average of all datasets used.		0.9998	99.6145	33.4635

Table 10 Comparison of SSIM, NPCR & UACI with Other Methods

Other methods	SSIM	NPCR (%)	UACI (%)
Catherine Bhel B. Aguila, et.al., [4]	NA	99.6	31.9
Shabir A. Parah et.al., [15]	0.9984	NA	NA
Proposed method	0.9998	99.6145	33.4635

RESEARCH ARTICLE

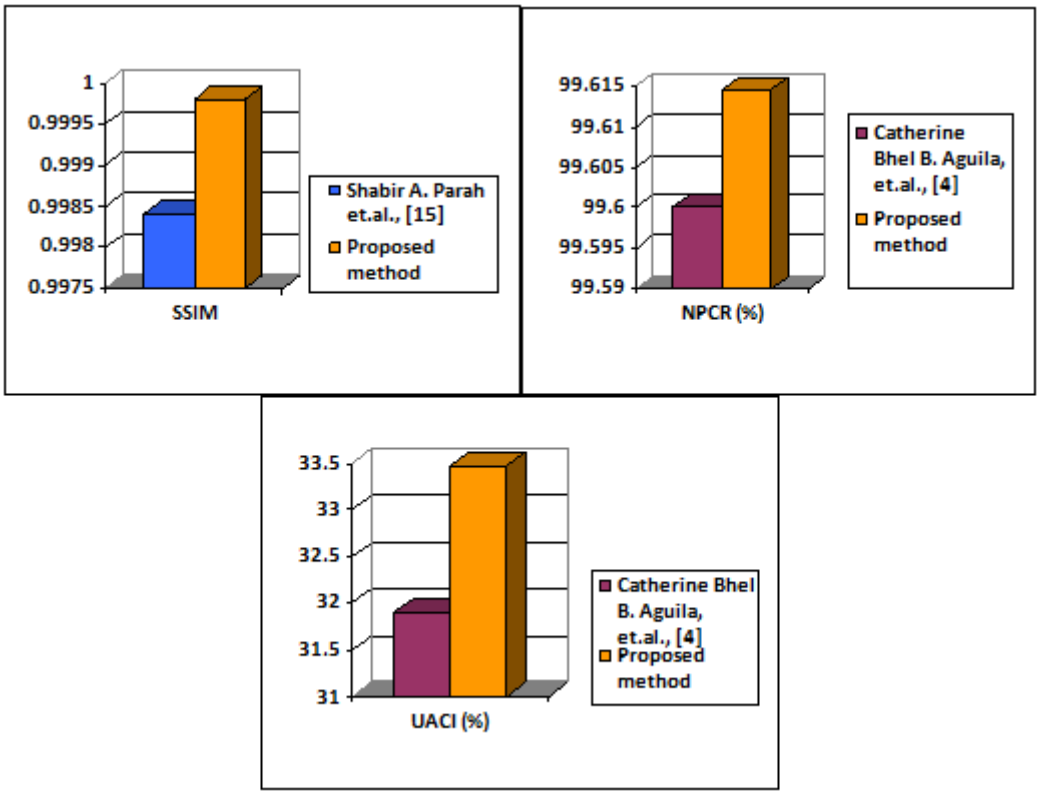

Figure 9 Comparison Plot of SSIM, NPCR (%) & UACI (%) with Other Methods

6.1.3. Information Entropy

Entropy is used as a statistical measure of randomness to determine the texture of an image and it should be 8 for a cipher image [26]. It can be calculated by using the Eq. (19)

$$E = \sum_{i=1}^{X-1} I(Y_i) \log_2 I(Y_i) \qquad (19)$$

where X is the total symbols, and $I(Yi)$ is the probability of the existence of the symbol (Yi).

Tables 11 & 12 present information entropy at different stages for input images and datasets. It is observed that the information entropy of the cipher is approximate 8. So, the proposed approach is successful in randomizing the pixels in cipher images. The embedding method gives good results as it is observed that there is very little difference in the information entropy of the cover & stego image.

