



Research Article

RGB Image Encryption Algorithm Using RSA Algorithm and 3D Chaotic System

H. J. Yakubu¹, S. B. Joseph² and N. M. Yahi³

¹Department of Mathematical Science, Faculty of Science, University of Maiduguri, Borno State, Nigeria

²Department of Computer Engineering, Faculty of Engineering, University of Maiduguri

³Department of Electrical/Electronics, Umar Ibn Ibrahim El-kenemi College of Education, Science and Technology, Bama, Borno State, Nigeria

*Corresponding author: yakubuhj@unimaid.edu.ng, doi.org/10.55639/607.080706

ARTICLE INFO:

Keyword:

Cipher image,
Confusion-diffusion,
Chaotic map,
Asymmetric/Symmetric keys

ABSTRACT

The Internet which is the global network is exposed to various threats. Therefore, the search for a better way of securing sensitive information either in transit or in storage is on the increase. A recent study on the RSA algorithm shows that gray scale images can be well secured using improved RSA algorithm that utilizes a 1-D chaotic map. However, today we have many sensitive images in RGB form and this necessitates the need to extend an improved RSA on grayscale imaging to colour imaging. In this paper, we adopted the confusion-diffusion technique where the RSA algorithm was used for image diffusion and a 3-D chaotic system called Shimizu-Morioka System was used for image confusion. A standard test image (Mandrill_colour_200.tif) was used for testing the proposed algorithm using three different sets of keys. Security analysis such as histogram uniformity analysis and correlation coefficient analysis were used in determining the strength of the proposed algorithm. Results from the analyses show that the proposed scheme is highly effective and can withstand any statistical and brute-force attacks.

Corresponding author: H. J. Yakubu, Email: yakubuhj@unimaid.edu.ng
Department of Mathematical Science, University of Maiduguri, Borno State, Nigeria

INTRODUCTION

The need for maintaining privacy between two communicating parties over the public or private network cannot be overemphasized. The Internet which is the global network is exposed to various threats. Ways of securing sensitive information either on transit or on storage is on the increase. Steganography and Cryptography are the two popular methods for concealing sensitive information. Steganography is a method of hiding secret messages in a cover object while Cryptography is a technique that transforms information to be transmitted into an unreadable and unintelligent form so that only authorized persons can correctly recover the information by decryption process (Delfs and Knebl, 2007, Abd El-Samie *et al.*, 2014). The word "Cryptography" was derived from the Greek words *kryptos*, meaning hidden and *graphikos*, meaning writing (Hoffstein *et al.*, 2008) and came in as a means to enable parties communicate with each other even in the presence of an adversary that has access to the communication channels. It has been in existence almost since writing was invented though in different forms (Bellare and Rogaway, 2008). Different authors defined cryptography in different ways. Delfs and Knebl (2007) defined cryptography as the science of keeping secrets secret, and according to Hankerson *et al.*, (2004), cryptography is defined as the design and analysis of mathematical techniques that enables secure communications in the presence of malicious adversaries, while Goldreich (2004) defined cryptography as the art of building encryption schemes that allows secret data exchange over insecure channels. Providing confidentiality using encryption methods is the fundamental and classical goal of cryptography. Furthermore, cryptography has now gone beyond secret communication. It can perform functions which include message authentication, digital signatures, protocol for exchanging secret keys, etc. (Taki El-Deen *et al.*, 2014, Hoffstein, *et al.*, 2008). Symmetric-key cryptography and Asymmetric-key cryptography are basically the two categories of cryptography that exist. The Symmetric-key cryptography is where the sender and the receiver each has a single secret key that are alike which are used both for encryption and decryption (i.e. $K_e = K_d$). The key must be transmitted from sender to receiver via a separate

secret channel while the Asymmetric-key cryptography (also called Public-key cryptosystem) is where each party involved has a pair of different keys that are mathematically linked (K_e, K_d). The encryption key K_e is made public and is different from the decryption K_d that is kept secret (i.e. $K_e \neq K_d$). Here, no additional secret channel is needed for the key transfer (Delfs and Knebl, 2007, Kaliski, 2012). Symmetric key cryptosystem provides a secured communication channel to each pair of users after agreeing on a common secret key which is being shared between the pair. It also provides confidentiality and data integrity. However, secured delivery of the secret key is observed to be its major setback. Other weaknesses observed are lack of good methods for authentication and non-repudiation (Mishkovski and Kocarev, 2011). The public-key encryption algorithms which provide a secured delivery of secret key and also have protocols that provide authentication and non-repudiation were introduced by Diffie and Hellman in 1976. Since then, numerous public-key encryption algorithms have been proposed among these, the Rivest-Shamir-Adleman (RSA) algorithm, the ElGamal algorithm, and the Robin cryptosystems are the three most widely used public-key cryptosystems. The RSA algorithm happens to be the most popular and the most secured public-key encryption algorithm (Chandel and Patel, 2013, Mishkovski and Kocarev, 2011, Delfs and Knebl, 2007).

The RSA algorithm was primarily designed for text and its application has been extended to digital images. However, its direct application on digital images was found not suitable as observed by Yakubu and Aboiyar (2016). The results of their study reveals that RSA algorithm is image dependent (the higher the correlation between adjacent pixels the poorer the cipher image). This conclusion was drawn from observation made on encrypted images obtained with the RSA algorithm using five different set of keys which exposed some hints about their plain images on visual inspection irrespective of the primes size used and with primes below 25; the plain image is completely exposed in the cipher image

(Yakubu and Aboiyar, 2016). Despite these weaknesses, its application in some areas remains very vital in particular, medical imaging where every pixel in the plain-image is important and needs to be recovered exactly in its decrypted image. That is to say when you compare the plain image and the decrypted image in terms of pixel values, they are exactly the same. These features are not obtainable with chaotic encryption schemes.

In this paper, RSA encryption algorithm for RGB images was proposed using a 3-D chaotic system that employed confusion-diffusion technique. First the pixel values of the plain image were repositioned using the 3-D chaotic system, thereby breaking the correlation between adjacent pixels in the plain image and then generated the cipher image with the RSA encryption scheme. A standard test image was used for testing the proposed algorithm. Security analysis such as histogram uniformity analysis and correlation coefficient analysis were used in testing the strength of the proposed algorithm.

