IJAMEC
e-ISSN: 2147-8228

INTERNATIONAL JOURNAL OF APPLIED MATHEMATICS ELECTRONICS AND COMPUTERS

www.dergipark.org.tr/ijamec

International Open Access

Volume 08
Issue 03

September, 2020

Research Article

Haar wavelet transformation and RC4 algorithm based Image Encryption

Elham Yasin[a], *Rıdvan Saraçoğlu*[b,*]

[a]*Information Technology Department, Lebanese French University, Erbil 44001, Iraq*
[b]*Electrical Electronics Engineering Department, Van Yüzüncü Yıl University, Van 65080, Turkey*

ARTICLE INFO

Article history:
Received 6 July 2020
Accepted 28 September 2020

Keywords:
Cryptography
Haar transform
Image compression
Image encryption
Information security
RC4 stream cipher

ABSTRACT

Recently the protection and privacy of information or data have become a major concern to deal with. Developed coding for secure transmission and decrypting the image are steadily more needed for specific military, corrective, country defense, and various applications. Variance sorts of security information or data increment strategies are being created as of now, cryptographic systems are one basic path. Keep the message private by translating data or information into an alternative frame, such that the message is not perceivable. This study aims to expect the security image arrangement to be upgraded by following the Haar wavelet transformation and the RC4 encryption algorithm. For simplicity, the Image compression executed by Haar wavelet transformation to compress the image and to calculate high-speed performance. For image protection process, the RC4 encryption algorithm is applied that is also for secure image transformation.

1. Introduction

The fast development of PC networks permitted extensive files, for example, advanced pictures, to be easily transmitted over the web. Information encryption is frequently applied to guarantee secure data however; the majority of the accessible encryption calculations are utilized for content information [1]. Because of huge information size and continuous limitations, calculations that are useful for textual information may not be appropriate for sight and sound information [2]. Encryption will be the procedure of transforming the data with protected its security.

With the immense advancement of PC networks and some of the later progress in computerized innovations, a huge digital information is being exchanged over many networks. An important part of this information is confidential and private information. Consequently, unexpected security methods have been utilized to provide essential assurance. The security of digital images has turned out to be increasingly critical because of the quick development of the Internet in today's electronic age. Digital image protection has been taken into consideration more recently, and a wide variety of photo encryption techniques have been suggested to enhance the security of these pictures.

Image encoding strategies try to switch one image to another that is difficult to obtain from first one (Figure 1). Then again, image decoding recovers the original image from the encoded one. There are different image encryption frameworks to encode and decode information, and there will be no absolute encryption calculations to fulfill the different image sorts.

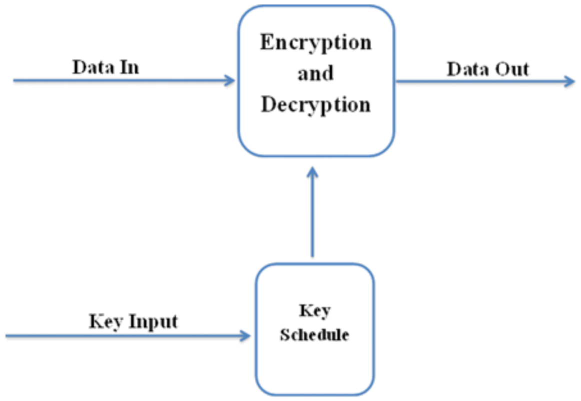

Figure 1. Encryption/Decryption diagram

* Corresponding author. E-mail address: ridvansaracoglu@yyu.edu.tr

DOI: 10.18100/ijamec.763283

2. Related Works

Throughout the years a wide variety of techniques for image encryption for the safe transmission of images over the network have been introduced. Some related works are clarified below:

The Advanced Encryption Standard (AES) was analyzed, and a keystream generator was added to this standard to improve performance [3].

A strong partial image encryption scheme in this paper used a Discrete Wavelet Transform with RC4 Stream Cipher. In the method, Matrix of approximation (lowest frequency band) encrypted using the stream cipher, since it contains much of the picture information. Encryption time is shortened by encrypting only a portion of the image. Good protection is provided by rearranging the remaining of the image and use a shuffling technique. Selected encryption is the latest approach to reducing computational requirements for massive amounts of images [4].