Table 11 Information Entropy at Different Stages

Sl. No.	Input Secret images	Secret image	Using RC6	Using OTP	Cover image	Stego image
1.	Mandril.tiff	6.1309	7.9878	7.9902	7.5818	7.5829
2.	4.1.05.tiff	5.1245	7.9885	7.9873	7.5818	7.5826
3.	CT scan.tiff	3.5508	7.9859	7.9898	7.5818	7.5828
4.	Peppers.tiff	6.4288	7.9886	7.9878	7.5818	7.5829
5.	House.tiff	5.4535	7.9897	7.9890	7.5818	7.5830

RESEARCH ARTICLE

Table 12 Information Entropy for Datasets

Datasets		Information entropy			
		Input secret image	Cipher image	Cover image	Stego image
USC-SIPI	Aerials	6.0729	7.9891	7.5818	7.5828
	Miscellaneous	6.5880	7.9886	7.5818	7.5828
Kodak		6.0744	7.9886	7.5818	7.5828
FAU_orig		6.8461	7.9887	7.6573	7.6597
Average of all datasets used.		6.3954	7.9888	7.6007	7.6020

6.1.4. Correlation Coefficient

The correlation coefficient characterizes the interrelation between any two variables [21]. If the value of coefficient outreach to zero, then the image has been ciphered with a better system. The correlation coefficient is computed for horizontal, vertical & diagonal positions of input and cipher images. It can be calculated by Eq. (20)

$$C_{x1,x2} = \frac{1}{\sigma_{x1} * \sigma_{x2}} Cov(x1, x2) \quad (20)$$

Where $C_{x1,\ x2}$ is the correlation coefficient, *Cov* is the covariance of variables *x1 & x2*, σ_{x1} & σ_{x2} are standard deviations of x1 & x2, respectively.

Table 13 presents the correlation coefficient values for different secret images. It shows that ciphering has generated a value closer to zero, thereby effectively reducing the correlation of adjacent picture elements in a cipher. Figure 10 shows the results of the distribution of correlation coefficient for secret, cipher, cover, stego, and extracted secret images, respectively. For cipher, the correlation coefficient value is uniformly distributed when compared to the secret image. But for cover & stego, the distribution remains the same after embedding. For extracted it's the same as the input secret image. Therefore, the proposed method gives more security for the input secret images.

Table 13 Results of the Correlation Coefficient for Different Secret Images after Ciphering

Secret images	Three channels	Horizontal		Vertical		Diagonal	
		Input	cipher	Input	cipher	Input	cipher
Mandril.tiff	Y	0.925	0.027	0.913	-0.021	0.9238	0.026
	Cb	0.865	0.023	0.869	0.031	0.8608	0.013
	Cr	0.908	0.005	0.904	0.002	0.9071	-0.02
4.1.05.tiff	Y	0.971	-0.01	0.965	-0.018	0.9660	-0.02
	Cb	0.981	0.014	0.983	-0.031	0.9843	-0.01
	Cr	0.983	0.010	0.982	-0.005	0.9838	0.023
CT scan.tiff	Y	0.970	-0.019	0.974	0.023	0.9675	0.012
	Cb	0.949	0.001	0.957	0.013	0.9578	-0.02
	Cr	0.963	-0.010	0.965	0.008	0.9594	0.011
Peppers.tiff	Y	0.963	0.001	0.962	0.008	0.9597	0.006
	Cb	0.977	0.004	0.980	0.004	0.9798	0.015
	Cr	0.964	-0.018	0.971	-0.013	0.9687	-0.02
House.tiff	Y	0.953	-0.031	0.952	-0.013	0.9572	-0.01
	Cb	0.935	-0.031	0.931	-0.013	0.9427	-0.01
	Cr	0.969	-0.019	0.972	-0.011	0.9719	-0.01

