JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 05 Issue 02
2023

Research Article
https://doi.org/10.56979/502/2023

FuzzyRSA-ChaosCrypt: Secure Text-to-Image Encryption for Communication

Laraib Liaquat[1*], Naeem Aslam[1], Kamran Abid[1], Ahmad Naeem[1], and Muhammad Fuzail[1]

[1]Deparment of Computer Science, NFC-IET, Multan, Pakistan.
[*]Corresponding Author:Laraib Liaquat. Email: laraibliaquat392@gmail.com

Received: June 10, 2023 **Accepted:** August 15, 2023 **Published:** September 17, 2023

Abstract: Digital image encryption is crucial for user privacy while it is being shared over the internet. Methods like steganography and encryption-decryption play a vital role in this objective. Researchers and scholars are paying attention to these methods to keep data safe from hackers. The implementation of of these methods and tools ensures reliability of such algorithms. In this research work, a novel methodology FuzzyRSA-ChaosCrypt is developed by combining various techniques and components for encryption methods to protect communication and secure sensitive digital image data over unsecure computer network. In this method firstly, the most popular asymmetric cryptographic algorithm RSA (Rivest-Shamir-Adleman) and Optimal Asymmetric Encryption Padding (OAEP) for RSA public key encryption are employed. Secondly, it also includes fuzzylogic-based encryption functions and chaotic maps, which increase the encryption complexity and provide flexibility in cryptographic applications. Thirdly, during the encryption process, a specified degree of randomness is introduced by utilization of fuzzy triangular membership function. Fourthly, encryption key comprises the settings of the fuzzy function and the starting values of the chaotic maps. Using this key, the image is encrypted, resulting in a visually encrypted representation. Additionally, asymmetric RSA encryption is applied to securely insert a user-supplied message into the encrypted image. After encrypting the message using a strong RSA key pair, its binary representation is embedded into the least significant bits (LSB) of the encrypted image. This method is resistant to various attacks i.e., Brute-Force attacks, statistical attacks, known plain text attacks, and chosen plain text attacks. Even though provided method is robust and provides high encryption but it is limited to real time applications such as online video streaming.

Keywords: Cryptography, chaotic map, fuzzy triangular membership function, Rivest-Shamir-Adleman (RSA), image encryption.

1. Introduction

A steganography and image encryption method was presented for multimedia communication. A chaotic map and fuzzy function were employed. Dhall et al. [1] introduced a chaos-based system for image encryption. It uses a symmetric key encryption technique but requires many other symmetric methods for encryption of images. Wen et al. [2] introduced image encryption method that is also based of chaos-based system. Quantization and DCT operation are also applied during generation of ciphertext image. Unfortunately, this method lacks flexibility and offers less security. In another study Mfungo et al. [3] applied chaotic maps and fuzzy membership function for secure data transmission. Triangular membership function is applied for generation of secret key that can be predicted, furthermore, this approach requires input with limited size with gray scale conversion.

Today's expanding network users and data transmissions have prompted security experts to develop more secure infrastructure and cryptographic techniques. However, increased processing power has also allowed cryptanalysts to put these novel creations to the test.

An image contains a wealth of information. Human cortical brain area dedicates over a third of its processing power to visually processing this information. Various sectors utilize images as a crucial source of knowledge. These sectors include collecting satellite images, capturing interplanetary motion images through observatories, storing patient medical data, and storing individual fingerprints or iris images, among others [4]. Encryption is one of the safest methods for data transmission, securing the data while it travels through networks. It involves both encryption and decryption to ensure a secure transfer. To achieve this, two different types of keys are used: the secret key and the private key. Private key encryption, which provides more protection than perfect encryption, is considered the more optimal option [5]. As electronic communications continue to rise, data security becomes increasingly critical in traditional systems. Among the various approaches, the secret key stands out as one of the most secure methods for data protection [6]. Another cryptographic technique that can be used is the modular multiplication sequence. However, it should be noted that this method takes a considerable amount of time to perform the encryption and decryption [4] of the modular layer. Various studies have been conducted to provide more robust and high-level data transmission security over computer networks such as Advance Encryption Algorithm (AES), but it is vulnerable to weak value insertion in data [7].

Digital images play a prominent part in a diverse array of applications, including military communication, the medical industry, and remote sensing, facilitated by scientific developments. Usually, these images are sensitive and contain secret information, requiring robust security measures against unauthorized contact [8]. Encryption is one of the profound methods for securing these images; it transforms a plain image into encrypted and unreadable data using encryption algorithms and secret key [6]. When these encryption algorithms are applied, secret image is converted into noisy image (see Figure 1 and Figure 2) which ensures that data in image is hidden. The resulting chaotic appearance of encrypted images acts as a preventive to potential attackers. However, the risk of sensitive information exposure persists when images are taken and layered. Hence, a comprehensive security approach encompassing encryption and complementary measures is essential to ensure the protection of digital images. Through the utilization of comparable keys and the incorporation of confusion and diffusion processes, the conversion of image data results in the alteration of both the positions and values of image pixels [9], [10], [11].

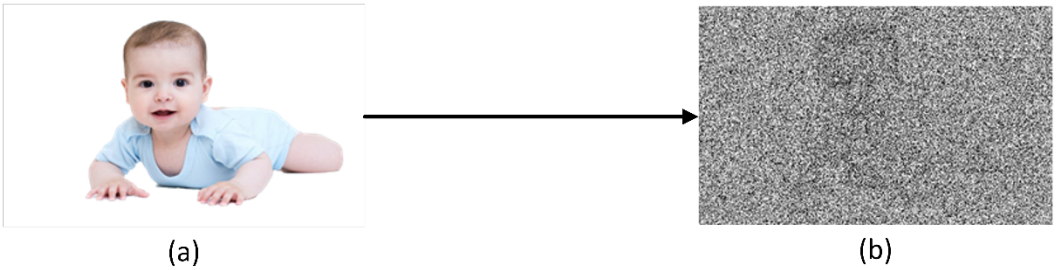


Figure 1. Conversion of original secret image into encrypted noisy image, (a) represents input original image and (b) represents encrypted noisy image as result of encryption method that hides all information in the image.

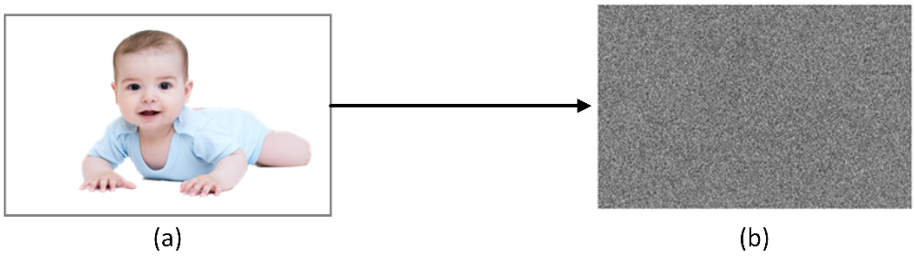


Figure 2. Conversion of original secret image into encrypted image with texture noise, (a) represents input original image and (b) represents encrypted image having texture-based noise as result of encryption method that hides all information in the image.

The core of the key expansion algorithm revolves around a chaotic system, wherein two types of secret keys are integrated. The first type, known as the external key, is represented as a byte and undergoes preprocessing through bit operations and numerical system conversion to derive the original state ciphers of

the chaotic system. Subsequently, these derived values are incorporated into the chaotic system, initiating the generation of an iterative sequence of chaotic states. These states then undergo rounding operations [12], [13], [14], resulting in the creation of corresponding keys. In contrast, the direct key is utilized in alternative approach. This key comprises all the initial parameters of the chaotic system. Consequently, utilizing it facilitates the expeditious generation of identical keys by the chaotic system [15], [16], [17].