An image encryption algorithm based on Haar wavelet transformation (HWT) and DNA technique was proposed, which image is compressed using Haar transformation and then the image is encrypted by DNA algorithm [5]. The wavelet transformation transforms data from the spatial domain to the frequency domain and afterward stores each component with the appropriate scale size. DNA algorithm used for further encrypting the image, this method changes the data into an unreadable form.

The binary code of the pixel values of the color image was extracted and permuted to the 8-bit key entered, followed by a permutation of every 8 consecutive pixels. The picture is further segmented into blocks that are transferred accordingly. To further implement the encryption, a separate method is introduced that includes a 43-digit key. The encryption consists of a total of 10 rounds in which two keys are used, which were both extracted from the 43 digits inserted in the key [6].

A discrete Haar wavelet transform (DWT) for image compression was presented in the analysis [7]. Use Haar Discrete Wavelet Transform (HDWT) to compress the signal. The techniques of image compression are loosely divided into two groups based on whether or not a copy of the original image could be reproduced using the compressed image.

A paper proposed an Effective analysis scheme for 2D-HWT in image processing [8]. The word proposed focused on going to build computational complexity and effective imaging compression algorithms for lossy images, using wavelet techniques. This research focuses in particular on wavelet image compression using Haar Transformation with the goal of reducing computational criteria by adding specific levels of compression to wavelet coefficients, which are accomplished in a fraction of a second and thus improve the quality of the reconstructed image. The positive results were collected regarding recreated image quality as well as the sustainability of significant image detail.

A systematic overview of the cryptanalysis of the RC4 stream cipher was presented in the report [9]. We listed the various shortcomings of the RC4 algorithm. It has been developed that creative research efforts are needed to develop a safe RC4 algorithm that can resolve the vulnerabilities of RC4, such as bias bytes, key collisions, and key WPA recovery attacks.

This study [10] has introduced a novel lossless technique. The existing methods includes a domain transformation. Besides the image sub-bands, they are encoded to provide a stable, accurate and strong form. The algorithm was designed to change and return back the increasing frequency signal to the transformed image until the image frequency was transferred back to the initial domain. The results give a complete deviation of the pixel values in between first and last form of images. The decipher algorithm reverses the process and redintegrate the image to its initial state.

Based on DNA subsequence a cryptosystem has been proposed [11]. Here only DNA subsequence operation is used hence it does not have any match with the traditional DNA approach for encryption. Location and the value of a pixel of an image are scrambles using a logistic chaotic map. The encryption process based on this approach has good security and efficiency.

In another paper, Jolfaei introduced an image encryption framework used hybrid technique included a chaotic baker's map and an updated S-AES version [12]. A map of Baker is used to produce a matrix of permutations. The paper is composed of a pixel shuffler unit and a block cipher component. Pixel shuffling extends the diffusion process and dissipates two neighboring pixels in longitudinal, horizontal, and diagonal association.

This introduced a new visual encryption theme [13]. Shuffling the positions and changing the gray values of the image pixels are combined at the same time to guarantee the method's security. The encryption algorithm encompasses two steps: First, the pixels of the original image are shuffled. the pixel values of the shuffled image are encrypted.

In Hyper-Chaos-based Image Encryption Algorithm a new image complete shuffling matrix was implemented to shuffle the pixel positions of the plain image and after that the pairing of the hyper-chaos state is used to change the gray values of the shuffled image [14].

A new method of image encryption was introduced in [15]. The proposed method used the flexibility of the gradient HWT and chaotic property of the rational order chaotic maps to produce the encrypted images. Haar wavelet is one of the best numerical algorithms for the cryptography and analysis of images. This approach uses linearity properties of the scaling function of the Haar Wavelet gradient and deterministic behaviors of rational order chaotic maps to produce high-security encrypted images.

.