RESEARCH ARTICLE

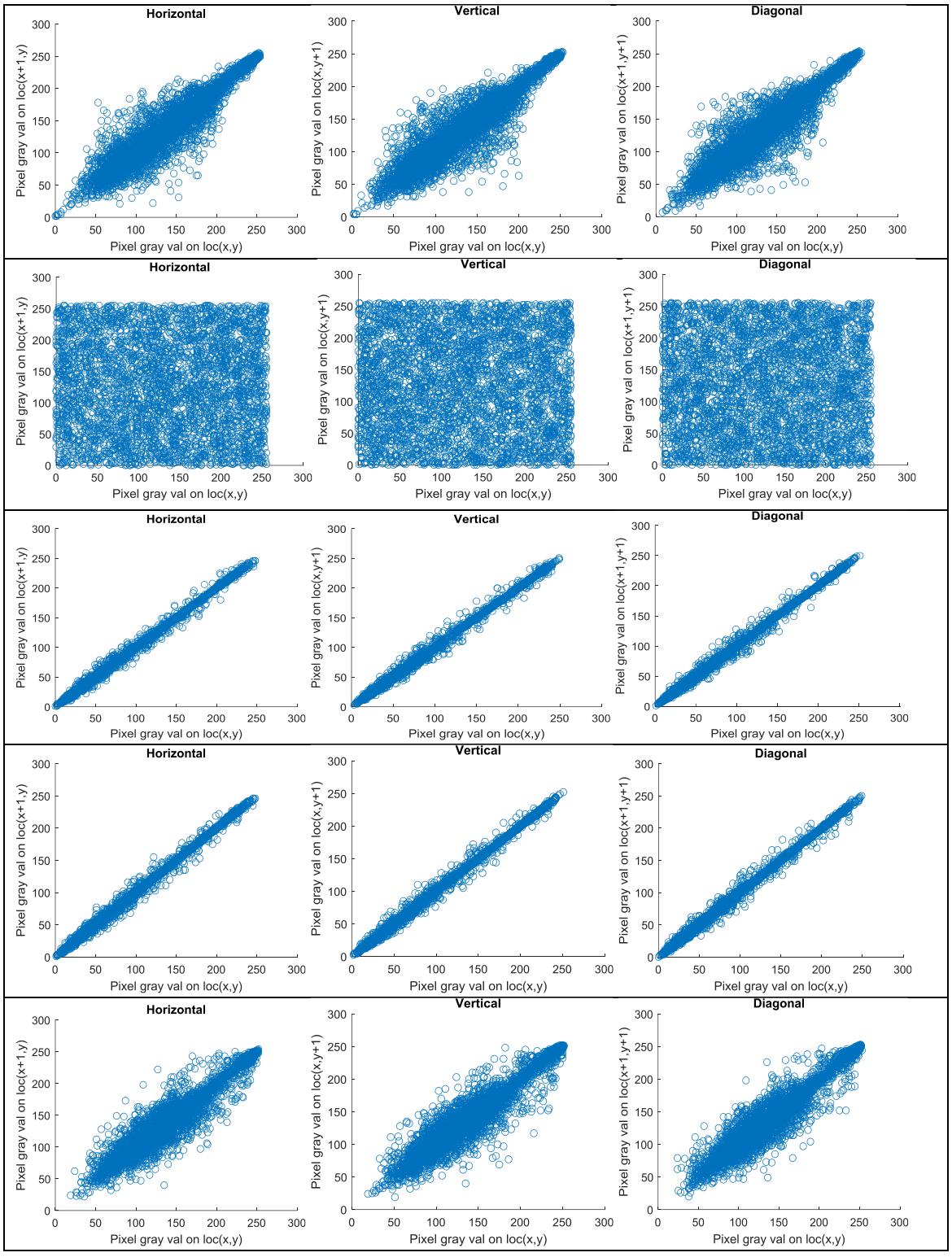

Figure 10 Distribution of Correlation Coefficient Values for the Images of Input Secret, Cipher, Cover, Stego, & Decrypted

RESEARCH ARTICLE

6.1.5. Avalanche Effect

The Avalanche effect is one of the desirable metrics to measure the quality of the encryption algorithm. If the slight change in the input secret image or the keys may cause a completely different cipher image [18]. Higher the avalanche effect, difficult for the attacker to decrypt the cipher image. The encryption algorithm is good if the avalanche effect is greater than 50%. The avalanche effect can be calculated by the Eq. (21)

$$Avalanche\ effect(\%) = \frac{Number\ of\ bits\ flipped\ in\ cipher}{Number\ of\ bits\ in\ cipher} * 100 \quad (21)$$

It indicates how many bits of the cipher are flipped after a change in the input secret image or a key when compared to the actual cipher. Avalanche effect on the cipher when a single bit in the input image, key, and on both input image as well as on key, is presented in Table 11. A comparison plot is shown in Figure 11. It is observed that the avalanche effect for all the cases is above 49% and the average is above 50%. Therefore, the proposed method is resistant to a brute-force attack.