LITERATURE SURVEY

Shankar (2018) proposed an optimal RSA encryption algorithm for secret images that used the method that divided plain image into blocks which were then encrypted and decrypted using RSA algorithm. Analyses of the experimental results show that the proposed scheme not only achieved good encryption but also resist statistical and differential attacks. Yakubu *et al.* (2018) proposed an improved RSA image encryption algorithm using 1-D Logistic map for grayscale images. In this scheme, 1-D logistic map was used in shuffling the pixels of the plain image thereby breaking the correlation between adjacent pixels before being encrypted with the RSA algorithm. The results of the analysis show that the proposed scheme is highly secured and stronger against the brute-force attack (the encrypted image does not reveal any hint about the plain image to the attacker and also its key space has double: the two primes, initial condition and control parameter) than the RSA image encryption scheme. Gafsi *et al.* (2020) also proposed an improved chaos-based

cryptosystem for medical image encryption and decryption. A complex chaos-based PRNG is suggested to generate a high-quality key that presents high randomness behaviour, high entropy, and high complexity. An improved architecture is proposed to encrypt the secret image that is based on permutation, substitution, and diffusion properties. In the first step, the image's pixels are randomly permuted through a matrix generated using the PRNG. Next, pixel's bits are permuted using an internal condition. After that, the pixels are substituted using two different S-boxes with an internal condition. In the final step, the image is diffused by XORing pixels with the key stream generated by the PRNG in order to acquire an encrypted image. R rounds of encryption can be performed in a loop to increase the complexity. The obtained simulation results demonstrate that the system enables high-level security and performance. It also provides a large key space of 2^{192} which resists the brute-force attack. A fast medical image security algorithm for color images that uses both Watermarking and Encryption of each color channel was proposed by Bala (2020). The proposed method starts with embedding of a smoothed key image (K) and patient information over the original image (I) to generate a watermarked image (W). Then, each color channel of the watermarked image (W) is encrypted separately to produce an encrypted image (E) using the same smoothed key image (K). Qualitative and quantitative results of the proposed method show good performance when compared with the existing method with high Mean, PSNR and Entropy. Manjula and Mohan (2020) proposed a secure framework for Medical Image Encryption Using Enhanced AES Algorithm. In this paper, we briefly evaluate the overall organization of Rijndael AES algorithm and a new dynamic S-Box is spawned using a Hash function to provide robust security. The results show that the proposed system is effective and well secured. Xue *et al.* (2021) observed that the Current image encryption algorithms have various deficiencies in effectively protecting medical images with large storage capacity and high pixel correlation

and proposed a medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length. First, the original image is encoded dynamically according to the binary bit from a pixel, and the DNA sequence matrix is scrambled. Second, DNA sequence matrices are dynamically segmented into DNA chains of different lengths. After that, row and column deletion operation and transposition operation of DNA dynamic chain are carried out, respectively, which made DNA chain matrix double shuffle. Finally, the encrypted image is got after recombining DNA chains of different lengths. The proposed algorithm was tested on a list of medical images. Results showed that the proposed algorithm showed excellent security performance, and it is immune to noise attack, occlusion attack, and all common cryptographic attacks. Srushti and Ravi (2022) also proposed a digital image encryption scheme using RSA and linear feedback shift register (LFSR) where keys are generated using random number generator which is grounded on LFSR and the image was encrypted using RSA algorithm. The results show that the method is effective.

Related Literature

Cryptanalysis, which is the art of deciphering an encrypted message as a whole or in part when the decryption key is not known, has been a source of concern to cryptographic scheme researchers. When cryptanalyzing a ciphering algorithm, the fundamental assumption is that the cryptanalyst knows exactly the design and working of the cryptosystem under study except the secret key (Mishra and Mankar, 2011, Stinson, 2006). This assumption was made by A. Kerkhoff in the 19th century and is usually referred to as Kerkhoff's Principle (Delfs and Knebl, 2007, Stinson, 2006). Thus, according to this principle, the security of a cryptosystem must be entirely based on the secret key. However, the possible attacks depend on the actual resources of the adversary. The most common attacks on cryptosystems are briefly explained as follows (Delfs and Knebl, 2007, Abd El-Samie *et al.*, 2014):

- i. **Ciphertext-only attack:** The attacker has access to one or more encrypted messages.

- ii. **Known plaintext attack:** The attacker possesses some knowledge about the plaintext corresponding to the given ciphertext. This may help it determine the key or part of the key.
- iii. **Chosen plaintext attack:** The attacker can feed the chosen plaintext in to the black box that contains the encryption algorithm and the encryption key that gives the corresponding ciphertext. The accumulated knowledge about the pair of plaintext-ciphertext may reveal the key or part of the key.
- iv. **Chosen ciphertext attack:** The attacker can feed the chosen ciphertext into the black box that contain the decryption algorithm and the decryption key which produces the corresponding plaintext. By analyzing the accumulated ciphertext-plaintext pairs, the attacker may obtain the secret key of part of the key.
- v. **Brute-Force Attack:** A brute force attack is the method of breaking a cipher based on the exhaustive key search. It is the most expensive attack.

In addition to the five general attacks described above, there are some other specialized attacks, like, the differential and the linear attacks. The differential cryptanalysis is a kind of chosen-plaintext attack aim at finding the secret key in a cipher, while the linear cryptanalysis is a type of known-plaintext attack, whose purpose is to construct a linear approximate expression of the cipher under study (Mishra and Mankar, 2011)

METHODOLOGY

The RSA Algorithm

The RSA algorithm was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology and by 1978; it was published as the first public-key cryptosystem that could function as both a key agreement mechanism and as a digital signature (Mishra and Mankar, 2011, Kokarev, and Makraduli, 2005). In RSA algorithm, each communicating party uses two different but mathematically linked keys called the public-key and the private-key. The public-key of

the recipient is made public for anyone that would like to send a private message to him/her uses, whereas the private-key must be kept secret by the recipient to decrypt encrypted messages received (Taki El-Deen *et al.*, 2014, Kaliski, 2012). It is important to know that either of the Keys (public-key or the private-key) can be used for encrypting a message; the opposite key from the one used to encrypt a message is used to decrypt it. The security of the RSA encryption function depends on the tremendous difficulty of factoring, but the equivalence is not proven. Multiplying two large primes is easy but determining the two prime factors from the product is considered infeasible due to time it would take even with today's Super computers (Delfs and Knebl, 2007). This attribute has made RSA become the most widely used asymmetric-key algorithm that provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. The RSA cryptosystem has stood the test of time to this day, where it is used in cryptographic applications from banking, e-mail security to e-commerce on the Internet () and to securing medical imaging such as X-ray images (Taki El-Deen *et al.*, 2014, Yakubu *et al.*, 2018).

