

Triple Encryption of Images based on RC4, Zigzag, and Elliptic Curve Algorithms for Enhanced Security

Raghda Sattar Jabbar

Department of Quality Assurance and University Performance, Mustansiriyah University, Baghdad-Iraq

ARTICLE INFO

Article History:

Accepted: 05 March 2023

Published: 20 March 2023

Publication Issue

Volume 10, Issue 2

March-April-2023

Page Number

93-100

ABSTRACT

The security of digital images is of paramount importance in today's digital world. Encryption is a technique used to secure digital images from unauthorized access. The encryption technique transforms the original image into a scrambled form, which is unreadable to anyone without the proper decryption key. Several encryption techniques have been proposed to secure digital images, including DES, AES, RSA, and ECC. These methods, however, are susceptible to side-channel and brute-force attacks. Hence, new encryption methods that offer more security are required. The new multi-encryption algorithm for secure digital image encryption is presented in this research. The suggested approach combines the RC4, Zigzag transformation, and Elliptic Curve Cryptography (ECC) algorithms to increase the security of picture encryption. Data is encrypted using the RC4 stream cipher, image data is scrambled using the Zigzag method, and the key used in the transformation is encrypted using the ECC technique. The proposed algorithm was tested using several standard metrics, and the results show that it outperforms existing encryption techniques in terms of security.

Keywords : Security, RC4, Zigzag transformation, and Elliptic Curve Cryptography

I. INTRODUCTION

Information security relies heavily on cryptography techniques to safeguard the secrecy, integrity, and validity of data. Data is encrypted and decrypted using cryptography methods to establish a safe channel of communication between two parties [1].

Cryptography has a long history dating back to ancient civilizations, where secret codes and ciphers were used to protect sensitive messages. Today, cryptography has become increasingly important with the widespread use of computers and the internet. Symmetric key and public key cryptography are the two basic categories into which cryptography algorithms fall. Public key cryptography employs two

separate keys, one for encryption and the other for decryption, whereas symmetric key cryptography only uses one key [2].

The Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Blowfish are examples of symmetric key encryption methods. These algorithms are generally faster and more efficient than public key cryptography algorithms, but they are not suitable for scenarios where secure communication between two parties who have never interacted before is required. As one key can be made public while the other is kept private, public key cryptography techniques like the Rivest-Shamir-Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC) enable secure communication between parties that have never interacted before. These algorithms, however, typically take longer and use more resources than symmetric key techniques [3,4]. Cryptography algorithms must be designed to be resistant to attacks from malicious actors. Attackers can use various methods, such as brute force attacks and cryptanalysis, to try to break the encryption and access the underlying data. Therefore, cryptography algorithms must undergo rigorous testing and analysis to ensure their security. In recent years, there has been growing interest in post-quantum cryptography, which aims to develop cryptography algorithms that can resist attacks from quantum computers. Quantum computers have the potential to break many of the currently used cryptography algorithms, and therefore, there is a need for new algorithms that can resist attacks from quantum computers [5]. The remainder of this paper is structured as follows: An overview of the proposed schemes' algorithms is provided in Section 2, the proposed technique is implemented in Section 3, its practical application is covered in Section 4, and experimental findings are presented in Section 5. Lastly, section 6 presents the conclusions.

II. OVERVIEW OF ALGORITHM

To safeguard the encryption of digital photos, a new Triple-encryption technique is proposed in this study. To improve image encryption security, the proposed algorithm combines RC4, zigzag transformation, and elliptic curve coding (ECC) algorithms.