Table 11 Avalanche Effect on the Cipher of the Input Secret Images

Sl. No.	Input Secret images	Change a bit in the input image	Change a bit in the key	Change a bit in the input image & key
1.	Mandril.tiff	50.2067 %	50.0107%	50.2136%
2.	4.1.05.tiff	50.0183%	50.1251%	50.0671%
3.	CT scan.tiff	50.1259%	49.8321%	49.9626%
4.	Peppers.tiff	50.0107%	50.1594%	50.0236%
5.	House.tiff	49.9626%	50.0687%	50.0747%
6.	Average	50.06%	50.04%	50.07%

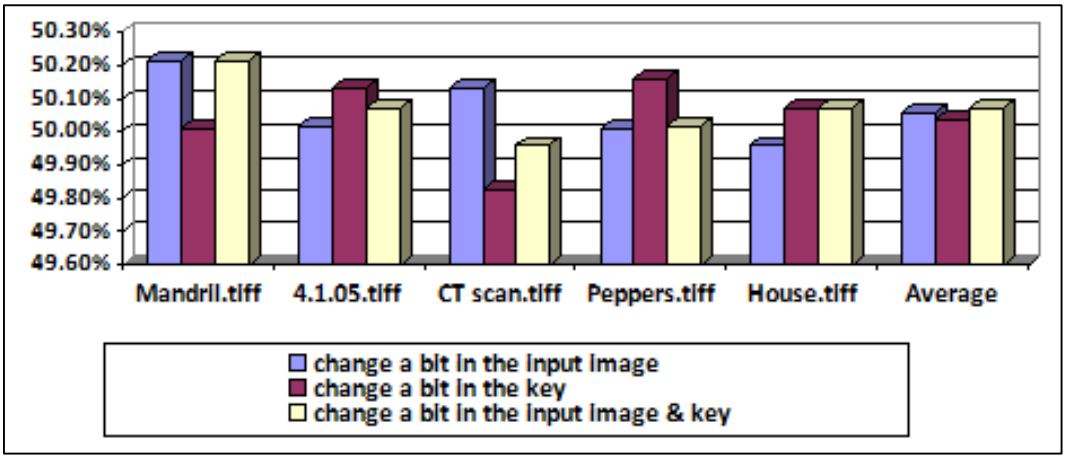

Figure 11 A Plot of Avalanche Effect on the Cipher of the Input Secret Images

7. CONCLUSION AND FUTURE SCOPE

The proposed approach is a combination of symmetric & asymmetric key methods with scrambling & hiding of data. The combination of these algorithms is used to achieve security issues like confidentiality and message integrity. Scrambling of input secret images is carried out by using symmetric algorithms, whereas scrambling of the keys is carried out by MRSA. So, the proposed method provides two-layer security for the secret image as well as for the keys. The security analysis for cipher and stego images is carried out. For cipher image, PSNR=14.01, MSE=2.62e+03, NPCR=99.6145, UACI=33.4635 & Information entropy= 7.9888 are achieved. For stego image, PSNR=64.6810, MSE=0.0221 & SSIM= 0.9998 are achieved. The analysis shows that PSNR and MSE value works perfectly with minimal distortion for image quality. The values of SSIM, NPCR, and UACI are also good. A very less correlation coefficient value shows that the ciphering method has resulted

RESEARCH ARTICLE

in more randomness in the scrambled image, thereby helping to improve message confidentiality and integrity. As the proposed method generates a good avalanche effect of greater than 50%, it can withstand brute force attacks and other cryptographic/steganographic attacks.