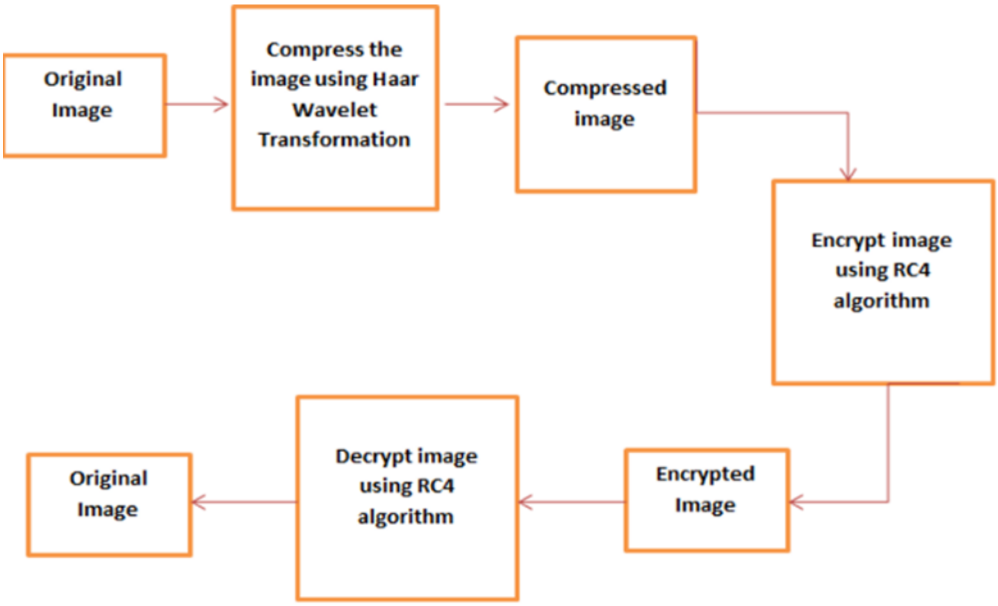
Original Image
Compress the image using Haar Wavelet Transformation
Compressed image
Encrypt image using RC4 algorithm
Encrypted Image
Decrypt image using RC4 algorithm
Original Image

Figure 2. Diagram of the Method

A paper implies an algorithm for image encryption which uses a generator of random bit sequences and is dependent on chaotic maps [16]. Chaotic Logistics and Tent maps are focus of this study.

Using these disorderly features, basic image pixels of the plain image are permuted, then, the image is segmented into eight parts. A method based on changing random bits is used. Thus, necessary modifications are made.

In the map's permutation stage, the pixels and bits of the images are modified using the chaotic random ergodic matrix. This process procreates an encrypted script, the output of which is measured using some statistical test, number of pixel of change rate (NPCR), the cumulative average increase in strength (UACI) and the keyspace.

It has been observed that even a small change in the original image caused big changes in the encrypted image.

The complete key area for the proposed method (2∧2,160) protects image to any brute-force attack [16]

In the proposed encryption scheme, row and column shuffling are realized based on the Ikeda map, and the substitution process is realized via the Henon map [17]. The aim of this study is to make up for deficiencies. Rows and columns of the image are shuffled first in the algorithm, and then grey levels of the image are changed. After that, the shuffling process is realized again. For a color image, these processes are applied separately to red, green and blue components.

3. Proposed Methods

In this segment, we will introduce the scheme utilized for image compression and image encryption alongside the calculation of the HWT and RC4 method. The framework of study is shown in Figure 2. The essential thought behind the study is to first compress the image with the goal that we can send it over the network rapidly and encode it so we can transmit it over any networks safely and securely.

Initially, we compress the image utilizing HWT. Wavelets are an arrangement of numerical bases functions. While approximating a function as far as wavelets, the wavelet basis functions are assigned to concur to the purpose of being approached. Wavelets utilize a dynamic arrangement of basic functions that stand for the input function in the most effective way. In this way, wavelets can give a great deal of compression and are thus extremely well known in the sector of image and signal processing.