The Mathematics of RSA

Divisibility and Greatest Common Divisors (gcds):

Definition 3.1: Let $a, b \in \mathbb{Z}$, with $b \neq 0$. We say that b divides a , or that a is divisible by b , if there is a number $c \in \mathbb{Z}$ such that $a = b \cdot c$. Thus, $b|a$ to indicate that b divides a .

Proposition 3.1: Let $a, b, c \in \mathbb{Z}$, then the following holds:

- (a) If $a|b$ and $b|c$ then $a|c$.
- (b) If $a|b$ and $b|a$, then $a = \pm b$.

Proposition 3.4: Let p be a prime and let $e \in \mathbb{Z}^+$ satisfying $\gcd(e, p-1) = 1$. Then proposition 3.3 tells us that e has an inverse modulo $p-1$ say $de \equiv$

(c) If $a|b$ and $a|c$ then $a|(b+c)$ and $a|(b-c)$.

Definition 3.2: A common divisor of $a, b \in \mathbb{Z}$ is a number $d \in \mathbb{Z}^+$ such that $d|a$ and $d|b$.

Definition 3.3: The greatest common divisor of $a, b \in \mathbb{Z}$ is the largest number $d \in \mathbb{Z}^+$ such that $d|a$ and $d|b$. It is denoted by $\gcd(a, b)$.

Theorem 3.1 (Extended Euclidean Algorithm); Let $a, b \in \mathbb{Z}^+$. Then the equation $au + bv = \gcd(a, b)$ always has a solution in integers u and v .

Modular Arithmetic:

The theory of congruence is a powerful method in number theory that is based on the simple idea of clock arithmetic.

Definition 3.4: Let $n \in \mathbb{Z}^+$ and $n \geq 2$, we say that $a, b \in \mathbb{Z}$ are congruent modulo n if $n|(a-b)$. Written as $a \equiv b \pmod{n}$ where n is called the modulus.

Proposition 3.2: Let $n \in \mathbb{Z}^+$ and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ so, If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{n}$ and $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$.

Prime Numbers and Exponentiation:

Definition 3.5: An integer $p > 1$ is called a **prime number** or simply **prime** if 1 and p are the only divisors of p otherwise, p is called **composite**.

Definition 3.6: Let $a, b \in \mathbb{Z}$, we say that a and b are relatively prime (also called coprime) if $\gcd(a, b) = 1$.

Proposition 3.3: Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ then $a \cdot b \equiv 1 \pmod{n}$ for some $b \in \mathbb{Z}$ if and only if $\gcd(a, n) = 1$. Then a is relative prime to n . If such an integer b exists, we say that b is the (multiplicative) inverse of a modulo n .

$1 \pmod{p-1}$; thus, the congruence $x^e \equiv c \pmod{p}$ has the unique solution $x \equiv c^d \pmod{p}$.

Proposition 3.5: Let p and q be two distinct prime numbers and let $e \in \mathbb{Z}^+$ satisfying $\gcd(e, (p-1)(q-1)) = 1$. From proposition 3.3 we see that e has an inverse modulo $(p-1)(q-1)$ say $de \equiv 1 \pmod{(p-1)(q-1)}$. Then the congruence $x^e \equiv c \pmod{pq}$ has the unique solution $x \equiv c^d \pmod{pq}$.

Exponentiation is the successive multiplication of a number by itself up to n times and is often used in cryptography such as computing α^e or $\alpha^e \pmod n$. This can be done efficiently by the fast exponentiation algorithm. The idea is that if the exponent e is a power of 2, say $e = 2^k$, then we can exponentiate by successive squarings: that is, $\alpha^e = \alpha^{2^k} = (((\dots ((\alpha^2)^2) \dots)^2)^2)$. In this way, we compute α^e by k squarings. For example, $\alpha^{16} = \alpha^{2^4} = (((\alpha^2)^2)^2)^2$. If the exponent is not a power of 2, we use the binary expansion of the exponent e to convert the calculation of α^e into a succession of squaring and multiplications. For example, to evaluate α^{29} using this approach, first we write 29 in binary form $29 = 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$, it then follows that $\alpha^{29} = \alpha^{1 \cdot 2^4} \cdot \alpha^{1 \cdot 2^3} \cdot \alpha^{1 \cdot 2^2} \cdot \alpha^{0 \cdot 2^1} \cdot \alpha^{1 \cdot 2^0} = (((\alpha^2 \cdot \alpha^2) \cdot \alpha^2) \cdot \alpha^0)^2 \cdot \alpha$. Thus, only four squarings and three multiplications are needed to compute $\alpha^{29} \pmod n$ as compared to naive approach. It is important that the reduction modulo n be done at each squaring or multiplication to avoid large intermediate integers.

Shimizu-Morioka System

In 1980, Shimizu and Morioka studied a simplified model of the well-known Lorenz system for large Rayleigh number called Shimizu-Morioka System. It is a classical 3-

D chaotic system defined by the following nonlinear equations:

$$\dot{x} = y, \dot{y} = -xz + x - \beta y, \dot{z} = x^2 - \alpha z. \tag{1}$$

Where $(x, y, z) \in \mathbb{R}^3$ are state variables, the dot $(\dot{\cdot})$ on a variable indicates the derivative of the variable with respect to time t , while α and β are positive constant parameters (Shimizu and Morioka, 1980). The stable symmetric and asymmetric periodic motions as well as stochastic behaviour of trajectories were discovered by Shimizu and Morioka through a computer simulation and came up with the following observations (Shil'nikov, 1991):

- (i). The Shimizu-Morioka system is invariant with respect to the substitution $(x, y, z) \rightarrow (-x, -y, z)$ as in the Lorenz model,
- (ii). System (1) has three equilibrium states: $(0,0,0)$, $(\sqrt{\alpha},0,1)$ and $(-\sqrt{\alpha},0,1)$.