In the domain of image processing, confusion and diffusion stand as two fundamental techniques employed for enhancing security and confidentiality. Among the regularly utilized confusion algorithms are chaotic maps [18], matrix transformation based on cat map [19], Arnold's cat map , sorting scrambling [20], Advanced Encryption Standard (AES) [21], random walk algorithm [22], bit-level-based permutation [23], substitution-permutation networks (SPN) [24], and other methodologies. Confusion entails the displacement of picture pixel locations while retaining their original values, introducing an additional layer of complexity to the encrypted image.

Furthermore, a variety of well-established diffusion algorithms contribute significantly to the overall image processing security. These include linear transformation-based algorithm [25], error diffusion [26], sequential XOR [27], discrete cosine transform (DCT) diffusion [28] or modular operation [29], cyclic shift [30], filter-based algorithm [31], permutation-based diffusion [32], bit-layer-based algorithm [33], pixel scrambling [34], and chaos diffusion [35] among others. These diffusion techniques play a vital role in spreading the influence of each pixel throughout the image, thereby ensuring the confidentiality and integrity of sensitive image data.

Cryptographic systems are developed based on chaotic system, having two main parts image data transformation and key expansion [36]. Cryptanalysis has made progress after development of encryption algorithms. Various cryptosystems have been found insecure.

2. Related Work

Many researchers have presented encryption and decryption algorithms for security of digital image while transmitting it over computer network, these algorithms are based on chaotic maps [37], [38]. These chaotic maps are resilient against differential attacks and provide secure communication. Chaos system was described in [2] that utilized Discrete Cosine Transform (DCT) frequency domain compression for image encryption. Hash value was used to generate encryption key for plain image which is then utilized to generate pseudo-random sequence. DCT was applied to transform image from time domain to frequency domain, and quantization was applied to generate coefficient matrix. RSA algorithm and Arnold map-based methodology was proposed in study [39] to encrypt an image; secondly, XOR diffusion and rows-columns based cyclic confusion are applied twice to hide pixel values and generate cipher image. The author in another study [40], also applied RSA and chaos-based encryption-based system to encrypt color images; additionally, each pixel value is diffused by means of Hartley domains.

The author [41] applied hyper-chaotic map and RSA algorithm to develop image encryption system, secret is utilized to increase security level, Arnold map is applied to transform it into cipher text, then this cipher text and image are merged to generate carrier image which provides visual security. Chaotic map, Arnold map, RSA algorithm, and DNA encoding is applied to develop multiple-image encryption system. The proposed system [42] is resistant against differential and statistical attack. RSA and 3D chaotic map-based image encryption framework was proposed [43], resistant to various attacks such as brute-force-attack, known and chosen plain text attacks, replay, side channel, and many other attacks. 3D map improves chaotic behavior, key stream for improved security of plain digital images, innovative process model for uniform chaotic sequences, random matrix with XOR operation during encryption process, and permutation of rows and columns in forward and backward direction with XOR diffusion module.

A novel image encryption system [44] was developed by using RSA algorithm with OAEP and SHA-1 hash algorithm. The proposed system is resistant to various attacks namely: data tempering, unauthorized access, MIM attacks, and collision attacks. But this was limited to image encryption, other digital media such as audio and video can not be encrypted using this framework.

In the study [45], author employed various color modes instead of using only RGB, for encryption and decryption of Arabic and English text to image, and relatively achieved higher capacity. A novel method was proposed [46] to encode color image using structure of DNA strand, consisting of encryption

and decryption phases, many operations were performed including XOR operation and binary encoding. The performance was evaluated in terms of time, MSE, and PSNR for encryption and decryption processes.

A novel security level was proposed for securing data in study [47], it was based on Diffie Hellman technique for text-to-image encryption algorithms. In another study [48], a text-based image encryption and decryption method was proposed using RSA algorithm, square root of encryption keys, XOR operation, PSNR, BER, and MSE techniques.

The study by Alsafyani et al. [49] utilized chaotic maps and adversarial neural networks for encryption and decryption of digital face images. Deep learning was employed to optimize the image, Region of interest network is applied for the extraction of items in the image, and achieved high performance in terms of PSNR 92% and encryption time 88%. The author in [1] also utilized chaos map using probabilistic encryption. It includes diffusion of random bits and XOR operation. Author claimed persistence of this method against crypt analytical and statistical attacks.

The author in study [38], also utilized chaotic system for encryption of image based on fuzzy neural network using various time delays and employs a controller for data samples for secure communication. It was investigated that these networks are better for image processing. Internet of Things (IoT) and encryption algorithms were combined in study [50], for secure communication and authentication of users. Applied techniques are fingerprint from biometric process, CNN are used for authentication of these prints, fuzzy logic for encoding, and Huffman for data compression.

The study [51] presents an advanced and rapid encryption algorithm and color image scrambling that harness diverse chaotic map types alongside an S-box derived from hyperchaotic map principles. This approach involves dual scrambling stages, binary conversions, and key matrix generation utilizing XOR operations. Notably, the algorithm exhibits exceptional efficiency in minimizing computational overhead while effectively countering a wide array of cryptographic attacks. The author in study [52] proposed image encryption algorithm using integration of digital signal and secret image for encryption, Least Significant Bit (LSB) for embedding signature into image, and Lifting Wavelet Transform (LWT) to create encrypted image.

A novel method was proposed in [53] by utilizing public key elliptic curve and compression sensing for image encryption. Discrete wavelet transformation (DWT) and their coefficients, compression of quantization matrix, and elliptic curve to encrypt this matrix. The researchers designed an image encryption algorithm based on Secure Hash Algorithm-256 (SHA-256) and Composite Logistic Sine Map (CLSM) [54]. The approach employs the CLSM-generated pseudo random number sequence (PRNS) to initially scramble the pixels of the original plain picture. Subsequently, the pixel values are distributed using values generated by SHA-256. The algorithm's key is formed by combining the CLSM's initial conditions, parameters, and a user-selected nonce. During the diffusion phase, the SHA-256 initializes and creates hash values using the provided nonce.

In study [55], the author transmitted and encrypted visual data utilizing the Rubik's cube encryption concept. The process involved using the XOR operator, derived from the well-known cube's method, to scramble the original picture. Further encryption was applied to the image's rows and columns using two secret keys. As a result of this technique, statistical and differential assaults are rendered ineffective against the encryption. Steganography is technique used to hide secret information using one of three methods: Least Significant Bit (LSB), Discrete cosine transform, and Discrete Wavelet transform. Summary of related work is presented in Table 1.

Table 1. Summary of related work representing techniques used for image encryption-decryption, their limitations, issues and challenges.

Ref.	Year	Technique	Limitation	Advantages
[2]	2022	High quality image restoration, DCT	Requires more computational resources.	Provide secure communication for big data.

[45]	2022	A Text-to-Image Encryption-Decryption algorithm.	Requires more processing time.	Provides four times security than RGB image encryption methods.
[46]	2022	Advanced Encryption Standard (AES) cryptography and DNA steganography.	Decrypted images are completely not similar to the original images.	More work is required for encrypted image.
[47]	2019	Diffie Hellman and Text-to- Image encryption algorithm.	Testing data consists of large-scale collection and secret key size is higher than 624 which is relatively large value.	Greater key size is required to secure communication.
[48]	2022	The Rivest Shamir Adleman 3 key (RSA3k) algorithm is used.	Security needs to be improved by means of another algorithm integration.	It is capable for securing digital images as well as text data.
[50]	2022	Fuzzy logic, IoT, and Biometric system.	Vulnerable to various attacks such as MIM, identity theft, etc.	High security due to biometric based encryption system.
[49]	2023	Convolution Neural Network (CNN) algorithm is used, encryption is based on face patterns.	This technique is less reliable due to absence of asymmetric encryption method.	A novel encryption technique is presented based on deep learning and cryptography.
[52]	2023	Encryption algorithm for image.	More work is required in digital signature.	A carrier visually conceals the presence of both the secret image and the digital signature.
[51]	2022	A fast color image scrambling and encryption algorithm is used.	Lack of real-world applicability and comparison with existing techniques.	Low computational cost and resistant to cryptographic attacks.