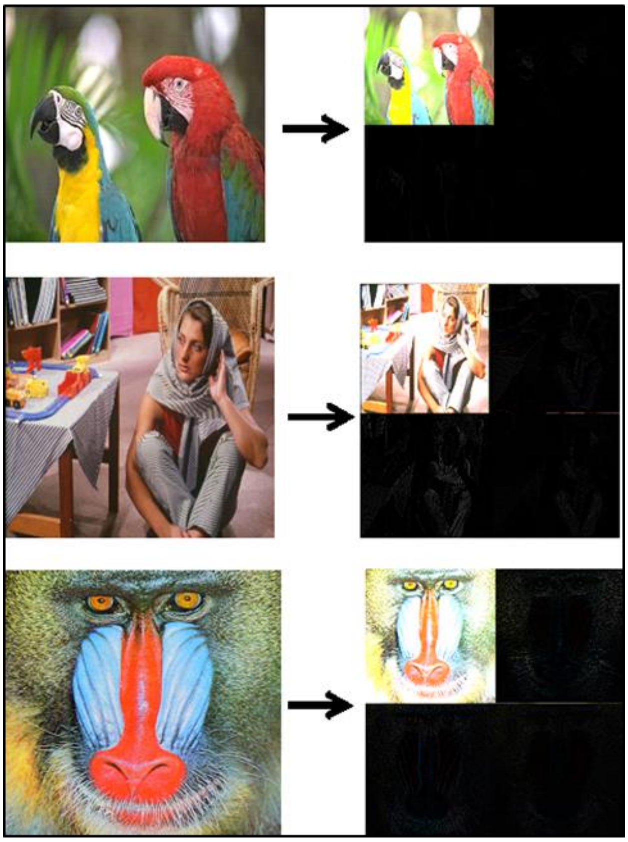

Figure 3. Compression with Haar wavelet transformation results

A wavelet transformation switches over information from the spatial domain to the frequency domain and then stores each segment with a coordinating determination scale. By applying HWT, we may stand for such an image in terms of a low-determination image and the arrangement of description coefficients. Haar Transform is only averaging and differencing. Figure 3 shows Haar compression for some images.

A symmetric key algorithm, RC4 is a stream cipher, developed by Ronald Rivest in 1987. The RC4 encryption method is used for some standards. This is also found in other business software packages.

The phases for this algorithm are as follows:

1- Take the data you want to encrypt and the key you select.

2- Generate two arrays of strings.

3- Introduce an array which is included numbers between 0 and 255.

4- Load the other array with the selected key.

5- Randomize the original array by based on the main array.

6- Randomize the original array to produce the last key-stream.

7- XOR the last key-stream of the content to be encoded to send cipher-text.

4. Experimental Results

Encryption result of some images is shown in Figure 4. Execution of selective HWT image encryption with RC4 stream cipher is evaluated using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Histogram Analysis, as well as Entropy whereas in Table 1. Presents the results of this in Figure 5.