Stability Analysis of the Equilibrium points of system (1)

The following observations were made (Salih, 2011):

- a) If $\alpha \geq 0$ then system (1) has three isolated equilibrium points: $P_0(0,0,0)$, $P_1(\sqrt{\alpha},0,1)$ and $P_2(-\sqrt{\alpha}, 0,1)$ and for $\alpha < 0$, it has only one isolated equilibrium point $P_0(0,0,0)$.
- b) The equilibrium point $P_0(0,0,0)$ is unstable for all $\alpha \in \mathbb{R}$
- c) The equilibrium point $P_1(\sqrt{\alpha},0,1)$ is asymptotically stable if and
- d) The equilibrium point $P_1(\sqrt{\alpha},0,1)$ is unstable if and only if $\alpha < \alpha_0 = \frac{2-\beta^2}{\beta}$

where $\beta \in (0, \sqrt{2})$.

Phase portrait of the Shimizu-Morioka chaotic system

The Shimizu-Morioka chaotic system is described by equation (2).

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1-z & -\beta & 0 \\ x & 0 & -\alpha \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1-z & -0.9101 & 0 \\ x & 0 & -0.3591 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad (2)$$

where the parameters value are defined as $\beta = 0.9101$ and $\alpha = 0.3591$. Using a MATLAB/Simulink model, version 7.10.0 (R2016a) the phase portraits of the Shimizu-Morioka chaotic system in the xy , xz , yz , and

xyz phase space were obtained as shown in Figure 1 by a, b, c, and d respectively when initial conditions are chosen as $x_0 = 0.1$, $y_0 = 0.1$, and $z_0 = 0.1$

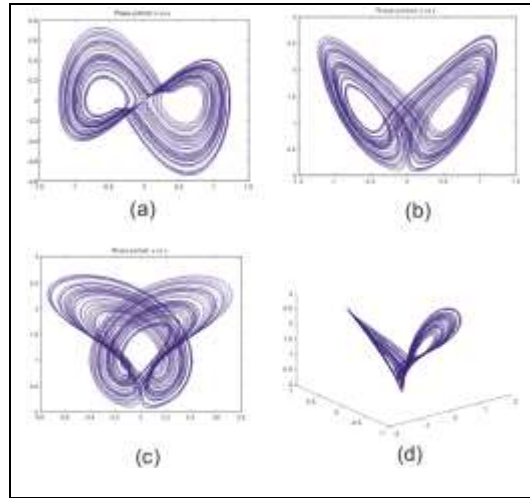


Figure 1: Phase portrait of system (2) in the **a).** xy , **b).** xz , **c).** yz , **d).** xyz phase space

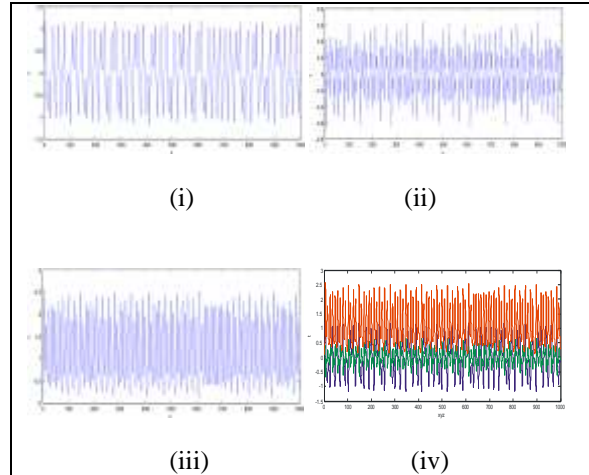


Figure 2: Time Series of System (2) in the **i).** xy, **ii).** xz, **iii).** yz, **iv).** xyz phase plain

The Proposed Algorithm

The proposed encryption scheme consists basically of two stages. The first stage is the permutation stage where the rich chaotic properties of the Shimizu-Morioka chaotic system was used in shuffling the pixels values of the plain image using initial conditions and control parameters as the key. That breaks the correlation between adjacent pixels of the plain image. In the second stage, the RSA algorithm was applied to the shuffled image to obtain the cipher (encrypted) image. The decrypted image is obtained by applying the same operations carried out in the encryption process using the same initial conditions and control parameters but in the reverse order. The details algorithms for Key generation, encryption and decryption processes are presented below.

Key Generation Algorithm

- i. Generate two distinct large primes' p and q,
- ii. Compute the modulus n as $n = pq$ and $\phi(n) = (p-1)(q-1)$,
- iii. Chose public exponent e to be relative prime to $\phi(n)$, with $1 < e < \phi(n)$,
- iv. Form the pair (n,e) and publish it as public-key,
- v. Find an integer d with $1 < d < \phi(n)$ such that $ed \equiv 1 \pmod{\phi(n)}$,

- vi. Form the pair (n,d) and keep it secret as secret-key.

Encryption Algorithm

- i. Read RGB image from a file as I,
- ii. Convert the image to double
- iii. Obtain the image dimension $m \times n \times 3$,
- iv. Compute number of pixels per colour ($N = m * n$),
- v. Enter the parameters value for $\alpha, \beta, x_0, y_0, z_0, h$,
- vi. Solve the Shimizu-Morioka chaotic system up to N times steps using the
- vii. Euler's method to obtain solutions in vector form as X, Y, Z,
- viii. Add confusion to the solution using round function,
- ix. Sort the vectors X, Y, and Z to obtain X1, Y1, and Z1 with their list of indices l_x, l_y , and l_z .
- x. Define A1, B1, and C1 to be matrices for red, green and blue intensities respectively.
- xi. Reshape A1, B1, and C1 into row vectors as A2, B2, and C2.
- xii. Use the indices l_x, l_y , and l_z . obtained in viii to scramble the row vectors A2, B2, and C2 and obtained new row vectors as A3, B3, and C3,
- xiii. Encrypt the row vectors A3, B3, and C3 using the formula $c_i = E_{(n,e)}(m_i) = m_i^e \pmod{n}$.with the public-key to obtain the vectors A4, B4 and C4

- xiv. Reshape A4, B4, and C4 into $m \times n$ matrices to obtain A5, B5 and C5.
- xv. Form the encrypted image I1 by merging A5, B5 and C5.
- xvi. Convert the image I1 to uint8.
- xvii. Display the encrypted image I1.
- xviii. Save the encrypted image I1.