[53]	2021	Double image encryption algorithm is used, 3D chaotic map is designed for improved security, and discrete wavelet transformation.	This research lacks comprehensive security analysis.	The security is enhanced as attackers are unable to directly perceive the existing secrets from a meaningful carrier image.
[1]	2018	Chaos-based probabilistic symmetric encryption scheme is used.	Require more techniques in symmetric encryption scheme.	Intended to design more schemes for different forms of media exploiting the scope of probabilistic approach in symmetric-key encryption. Less computational power is required.
[54]	2021	Encryption algorithm is used. SHA-256 and logistic map-based encryption system.	Encryption time is large. More work is required.	Due to implementation of SHA-256 algorithm, it is difficult to access original data for intruders.
[55]	2022	Rubik's cube encryption algorithm-based technique, sensor-based network	It lacks mathematical proof of security due to Rubik's cube algorithm.	More profound, creative. and effective levels of protection.

3. Proposed Methodology

In this research work, a novel cryptographic technique FuzzyRSA-ChaosCrypt is developed for encryption and decryption of digital image data while being communicated over unsecured computing devices. Various cryptographic techniques and algorithms are integrated including most popular OAEP, RSA, chaotic map, and fuzzy function to generate stego image. In the following encryption and decryption is explained.

3.1. Image preprocessing

Two preprocessing steps are applied to image before encryption namely: conversion into gray scale and resizing. Before encrypting an image, resizing it offers numerous advantages in terms of both performance and security. The reduced dimensions of an image significantly accelerated encryption and decryption tasks by reducing the volume of data that requires processing during the encryption phase. Moreover, resizing introduces a controlled degree of noise to the image, rendering it more challenging for potential attackers to identify hidden information or patterns. This process contributes to enhancing the overall security of the encryption by mitigating the potential impact of noise on the encrypted data. During the process of gray scale conversion of color image, each pixel value of original image is transformed into shades of gray. The color image consists of three channel colors RED, GREEN, BLUE (RGB). $f(i)$ is the function that converts input image i into gray scale using following equation:

$$f(i) = (0.2989 \text{ x } R) + (0.5870 \text{ x } G) + (0.1140 \text{ x } B) \quad (1)$$

Here R, G, and B have actual pixel values of color image in range [0-255],

By applying this equation to each pixel in the image, the grayscale value is obtained, representing the pixel's brightness. The resulting grayscale image consists of a single channel (intensity) and lacks color, displaying a variety of grayscale tones. This grayscale representation significantly reduces computational complexity compared to working with full-color images. Results of this function is shown in figure 3.

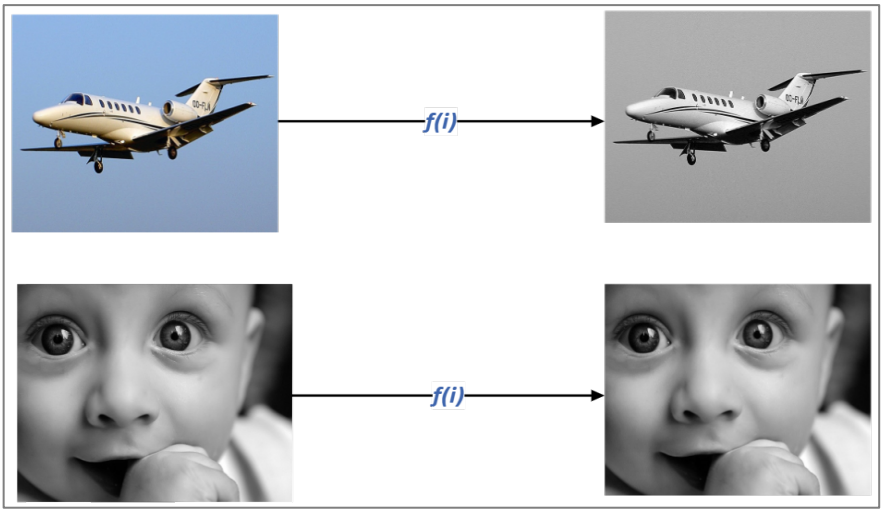


Figure 3. Conversion of plain image into gray scale.

Image resizing entails a mathematical procedure that alters the dimensions of the image while maintaining its original aspect ratio. Suppose the initial image has a width of "O_w" pixels and a height of "O_h" pixels. Then resized image has new height R_H and width of R_W.

If "H" is the new height, R_{aspect} is ratio of aspects, then width ("W") is calculated by following:

$$W = R_{aspect} \text{ x } H \quad (2)$$

$$R_{aspect} = \frac{W}{H} \quad (3)$$

If new width is W, then height is calculated by following:

$$H = \left(\frac{1}{R_{aspect}}\right) \text{x } W \quad (4)$$

Resizing an image results in a transformed version, that retains the same visual content but differs in size. This resized image is then used as the input for encryption, bringing advantages such as improved computational efficiency, potential enhancement of security, and the introduction of additional noise. The results of resizing the image are shown in figure 4.

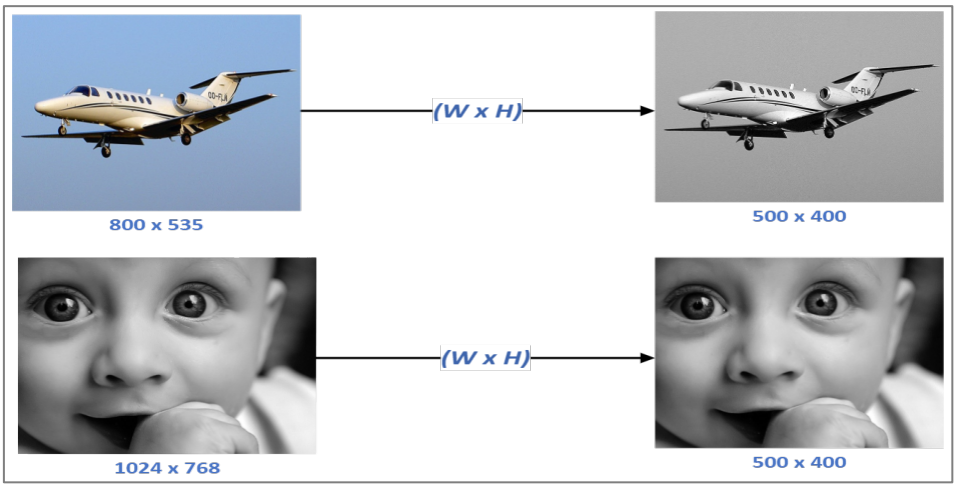


Figure 4. Results of resized images

3.2. Image Encryption

Following are steps that are followed to encrypt given plain image into stego image:

Step 1: Conversion of image into grayscale.

Step 2: Resize image into 512x512 (height, width).

Step 3: Generating RSA key pair (public key, private key).

Step 4: Encryption of secret message (key) into encrypted message using RSA key and OAEP padding algorithms.

Step 5: Conversion of encrypted message into binary format.

Step 6: Defining chaotic map functions and fuzzy logic (fuzzy membership function).

Step 7: Encryption of grayscale image into stego image using chaotic maps and fuzzy function.

Step 8: Storing encrypted image.

Step 9: Embedding encrypted message bits into image using least significant bit of pixel values.

A block diagram is presented in figure 5, to demonstrate working principle of encryption.

