IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 17, 2020, accepted May 8, 2020, date of publication May 14, 2020, date of current version June 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2994583

Efficiently Encrypting Color Images With Few Details Based on RC6 and Different Operation Modes for Cybersecurity Applications

OSAMA S. FARAGALLAH[1,4], ASHRAF AFIFI[1,5], WALID EL-SHAFAI[2], HALA S. EL-SAYED[3], MOHAMMED A. ALZAIN[1], JEHAD F. AL-AMRI[1], AND FATHI E. ABD EL-SAMIE[2,6]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Saudi Arabia
[2]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3]Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt
[4]Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[5]Department of Electrical Engineering and Computers, Higher Technological Institute, 10th of Ramadan 228, Egypt
[6]Department of Information Technology, College of Computer and Information Sciences, Princess NourahBint Abdulrahman University, Riyadh 21974, Saudi Arabia

Corresponding author: Osama S. Faragallah (o.salah@tu.edu.sa; osam_sal@yahoo.com)

This work was supported by the Deanship of Scientific Research, Taif University, Saudi Arabia, through a research project under Grant 1-439-6083.

ABSTRACT Recently, massive research works have been accomplished for augmenting privacy and security requirements for cybersecurity applications in wireless communication networks. This is attributed to the fact that conventional security processes are not appropriate for robust, efficient, and reliable multimedia streaming over unsecure media. Therefore, this paper presents an efficient color image cryptosystem based on RC6 with different modes of operation. The proposed cryptosystem is composed of two phases: encryption and decryption. The encryption phase starts by decomposing the color plainimage with few details into its RGB components, which in turn, are segmented into 128-bit blocks. These blocks are then enciphered using RC6 with an appropriate mode of operation. After that, the corresponding enciphered blocks of RGB components are multiplexed for constructing the final cipherimage. This scenario is reversed in the decryption phase. The performance of the proposed cryptosystem is gauged via simulation using a set of encryption quality metrics. The simulation results reveal that the proposed cryptosystem with cipher block chaining (CBC), cipher feedback (CFB), and output feedback (OFB) modes can efficiently and effectively hide all information of the color images with few details even in the presence of some input blocks with similar data. On the other hand, the results show that the electronic codebook (ECB) mode is not effective at all in hiding all details of images. Finally, the obtained results ensure the applicability of the proposed cryptosystem and its efficiency in encrypting images in terms of security, encryption quality, and noise immunity.

INDEX TERMS Image encryption, ECB, CBC, OFB, CFB, Digital communications, Color images with few details.

I. INTRODUCTION

In recent years, information privacy and security have played an essential role in our daily and modern cybersecurity applications. The dramatic advances in computers, mobiles, and communication technologies have led to a massive increase in the usage of digital communications. Therefore, digital communications invaded almost all fields of our modern lives such as training, e-commerce, military, e-learning, multimedia broadcasting, politics, banking, education, telemedicine, pay-TV, etc. As a result, a huge amount of data is daily transmitted using shared public networks, most popularly the Internet. A major part of such data is either governmental or private sensitive documents transmitted as images. Protecting the stored and transmitted data over cloud computing data centers and modern communication systems is one of the major concerns of cybersecurity applications. Consequently, securing images transmitted via digital communication systems to keep them away from modification, partial or total removal of their contents, and addition of

The associate editor coordinating the review of this manuscript and approving it for publication was Qiang Lai.

fake information has become a vital research problem for scholars. Hence, various image ciphering techniques have been proposed to secure transmitted digital images [1]–[15].

One of the most important challenges in cybersecurity applications and cloud data storage is the requirement of security and authenticity of the data being uploaded, downloaded, and stored, and the need for securing this data from unlicensed and illegal admission and access. Over the years, it has been claimed that chaos-based image/video encryption proposals are preferred in image encryption due to their potential reduction of computational effort compared with conventional ciphers. In [16], it was proved that this argument is not correct in the scenarios of encrypting color images with few details as they offer high correlation between similar pixels after the encryption process.

Numerous cybersecurity procedures, such as digital signature authentication and cryptographic methods, are exploited to safeguard stored and transmitted digital images from unlawful attacks. Traditional ciphering techniques like DES, IDEA, ElGamal, and RSA have been constructed based on complicated mathematical problems [17]. They can be categorized into single-key and double-key encryption systems, and they have been implemented only in encrypting textual data [18]. In contrast to textual data, images are characterized by various features such as a large number of data blocks, which cannot be processed with traditional ciphering techniques. The main barrier for constructing an influential image ciphering system based on traditional techniques is that diffusing and shuffling image data using such techniques is an extremely tough process [19]. One more barrier is that such traditional techniques need extra processing steps for handling the data of compressed images. Consequently, they require a huge processing capacity and a long computational time.

Various block ciphering techniques such as RC5 [20], RC6 [21], and Rijndael [22], [23] have been proposed to overcome such limitations of traditional ciphering techniques. These techniques are symmetric. The symmetry property means that they utilize the same key in encrypting and decrypting information. The block processing means that the information to be encrypted is partitioned into several partitions of the same size called blocks before submission to the ciphering algorithm. Consequently, block ciphering techniques are intensively utilized in the coding of long files such as E-mails, and files on computers.

The RC6 has emerged in 1998 as a development of RC5 to satisfy the Advanced Encryption Standard (AES) requirements [23]. It massively utilizes data-dependent rotations to overcome the limitations of traditional ciphering techniques. It employs four 32-bit registers, and it includes integer multiplication as an extra operation, which significantly increases the attained diffusion per iteration [24]. It can process blocks of 128 bits, and it can be easily implemented. Consequently, it increases the security level and throughput.

The encryption of color images with few details represents a great challenge for the majority of ciphering techniques. Block ciphering techniques cannot efficiently hide the features of color images with few details, because the values of the pixels incorporated in the encryption process are very close to each other. Indeed, the spatial domain chaotic encryption techniques have a drawback of keeping analogous histograms to those of the plainimages. The problem of encrypting images with few details represents a great challenge for the majority of encryption techniques that have not been studied in detail, yet.

Based on our knowledge, the only related research was given in [25], which introduced a cryptosystem for enciphering of gray-scale images with few details. This cryptosystem is constructed using wavelet fusion as a pre-processing operation on the images before encryption aiming to hide the flat patterns. This can be achieved through fusing the plainimage with another wide-histogram image. After the fusion step, the fused image is then encrypted using RC6 or chaotic Baker map. The authors evaluated the performance of their system using various quality indicators. The effectiveness of this cryptosystem has been examined in the presence of noise before the decryption process. The results reveal that this cryptosystem can efficiently and securely encrypt gray-scale images with few details. Indeed, the application of encryption techniques with different modes of operation (ECB, CBC, CFB, and OFB) for encrypting normal gray-scale digital images reveals improvement in the encryption quality [19]. Such results encouraged us to apply the RC6 with different modes of operation to encrypt color images with few details, which cannot be encrypted efficiently with traditional RC6 or other encryption techniques.