Decryption Algorithm

- i. Read the encrypted image I1,
- ii. Convert the image to double,
- iii. Define A6, B6, and C6 to be matrices for the red, green and blue intensities respectively for I1.
- iv. Reshape A6, B6, and C6 into row vectors to obtain A7, B7, and C7,
- v. Decrypt the row vectors A7, B7, and C7 with the formula

$$m_i = D_{(n,d)}(c_i) = c_i^d \pmod{n}$$
 using the secret-key to obtain the row vectors A8, B8, and C8.
- vi. Reposition the entries in A8, B8, and C8 using the indices l_x , l_y , and l_z to

obtain new row vectors A9, B9, and C9.

- vii. Reshape A9, B9, and C9 into square matrices to obtain A10, B10, and C10.
- viii. Form the decrypted image as I2 by merging the A10, B10, and C10.
- ix. Convert the decrypted image I2 to uint8.
- x. Display the decrypted image I2.
- xi. Save the decrypted image I2 in a file.

RESULTS AND DISCUSSION

Implementation

The proposed encryption algorithm was tested on a standard test digital colour image of size 200 x 200 and stored with TIF file format (Mandrill_colour_200.tif) as our input data as shown in Figure 3 using three (3) different sets of keys. The code for the proposed scheme was implemented in MATLAB version 7.10.0 (R2016a) to simulate the proposed encryption algorithm.

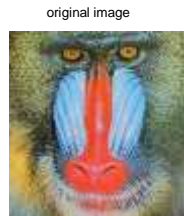


Figure 3: Plain image (Original-image)

Results Obtained

After applying the proposed algorithm to the plain image shown in Figure 3 using three different sets of keys (first the public key

used for encryption followed by the private used for decryption), the results obtained are shown in Figure 4.

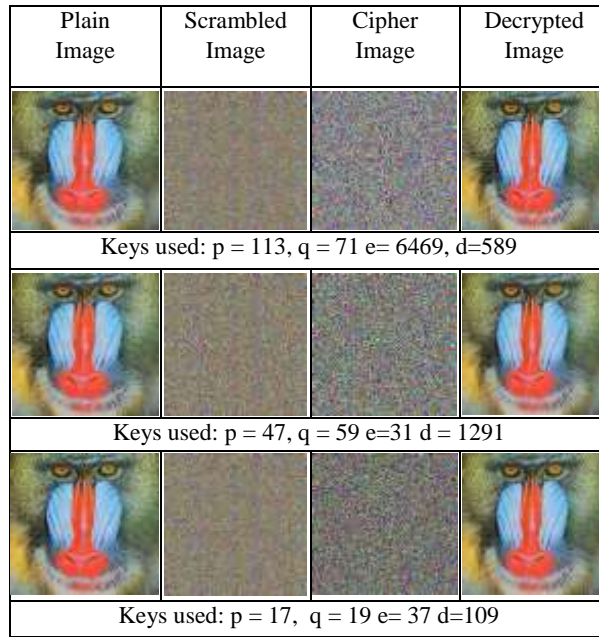


Figure 4: Plain, Scrambled, Cipher and Decrypted Images

SECURITY ANALYSIS

It is expected that when an encryption algorithm is applied to a plain image, you get a cipher image whose pixels' values must be different when compared with the plain image. For an encryption algorithm to be considered good enough, these changes must be in an irregular manner that maximizes the difference in pixel values between the plain image and the encrypted image. Also, a good encrypted image must be composed of totally random patterns that do not reveal any of the features of the original image (Abd El-Samie *et al.*, 2014). To test the robustness of the proposed scheme, security analysis such as Histogram Uniformity analysis, and Correlation Coefficient analysis were carried out on the results obtained from the proposed scheme.

Histogram Uniformity Analysis

For image encryption algorithm to be considered worthy of use, the histogram of the encrypted image must satisfy these two properties (Abd El-Samie *et al.*, 2014):

- It must be totally different from the histogram of the original image.
- It must have a uniform distribution, which means that the probability of occurrence of any gray scale value is the same.

Figure 5 shows the histogram of the plain image in the Red, Green and Blue intensities and Figures 6 to 8 shows the histogram of the encrypted (cipher) image also in Red, Green and Blue intensities for the three different sets of public and private keys used.

On comparing the two, one can see clearly that the histograms of the cipher image in the three intensities (Red, Green and Blue) for the three different sets of keys are completely different from that of the plain image and not only that the histograms of the cipher image in all the intensities are more or less uniformly distributed. Thus, the proposed scheme satisfies the two conditions of histogram uniformity analysis indicating that the attacker cannot obtain any hint about the plain image from the cipher image.