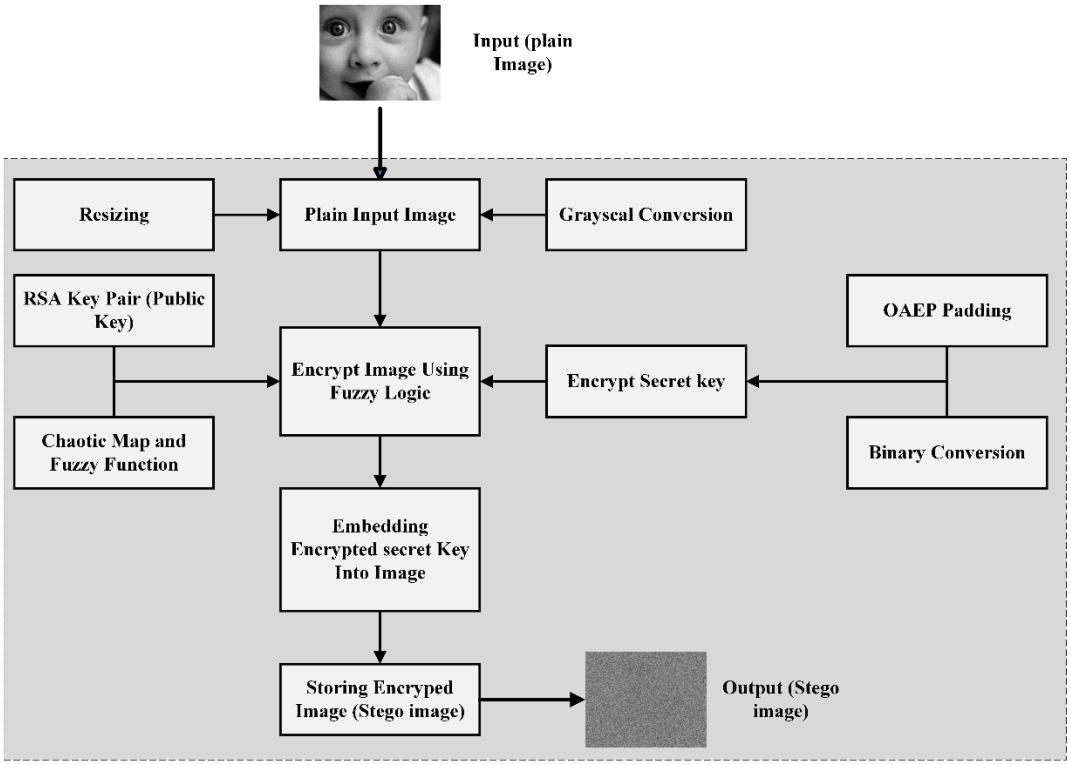


Figure 5. Proposed FuzzyRSA-ChaosCrypt based encryption of plain image into stego image.

In the following, these techniques are explained:

3.2.1. Rivest-Shamir-Adleman (RSA)

Public key cryptography effectively resolves key distribution, key management, and other security concerns while providing a new theoretical and technological foundation for advancing cryptography. The field of information security now considers it the fundamental technology. The RSA algorithm [3], which is a part of the public key cryptosystem, demonstrates strong performance. For the implementation of RSA, public and private keys are generated as follows:

Step 1: Defining a and b, where both these are random, secret, and prime numbers.

Step 2: Computation of these numbers:

$$n = a * b \tag{5}$$

$$\varphi(o) = (a - 1)(b - 1) \tag{6}$$

Here $\varphi(o)$ is Euler function that is applied on o.

Step 3: Public key k is selected randomly, that satisfies following:

$$1 < k < \varphi(o) \tag{7}$$

$$gcd(k, \varphi(o)) \tag{8}$$

Where k and $\varphi(o)$ are prime numbers.

Step 4: private key l is calculated by following:

$$l = k * l \; mod \; (\varphi(o)) = 1 \quad (9)$$

In this RSA cryptographic system, two types of keys are applied:

$$\text{private key} = (l, o) \text{ and} \quad (10)$$

$$\text{public key} = (k, o) \quad (11)$$

To communicate and receive image data, the sender encrypts it first using a public key, and the recipient decrypts the cipher data using their private key. The attackers only know the public key and must break the huge integer "o" into two smaller components, "a" and "b," to decipher the encrypted message. However, factorizing large integers requires a substantial assessment in time and resources.

3.2.2. Chaotic Map

There are two kinds of chaotic maps used: one-dimensional maps and multi-dimensional maps. One-dimensional chaotic maps have a faster processing speed and are less complex, distinguishing them from multi-dimensional chaotic maps, which have computational overhead due to their complex structure. However, one disadvantage of 1D maps is their limited range of starting variables and inputs, whereas multi-dimensional maps can be expanded and offer a greater range. These maps are defined in the following:

$$C_l = (x, r) \quad (12)$$

C_l is logistic chaotic map which takes two arguments x, r representing input and control parameter respectively. r is used to generate chaotic sequence. It is single dimensional map.

$$C_t = (x, a, b) \quad (13)$$

C_t is tent chaotic map which takes three arguments x, a, b representing (x) as input and (a, b) are two control parameters. (a, b) are used to generate chaotic sequence. It is single dimensional map.

$$C_{ls} = (x, r, alpha) \quad (14)$$

C_{ls} is logistic sin map, that is also single dimensional map. Only x is used an input and $(r, alpha)$ are two control parameters to generate chaotic sequences.

$$C_h = (x, y, z, a, b, c, d, e, f, alpha) \quad (15)$$

C_h is hybrid multidimensional chaotic map, it is previous one-dimensional maps as follows:

$$C_h = C_l + C_t + C_{ls} \quad (16)$$

x, y, z are three input variables, and remaining $a, b, c, d, e, f, alpha$ are control parameters used to generate chaotic sequence.

The core of a chaos-based image cryptosystem is the diffusion-confusion stage, which dominates the system's design [56]. During the confusion stage, pixel permutation takes place, causing the image's pixel positions to be shuffled randomly while their original values remain intact. This results in the image losing its distinct structure. As a result, the secret key is constructed from a combination of control parameters and initial conditions. However, relying solely on the permutation step for security isn't particularly robust, as it could be compromised by potential attacks. The subsequent step in the encryption process focuses on altering the pixel values throughout the entire image to enhance overall security [57]. In the diffusion step, the sequence generated by the chaotic systems sequentially alters the pixel values. To achieve a satisfactory level of security, it's necessary to repeat the complete confusion-diffusion cycle multiple times. Chaotic maps are well-suited for image encryption owing to their inherent unpredictability [58].

3.2.3. Fuzzy Membership Function

Fuzzy numbers describe uncertainties and ambiguity in data and finds application in the field of image processing for encryption. Unlike standard numbers, fuzzy numbers represent a range of potential values rather than precise values. The function of membership assigns each element in the discourse universe a membership level between 0 and 1, where 0 denotes no membership and 1 denotes complete membership. In the context of encryption, fuzzy numbers are utilized to handle imprecise pixel values and other uncertainties in image data. If "x" is pixel value of input image being encrypted, $, a, b$ are controlling parameters, then triangular fuzzy membership function M_{fuzzy} is calculated as follows:

$$M_{fuzzy}(x) = 0 \quad \text{if } x < a \quad (17)$$

$$M_{fuzzy}(x) = 0 \quad \text{if } x > b \tag{18}$$

$$M_{fuzzy}(x) = 2 * \left(\frac{(x-a)}{(b-a)}\right) \quad \text{if } a \leq x \leq \frac{(a+b)}{2} \tag{19}$$

$$M_{fuzzy}(x) = 2 * \left(\frac{(b-x)}{(b-a)}\right) \quad \text{if } \frac{(a+b)}{2} \leq x \leq b \tag{20}$$

(a, b) are lower and upper bounds of fuzzy membership function respectively. The fuzzy triangular membership function M_{fuzzy} is utilized in the image encryption process to calculate the membership values (fuzzy values) for (x) pixel values. x is then used in the encryption and decryption functions to modify the pixel values based on the chaotic maps and fuzzy logic. Fuzzy logic originates from the concept of Fuzzy Set [59], where parameters can possess truth values between 0 and 1. It extends beyond Boolean algebra to accommodate partial truth. This allows it to model non-linear functions with precision within a restricted set. The input involves a vector representing picture A, evaluated using performance metrics (characteristics). The initial algorithm step is fuzzyfication, which transforms the value of each image characteristic into fuzzy sets based on their specific membership functions [59].