A. Rivest Cipher 4 (RC4)

Data encryption is frequently performed using the symmetric stream cipher known as the RC4 technique. Ron Rivest created it in 1987; other names for it include "Rivest Cipher 4" and "ARCFOUR" (Alleged RC4) [6]. Here is how the RC4 algorithm operates:

1. **Key Setup:** To create a 256-byte state vector S , the technique uses a variable-length key (between 1 and 256 bytes). The state vector S is initialized with values from 0 to 255 in increasing order.
2. **Key Scheduling:** Using the key, the method creates a keystream using a pseudo-random generation algorithm (PRGA). For each byte of the keystream, the following processes are repeated to create the keystream:
 - a. The state vector S is updated based on the key using a swapping algorithm.
 - b. The algorithm generates a pseudo-random byte by selecting a byte from the state vector S [7].
3. **Encryption:** To encrypt data, the algorithm XORs each byte of the plaintext with the corresponding byte of the keystream. The resulting bytes are the cipher text [8].
4. **Decryption:** To decrypt the cipher text, the algorithm XORs each byte of the cipher text with the corresponding byte of the keystream. The resulting bytes are the plaintext [8].

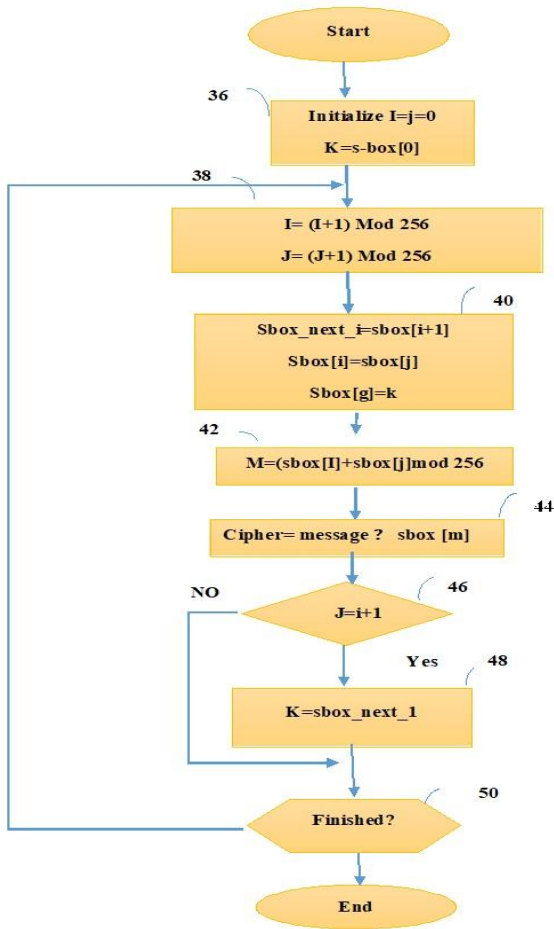


Figure 1:RC4 Algorithm [8]

The RC4 technique has the benefit of being quick and easy to use, making it effective for encrypting huge volumes of data, especially when using unreliable or low-bandwidth communication routes. However, RC4 has some weaknesses that have been discovered over the years, and it is no longer recommended for new applications. In particular, RC4 is vulnerable to many attacks, including the "Fluhrer-Mantin-Shamir" (FMS) attack and the "Key Reconstruction" attack [7], [8].

2.3. The Zigzag Algorithm [9,10,11,12]

The Zigzag algorithm is a technique used to reorder the image data in a way that reduces the redundancy in the data. This technique is commonly used in image compression. The Zigzag method reorders the image data by going from the top-left corner to the bottom-right corner in a zigzag pattern.

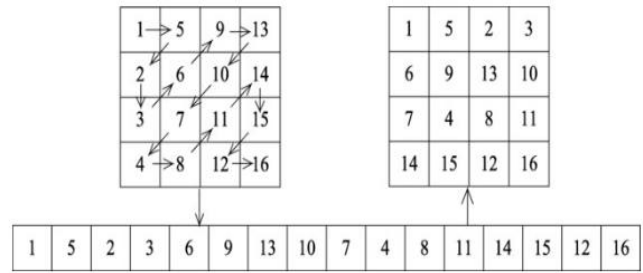


Figure 2: Zigzag Transform [13]

B. The Elliptic Curve Algorithm

Using elliptic curves over finite fields, elliptic curve cryptography is a technique for public-key encryption. First introduced in 1985 by Victor Miller and Neal Koblitz. The fundamental building block of ECC is the well-known NP-Hard issue called the Elliptic Curve Discrete Logarithm problem. According to the equation, an elliptic curve exists [14].

$$y^2 + xy = x^3 + ax + b \dots \dots \dots (1)$$

can also be used in the form:

$$y^2 = x^3 + ax + b \dots \dots \dots (2)$$

Public and private keys are generated for encryption and decryption using the mathematical features of elliptic curves. Because it offers a high level of security with little processing expense, the Elliptic Curve technique is frequently employed in mobile devices [14].

