

## A new method to encrypt images based on triple encryption methods

Raghda Sattar Jabbar <sup>1,\*</sup>, Israa Shihab Ahmed <sup>2</sup> and Saadi Mohammed Saadi <sup>3</sup>

<sup>1</sup> Department of Quality Assurance and University Performance, Mustansiriyah University, Baghdad, Iraq.

<sup>2</sup> Informatics Institute for Postgraduate studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq.

<sup>3</sup> Ministry of Education, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2023, 14(03), 121–130

Publication history: Received on 04 February 2023; revised on 20 March 2023; accepted on 23 March 2023

Article DOI: <https://doi.org/10.30574/gjeta.2023.14.3.0053>

### Abstract

Information security has become a significant concern, and the protection of images transmitted over the Internet is vital, which requires a high level of security. The information in these images has been used without permission and, therefore, will have serious consequences, and the images can be secured in several ways. Data encryption and decryption have recently received much attention and development. Strong encryption and decryption is required, which is incredibly difficult to crack. In this paper, an encryption environment consisting of triple encryption methods was used to create a new encryption system, which depends on several stages, including the step involving the process of creating the key using the RSA algorithm and then using this generated key with the same RSA algorithm to encrypt the image, in the second stage using a method "zig\_zag" in order to encrypt the image again based on the encrypted pictures generated from the first stage, in the third stage, encrypt the image generated from the second stage using the 2D CAT method. As for the setting of retrieval of the original photos using triple decryption methods in a reverse way, the idea was returned without losing its data. The image quality was excellent.

**Keywords:** RSA Algorithm; 2D CAT MAP; Encryption; ZIG-ZAG; Decryption

### 1. Introduction

By converting sensitive information into an incoherent format (encryption) that the authorized recipient can only decode, encryption enables secure communication and protects that information (decryption). Unauthorized access is mitigated through various mathematical compromises, including cryptography algorithms [1, 2, 3]. Scrambling encryption, an essential part of picture security, is now a widely investigated image steganography technology. For example, each encryption algorithm has its benefits and drawbacks: Rubik's cube matrix transformation, zig\_zag transform, Arnold transform, Hilbert curve transformation, and son. Take, for example, the obfuscation cipher. While just the pixel positions and values are modified, an attacker can still restore it in an all-out attack that doesn't care how long it takes if he tries to decrypt the obfuscated image [4]. As a result, rather than using only one sort of scrambling technique, multiple distinct scrambling algorithms or other cryptographic algorithms should be mixed to encrypt an image. A new picture encoding approach based on a combination of the d-zigzag scrambling algorithm, the 2D CAT map, and the RSA algorithm has been developed for this purpose. RSA is an asymmetric block cipher based on number theory (public key). Its safety depends on the difficulty of many prime factors, a well-known mathematical problem with no solution [5].

### 2. Algorithms overview

In this part, the most important algorithms used in the proposed method are explained.

\* Corresponding author: Raghda Sattar Jabbar

### 2.1. 2D CAT MAP Method

In the field of ergodic theory, V.I. Arnold was the first to present a 2D Cat map [6,7]. The cat map changes the arrangement of pixels in an original image by replacing the pixel points' locations with new coordinates. After numerous rounds, the relationship between adjacent pixels is totally broken, and the image seems distorted and meaningless. However, after many iterations, it will eventually return the original image, showing that the Cat map is periodic. An array relation,  $P = (x, y) | x, y = 1, 2, 3, \dots, N$ , can be utilized in encryption and is written as follows:

$$[x' \ y'] = [x \ y] \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \pmod{N} \dots\dots\dots(1)$$

The inverse array relation for decrypting a 2D Cat map is as follows:

$$[x \ y] = [x' \ y'] \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \pmod{N} \dots\dots\dots(2)$$

The pixels in the image created by the previous decoding strategy must be modified [8].

### 2.2. Zig\_zag scrambling Method

The zig\_zag pattern [3,9,10] refers to the matrix structure of the N2 integers that increases anti-diagonally along the arrays. Figure 1 depicts the various types of zig\_zag designs. A parallel zig\_zag pattern is a motive wave that goes on a similar trend (see fig.1) (a). The diagonal zig\_zag pattern is a motive wave that goes on a sloping trend (see fig.1). (b). The proposed approach is based on a similar zig\_zag encryption pattern (see Figure 1). (a).