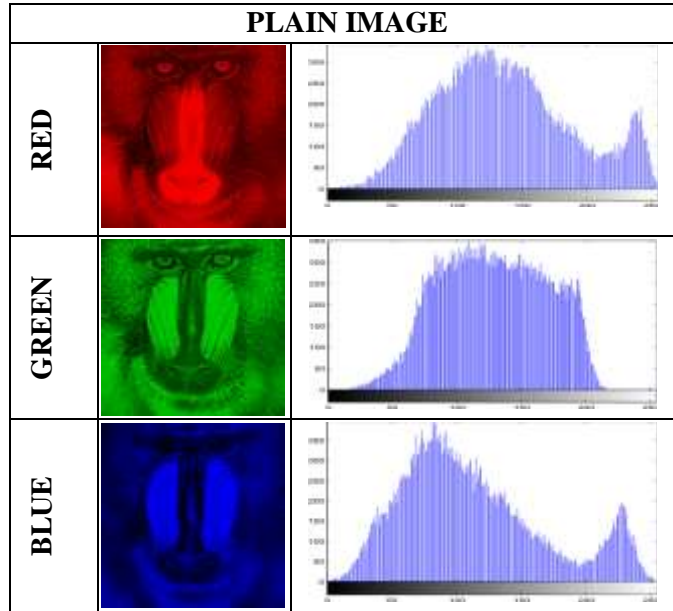


Figure 5: Histogram of the Plain Image

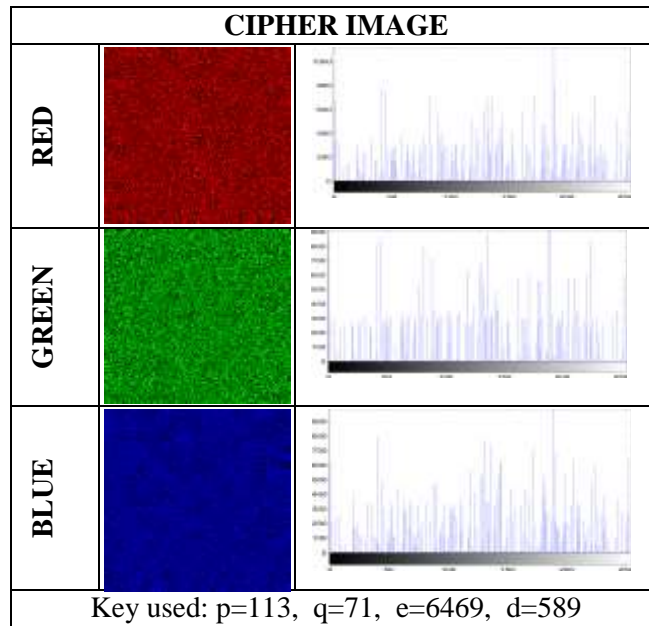


Figure 6: Histogram of the Cipher Image

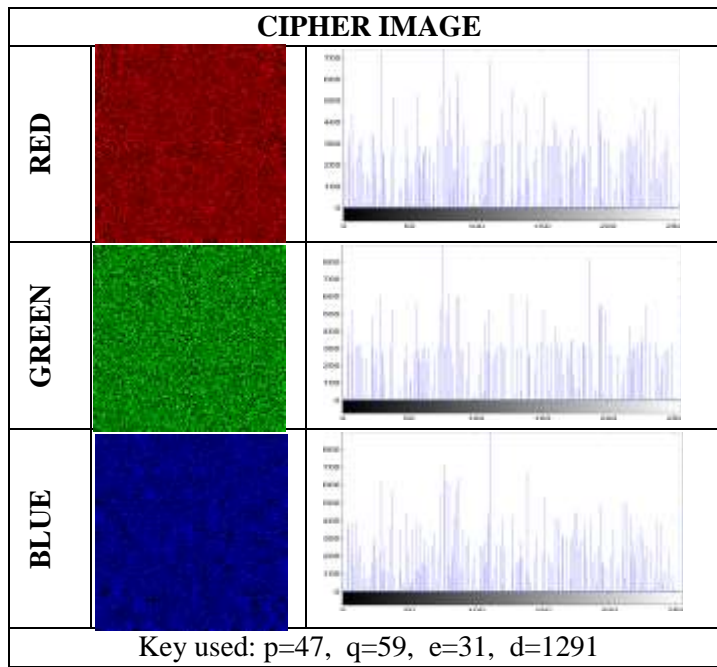


Figure 7: Histogram of the Cipher Image

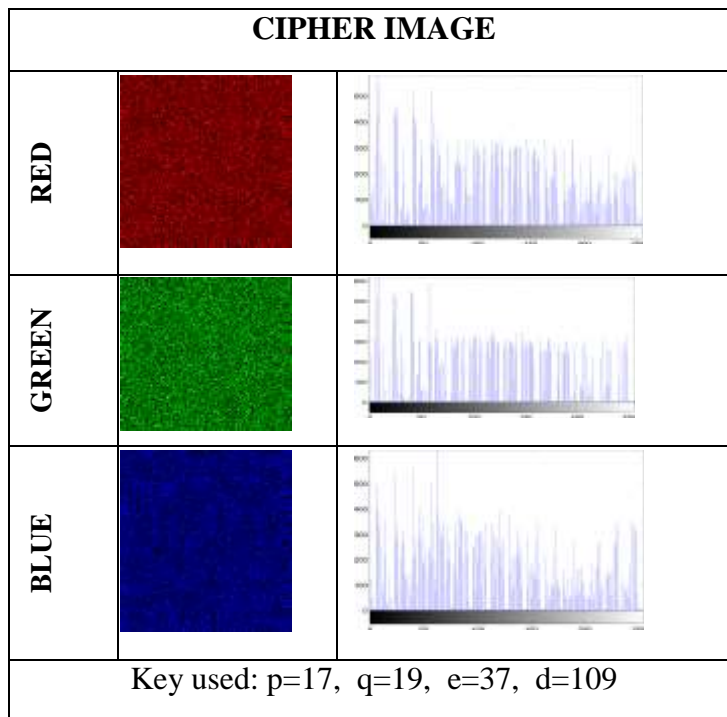


Figure 8: Histogram of the Cipher Image

Correlation Coefficient Analysis

This is one of the metric used for assessing the encryption quality of any image encryption scheme. Correlation coefficient between adjacent pixels of the cipher-image

obtained from the proposed scheme is used for the quality test. Out of the 40,000 pixels of the plain image used, only the first 4000 pixels were used in the analyses for

determining the correlation between two vertically adjacent pixels, two horizontally

adjacent pixels and two diagonally adjacent pixels in the cipher-image as well as the plain-image for comparison purposes. This correlation coefficient denoted by r_{xy} is calculated as follows:

$$E(x) = \frac{1}{L} \sum_{i=1}^L x_i, \quad D(x) = \frac{1}{L} \sum_{i=1}^L (x_i - E(x))^2, \quad \text{and} \quad cov(x,y) = \frac{1}{L} \sum_{i=1}^L (x_i - E(x))(y_i - E(y)) \quad (4)$$

where L is the number of pixels involved in the calculations. **The closer the value of r_{xy} to zero, the better the quality of the encryption algorithm is** ((Abd El-Samie *et al.*, 2014).