III. IMPLEMENTING THE PROPOSED METHOD

The triple-encryption algorithm for picture encryption combines the RC4, Zigzag, and Elliptic Curve methods to offer a high level of security. The following steps are part of the encryption process:

Step1: is to transform the image into a matrix of pixel values.

Step 2: Use the RC4 algorithm to encrypt the image.

Step 3: Apply the Zigzag algorithm to the output image.

Step 4: Use the Elliptic Curve technique to create the public and private keys and encrypt the RC4 and zigzag-encrypted image.

To decrypt images using the Triple-encryption algorithm, you can follow these steps:

Step 1: Start with the encrypted image data that you want to decrypt.

Step 2: Use the inverse Elliptic Curve algorithm on the encrypted image. This will produce a decrypted image, which may still be in a different format than the original image.

Step 3: Apply the inverse ZIGZAG transform on the decrypted image to convert it back into a format that can be understood by image-viewing software.

Step 4: Finally, apply the inverse RC4 algorithm on the result of the previous step to fully decrypt the image.

IV. The Suggested Method's Practical Aspect

This section will cover how the suggested approach for encrypting and decrypting digital photographs is put into practice. The interface used to generate the key and upload the input image will be demonstrated, along with a thorough explanation of the implementation procedures.

Step 1: Upload the original image. Figure 3 depicts the uploading interface for the original image.

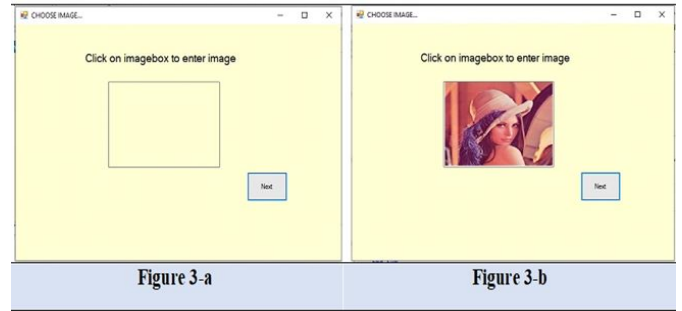


Figure 3 The Uploading Interface for the Original Image.

Step 2: Encrypt the input image using the RC4 algorithm.

After the original image has been uploaded, the RC4 algorithm is utilized to encrypt it. Figure 4 displays the RC4 algorithm's encryption interface.

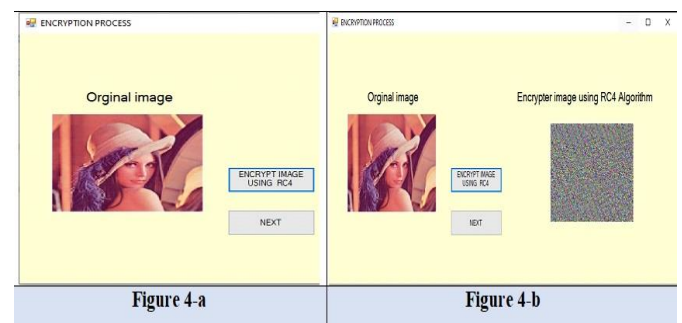


Figure 4: Interface for the RC4 Algorithm's Encryption

Step 3: Encrypt the output of the RC4 using the Zigzag algorithm.

The Zigzag technique is used to further encrypt the image after it has been encrypted using the RC4 algorithm. The Zigzag encryption interface is depicted in Figure 5.