In this research, an efficient color image cryptosystem based on RC6 for images with few details is presented. It employs RC6 with different modes of operation. This cryptosystem begins by extracting the RGB components, which in turn are divided into 128-bit blocks. These blocks are then fed to the RC6 algorithm with different operation modes, and the corresponding enciphered blocks are assembled after that to construct the encrypted color image. This scenario is reversed in the decryption phase. The performance of the proposed cryptosystem is assessed and evaluated using different quality metrics via simulation. The results show that the proposed cryptosystem with CBC, CFB, and OFB modes can effectively encrypt the color images with few details and hide their features. In contrary, the proposed cryptosystem, when implemented using RC6 with ECB mode, cannot efficiently hide the details of the plainimages. The obtained results ensure that the proposed cryptosystem is applicable and efficient from the security, ciphering quality, and noise immunity perspectives.

The remaining paper parts are structured as follows. Section II describes shortly the RC6. In section III, the operation modes details are presented. Section IV presents the proposed image cryptosystem. Section V gives the encryption quality indicators used in evaluating the performance of the proposed cryptosystem. Section VI covers the obtained simulation results with some observations.

Finally, Section VII gives the conclusions and the new research directions.

II. RELATED WORK

This section presents the fundamentals of the RC6 and the different operation modes. The RC6 is a direct development of RC5, and it depends on the utilization of four 32-bit registers instead of only two registers in RC5. Therefore, it can process I/O blocks of 128 bits. The utilization of four 32-bit registers in RC6 is motivated by conducting two rotations in each round instead of one rotation in a half round in RC5. More data bits are utilized in every round to define the amount of rotation.

The RC6 has three variable parameters: size of the word (w) in bits, number of rounds (r) which is a non-negative integer and length of the secret key in bytes (b) that is used in both encryption and decryption phases [21], [23], [26], [27]. Based on the values of such parameters, the RC6 is precisely identified as RC6-w/r/b. The RC6 is composed of two Feistel networks in which the data are merged through certain relations that are data-dependent. Every iteration of the RC6 has certain operations: the $f(x) = x(2x + 1) \bmod 2^{32}$ function that is applied twice, two fixed 32-bit iterations, two 32-bit iterations of data-dependent rotation, two XOR operations and two modulo-2 additions for 32 bits. The diffusion achieved per iteration is strongly increased by the addition of a multiplication operation, which improves security, and throughput, and at the same time minimizes the number of rounds. One more final issue is that the RC6 employs an extended table of keys, $S[0, \ldots, t - 1]$, comprising $t = 2r + 4$ w-bit words as keys [20], [21]. For more information about the RC6 ciphering technique, the reader is referred to [20], [21], [26].

The operation mode in cryptography is a procedure, which is utilized with block ciphering for providing various information services like authenticity and confidentiality [28]. Any stand-alone block ciphering technique is appropriate only for encrypting and decrypting a single fixed-length set of bits known as a block [29]. The operation mode determines how one can repetitively execute a one-block ciphering technique for securing and transmitting an amount of information larger than one block [29], [30]. Straightforward utilization of block ciphering techniques is not advisable at all. Any intruder can easily break the encryption algorithm. To avoid such problem, various operation modes can be applied with block ciphering techniques. Such application enables users to select the suitable mode, which can satisfy the user requirements. These operation modes relay on the method in which the ciphering technique deals with the input data blocks. If a specified operation mode is employed in the encryption phase, it must be employed also in the decryption phase. In this section, we will discuss the operation modes recognized by the abbreviations ECB, CBC, CFB, and OFB, and how they can be used in block ciphering to construct a cryptosystem. During the discussion, the following variables are used: n length of block, K secret key, E_K encryption map and D_K decryption map.

A. THE ECB MODE

The ECB may be considered as the straightforward mode to be utilized with a block cipher. The information message to be encrypted is partitioned into blocks. Each block, in turn, is autonomously encrypted, which means that there is no dependency between blocks in the decryption process. If an error exists in a certain ciphered block, a decryption error will appear only in its corresponding decrypted block. That is the ECB is characterized by preventing error propagation, which is a major advantage. On the other hand, there is a one-to-one correspondence between input blocks and their corresponding output blocks. The original text is partitioned into equal-size blocks $(X_1, X_2, X_3, \ldots.)$, each of n bits. These blocks are mapped after the encryption process to $(Y_1, Y_2, Y_3, \ldots.)$ using Eq.1 and decrypted using Eq.2. Encryption and decryption are implemented with the same key.

$$Y_i = E_K(X_i) \tag{1}$$

$$X_i = D_K(Y_i) \tag{2}$$

This means that the original plaintext block X is encrypted using the secret key K to generate the ciphertext block Y.

The ECB mode is not recommended in the protocols of cryptography, otherwise these protocols will not be strong enough to protect integrity. Indeed, they will be subjected to replay attacks as every block can be decrypted using the same method. An intruder can construct a codebook as the ECB is not semantically secure. Moreover, in the ECB mode, identical input blocks always have similar ciphered output blocks, and they are encrypted in the same way. This feature is considered as a major drawback of the ECB operation mode, because it does not hide fixed patterns of data. The effect of this drawback of the ECB mode becomes clear if it is applied for encrypting a digital image, which contains wide areas having identical colors or reiterated patterns. Such areas or repeated sections will be partitioned into several blocks having approximately similar patterns, and will consequently give approximately similar ciphertext blocks. As a result, the encrypted image may reveal some features of the source image. Such main disadvantage is avoided with the other operation modes.

B. THE CIPHER BLOCK CHAINING (CBC) MODE

The CBC operation mode is a popular one. It eliminates the main drawback of the EBC mode by XORing bits of the input plaintext block with the previously ciphered block before the encryption process. Consequently, every ciphertext block will be dependent on the entire blocks of the plaintext up to the current point [31], [32]. During the decryption operation, the XOR is conducted again to remove this effect. The enciphering process is initialized by a dummy selected message (block of a specified length that is known as the

Initialization Vector (IV)). This IV can be sent to the receiver, i.e., the security of the encryption system is based on securing the key not on securing the IV. A non-repeated and unique value of the IV is needed for every encryption process using the same key. The IV is utilized for ensuring that different ciphered blocks are obtained, if the same original plaintext block is encrypted many times individually using the same secret key [31]. Therefore, every ciphertext block relies on the IV value and the entire plaintext blocks preceding that block. In other words, the CBC operation mode is characterized by using a serial dependence technique. Consequently, similar input blocks are encrypted to different ciphertext blocks by utilizing distinct IV values for each block, and the last ciphertext block relies on the whole plaintext. The deciphering process can be parallelized, because only the j^{th} and $(j-1)^{\text{th}}$ ciphertext blocks are needed in obtaining the j^{th} plaintext block. The encryption and decryption procedures are performed in CBC mode according to Eq. 3 and Eq. 4, respectively.