REFERENCES

[1] Monu Singh, and Amit Kumar Singh, "A comprehensive survey on encryption techniques for digital images," Multimedia Tools and Applications, pp. 1-33, 2022. DOI:10.1007/s11042-022-12791-6

[2] Omega Sarjiyus, B Y Baha, and E. J. Garba, "Enhanced Security Framework for Internet Banking Services," Journal of Information Technology and Computing, Vol. 2, No. 1, pp. 9-29, 2021. DOI:10.48185/jitc.v2i1.162

[3] A.Nithya, B. Ramakrishnan, Resul Das, "A Novel Approach for Data Privacy Using Attribute Based Scheme Algorithm for Cloud Computing," International Journal of Computer Networks and Applications (IJCNA), Volume 3, Issue 4, 2016. DOI: 10.22247/ijcna/2016/v3/i4/48567

[4] Catherine Bhel B. Aguila, Ariel M. Sison, and Suji P. Medina, "Enhanced RC6 permutation-diffusion operation for image encryption," International Conference on Data Science and Information Technology, pp. 64-68. 2018. DOI:10.1145/3239283.3239308

[5] Denis R, "Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment," International Journal of Computer Networks and Applications (IJCNA), Volume 7, Issue 6, 2020. DOI: 10.22247/ijcna/2020/205321

[6] Mai Helmy, Walid El-Shafai, El-Sayed M. El-Rabaie, Ibrahim M. El-Dokany, and Fathi E. Abd El-Samie, "A hybrid encryption framework based on Rubik's cube for cancelable biometric cyber security applications," Optik 258 (2022): 168773. DOI: 10.1016/j.ijleo.2022.168773

[7] Yani Parti Astuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, and Christy Atika Sari "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), pp. 191-195, 2018. DOI: 10.1109/ICOIACT.2018.8350661

[8] Ali Ahmed and Abdelmotalib Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations," IJCSNS International Journal of Computer Science and Network Security, Vol. 20, No. 5, pp. 139-144, May 2020.

[9] De Rosal Ignatius Moses Setiadi and Eko Hari Rachmawanto, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1 – 11, April 2017. DOI: 10.33633/jais.v2i1.1330

[10] Ajib Susanto, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Ibnu Utomo Wahyu Mulyono, and Christy Atika Sari, "An Improve Image Watermarking using Random Spread Technique and Discrete Cosine Transform," IEEE International Conference on Information and Communications Technology (ICOIACT), pp. 168-173, 2019. DOI: 10.1109/ICOIACT46704.2019.8938498

[11] Rabia Abid, Celestine Iwendi, Abdul Rehman Javed, Muhammad Rizwan, Zunera Jalil, Joseph Henry Anajemba, and Cresantus Biamba, "An optimised homomorphic CRT-RSA algorithm for secure and efficient communication," Personal and Ubiquitous Computing, pp. 1-14, 2021. DOI:10.1007/s00779-021-01607-3

[12] May H Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," IEEE Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 86-90, March 2017. DOI:10.1109/NTICT.2017.7976154

[13] Vivek Kapoor and Rati Gupta, "Hybrid symmetric cryptography approach for secure communication in web application," Journal of Discrete Mathematical Sciences and Cryptography, Vol. 24, No. 5, pp. 1179-1187, 2021. DOI: 10.1080/09720529.2021.1936900

[14] Osama S. Faragallah, Hala S. El-sayed, Ashraf Afifi, and S. F. El-Zoghdy, "Small details gray scale image encryption using RC6 block cipher," Wireless Personal Communications, Vol. 118, No. 2, pp. 1559-1589, 2021. DOI:10.1007/s11277-021-08105-y

[15] Shabir A. Parah, Tabish Digoo, Gazanfar A. Hamdani, Asif A. Shah, Irfan Khan, Obaid Khan, Nazir A. Loan, and Javaid A. Sheikh, "A reversible and secure electronic patient record embedding technique using histogram bin shifting and RC6 encryption," Healthcare Data Analytics and Management, pp. 245-266. Academic Press, 2019. DOI:10.1016/B978-0-12-815368-0.00010-5

[16] Wellia Shinta Sari, Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi, and Christy Atika Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol.15, no.4, pp. 1987-1995, December 2017. DOI: 10.12928/TELKOMNIKA.v15i4.5883