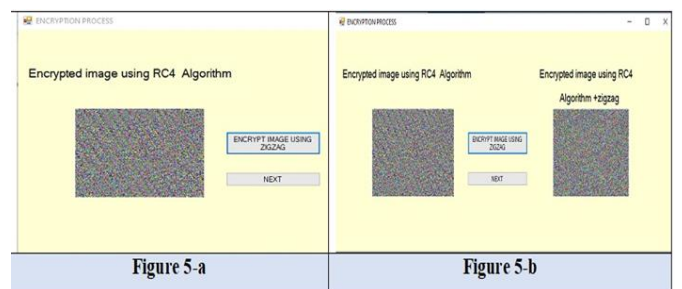


Figure 5 The Zigzag Encryption Interface.

Step 4: Encrypt the Zigzag algorithm output with the Elliptic curve algorithm.

Finally, the ECC algorithm is used to encrypt the output of the Zigzag algorithm. The interface used for the Elliptic curve algorithm. Once these steps are finished, the encrypted image will result, as illustrated in Figure 6.

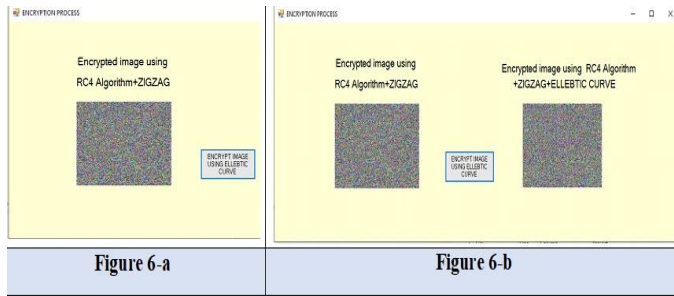


Figure 6. Final encryption based on triple encryption algorithms

The encryption process is followed by its opposite, or decryption. The following steps are involved in image decryption:

Step 1: Upload the encrypted image. Figure 7 depicts the upload interface for the encrypted image.

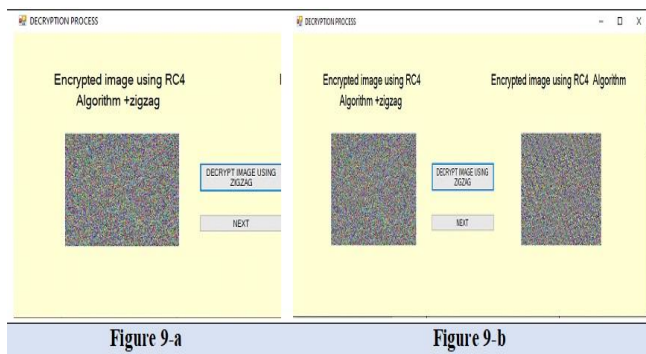


Figure 7. Upload the encrypted image

Step 2: Decrypt the encrypted image using the RC4 decryption key.

After the encrypted image has been uploaded, the RC4 decryption key is utilized to decrypt it. Figure 8 displays the RC4 decryption interface.

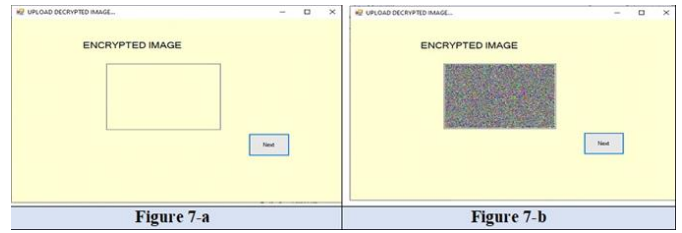


Figure 8. The Interface for RC4 Decryption

Step 3: Decrypt the output of the RC4 decryption using the Zigzag algorithm.

After decrypting the image using the RC4 decryption, the Zigzag algorithm is used to decrypt the image. The interface used for decryption is shown in Figure 9.