Even though the CBC operation mode is the most utilized mode, it suffers from some drawbacks. The first one is that the encryption process is conducted serially i.e., it cannot be performed in parallel. Therefore, its throughput is low. The second is that the length of original message to be encrypted must be an integer multiple of the block size, otherwise it is padded to satisfy such condition using a ciphertext stealing technique. One more drawback of the CBC mode is the error propagation as the existence of an error in the j^{th} encrypted block leads to errors in the decryption of j^{th} and $(j+1)^{\text{th}}$ blocks [32].

$$Y_j = E_K(Y_{j-1} \oplus X_j) \tag{3}$$
$$X_j = D_K(Y_j) \oplus Y_{j-1}, \quad j = 1, 2, 3, \ldots. \tag{4}$$
$$Y_0 = IV \tag{5}$$

C. THE CIPHER FEEDBACK (CFB) MODE

The CFB mode was proposed for encrypting and transferring some values of the plaintext instantaneously one after another. Using the CFB mode, some features of stream ciphering can be obtained with block ciphering. The decryption operation with the CFB mode is very similar to the reverse execution of the encryption operation with the CBC mode. This mode also depends on the IV that is selected similar to the CBC operation mode. The utilization of different IVs in ciphering the same input plaintext block yields different enciphered block [33]. Although the IV can be sent to the receiver openly, certain applications require securing it. The CFB operation mode employs the block cipher as a module in a generator of random numbers. The CFB operation mode works by XORing the recent block of plaintext with the former ciphertext block to create the recent ciphertext block. The XOR operation has a large effect on the patterns of the plaintext. The original plaintext cannot be processed directly without having retrieved blocks either from the start or the end of the ciphertext. The encryption and decryption procedures are performed with the CFB mode according to Eq. 6 and Eq. 7, respectively.

$$Y_j = X_j \oplus I_j \tag{6}$$
$$X_j = Y_j \oplus I_j \tag{7}$$
$$I_j = E_K(Y_{j-1}), \quad j = 1, 2, 3, \ldots. \tag{8}$$
$$Y_0 = IV \tag{9}$$

As in the CBC mode, error in the plaintext continually propagates in the ciphertext. Also, the encryption process cannot be conducted in parallel, while the decryption process can. If a one-bit is altered during the decryption process in the ciphertext, its effect will appear in two plaintext blocks; namely one-bit will be changed in the corresponding decrypted block, and the next decrypted block will be entirely corrupted.

D. THE OUTPUT FEED BACK (OFB) MODE

The OFB operation mode transforms block ciphering to concurrent stream ciphering. It produces blocks of key-stream. It allows different-block-size encryption as in the CFB mode, but the main difference between them is that in the OFB mode, the result of block encryption is the feedback rather than the ciphertext in the CFB mode. The ciphertext is obtained by XORing such key-stream blocks with blocks of plaintext. If a bit is flipped in the ciphertext, a flipped bit will result in the decrypted plaintext at the same position. Such feature enables various error fixing codes to work properly [34]. The encryption and decryption procedures are similar as a result of the symmetry property of the XOR operation. The OFB operation mode cannot be parallelized as every result of the feedback block cipher step relies entirely on the previously conducted ones [35]. The XOR value for every plaintext block is obtained autonomously from both the plaintext and the ciphertext. As in both the CBC and CFB operation modes, the OFB depends on an IV. The utilization of different IV values with the same plaintext block yields different ciphertext blocks. The encryption and decryption procedures are conducted according to Eq. 10 and Eq. 11, respectively.

$$Y_j = X_j \oplus I_j \tag{10}$$
$$X_j = Y_j \oplus I_j \tag{11}$$
$$I_j = E_K(I_{j-1}), \quad j = 1, 2, 3, \ldots. \tag{12}$$
$$I_0 = IV \tag{13}$$

III. THE PROPOSED COLOR IMAGE CRYPTOSYSTEM

Here, the proposed color image cryptosystem details are explored. To the best of our knowledge, the problem of encrypting color images with few details has not been studied before. The only related study was introduced in [25]. It presented a model for encrypting gray-scale images with few details. In this cryptosystem, the authors merge the image with few details with an auxiliary image using the DWT to remove the flat areas homogeneity prior to encryption. After that, they encrypt the fused image using the RC6 or Baker map.