3.2.4. Optimal Asymmetric Encryption Padding (OAEP)

In this research work, OAEP is utilized for encryption and decryption of message using RSA algorithm. OAEP is used as cryptographic padding outline to add randomness in x and improve security level of RSA. This method upsurges the length of message before encryption. It is not used directly in RSA for image encryption, rather used to encrypt message before it is embedded into message through steganography using LSB technique [60], a plain text data is transformed into Permutation of a one-way trapdoor. Following two hash functions are utilized in this process:

$$G: [0,1]^{K_0} \rightarrow [0,1]^{K+N} \tag{21}$$

$$H: [0,1]^{K+N} \rightarrow [0,1]^{K_1} \tag{22}$$

K_1 and K_0 represent security measures.

To facilitate message recognition, a sequence of zeros is introduced as redundant information. "|" signifies a concatenation of two strings.

$$s = G(r) \oplus (m \mid 0^{K_1}) \tag{23}$$

$$t = H(s) \oplus r \tag{24}$$

$$OAEP(m, r) = s \mid t \tag{25}$$

$$s \mid t =$$

$$(m \mid 0^{K_1}) \oplus G(r) \mid r \oplus H((m \mid 0^{K_1}) \oplus G(r))$$

Random numbers are added to image data before encryption, this is termed as padding.

This step increases noise and makes it challenging to understand patterns if attacker tries to access data in unauthorized way.

This padded image is then integrated with cryptographic hash function, which transforms it into value with fixed length called hash.

This hash value is then merged with random bits, previously added to create noise in image data.

This transformed padded data is then encrypted using RSA algorithm.

This method provides resistance to encrypted image against plain-text attacks.

It becomes challenging for attackers to deduce information by exploiting regularity in encrypted image, and get information about original image data.

The encryption system of entire FuzzyRSA-ChaosCrypt is enhanced, and it is robust against various known attacks.

3.3 Image Decryption

Image decryption process is presented as block diagram in figure 6, and following steps are followed for this purpose:

Step 1: Conversion of binary secret key into string, decryption using standard OAEP, and obtain original secret key (message).

Step 2: Decryption of stego image with chaotic map final values and private key of fuzzy function using original secret key.
Step 3: Displaying secret message and plain image.
The receiver has padded encrypted image data, RSA encryption process is reversed during decryption, and modified padded data is retrieved. Hash value and random values are extracted from it. Cryptographic based hash function is applied to generate new hash value. If this value matched with extracted hash value of encryption, the decryption process is successful. The padding process is reversed, random bits are extracted, and original padded image data is accessed.

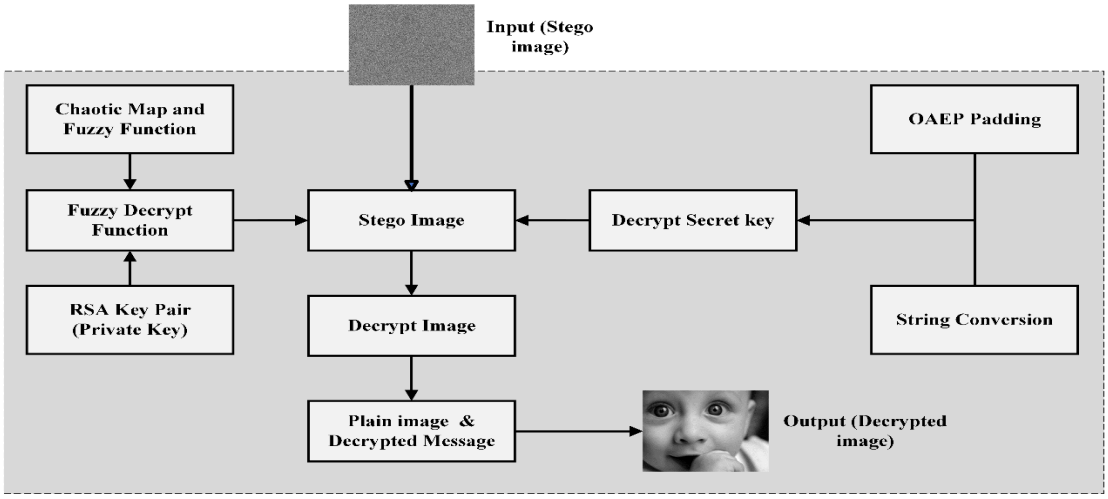
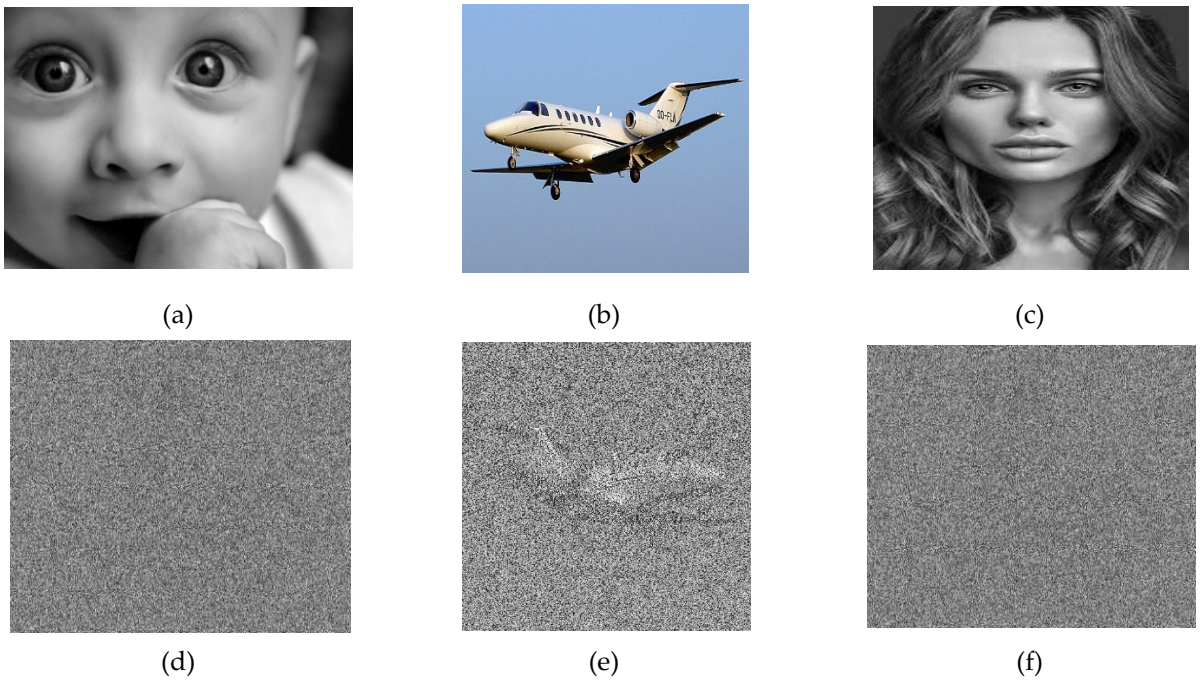


Figure 6. Proposed FuzzyRSA-ChaosCrypt based decryption of stego image into plain image.

4. Experimental Results

To evaluate the reliability and feasibility of proposed FuzzyRSA-ChaosCrypt image encryption-decryption technique, three random images were selected, "Baby", "Girl", and "Jet". These images are RGB and grayscale in pixel attributes. The simulation is conducted on Google Collaboratory (or Colab), 64-bit server, RAM 13-GB, and Intel Xeon CPU. Figure 7 depicts experiment results, it can be seen that no stego image gives any information, however, it's confusing.