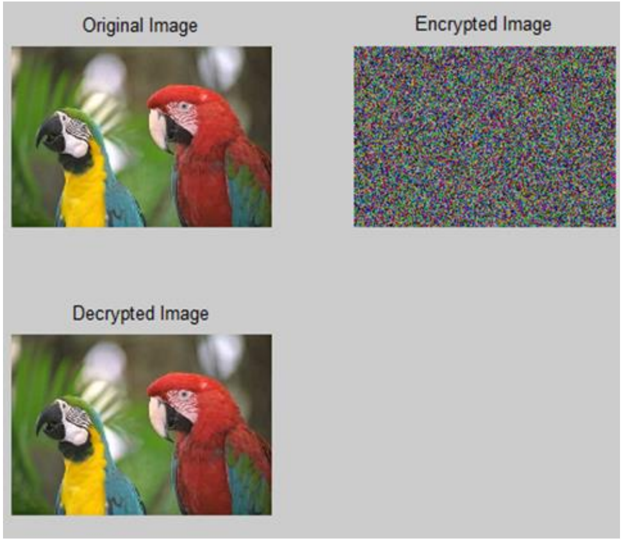

Figure 4(a). Bird encryption/decryption image

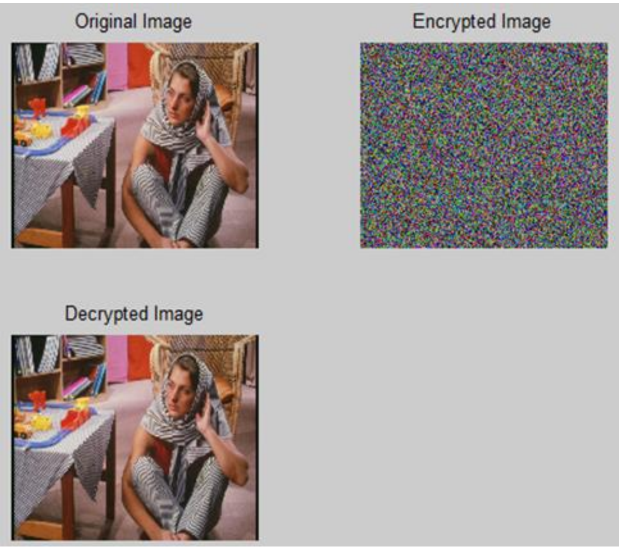

Figure 4(b). Barbara encryption/decryption image

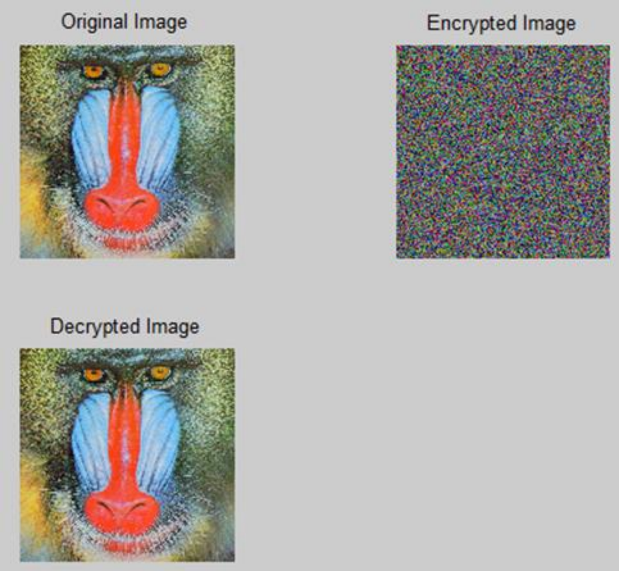

Figure 4(c). Baboon encryption/decryption image

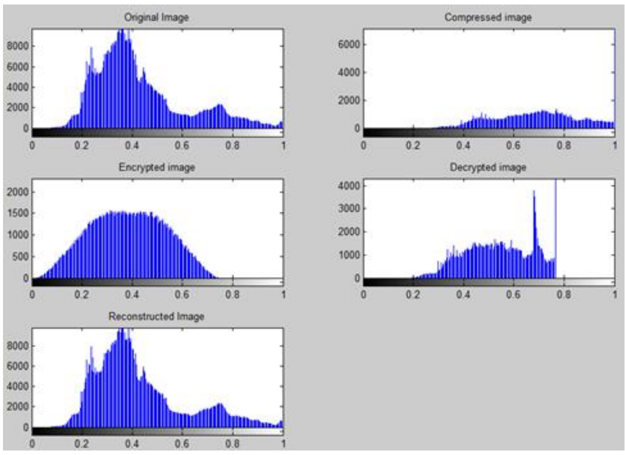

Figure 5(a). Histogram of Bird image

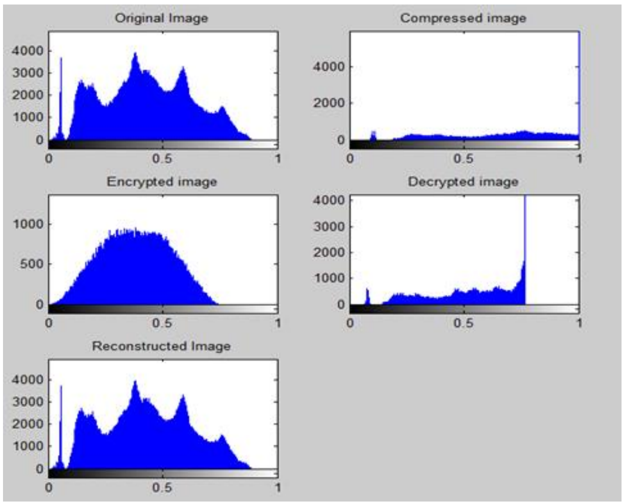

Figure 5(b). Histogram of Barbara image

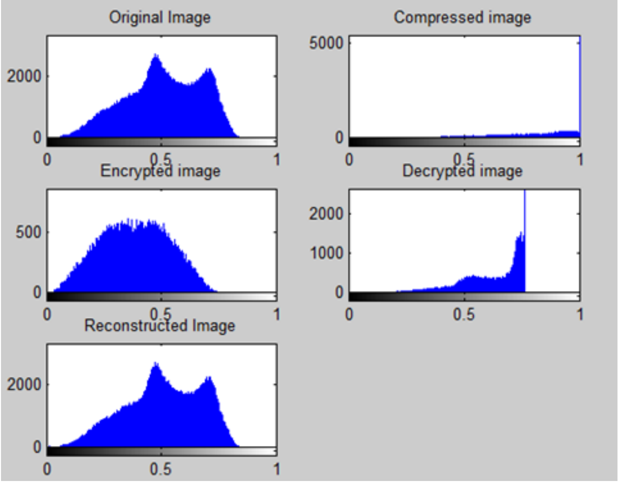

Figure 5(c). Histogram of Baboon image

Table 1. Ram position details of the motion segments

Images	Key length	PSNR	MSE	Size	Entropy
Bird	4	51.908	0.419	683x1024	6.435
Barbara	4	51.611	0.448	576x720	5.803
Baboon	4	50.394	0.593	512x512	5.095
Lena	4	52.658	0.352	512x512	6.350
Pepper	4	50.742	0.548	512x512	5.511

5. Conclusions

An image encryption mechanism for HWT-based images with RC4 Stream Cipher has been introduced in this document. The machine first compresses the image and then encrypts it, and the image is decoded and restored to the original image.

Some technologies need a speedy image compression technique, although most of the available technique requires an impressive amount of time. So this proposed algorithm (Haar) was used to compress the image quickly.

Examination of the RC4 parameters has shown that the speed of encoding or decoding time is specifically associated with the length of the encryption key and the calculation of the information record if the information is sufficiently comprehensive.

References

[1] P. Irfan, Y. Prayudi, and I. Riadi, “Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA),” Int. J. Comput. Appl., vol. 123, no. 6, pp. 11–16, 2015.

[2] K. Patel and S. Belani, “Image encryption using different techniques: A review,” Int. J. Emerg. Technol., vol. 1, no. 1, pp. 30–34, 2011.

[3] P. Irfan, Y. Prayudi, and I. Riadi, “Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA),” *Int. J. Comput. Appl.*, vol. 123, no. 6, pp. 11–16, 2015.