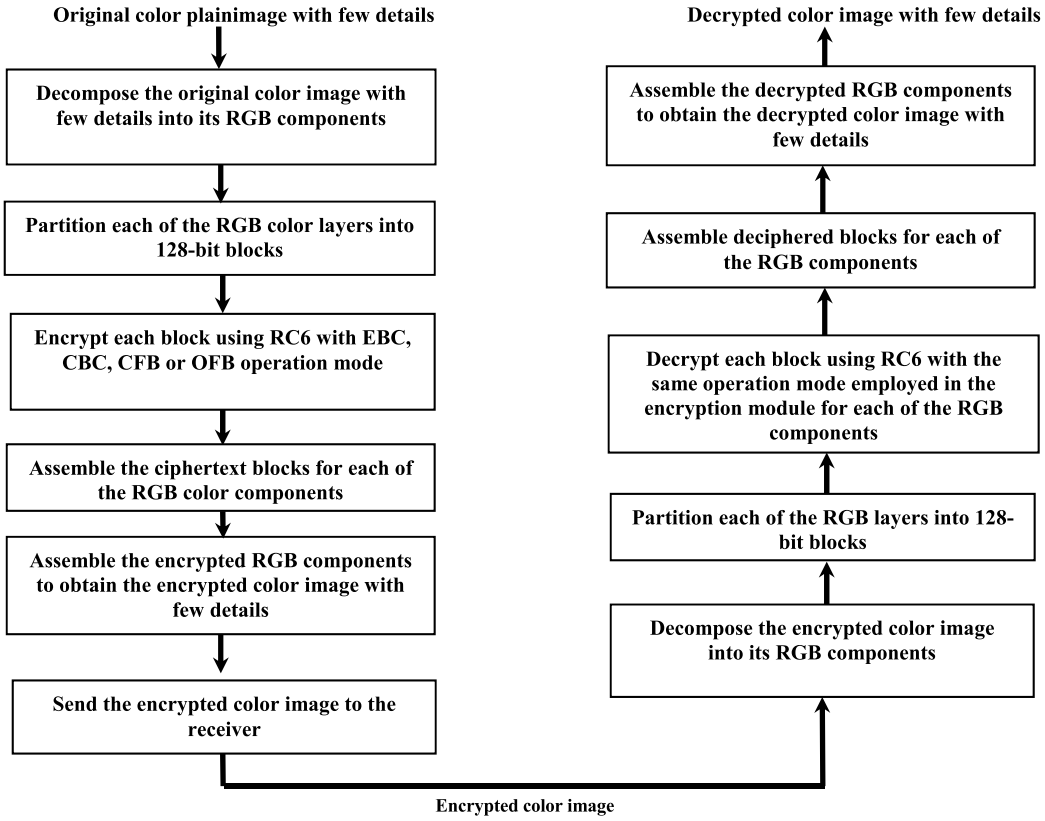


FIGURE 1. The proposed color image cryptosystem.

The proposed color image cryptosystem with different modes of operation is presented to overcome the limitations of encrypting color images with few details using traditional encryption techniques. The reasons for selecting RC6 are summarized as follows:

- The simplicity and appropriateness for real-time applications.
- The low computational load, which makes RC6 suitable for real-time implementation.
- The few resources represented in low memory required for implementation.
- The applicability on modern processors that allow parallel processing
- The elimination of any redundancy in the cipherimage.

The proposed color image cryptosystem depends on the implementation of RC6 with different modes of operation. As shown in Figure 1, it is composed of two modules for encryption and decryption. The encryption module starts by reading the color plainimage with few details and extracting its RGB components. Each of the RGB components is partitioned into 128-bit blocks, which are then fed to the RC6 encryption with the EBC, CBC, CFB or OFB operation mode. After that, the corresponding ciphertext blocks of the RGB components are assembled to construct the encrypted RGB components. Finally, the encrypted RGB components are assembled to construct the encrypted color image. The encryption steps can be summarized as follows:

1. Read the color plainimage with few details.
2. Decompose the color plainimage into its RGB components.
3. Segment each of the RGB components into 128-bit blocks
4. Apply the RC6 encryption with EBC, CBC, CFB or OFB operation mode on the blocks for each of the RGB components.
5. Assemble the corresponding ciphertext blocks for RGB components.
6. Assemble the encrypted RGB components to obtain the color cipherimage.

The receiver starts by decomposing the encrypted color image into its corresponding RGB components. After that, each of the RGB components is partitioned into 128-bit blocks and fed to the decryption module of the RC6 with the same operation mode utilized in the encryption module. After that, the corresponding deciphered blocks are assembled for each of the RGB components. Finally, the decrypted RGB components are multiplexed to reconstruct the decrypted color image.

The decryption steps can be summarized as follows:

1. Read the color encrypted image
2. Decompose the encrypted color image into its RGB components.
3. Segment each of the RGB components into 128-bit blocks.

4. Apply the proposed decryption module with the same operation mode (EBC, CBC, CFB or OFB) employed in the encryption module for each of the RGB components.
5. Assemble the corresponding deciphered blocks for each of the RGB components.
6. Assemble the decrypted RGB components to obtain the decrypted color image.

IV. ENCRYPTION PERFORMANCE METRICS

This section summarizes the utilized encryption evaluation metrics that will be used in assessing the performance of the proposed color image cryptosystem. The attained encryption/decryption quality is examined using visual inspection and evaluated with various encryption/decryption quality evaluation metrics. Table 1 summarizes the utilized encryption performance evaluation metrics and their formulas.

TABLE 1. Encryption evaluation metrics and their corresponding formulas.

Measure	Formulation
Entropy	$\text{Entropy} = -\sum_{i=1}^{n} P_r(x_i)\log P_r(x_i)$
CC	$CC(I,E) = \frac{\text{cov}(I,E)}{\sqrt{D(I)}\sqrt{D(E)}}$
ID	$ID(I,E) = \frac{\left\lvert\sum_{i=0}^{255} h_d(i)\right\rvert}{M \times N}$
NPCR	$NPCR(E_1,E_2) = \frac{\sum_{i,j} D(x_i,y_j)}{M \times N} \times 100\%$
UACI	$UACI(E_1,E_2) = \frac{1}{M \times N}\left[\sum_{x_i y_j} \frac{E_1(x_i,y_j) - E_1(x_i,y_j)}{255}\right] \times 100\%$
PSNR	$PSNR(I,D) = 10\log \frac{(255)^2}{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}[I(x_i,y_j) - D(x_i,y_j)]^2}$
SSIM	$SSIM(x,y\mid w) = \frac{(2\overline{w}_x\overline{w}_y + C_1)(2\sigma_{w_x w_y} + C_2)}{(\overline{w}_x^2 + \overline{w}_y^2 + C_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + C_2)}$
FSIM	$FSIM = \frac{\sum_{x\in\Omega} S_L(x).PC_m(x)}{\sum_{x\in\Omega} PC_m(x)}$

A. VISUAL INSPECTION

Visual inspection is a major indicator in evaluating the quality of encrypted images. If the image features are hidden well, this means that the utilized image cryptosystem is good in performance [15], [16], [20], [23], [25]. Moreover, it is known that visual examination does not detect the full relation between the original and the encrypted images. The visual inspection alone is not sufficient for evaluating the hiding efficiency of image details [23], [25], [36]. Consequently, other encryption quality evaluation metrics are needed.

B. ENTROPY

The entropy is utilized to investigative and assess the RGB components of the tested color images and to evaluate the information involved in these components. Eq. 14 defines how the entropy is computed [25], [36]:

$$\text{Entropy} = -\sum_{i=1}^{n} P_r(x_i)\log P_r(x_i) \tag{14}$$

where x_i is the i^{th} intensity value and P_r is its corresponding probability. Consequently, a large entropy value indicates good encryption.

C. ENCRYPTION QUALITY TESTS

A class of well-known quality metrics is utilized in evaluating and comparing the quality of encryption of different encryption techniques. These metrics include, but are not limited to, irregular deviation, correlation coefficient and histogram deviation.