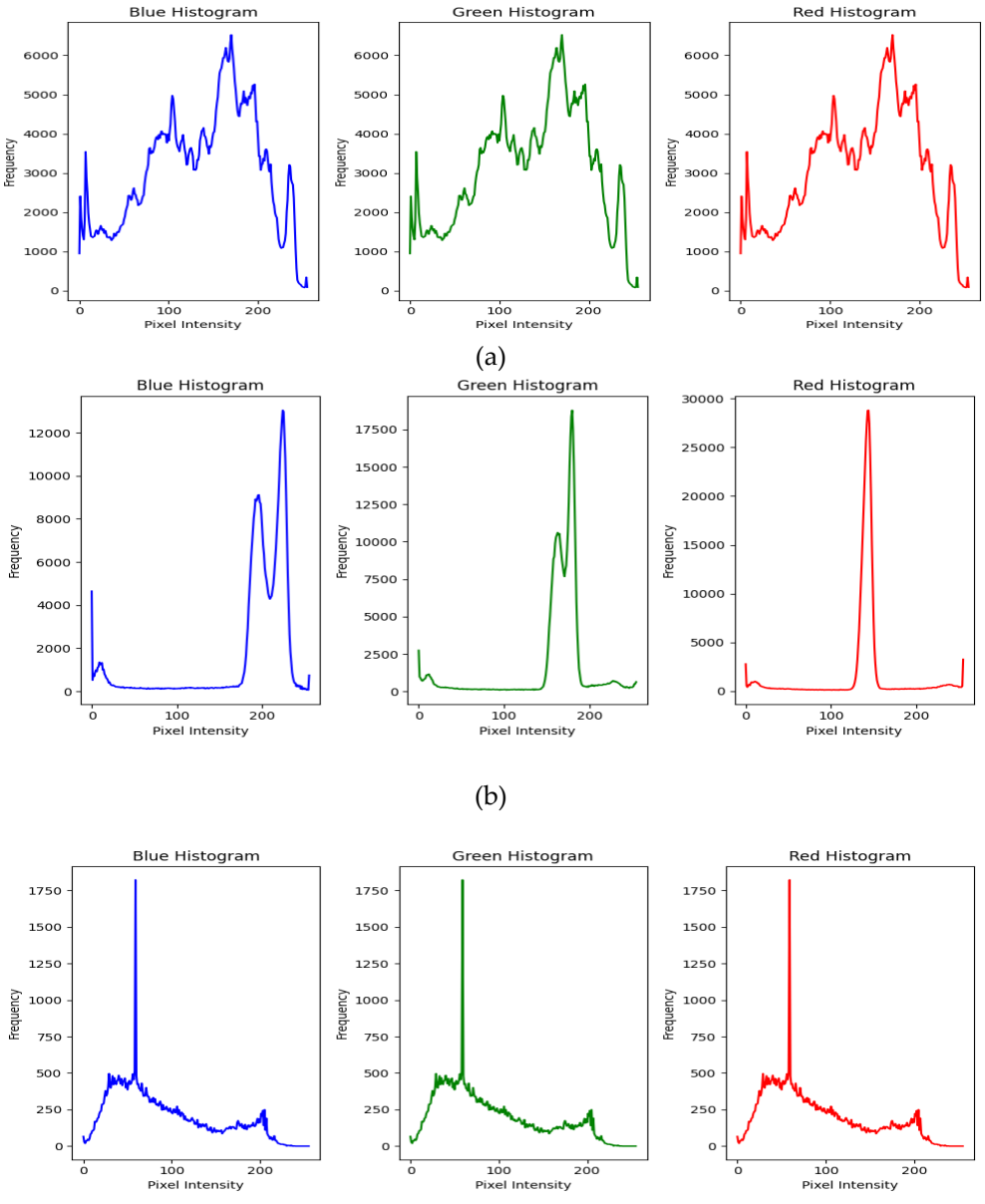
(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 7. Input plain images (a) Baby, (b) Jet, (c) Girl, Stego images: (d) Baby, (e) Jet, (f) Girl, decrypted images: (g) Baby, (h) Jet, (i) Girl.

While ideal stego images should produce equally distributed histograms, and they should not contain any gained data to hinder encryption, actual photos reveal unique patterns in their histograms. Steganography assaults and information leaks can be facilitated due to these patterns. Figure 8 displays the histogram testing results for sample plain images and Figure 9 shows histogram of stego images.



(a)

(b)

(c)

Figure 8. Histogram of plain images: (a) baby, (b) jet, (c) girl

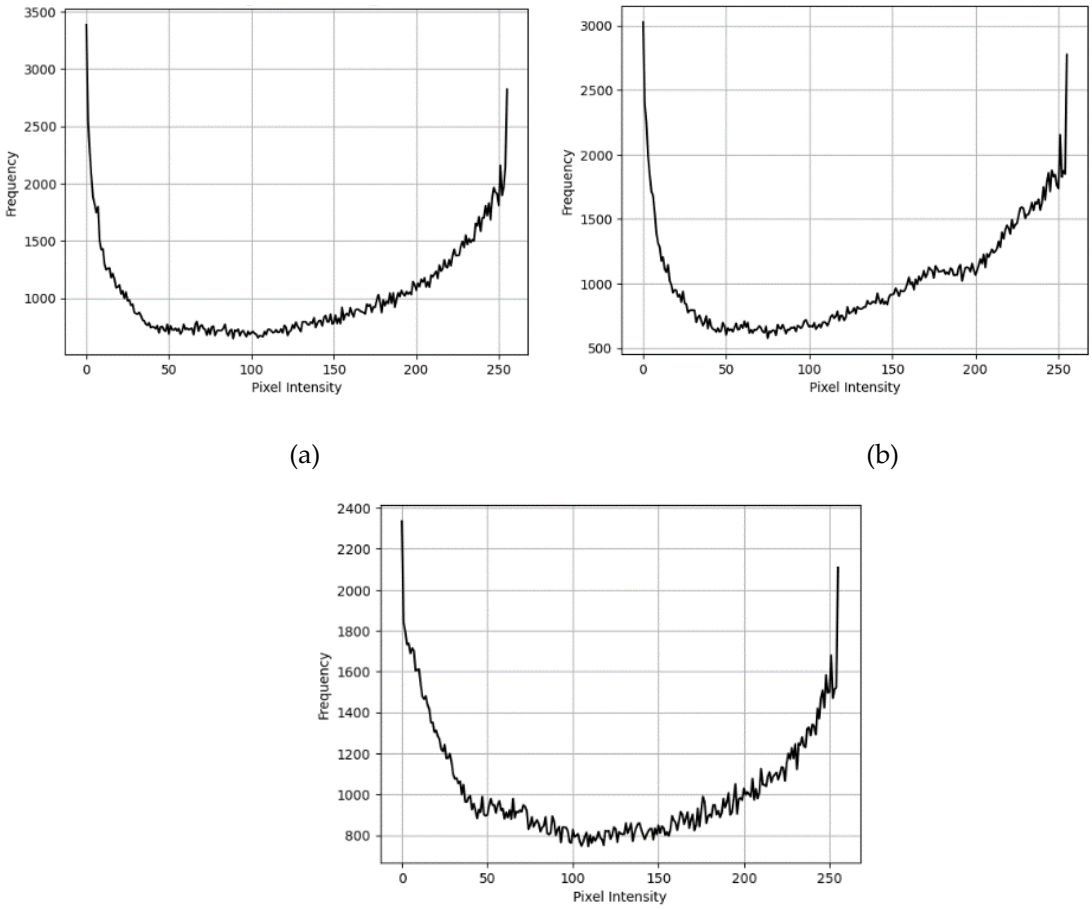


Figure 9. Histogram of stego images: (a) baby, (b) jet, (c) girl.

FuzzyRSA-ChaosCrypt has better performance as compared to other popular algorithms: DES, AES, and ElGamal as presented graph in figure 10.