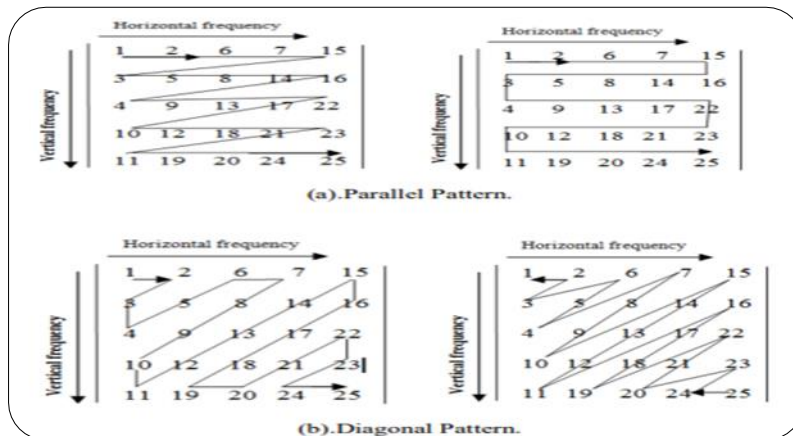


Figure 1 Various Zigzag Patterns

### 2.3. RSA Algorithm

A popular public key cryptography algorithm is the RSA. The first asymmetric algorithm is still widely used today. Rivets, Shamir, and Adelman, are the three mathematicians who developed RSA. This algorithm can be used for data encryption, key exchange, and digital signatures in many software packages. RSA utilizes a variable-sized encryption block and a varying key in this method. [11,12]

#### 2.3.1. \* Key generation

RSA employs two distinct key types (A public key and a private key). Everybody has access to the public key, which is used to encrypt messages. Only the secret key can quickly decrypt messages encrypted with the public key. [13,14]. The steps below are used to create keys for the RSA algorithm:

**Key generation**

Select $p, q$	$p$ and $q$ both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer $e$	$\text{gcd}(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate $d$	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

\*RSA encryption and decryption process

**Encryption**

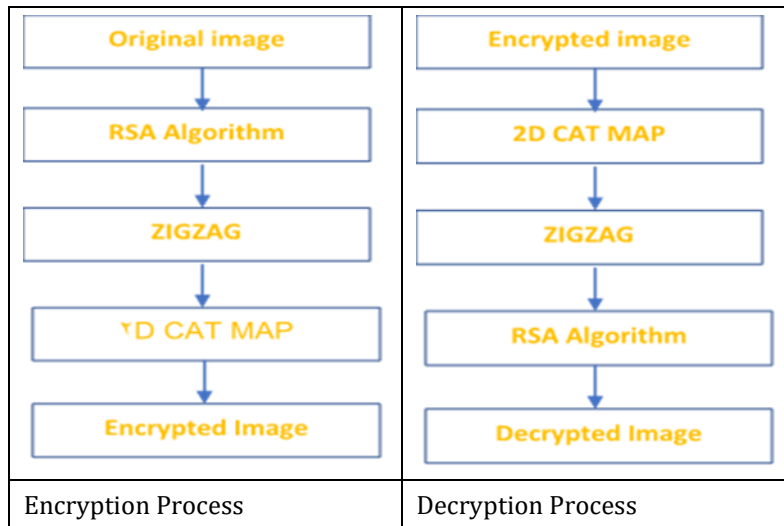
Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

**Decryption**

Ciphertext	$C$
Plaintext	$M = C^d \pmod{n}$

**3. The proposed method's general outline**

In this part, the architecture of the proposed method will be explained, which is the methodological framework that represents how to encode the color image based on the optimized algorithm and how to retrieve it, as shown in figure 2, which represents a detailed diagram of the proposed method.



**Figure 2** Suggested approach's general layout

#### 4. Implementation of the proposed method

This section will go over the actions taken to implement the proposed technique, broken down into three stages and depicted in Figure 3 below.

<b>Encrypt process</b>	<b>INPUT: Original image</b> <b>OUTPUT: Encrypted image</b>
Step1: at the sender side, use the RSA algorithm to generate key. Step2: upload the original image Step3: image encrypted based on RSA Algorithm Step4: image encrypted based on ZIGZAG method. STEP5: Using the 2D CAT technique, encrypt the final image.	
<b>Decrypt process</b>	<b>INPUT: Encrypted image</b> <b>OUTPUT: Original image</b>
Step1: at the recipient side, upload the encrypted image Step2: image decrypted based on 2D CAT method. Step2: image decrypted based on ZIGZAG method. STEP 3: The result image will be decrypted with the RSA Algorithm and the RSA Decryption Key (private key).	

Figure 3 Method Implementation Steps Proposed

##### 4.1. The Encryption processes

When encrypting an image, we first change its size to 200×200, convert it into an array, use the encryption key generated by the RSA algorithm, and use the following equation for encryption.:

$$C = Me \text{ mod } n$$

Then we use the resulting image as an input to the ZIG\_ZAG encoding method after converting the image into RGB arrays, as shown in figure 4.



Figure 4 Zigzag process

And the last step, we use the resulting image as an input to the 2D CAT method after converting the image into RGB arrays.