1) CORRELATION COEFFICIENT (*CC*)

The $CC(I, E)$ is calculated between the original $I(x_i, y_j)$ and the encrypted $E(x_i, y_j)$ versions of the RGB components of the tested color images as follows [37]–[39]:

$$CC(I,E) = \frac{cov(I,E)}{\sqrt{D(I)}\sqrt{D(E)}} \tag{15}$$

$$cov(I,E) = \frac{1}{L}\sum_{i=1}^{L}(I(i) - Mean(I))(E(i) - Mean(E)) \tag{16}$$

$$D(I) = \frac{1}{L}\sum_{i=1}^{L}(I(i) - Mean(I))^2 \tag{17}$$

$$D(E) = \frac{1}{L}\sum_{i=1}^{L}(E(i) - Mean(E))^2 \tag{18}$$

where L denotes the pixel count of the image. Consequently, the lower the value of $CC(I, E)$ between the original $I(x_i, y_j)$ and the encrypted $E(x_i, y_j)$ for all RGB components of the tested color images is, the better the encryption quality.

2) IRREGULAR DEVIATION (*ID*)

The *ID* approximates the encryption accuracy through measuring how much irregular deviation is caused by the encryption. According to [40]–[42], the *ID* can be calculated as follows:

$$ID(I,E) = \frac{\left\lvert\sum_{i=0}^{255} h_d(i)\right\rvert}{M \times N} \tag{19}$$

$$h_d(i) = |h(i) - M_h| \tag{20}$$

where $h(i)$ and M_h are the cipherimage histogram at every level i and the uniform histogram mean value for an ideal

encrypted image. Therefore, achieving low values for *ID* means high encryption quality.

D. DIFFERENTIAL EXAMINATION

This metric reveals the effect of a single pixel change on the entire encrypted image using the proposed cryptosystem. The following two differential test indicators are employed:

1) NUMBER-OF PIXELS CHANGING RATE (*NPCR*)

Suppose that E_1 and E_2 are two encrypted images whose original images have a single difference in one pixel. The *NPCR* is computed as the percentage of dissimilar pixels to the entire pixels of each of the two encrypted images. The values of pixels at location (x_i, y_j) in E_1 and E_2 are $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$. Suppose a bipolar array $D(x_i, y_j)$ which is equal in size to both encrypted images E_1 and E_2. The $D(x_i, y_j)$ is calculated for $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$ as follows:

$$D(x_i, y_j) = \begin{cases} 0 & if\ E_1(x_i, y_j) = E_2(x_i, y_j) \\ 1 & Otherwise \end{cases} \tag{21}$$

According to [25], [40], the *NPCR* can be calculated as follows:

$$NPCR(E_1, E_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\% \tag{22}$$

where M, and N are the E_1 and E_2 width and height.

2) UNIFIED AVERAGE CHANGING INTENSITY (*UACI*)

The *UACI* is the mean difference between two encrypted images E_1 and E_2. According to [25], the *UACI* can be calculated as follows:

$$UACI(E_1, E_2) = \frac{1}{M \times N}\left[\sum_{x_i y_j} \frac{E_1(x_i, y_j) - E_2(x_i, y_j)}{255}\right] \times 100\% \tag{23}$$

E. NOISE IMMUNITY TEST

1) PEAK SIGNAL-TO-NOISE RATIO (*PSNR*)

The proposed cryptosystem robustness to the presence of Additive White Gaussian Noise (AWGN) is examined during decryption. According to [25], the PSNR is calculated as follows:

$$PSNR(I, D) = 10 \log \frac{(255)^2}{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [I(x_i, y_j) - D(x_i, y_j)]^2} \tag{24}$$

where $I(x_i, y_j)$ and $D(x_i, y_j)$ are the original and decrypted color image pixel values at position (x_i, y_j), respectively. High values of *PSNR* indicate that the immunity to noise is high.

2) STRUCTURAL SIMILARITY (*SSIM*)

The *SSIM* is employed to assess the quality of the decrypted image. Based on [25], the *SSIM* is calculated as follows:

$$SSIM(x, y\,|w) = \frac{(2\bar{w}_x\bar{w}_y + C_1)(2\sigma_{w_x w_y} + C_2)}{(\bar{w}_x^2 + \bar{w}_y^2 + C_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + C_2)} \tag{25}$$

where C_1, and C_2 are infinitesimal constants to avoid division by zero, and $\bar{w}_x$ and $\bar{w}_y$ are the average values of w_x and w_y regions, respectively. $\sigma_{w_x}^2$ is the variance of w_x region and $\sigma_{w_x w_y}$ is the covariance between the two regions w_x and w_y. If the *SSIM* value is high, this means good immunity to noise.

3) FEATURE SIMILARITY INDEX (*FSIM*)

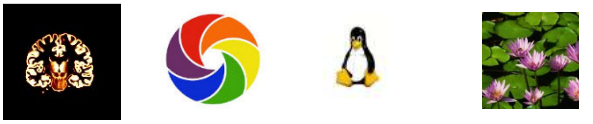
The *FSIM* is employed to assess the decrypted image quality. Based on [25], the *FSIM* is calculated as follows:

$$FSIM = \frac{\sum_{x \in \Omega} S_L(x).PC_m(x)}{\sum_{x \in \Omega} PC_m(x)} \tag{26}$$

where Ω, $S_L(x)$, and $PC_m(x)$ are the spatial domain, overall similarity between two images and the phase congruency value, respectively. High values of *FSIM* mean good noise immunity.

V. SIMULATION EXPERIMENTS

A simulation model using MATLAB is built to assess the performance of the proposed cryptosystem. Using this model, a set of experimental tests are conducted to study the effect of utilizing different operation modes (ECB, CBC, CFB, and OFB) with RC6 on the encryption of color images with few details. Various sets of performance indices are utilized in evaluating the proposed cryptosystem including general indicators like visual inspection, entropy, encryption quality metrics, differential metrics and noise immunity metrics. These tests are conducted using different 512 × 512 color images; namely Medical image, Bit Map, Tux and Water Lilies as illustrated in Figure 2.



a) Medical b) Bit Map c) Tux d) Water Lilies

FIGURE 2. Test color images.