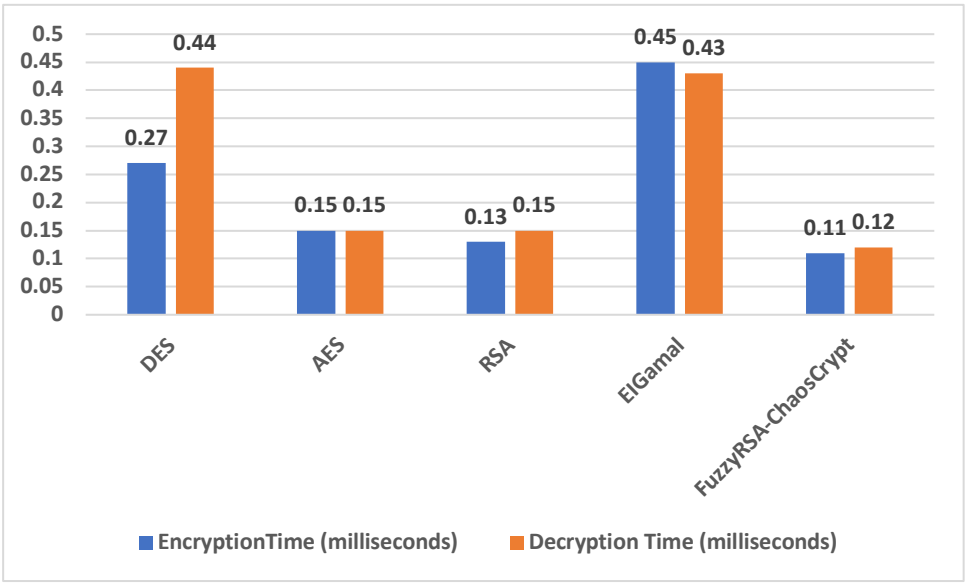


Figure 10. Results of encryption and decryption process on image file having 32kb of size [61].

Information entropy is statistical characteristics used to measure randomness. Following equation is used to calculate it:

$$Q(m,n) = jk + m + n \quad \text{mode } 256 \tag{26}$$

$here, m = 1,2,3,4, \ldots\ldots, j \; and \; n = 1,2,3,4, \ldots\ldots k$

Q is the matrix having size same as permuted image P.

Modulation function is applied on this matrix:

$$S = P + Q, \; Mode \; value \; 256 \tag{27}$$

S is the new image. In the table 2, images with their entropy information are presented.

Table 2. Information entropy values of encrypted images.

Input	Entropy value
Jet	7.89
Baby	7.89
Girl	7.95

5. Conclusions

In this study, a novel image encryption technique is proposed that integrates fuzzy logic functions, RSA algorithm, chaotic maps, OAEP padding, and secret key to encrypt and decrypt digital image.

Dhall et al. [1] introduced chaos-based system for image encryption. It uses symmetric key encryption technique but requires many other symmetric methods for encryption of images. This study utilized chaos-based system with asymmetric encryption algorithm that do not requires integration of further symmetric or asymmetric key encryption algorithms.

Wen et al. [2] introduced image encryption method that is also based of chaos-based system. Quantization and DCT operation are also applied during generation of ciphertext image. Unfortunately, this method lacks flexibility and offers less security; in contrast, proposed study is more flexible and provides enhanced security due to integration of multiple techniques. A user provided message is inserted into image as secret key to enhance the complexity of FuzzyRSA-ChaosCrypt system.

In another study Mfungo et al. [62] applied chaotic maps and fuzzy membership function for secure data transmission. Triangular membership function is applied for generation of secret key that can be predicted, furthermore, this approach requires input with limited size with gray scale conversion. In comparison, these limitations are improved in this research work, as image of any size can be transmitted and color to gray scale conversion is applied during the encryption process.

It ensures safe communication and data security by increasing encryption complexity and offering flexibility for cryptographic applications. The technique improves privacy for image storage and transmission while resisting several assaults, including brute-force attacks, differential attacks, and statistical attacks. However, this encryption method may not be appropriate for current applications due to its processing cost. In the future, author will apply parallelization to accelerate the encryption process on multicore processors. Additionally, a secure key management system will be developed. FuzzyRSA-ChaosCrypt, however, offers hope for protecting sensitive information in a variety of communication sceneries.

References

1. S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *J. King Saud Univ. Inf. Sci.*, vol. 34, no. 1, pp. 1533–1543, 2022.
2. H. Wen *et al.*, "High-quality restoration image encryption using DCT frequency-domain compression coding and chaos," *Sci. Rep.*, vol. 12, no. 1, p. 16523, 2022.
3. F. H. Hsiao, "Chaotic synchronization cryptosystems combined with RSA encryption algorithm," *Fuzzy Sets Syst.*, vol. 342, pp. 109–137, Jul. 2018, doi: 10.1016/J.FSS.2017.10.016.
4. C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, P. Kumaresan, and M. F. Ijaz, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," *Sensors 2020, Vol. 20, Page 5162*, vol. 20, no. 18, p. 5162, Sep. 2020, doi: 10.3390/S20185162.
5. A. Mittal and F. Sidney, "Secure Data Communication Using Padding Key Encryption Cryptography Algorithm," *2023 IEEE Int. Conf. Integr. Circuits Commun. Syst. ICICACS 2023*, 2023, doi: 10.1109/ICICACS57338.2023.10099570.
6. X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci. (Ny).*, vol. 539, pp. 195–214, Oct. 2020, doi: 10.1016/J.INS.2020.06.030.
7. L. Scripcariu, F. Diaconu, P. D. Matasaru, and L. Gafencu, "AES Vulnerabilities Study," *Proc. 10th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2018*, Apr. 2019, doi: 10.1109/ECAI.2018.8678930.
8. V. Himthani, V. S. Dhaka, M. Kaur, D. Singh, and H. N. Lee, "Systematic Survey on Visually Meaningful Image Encryption Techniques," *IEEE Access*, vol. 10, pp. 98360–98373, 2022, doi: 10.1109/ACCESS.2022.3203173.
9. A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimed. Tools Appl.*, vol. 79, no. 11–12, pp. 7951–7985, Mar. 2020, doi: 10.1007/S11042-019-08427-X/METRICS.
10. A. Gutub, N. Al-Juaid, and E. Khan, "Counting-based secret sharing technique for multimedia applications," *Multimed. Tools Appl.*, vol. 78, no. 5, pp. 5591–5619, Mar. 2019, doi: 10.1007/S11042-017-5293-6/METRICS.
11. X. Huang and G. Ye, "An image encryption algorithm based on irregular wave representation," *Multimed. Tools Appl.*, vol. 77, no. 2, pp. 2611–2628, Jan. 2018, doi: 10.1007/S11042-017-4455-X/METRICS.
12. X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, May 2017, doi: 10.1016/J.SIGPRO.2016.11.016.
13. K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process. Image Commun.*, vol. 80, p. 115670, Feb. 2020, doi: 10.1016/J.IMAGE.2019.115670.
14. B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13681–13701, Jun. 2017, doi: 10.1007/S11042-016-3769-4/METRICS.
15. A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Jan. 2018, doi: 10.1007/S11071-017-3874-6/METRICS.
16. P. Li and K. T. Lo, "Joint image encryption and compression schemes based on 16 × 16 DCT," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 12–24, Jan. 2019, doi: 10.1016/J.JVCIR.2018.11.018.
17. A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," *Optik (Stuttg).*, vol. 184, pp. 205–213, May 2019, doi: 10.1016/J.IJLEO.2019.03.065.
18. M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 25497–25518, 2022.
19. R. Kumar, B. Bhaduri, and B. Hennelly, "QR code-based non-linear image encryption using Shearlet transform and spiral phase transform," *https://doi.org/10.1080/09500340.2017.1395486*, vol. 65, no. 3, pp. 321–330, Feb. 2017, doi: 10.1080/09500340.2017.1395486.
20. X. Lv, X. Liao, and B. Yang, "Bit-level plane image encryption based on coupled map lattice with time-varying

delay," *https://doi.org/10.1142/S0217984918501245*, vol. 32, no. 10, Apr. 2018, doi: 10.1142/S0217984918501245.