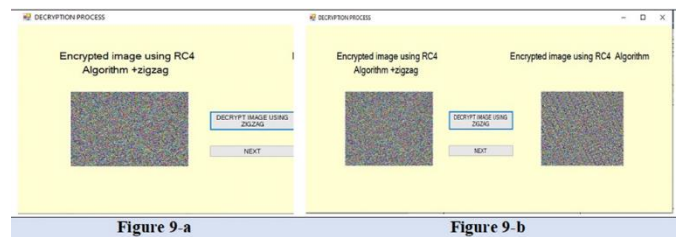


Figure 9. The interface used decryption Using Zigzag Algorithm

Step 4: Using the ECC algorithm, encrypt the output of the Zigzag decryption. Finally, the Zigzag decryption output is decrypted using the Elliptic curve technique. Figure 10 shows how the interface employed decryption.

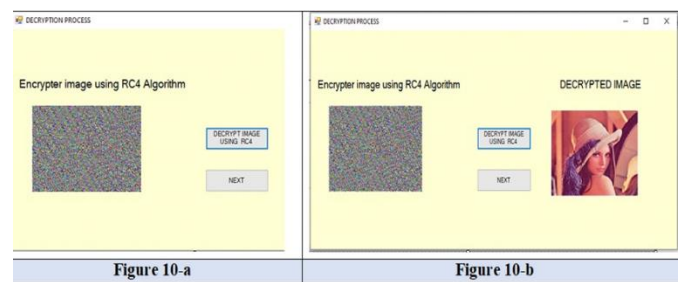


Figure 10. Decryption based on triple encryption methods.

V. Experimentation Results

I experimented with several reference images to see how well the suggested approach worked. The photographs were encrypted using the suggested strategy, and the suggested technique was also utilized

to decrypt the encrypted pictures. The original photographs and the decrypted versions were contrasted to determine how effectively the encryption functioned. The effectiveness of the suggested technique was evaluated using the correlation coefficient and NPCR.




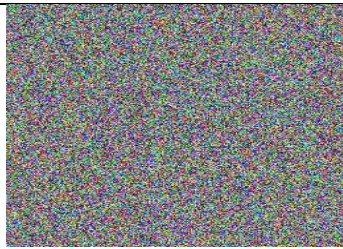


C. Correlation Coefficient

The encryption efficacy of the proposed approach was evaluated by determining the correlation coefficient between the original image and the encrypted image. It calculates how similar the two photos are. A lesser amount of encryption is indicated by a higher correlation coefficient, which also suggests a higher degree of resemblance between the images [15].

NPCR

NPCR, which stands for "Normalized Pixel Change Rate," is a metric used to compare two photographs. It is frequently used to assess how well digital picture encryption methods work. The percentage of pixels that differ between the two photos is obtained by comparing each pixel in the two images to determine the NPCR. The result is then normalized by dividing it by the total number of pixels in the image. The security of an image can be strengthened if the encryption approach is successful in changing the pixel values, as evidenced by a high NPCR value. The results of the proposed method's correlation coefficient and NPCR are displayed in the following table 1:

Table 1. Encryption Quality Measures

No.	Original image	NPCR	C.C	Encrypted image
1		0.9923	0.034	
2		0.9899	0.003	
3		0.9912	0.041	

The findings of the studies show that the proposed technology provides dependable image encryption.

1. The correlation coefficient between the original image and the encrypted image is nearly zero, indicating a high level of encryption. The results show that the proposed approach provides high encryption quality.
2. NPCR accounts for approximately 99% of the variance between the original and encrypted images. The outcomes also demonstrate that the suggested approach offers good encryption quality.

II. CONCLUSION

I've suggested a brand-new Triple-encryption technique for the safe encryption of digital photos in this work. The suggested approach combines Elliptic Curve Cryptography (ECC), Zigzag transformation, and RC4 algorithms to increase the security of encrypted images. Digital photographs can be protected from unauthorized usage by combining these algorithms with other security measures.