A. EXPERIMENT 1

In this experiment, the effects of the different modes of operation of the proposed cryptosystem on the encryption quality are investigated. The results of encrypting the RGB components for Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem and the cryptosystem of [25] are shown in Figures 3 to 6, respectively. Visual inspection reveals that both the proposed cryptosystem and that of [25] are good. Accordingly, as it could be seen easily from these figures, the proposed cryptosystem with different

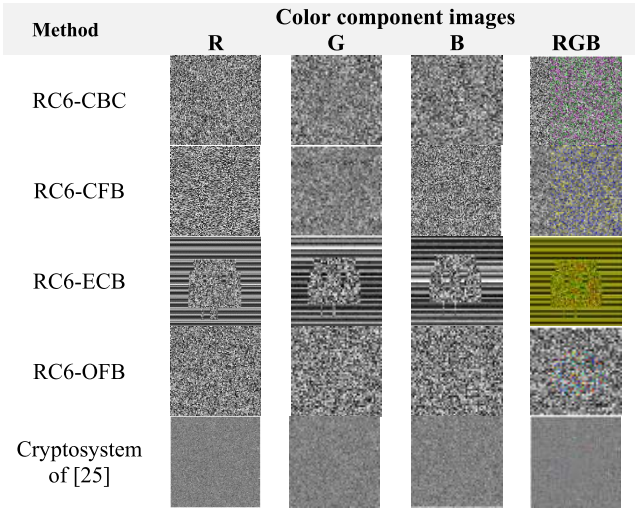


FIGURE 3. Encryption results for the Medical color image using the proposed cryptosystem with different operation modes.

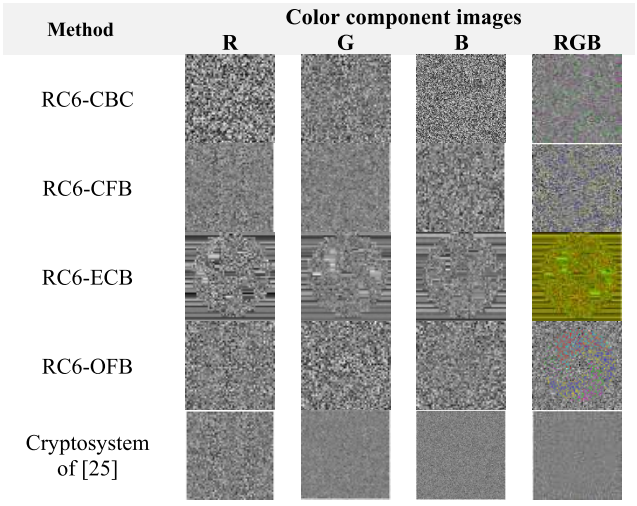


FIGURE 4. Encryption results for the Bit Map color image using the proposed cryptosystem with different operation modes.

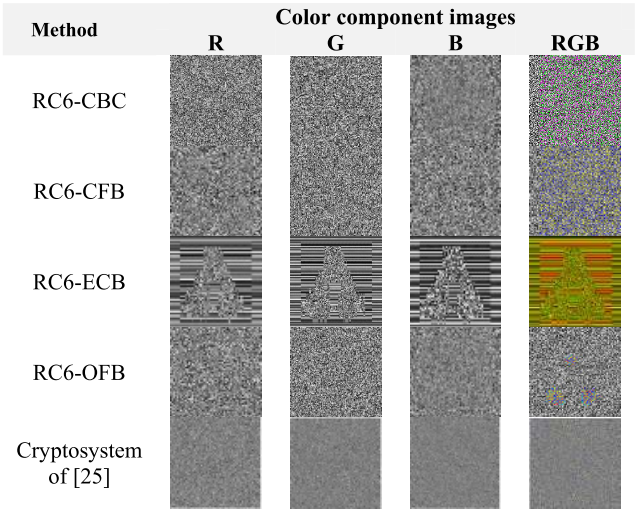


FIGURE 5. Encryption results for the Tux color image using the proposed cryptosystem with different operation modes.

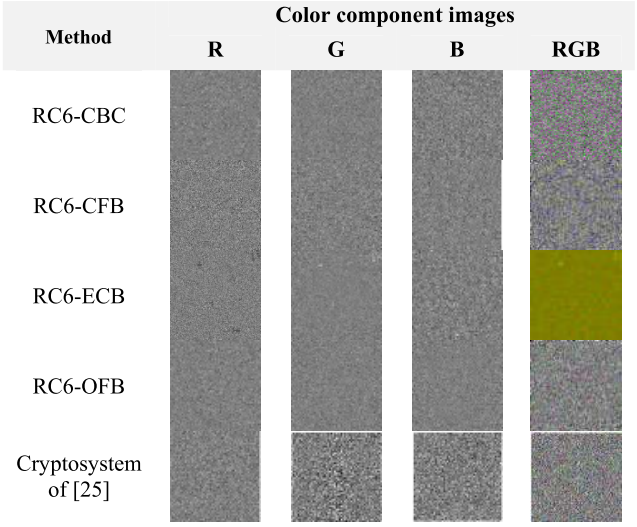


FIGURE 6. Encryption results for the Water Lilies color image using the proposed cryptosystem with different operation modes.

modes of operation works fine and produces good results with CBC, CFB, and OFB operation modes. Using these modes, the proposed cryptosystem hides completely all information and nothing is visible at all. No one can easily distinguish visually between the original image and encrypted one even if the original image has a large variance in the tone of color. In other words, if the original color image has some similar input data blocks, the proposed cryptosystem can encrypt such blocks efficiently to entirely different enciphered blocks.

In contrary, as shown in Figures 3 to 6, the proposed image cryptosystem with ECB operation mode cannot hide all of the original image information and any one can still identify the general pattern of the original image. Consequently, based on visual investigation of these results, one can generally say that employing CBC, CFB, OFB modes with the proposed color image cryptosystem can totally secure the transmitted information, but the ECB mode cannot do that. It is well-known that visual observation alone may not be considered adequate to evaluate the hiding efficiency of image details. Therefore, the proposed cryptosystem performance is assessed using encryption quality metrics in the following experiments to determine which mode is the best in hiding image details, and at the same time is immune to various attacks.

B. EXPERIMENT 2

In this experiment, the entropy is used to estimate the amount of information comprised in the encrypted color components: RGB components using the proposed cryptosystem and RGB components of the cryptosystem of [25].