[4] K. Patel and S. Belani, “Image encryption using different techniques: A review,” *Int. J. Emerg. Technol. …*, vol. 1, no. 1, pp. 30–34, 2011.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A modified AES based algorithm for image encryption,” *World Acad. Sci. Eng. Technol.*, vol. 1, no. 1, pp. 70–75, 2007.

[6] S. Sasidharan and D. S. Philip, “A Fast Partial Encryption Scheme with Wavelet Transform and RC4,” *Int. J. Adv. Eng. Technol.*, vol. 1, no. 4, pp. 322–331, 2011.

[7] R. Kumar, B. Pratap, and V. Singh, “Image Encryption Using a Combinantion of Haar and Dna Algorithm,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 3, no. 5, pp. 82–87, 2014.

[8] A. Dixit, P. Dhurve, and D. Bhagwan, “Image Encryption using Permutation and Rotation XOR Technique,” vol. 2, no. 4, 2012.

[9] M. Rathee and A. Vij, “Image Compression Using Discrete HAAR Wavelet Transform,” *Int. J. Eng. Innov. Technol.*, vol. 3, no. 12, pp. 47–51, 2014.

[10] S. . Tamboli and V. . Udupi, “Image Compression Using HAAR Wavelet Transform,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 8, pp. 3166–3170, 2013.

[11] P. Jindal and B. Singh, “RC4 Encryption-A Literature Survey,” *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 697–705, 2015.

[12] S. Tedmori and N. Al-Najdawi, “Image cryptographic algorithm based on the Haar wavelet transform,” *Inf. Sci. (Ny).*, vol. 269, no. March, pp. 21–34, 2014.

[13] Q. Zhang, X. Xue, and X. Wei, “A novel image encryption algorithm based on DNA subsequence operation.,” *ScientificWorldJournal.*, vol. 2012, p. 286741, 2012.

[14] A. Jolfaei, “Image Encryption Using Chaos and Block Cipher,” *Comput. Inf. Sci.*, vol. 4, no. 1, pp. 172–185, 2011.

[15] Z. H. Guan, F. Huang, and W. Guan, “Chaos-based image encryption algorithm,” *Phys. Lett. A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[16] X. Wang, J. Zhao, and H. Liu, “A new image encryption algorithm based on chaos,” *Opt. Commun.*, vol. 285, no. 5, pp. 562–566, 2012.

[17] S. Ahadpour, Y. Sadra, and M. Sadeghi, “Image Encryption Based On Gradient Haar Wavelet and Rational Order Chaotic Maps,” vol. 1, no. 1, pp. 1–8, 2016.