##### 4.2. The Decryption Process

This part indicates reversing the encoding process, but requires knowledge and the decryption key to retrieve the original image. As a result, an attacker will have difficulty detecting or guessing the key and the change in pixel positions caused by 2D CAT MAP and Zig zag methods.

### 5. The Practical Aspect of the Proposed Method

This part will clarify the implementation of the proposed method in the application according to the steps described in figure 10, which shows how to encode and retrieve the original image. Figure 5 depicts the interface for generating keys using the RSA algorithm:

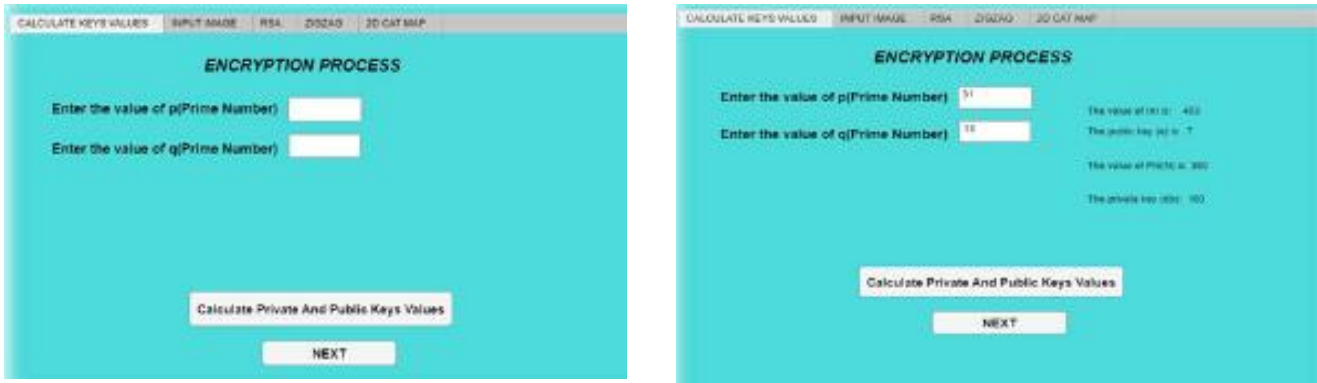


Figure 5 The suggested method-key generation interface

After that, as shown in Figure 6, click "input photo" to add a picture.



Figure 6 upload image

The original image is uploaded at this stage, after which you must click next to begin the encryption process: The first algorithm is the RSA algorithm; select RSA encryption to encrypt the input image, then select Next, as illustrated in Figure 7.



Figure 7 Encryption process using the RSA algorithm

Then, as shown in Figure 8, click next to encrypt the output image using the zig\_zag method.



Figure 8 Encryption process using the zig\_zag method

Then click next to encrypt the output image by the 2DCAT MAP method, as shown in figure 9



Figure 9 Encryption process using the 2DCAT MAP method.

Click the Decryption process at the receiving side image to decrypt the image, then uploads the encrypted image to decode the image using 2D CAT MAP, as shown in figure 10.



Figure 10 Decryption process using the 2DCAT MAP method.

then, as seen in figure 11, the image will be decrypted using zig\_zag method.



Figure 11 Decryption process using the zig\_zag method

Finally, as shown in Figure 12, the image will be decrypted using the RSA algorithm and a private key.



Figure 12 Decryption process using RSA algorithm

## 6. Results and discussion

In this paper, we used two scales to assess the quality of cryptographic and security analysis methods (statistical and differential attacks). The first is differential measures, which employ two standard measures, NPCR and UACI. Any modification to the conventional image will significantly impact how well the encrypted image can resist a differential attack. While UACI calculates the average intensity of distinctions between two images, NPCR measures the pixel value variance. The algorithm's sensitivity should always be reflected by NPCR values in the 99% band and UACI values of 33%. [15,16].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad \dots\dots\dots(3)$$




$$UACI = \frac{1}{M \times N} \left[ \sum_{i,j} \frac{D(i,j)}{255} \right] \times 100\% \quad \dots\dots\dots(4)$$

Values for C1(i, j) and C2(i, j) grid pixels (i,j).

D(i, j) is determined by C1(i, j) and C2(i, j). D(i, j) equals 1 if C1(i, j) and C2(i, j) are equal, else it equals 0. Differential assaults are worthless because the cipher picture might diverge greatly from the original image, even when only

marginally changed. Ideal encryption techniques favor higher NPCR values. The UACI values must fall between 33% and 35%. [15].