The entropy test results for the encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies

TABLE 2. Entropy test results of encrypted RGB components for Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

Image	The proposed color image cryptosystem with different operation modes												Cryptosystem of [25]		
	CBC			CFB			ECB			OFB					
	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
Tux	7.9968	7.9972	7.9972	7.9977	7.9977	7.9973	6.6417	6.6596	6.7093	7.9972	7.9970	7.9970	7.9892	7.9892	7.9893
Bit Map	7.9973	7.9971	7.9970	7.9970	7.9976	7.9971	7.2226	7.2405	7.2251	7.9971	7.9970	7.9971	7.9793	7.9792	7.9893
Medical	7.9887	7.9869	7.9899	7.9874	7.9874	7.9881	5.8032	5.7166	5.6215	7.9903	7.9898	7.9900	7.9892	7.9892	7.9892
Water Lilies	7.9974	7.9971	7.9971	7.9973	7.9975	7.9971	7.9929	7.9926	7.9946	7.9972	7.9970	7.9970	7.9892	7.9893	7.9892

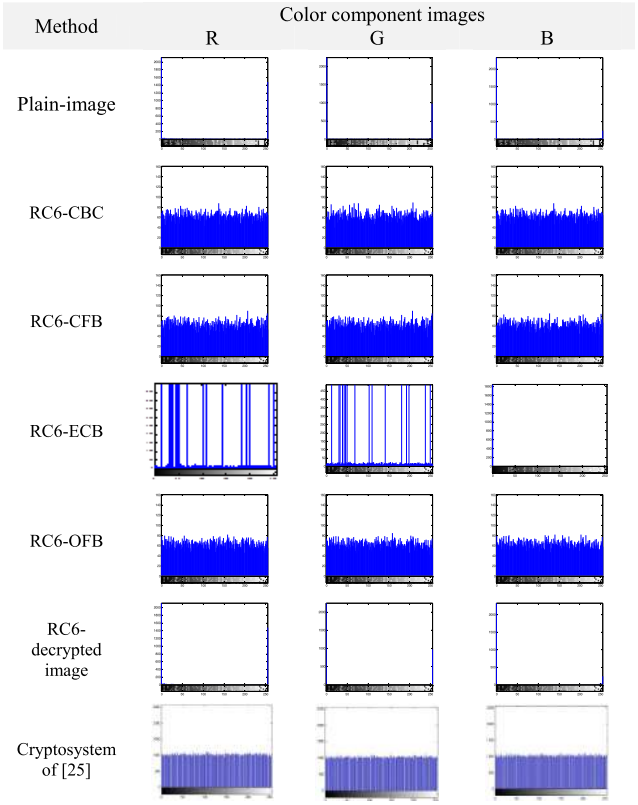


FIGURE 7. Histogram results of encrypted/decrypted RGB components for Medical color image using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

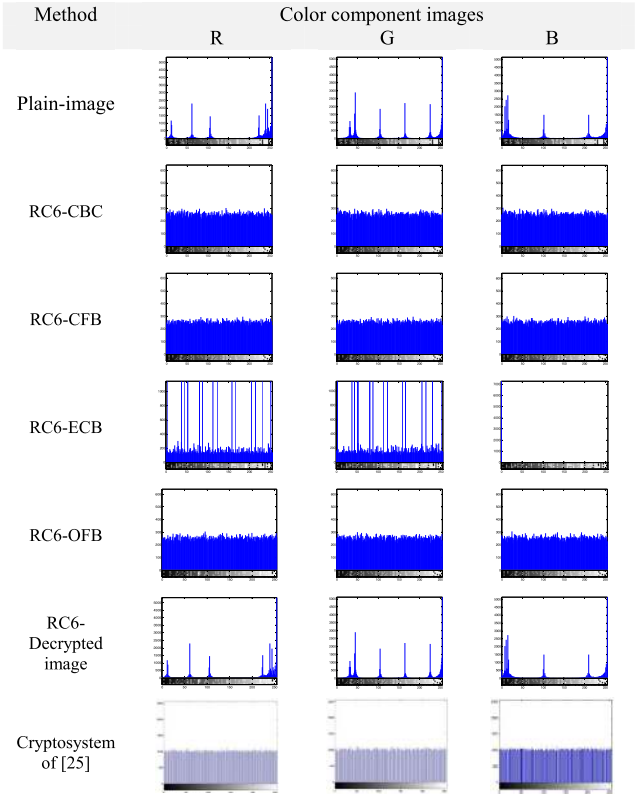


FIGURE 8. Histogram results of encrypted/decrypted RGB color components for Bit Map color image using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

color images with the proposed color image cryptosystem with CBC, CFB, ECB and OFB operation modes and the cryptosystem of [25] are shown in Table 2.

It is known that large entropy values indicate good encryption quality. Consequently, the results listed in Table 2 ensure the visual inspection interpretation of the results given in Figures 7 to 10. That is, the proposed color image cryptosystem with CBC, CFB, and OFB modes provides good entropy estimates compared with the cryptosystem of [25]. Also, it can completely secure information as it gives high and comparable entropy values for all tested color images. In other words, even if the original color image has some similar input data blocks, the proposed color image cryptosystem can encrypt such blocks efficiently to entirely different enciphered blocks. In contrary, the ECB operation mode gives the lowest entropy values with all tested color images, which means that the ECB operation mode should not be used. This goes in line with visual inspection interpretation of the results obtained in experiment 1.

C. EXPERIMENT 3

In this experiment, the performance of the proposed color image cryptosystem with different operation modes is investigated for encrypting RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using various encryption quality metrics. The following three main quality metrics are utilized.

1) CORRELATION COEFFICIENT (*CC*)

In this subsection, the performance of the proposed color image cryptosystem in encrypting RGB components of the

TABLE 3. Correlation coefficient between the original and the encrypted RGB components for Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

Image	The proposed color image cryptosystem with different operation modes												Cryptosystem of [25]		
	CBC			CFB			ECB			OFB					
	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
Tux	-0.002	0.0048	0.0067	-0.0074	-0.0065	0.0009	-0.0459	-0.0539	0.0243	-0.00055	0.0003	0.0005	-0.0023	-9.94×10^{-4}	7.95×10^{-5}
Bit Map	0.001	0.0055	0.0036	0.0035	0.0092	0.0016	-0.0339	-0.0525	0.0218	-0.0052	0.0054	0.0050	-0.0022	9.905×10^{-4}	0.0017
Medical	-0.012	0.0083	0.0048	-0.0093	-0.0094	0.0079	-0.0835	-0.0510	0.0417	-0.0055	-0.0043	0.0004	4.79×10^{-4}	0.0019	0.0025
Water Lilies	-0.005	0.0015	0.0065	-0.0058	-0.0057	0.0030	0.0036	-0.0171	0.0580	0.0031	0.0027	0.0030	-4.51×10^{-4}	-3.64×10^{-5}	0.0025

TABLE 4. Irregular deviation between the original and the encrypted RGB component for Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