The correlation coefficient of the plain image is shown in Figure 9 and from the Figure, one

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (3)$$

where x and y are the values of two adjacent pixels in the cipher-image. In numerical computations, the following discrete formulas can be used:

can see that the correlation between adjacent pixels in all the three directions of the plain image in the three intensities are strongly correlated with a minimum correlation coefficient of 0.8191 in the green channel and a maximum correlation coefficient of 0.9325 in the Blue channel.

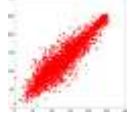
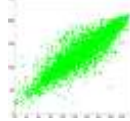
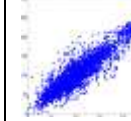
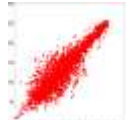
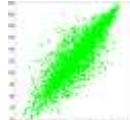
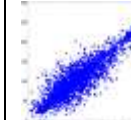
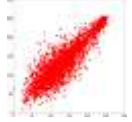

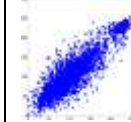
PLAIN IMAGE			
	Red Channel	Green Channel	Blue Channel
Horizontal			
r_{xy}	0.9284	0.8868	0.9325
Vertical			
r_{xy}	0.9134	0.8766	0.9259
Diagona			
r_{xy}	0.8906	0.8191	0.8950

Figure 9: Correlation between adjacent pixels of the Plain Image

However, the story is different with the cipher images shown in Figures 10 to 12 for the three different sets of keys used. In these Figures, there is almost no correlation between the adjacent pixels in all the three intensities and in all the three directions as

these can be seen clearly from their respective correlation coefficient values which are almost zero. This indicates that the proposed algorithm is effective


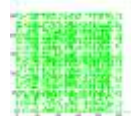
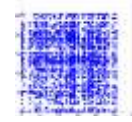
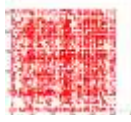
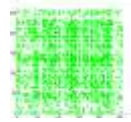

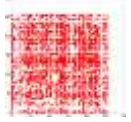
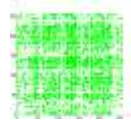

Cipher Image Obtained with the Key: p=113, q=71, e=6469, d=589			
	Red Channel	Green Channel	Blue Channel
Horizontal			
$r_{x'}_{x'}$	0.0078	0.0332	-0.0307
Vertical			
$r_{x'}_{y'}$	0.0339	0.0145	0.0177
Diagonal			
$r_{x'}$	-6.8829e-004	-0.0037	-0.0118

Figure 10: Correlation between Adjacent Pixels of the Cipher image


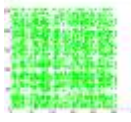
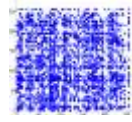


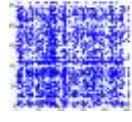
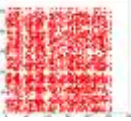
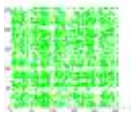
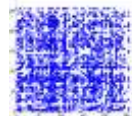
Cipher Image Obtained with the Key: p=47, q=59, e=31, d=1291			
	Red Channel	Green Channel	Blue Channel
Horizontal			
r_{xy}	0.0044	-0.0058	0.0107
Vertical			
r_{xy}	-0.0028	-0.0029	0.0242
Diagonal			
r_{xy}	-0.0188	0.0208	5.8947e-004

Figure 11: Correlation between Adjacent Pixels of the Cipher Image


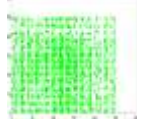
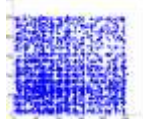

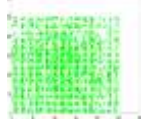


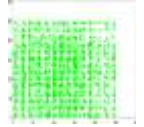

Cipher Image Obtained with the Key: p=17, q=19, e=37, d=109			
	Red Channel	Green Channel	Blue Channel
Horizontal			
r_{xy}	-0.0081	-0.0063	-0.0024
Vertical			
r_{xy}	0.0012	0.0036	-0.0027
Diagonal			
r_{xy}	-0.0149	-0.0156	-0.0158

Figure 12: Correlation between Adjacent Pixels of the Cipher Image

CONCLUSION

To have a high quality and well secured RGB image encryption algorithm, a cryptosystem was proposed that uses RSA algorithm and a 3-D chaotic system called the Shimizu-Morioka System. The 3-D chaotic system was considered for the purpose of weakening the correlation between the adjacent pixels of the plain image to obtain the shuffled image (since RSA algorithm is image dependent). The RSA algorithm was applied to the shuffled image using the set of public key to obtain the cipher image also called encrypted image. The private key was used in obtaining the decrypted image. The proposed scheme was tested on a standard test image of size 200 x 200 and stored in TIFF file format ('mandrill_colour_200.tif'). Security analysis such as Histogram uniformity analysis and Correlation coefficient analysis were performed on the results obtained from the proposed scheme. Results of the analysis obtained shows that proposed scheme is highly secured and can withstand any statistical and the brute-force attacks. It is also important to note that though RSA was primarily designed for text, it becomes very

useful in encrypting images because of the fact that one can recover the replica of the plain image when the cipher image is decrypted. That is to say that the plain image and the decrypted image are exactly the same not only to visual inspection but also in terms of pixels values when compared. This quality is highly required in securing sensitive medical imaging especially, the Optical Coherence Tomographic (OCT) imaging that could provide surgeons with a colour-coded map of a patient's brain showing which areas are and are not cancer. This innovation is expected to make surgical removal of tumours in the brain safer and more effective. As doctors rub minds on patient's information which is highly confidential, this proposed scheme is ideal for such online communications.