21. M. Khan and N. Munir, "A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic," *Wirel. Pers. Commun.*, vol. 109, pp. 849–867, 2019.
22. X. Wang and D. Xu, "A novel image encryption scheme using chaos and Langton's Ant cellular automaton," *Nonlinear Dyn.*, vol. 79, no. 4, pp. 2449–2456, Mar. 2015, doi: 10.1007/S11071-014-1824-0/METRICS.
23. Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci. (Ny).*, vol. 339, pp. 237–253, Apr. 2016, doi: 10.1016/J.INS.2016.01.017.
24. R. S. Mohammed, K. K. Jabbar, and H. A. Hilal, "Image encryption under spatial domain based on modify 2D LSCM chaotic map via dynamic substitution-permutation network," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 4, pp. 3070–3083, 2021.
25. M. Xu and Z. Tian, "A novel image cipher based on 3D bit matrix and latin cubes," *Inf. Sci. (Ny).*, vol. 478, pp. 1–14, Apr. 2019, doi: 10.1016/J.INS.2018.11.010.
26. P. A. Cheremkhin, E. A. Kurbatova, N. N. Evtikhiev, V. V Krasnov, V. G. Rodin, and R. S. Starikov, "Comparative analysis of off-axis digital hologram binarization by error diffusion," *J. Opt.*, vol. 23, no. 7, p. 075703, 2021.
27. L. Poongothai, K. Sharmila, C. Shanthi, R. Devi, and R. Anitha, "Retinal Encryption Using Snnipet Pixel XOR with Huffman Sequential Encoding for Privacy Augmentation," in *Sentimental Analysis and Deep Learning: Proceedings of ICSADL 2021*, Springer, 2022, pp. 757–767.
28. H. Alhumyani, "Efficient image cipher based on baker map in the discrete cosine transform," *Cybern. Inf. Technol.*, vol. 20, no. 1, pp. 68–81, 2020.
29. Q. Yin and C. Wang, "A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion," *https://doi.org/10.1142/S0218127418500475*, vol. 28, no. 4, May 2018, doi: 10.1142/S0218127418500475.
30. A.-V. Diaconu, "Circular inter–intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci. (Ny).*, vol. 355, pp. 314–327, 2016.
31. T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy*, vol. 21, no. 3, p. 319, 2019.
32. S. F. Raza and V. Satpute, "A novel bit permutation-based image encryption algorithm," *Nonlinear Dyn.*, vol. 95, pp. 859–873, 2019.
33. C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019, doi: 10.1007/S11042-018-6739-1/METRICS.
34. K. U. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Appl. Soft Comput.*, vol. 90, p. 106162, 2020.
35. B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," *IEEE Access*, vol. 9, pp. 137635–137654, 2021.
36. J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *https://doi.org/10.1142/S021812749800098X*, vol. 8, no. 6, pp. 1259–1284, Nov. 2011, doi: 10.1142/S021812749800098X.
37. C. Çokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 373, no. 15, pp. 1357–1360, Mar. 2009, doi: 10.1016/J.PHYSLETA.2009.02.030.
38. M. Kalpana, K. Ratnavelu, P. Balasubramaniam, and M. Z. M. Kamali, "Synchronization of chaotic-type delayed neural networks and its application," *Nonlinear Dyn.*, vol. 93, pp. 543–555, 2018.
39. K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, "Image encryption scheme based on a generalized Arnold map and RSA algorithm," *Secur. Commun. Networks*, vol. 2020, pp. 1–14, 2020.
40. U. H. Mir, D. Singh, and P. N. Lone, "Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain," *Inf. Secur. J. A Glob. Perspect.*, vol. 31, no. 1, pp. 49–63, 2022.
41. Q. Xu, K. Sun, and C. Zhu, "A visually secure asymmetric image encryption scheme based on RSA algorithm and

hyperchaotic map," *Phys. Scr.*, vol. 95, no. 3, p. 35223, 2020.

42. M. Babu, G. S. Devi, N. Iswarya, M. V. Prasanna, and M. Y. Krishna, "Image encryption using chaotic maps and DNA encoding," *J. Xidian Univ.*, vol. 14, no. 4, 2020.
43. G.-D. Ye, H.-S. Wu, X.-L. Huang, and S.-Y. Tan, "Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map," *Chinese Phys. B*, vol. 32, no. 3, p. 30504, 2023.
44. K. K. K. Oo and Y. N. Soe, "IMPLEMENTATION OF SECURE IMAGE TRANSFERRING BY USING RSA AND SHA-1," *Int. J. All Res. Writings*, vol. 2, no. 11, pp. 9–13, 2020.
45. N. S. Noor, D. A. Hammood, A. Al-Naji, and J. Chahl, "A fast text-to-image encryption-decryption algorithm for secure network communication," *Computers*, vol. 11, no. 3, p. 39, 2022.
46. I. A. Aljazaery, H. T. H. Salim ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor.," *Int. J. Online Biomed. Eng.*, vol. 18, no. 3, 2022.
47. A. Abusukhon, M. N. Anwar, Z. Mohammad, and B. Alghannam, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," *J. Discret. Math. Sci. Cryptogr.*, vol. 22, no. 1, pp. 65–81, 2019.
48. S. A. Shawkat and I. Al-Barazanchi, "A proposed model for text and image encryption using different techniques," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 20, no. 4, pp. 858–866, 2022.
49. M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, "Face Image Encryption Based on Feature with Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map," *Sensors*, vol. 23, no. 3, p. 1415, 2023.
50. M. Moradi, M. Moradkhani, and M. B. Tavakoli, "A real-time biometric encryption scheme based on fuzzy logic for IoT," *J. Sensors*, vol. 2022, 2022.
51. Z. A. Abduljabbar *et al.*, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022.
52. X. Huang, Y. Dong, G. Ye, W.-S. Yap, and B.-M. Goi, "Visually meaningful image encryption algorithm based on digital signature," *Digit. Commun. Networks*, vol. 9, no. 1, pp. 159–165, 2023.
53. G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Eng. J.*, vol. 61, no. 9, pp. 6785–6795, 2022.
54. R. R. Suman, B. Mondal, and T. Mandal, "A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256," *Multimed. Tools Appl.*, vol. 81, no. 19, pp. 27089–27110, 2022.
55. M. B. Salunke, P. N. Mahalle, and G. R. Shinde, "Rubik's cube encryption algorithm-based technique for information hiding during data transmission in sensor-based networks," *Int. J. Intell. Syst. Appl. Eng.*, vol. 10, no. 1s, pp. 429–439, 2022.
56. K. Sakthidasan and B. V. S. Krishna, "A new chaotic algorithm for image encryption and decryption of digital color images," *Int. J. Inf. Educ. Technol.*, vol. 1, no. 2, p. 137, 2011.
57. Z. Liu *et al.*, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Opt. Commun.*, vol. 284, no. 1, pp. 123–128, 2011.
58. P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: a survey," in *2014 fifth international conference on signal and image processing*, IEEE, 2014, pp. 102–107.
59. I. Bisio, S. Delucchi, F. Lavagetto, and M. Marchese, "Performance comparison of network selection algorithms in the framework of the 802.21 standard," *J. Networks*, vol. 10, no. 1, p. 51, 2015.
60. J. Liu and J. Li, "A Novel Key Exchange Protocol Based on RSA-OAEP," in *2008 10th International Conference on Advanced Communication Technology*, 2008, pp. 1641–1643. doi: 10.1109/ICACT.2008.4494096.
61. F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017.

62. D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," *Appl. Sci.*, vol. 13, no. 12, p. 7113, 2023.