III. ACKNOWLEDGMENT

The author would like to thank Mustansiriyah University ([www. uomustansiriyah.edu.iq](http://www.uomustansiriyah.edu.iq)) in Baghdad - Iraq for its support in the present work.

IV. REFERENCES

- [1]. Baha Eldin Hamouda Hassan Hamouda, "Comparative Study of Different Cryptographic Algorithms", *Journal of Information Security*, Vol.11 No.3, July 2020, DOI: 10.4236/jis.2020.113009.
- [2]. Karule, K.P. and Nagrale, N.V. (2016) Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. *International Journal of Scientific Engineering and Applied Science*, 2, 495-498.
- [3]. Srinivas Koppul and V. Madhu Viswanatham2, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform", *Modelling and Simulation in Engineering Volume 2017*, Article ID 7470204, 12 pages <https://doi.org/10.1155/2017/7470204>.
- [4]. Ahmed Othman Khalaf 1, Shaimaa Khudhair Salah2, Hind Jumaa Sartep3, and Zainab Khyoon Abdalrdha4, "Subject Review: Comparison between RSA, ECC & NTRU Algorithms", *International Journal of Engineering Research and Advanced Technology (IJERAT)*, Volume.5, Issue 11 November -2019 DOI: 10.31695/IJERAT.2019.3582
- [5]. Zolfaghari, B.; Bibak, K.; Koshiba, T. The odyssey of entropy: Cryptography. *Entropy* 2022, 24, 266. <https://doi.org/10.3390/e24020266>.
- [6]. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," *International Journal of Computer Science and Engineering*, vol. 3, no. 7, pp. 1-6, 26 04 2016.
- [7]. A. P. U. Siahaan, "Blum Blum Shub in Generating Key in RC4," *International Journal of Science & Technology*, vol. 4, no. 10, pp. 1-5, 2016.
- [8]. Sumartono, Isnar & Siahaan, Andysah Putera Utama & Mayasari, Nova. An Overview of the RC4 Algorithm. *IOSR Journal of Dental and Medical Sciences*. 18. 2278-661. 10.9790/0661-1806046773, 2016.
- [9]. HAO GAO AND XINGYUAN WANG, "Chaotic Image Encryption Algorithm Based on Zigzag Transform with Bidirectional Crossover from Random Position", Received June 10, 2021, accepted July 16, 2021, date of publication July 26, 2021, date of current version August 3, 2021. DOI.10.1109/ACCESS.2021.3099214.
- [10]. Lu Zhentai, Xin Xuegang, Chen Wufan. Digital image encryption based on zigzag coding.

- Computer Engineering and Design, 2009,30(09): 2145-2146+21.
- [11]. Padmaa M, Venkataramani DY. ZIG-ZAG PVD- A Nontraditional Approach. International Journal of Computer Applications, 2010,5(6):5-10.
- [12]. Xu X, Feng J. Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector. 2010 IEEE International Conference on Granular Computing. IEEE, 2010: 556-561.
- [13]. Xiaoqiang Zhang *, Mi Liu, Jingxi Tian, and Zhengjun Gong,"Color Image Encryption Algorithm Based on Dynamic Block Zigzag Transformation and Six-Sided Star Model", Electronics 2022, 11, 2512.<https://doi.org/10.3390/electronics11162512>
- [14]. Zargar, A. J., Manzoor, M., & Mukhtar, T., "Encryption/Decryption Using Elliptical Curve Cryptography". International Journal of Advanced Research in Computer Science, 8(7),2017.
- [15]. Ashwaq T. Hashim* & Baedaa H. Helal," Measurement of Encryption Quality of Bitmap Images with RC6, and two modified version Block Cipher", Eng. & Tech. Journal, Vol.28, No.17, 2010.

Cite this article as :

Raghda Sattar Jabbar , "Triple Encryption of Images based on RC4, Zigzag, and Elliptic Curve Algorithms for Enhanced Security ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 2, pp. 93-100, March-April 2023. Available at doi : <https://doi.org/10.32628/IJSRSET231023>
Journal URL : <https://ijsrset.com/IJSRSET231023>