REFERENCES

- Abd El-Samie, E. F., Ahmed, H. E. H., Elashry, F. I., Shahieen, H. M., Faragallah, S.O., El-Rabaie, M. E., and Alshebeili, A. S.(2014), Image Encryption- A Communication Perspective. 1st Ed., CRC Press, London, pp.: 1-86.
- Abraham L. and Daniel N. (2013), "Secure Image Encryption Algorithms: A Review", *International Journal of Scientific and Technology Research*, Vol. 2, No. 4, pp.: 186 – 189.
- Bala I. V. (2020), "Fast Medical Image Security Using Color Channel Encryption", *Engineering, Technology and Techniques-Brazilian Archives of Biology and Technology*, <https://doi.org/10.1590/1678-4324-2020180473>
- Ballare, M., and Rogaway, P. (2005)., Introduction to Modern Cryptography-Principles and Protocols, 1st Ed., CRC Press Book, California, USA, pp.: 1-35.
- Chandel, J. S., and Patel, P. (2013), "A Review: Image Encryption with RSA and RGB Randomized Histograms", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 11, pp.:4397 – 4401.
- Delfs, H., and Knebl, H. (2007), "Introduction to Cryptography-Principles and Applications", 2nd Ed., Springer Berlin Heidelberg, New York, USA, pp.: 1-65.
- Diffie, W., and Hellman, M. E. (1976), "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp.: 644-654.
- Gafsi M., Abbassi N., Hajjaji M. A., Malek J., and Abdullatif M. (2020), "Improved Chaos-Based Cryptosystem for Medical Image Encryption and Decryption", *Scientific Programming*, Article ID 6612390, 22p.
- Goldreich, O. (2004), Foundations of Cryptography-Basic Techniques, 2nd Ed., Cambridge University Press, UK, pp.: 1-63.
- Hankerson, D., Menezes, A. and Vanstone, S. (2004), Guide to Elliptic Curve Cryptography, Springer-Verlag Inc., New York, USA, pp.: 10-15.
- Hoffstein, J., Pipher, J. and Silverman, J. H. (2008), An Introduction to Mathematical Cryptography, 1st Ed., Springer Science + Business Media, New York, USA, pp.: 10-65.
- Kaliski, B. (2012), The Mathematics of the RSA Public-key Cryptosystem. <http://www.mathaware.org/mam/06/Kaliski.pdf>.
- Kokarev, L., and Makraduli, J. (2005), "Public-Key Encryption based on Chebyshev Polynomials", *Circuits, Systems and Signal Processin*, vol. 24, No. 5, pp.: 497-517.
- Kumar, A., and Sharma, R. (2013), "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, No. 7, pp.: 363 – 372.
- Köse, E., (2015), Controller Design by Using Sliding Mode and Passive Control Methods for Continuous Time Non-linear Shimizu- Morioka Chaotic System. *International Journal of Engineering Innovation and Research*, Vol. 4, No. 6, pp.: 895-902.
- Mishkovski, I. and Kocarev, L., (2011), Chaos-Based Public-key Cryptography, Springer-Verlag Berlin Heidelberg, SCI 354, pp.: 27-65.,
- Mishra, M., and Mankar, V. H. (2011), "Chaotic Encryption Scheme Using 1-D Chaotic Map", *International Journal of Communications, Network and System Sciences*, Vol. 4, No.10, pp.: 452 – 455.
- Monjula G. Mohan H. S. (2020), "A Secure Framework For Medical Image Encryption Using Enhanced AES Algorithm", *International Journal of Scientific & Technology Research*, Vol. 9, No. 2, pp.:3837-3841.
- Ramadan, N., Ahmed, H. H., Elkhamy, S. E., Abd Abd El- Samie, F. E., (2016), "Chaos-Based Image Encryption Using an Improved Quadratic Chaotic Map",

- American Journal of Signal Processing*, Vol. 6, No. 1, pp.: 1-13.
- Salih H. R. (2011), "The Stability Analysis of the Shimizu-Morioka System with Hopf Bifurcation", *Journal of Kirkuk University- Scientific Studies*, Vol. 6, No. 2, pp.: 184-200.
- Sathishkumar G. A., Bagan K. B., and Sriraam N. (2011), "Image Encryption Based on Diffusion and Multiple Chaotic Maps", *International Journal of Network Security and its Applications*, Vol. 3, No. 2, pp.: 181 – 194.
- Shankar K. (2018), "An Optimal RSA Encryption Algorithm for Secret Images", *International Journal of Pure and Applied Mathematics*, Vol. 118, No. 20, pp.:2491-2500.
- Shil'nikov A. L., (1991), "Bifurcation and Chaos in the Shimizu- Morioka System", *Selecta Mathematica Sovietica*, Vol. 10, No. 2, pp.: 105-117.
- Shimizu T. and Morioka N. (1980), "On the Bifurcation of a Symmetric Limit Cycle to an Asymmetric one in a Simple Model", *Physics Letters A*, 76:201-204.
- Srushti G., and Ravi G. (2022), "Digital Image Encryption using RSA and Linear Feedback Shift Register(LFSR)", *International Journal of Engineering Science Technologies*, Vol. 6, No. 4, pp.:36-52.
- Stinson D. R. (2006), *Cryptography Theory and Practice*, 3rd Ed., Chap-man & Hall/CRC. New York, pp.: 1-186.
- Taki El-Deen, A. E., El-Badawy, E. A., and Gobran, S. N. (2014), "Digital Image Encryption Based on RSA Algorithm", *Journal of Electronics and Communications Engineering*, Vol. 9, No.1, pp.: 69-73.
- Xue X., Jin H., Zhou D., and Zhou C. (2021),"Medical Image Protection Algorithm Based on Deoxyribonucleic Acid Chain of Dynamic Length", *Frontiers in Genetics*, Vol. 12-2021 /<https://doi.org/103389/fgene.2021.654663>
- Yakubu H. J. and Aboiyar T. (2018), "A Chaos Based Image Encryption Algorithm using Shimizu-Morioka System", *International Journal of Communication and Computer Technologies*, Vol. 6, No. 1, pp.: 07-11.
- Yakubu H. J., Aboiyar T., and Zirra P. B. (2018), "An improved RSA image encryption algorithm using 1-D logistic map", *International Journal of Communication and Computer Technologies*, Vol. 6, No. 1, pp.: 01-6.
- Ye R. (2013), "A Highly Secure Image Encryption Scheme Using Compound Chaotic Maps", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 4, No. 6, pp.: 532 – 544.