**Table 1** Presents the NPCR and UACI values for the three images obtained using the proposed method

Image	NPCR method values			UACI method values		
	Red	Green	Blue	Red	Green	Blue
	99.4%	99.6%	99.6%	22%	32%	27%
	99.5%	99.5%	99.8%	25%	30%	44%
	99.7%	99.8%	99.3%	37%	36%	24%

The second metric is the correlation coefficient. The analysis evaluates the image's relationship to its encryption variables. It demonstrates the proposed encryption algorithm's resistance to statistical attacks. As a result, the encrypted image must differ significantly from the original [10]. The equations are used to calculate the correlation coefficient. [15,16]:

$$C.C = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}}, \dots\dots\dots(5)$$

C.C: correlation coefficient




$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \dots\dots\dots(6)$$

x and y: the gray-scale pixel values of the unencrypted and encrypted images. The original image's correlation coefficient is often high (nearly one). When the correlation coefficient of the encrypted image is lower, the method operates more effectively. [15].

**Table 2** Displays the results of the C.C values of the three images calculated using the proposed method

Image	C.C
-------	-----



	0.076
	0.043
	0.010

The correlation coefficient can be seen in the table. Image values are shallow.

## 7. Conclusion

In terms of communication security, the encryption algorithm is crucial. We encrypt the image with RSA, apply Zig\_zag transformation, and finally use the 2D CAT MAP method, which is simple to implement and has low time complexity. It may also successfully shift data's initial position and is often used to process digital photographs. In addition, it can modify the suggested method to encompass multiple media such as video, audio, and so on.

## Compliance with ethical standards

### *Acknowledgments*

The author would like to thank Mustansiriyah University ([www.uomustansiriyah.edu.iq](http://www.uomustansiriyah.edu.iq)), Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics (<https://iips.edu.iq/>), and the Ministry of Education - Gifted Care Authority ([www.https://epedu.gov.iq/](http://www.https://epedu.gov.iq/)), Baghdad - Iraq for its support in the present this work.

### *Disclosure of conflict of interest*

All authors declare that they have no conflict of interest.

## References

- [1] N. Kumar and P. Chaudhary, "Performance evaluation of encryption/decryption mechanisms to enhance data security," *Indian Journal of Science and Technology*, vol. 9, no. 20, 2016.
- [2] M. Ebrahim, S. Khan, and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," *International Journal of Computer Applications*, vol. 61, no. 20, pp. 12–19, 2013.
- [3] Disina, A. H., Pindar, Z. A., & Jamel, S., "Enhanced Caesar Cipher to Exclude Repetition and Withstand Frequency Cryptanalysis," In *Proceedings of the International Conference on Information Science and Security (ICISS)*, 2015.
- [4] Xu Xiaolin, Feng Jiali: Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector, 2010 IEEE International Conference on Granular Computing.
- [5] A. Murugan, R. Thilagavathy: Triple Encryption Scheme with Parallel Zigzag Pattern for Cloud Data Storage Scheme, *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 13, Number 22 (2018).

- [6] Nivetha,A ,Preethy Mary S sSantosh kumar J: Modified RSA Encryption Algorithm using Four Keys, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 (2015)
- [7] Swapnil Shrivastava: A Novel 2D Cat Map based Fast Data Encryption Scheme, International Journal of Electronics and Communication Engineering. ISSN 0974-2166 Volume 4, Number 2 (2011).
- [8] Enas Yahya Abdullah, Nidhal Khedhair El abbadi, Ahmad Abbas mohammed Aladdilee:Digital RGB Image Encryption Based On 2D Cat Map and Shadow Numbers,( 2018)
- [9] HAO GAO AND XINGYUAN WANG : Chaotic Image Encryption Algorithm Based on Zigzag Transform With Bidirectional Crossover From Random Position,( 2021)
- [10] Mu. Annalakshmi, Mu. Annalakshmi: Zigzag Ciphers: A Novel Transposition Method, International Journal of Computer Applications (0975 – 8887) International Conference on Computing and information Technology (IC2IT-2013).
- [11] Ankit Gupta , Namita Tiwari ,Bhopal Meenu Chawla, Madhu Shandilya:An Image Encryption using Block based Transformation and Bit Rotation Technique, International Journal of Computer , Volume 98– No.6, (2014).
- [12] Haitao, W., Penghui, L.: An improved security algorithm based on RSA. Measure. Control Technol. 38(10), 104–107 (2019)
- [13] Haiyan, B., Cailin, L.: Homomorphic encryption of privacy data set based on improved RSA algorithm. J. Terahertz Sci. Electron. Inf. Technol. 18(05), 929–933 (2020)
- [14] Haifeng, L., Yang, L., Xingliang, L.: A QR code encryption technique combining optimized AES and RSA algorithms. J. Shaanxi Univ. Sci. Technol. 37(6), 153–159 (2019)
- [15] M. Bala Kumar , P. Karthikka , N. Dhivya ,T. Gopalakrishnan: A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, ( 2014)
- [16] Ran, B.; Zhang, T.; Wang, L.;Liu, S.; Zhou, X. ,” Image Security Based on Three-Dimensional Chaotic System and Random Dynamic Selection.”, Entropy 2022, 24, 958.<https://doi.org/10.3390/e24070958>.