[17] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, M. K. Sarker, "LSB-based bit flipping methods for color image steganography," J. Phys. Conf. Ser., vol. 1501, March 2020. DOI:10.1088/1742-6596/1501/1/012019

[18] Abhishek Majumdar, Arpita Biswas, Atanu Majumder, Sandeep Kumar Sood, Krishna Lal Baishnab, "A novel DNA-inspired encryption strategy for concealing cloud storage," Front. Comput. Sci., 2021, 15(3): 153807. DOI: 10.1007/s11704-019-9015-2

[19] Dwi Yuny Sylfania, Fransiskus Panca Juniawan, Laurentinus, and Harrizki Arie Pradana, "SMS Security Improvement using RSA in Complaints Application on Regional Head Election's Fraud," Jurnal Teknologi dan Sistem Komputer, Vol. 7, No. 3, pp. 116-120, 2019. DOI:10.14710/jtsiskom.7.3.2019.116-120

[20] Md. Sagar Hossen, Md. Ashiqul Islam, Tania Khatun, Shahed Hossain, and Md. Mahfujur Rahman, "A New Approach to Hiding Data in the Images Using Steganography Techniques Based on AES and RC5 Algorithm Cryptosystem," IEEE International Conference on Smart Electronics and Communication (ICOSEC), pp. 676-681, 2020. DOI:10.1109/ICOSEC49089.2020.9215442

[21] Amin Subandi, Maya Silvi Lydia, Rahmat Widia Sembiring, "Analysis of RC6-Lite Implementation for Data Encryption," In Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology (ICEST 2018), pp. 42-47, 2021. DOI: 10.5220/0010037500420047

[22] Ganavi M and Prabhudeva S, "A Secure Data Transmission using Modified RSA and Random Pixel Replacement Steganography," Proceeding of 2018 IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India 2018. DOI: 10.1109/ICCTCT.2018.8550848

[23] USC-SIPI Image Database Website. http://sipi.usc.edu/database

[24] KODAK Image Dataset Website. http://r0k.us/graphics/kodak

[25] Image Manipulation Dataset Website. https://www5.cs.fau.de/research/data/image-manipulation/orig

[26] Said e. el-khamy, Noha o. korany and Amira g. Mohamed, "A New Fuzzy-DNA Image Encryption and Steganography Technique," IEEE Access, vol. 8, pp. 148935-148951, August 11, 2020. DOI: 10.1109/ACCESS.2020.3015687.

Authors

Ganavi M is working as an Assistant Professor in the Department of Computer Science & Engineering (CSE) at Jawaharlal Nehru New College of Engineering (JNNCE), Shivamogga, Karnataka, India. She is pursuing a Ph.D. in Computer Science and Engineering from the Department of CSE, JNNCE, Shivamogga, affiliated with Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India. Her research interests include Cryptography and information security.

RESEARCH ARTICLE

Prof. Prabhudeva S is working as a Professor and Director in the Department of Master of Computer Applications (MCA) at Jawaharlal Nehru New College of Engineering (JNNCE), Shivamogga, Karnataka, India. He received his Ph.D. degree in Reliability Engineering from IIT Bombay, India in 2010. Presently three research scholars are pursuing Ph.D. under his guidance. His research interests include Reliable and Security Modelling. He has published 18 papers in international journals and conferences. He has 17 years of research experience.

Dr. Sankhya N Nayak is working as an Associate Professor in the Department of Computer Science & Engineering (CSE) at Jawaharlal Nehru New College of Engineering (JNNCE), Shivamogga, Karnataka, India. She has received her Ph.D. in Computer Science and Engineering from the Department of CSE, BIET, Davangere, affiliated with Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India. Her research interests include image processing, machine learning, and information security.

How to cite this article:

Ganavi M, Prabhudeva S, Sankhya N Nayak, "A Secure Image Encryption and Embedding Approach using MRSA and RC6 with DCT Transformation", International Journal of Computer Networks and Applications (IJCNA), 9(3), PP: 262-278, 2022, DOI: 10.22247/ijcna/2022/212553.