Image	The proposed color image cryptosystem with different operation modes												Cryptosystem of [25]		
	CBC			CFB			ECB			OFB					
	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
Tux	0.0175	0.0210	0.0204	0.0167	0.0204	0.0186	0.2860	0.2847	0.4118	0.0186	0.0180	0.0217	0.0517	0.0706	0.0545
Bit Map	0.0366	0.0506	0.0358	0.0375	0.053	0.0363	0.1870	0.3134	0.4251	0.0370	0.0518	0.0359	0.1426	0.2013	0.1379
Medical	0.0067	0.0067	0.0062	0.0069	0.0697	0.0067	0.856	0.0874	0.1136	0.0064	0.0063	0.0064	0.0596	0.0547	0.0519
Water Lilies	0.1084	0.1466	0.0560	0.1084	0.1462	0.0583	0.1107	0.1443	0.2739	0.1089	0.1477	0.0575	0.4354	0.5895	0.0519

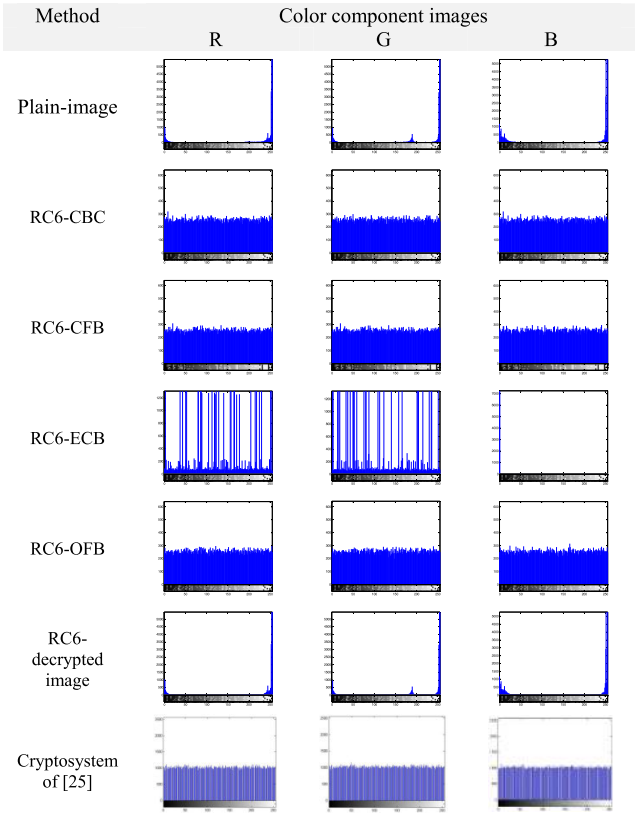


FIGURE 9. Histogram results of the encrypted/decrypted RGB color components for Tux color image using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

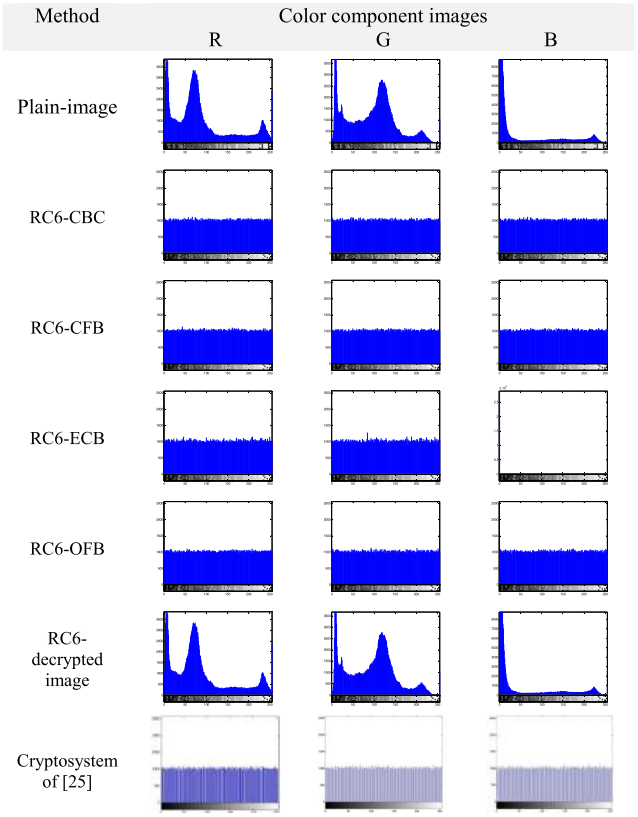


FIGURE 10. Histogram results of the encrypted/decrypted RGB color components for Water Lilies color image using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

tested color images is examined using *CC*. It is known that low values of *CC* between the original $I(x_i, y_j)$ and the encrypted $E(x_i, y_j)$ components of the RGB image means high encryption quality. The *CC* values between the original and the encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25] are presented in Table 3.

From Table 3, it is easy to notice that the *CC* values between the original and encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with CBC, CFB

TABLE 5. The NPCR and UACI estimations for the encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25].

Image		The proposed color image cryptosystem with different operation modes												Cryptosystem of [25]		
		CBC			CFB			ECB			OFB					
		R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
Tux	NPCR	99.118	99.64	99.624	99.643	99.603	99.608	99.921	99.896	99.91	99.90	99.881	99.893	99.157	99.151	99.178
	UACI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit Map	NPCR	99.574	99.64	99.597	99.623	99.617	99.614	99.796	99.788	99.80	99.795	99.787	99.804	98.961	98.962	98.989
	UACI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medical	NPCR	99.658	99.61	99.567	99.664	99.530	99.652	99.921	99.896	99.91	99.920	99.896	99.908	98.452	98.441	98.441
	UACI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Water Lilies	NPCR	99.597	99.59	99.64	99.629	99.641	99.622	99.591	99.634	99.63	99.606	99.606	99.588	99.616	99.604	98.441
	UACI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

and OFB operation modes and the cryptosystem of [25] are very low and are close to zero. This indicates a good encryption quality for both the proposed color image cryptosystem with such modes and the cryptosystem of [25]. In other words, even if the original color image has some similar input data blocks, the proposed color image cryptosystem can encrypt such blocks efficiently to entirely different enciphered blocks. On the other hand, the obtained *CC* values for RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with ECB operation mode are the highest among the obtained *CC* values, which again ensures the unsuitability of this mode to the task of securing the information.

2) IRREGULAR DEVIATION (*ID*)

The performance of the proposed color image cryptosystem with different operation modes and the cryptosystem of [25] in encrypting RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images is investigated using *ID* in this subsection. It is known that achieving low values of *ID* means high encryption quality. The attained *ID* results for encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes and the cryptosystem of [25] are presented in Table 4. As could be easily seen from Table 4, the achieved *ID* values for the encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with CBC, CFB and OFB operation modes are very low compared to those of the cryptosystem of [25]. Such results reflect the high quality of encrypted images using these operation modes. In contrary, the obtained *ID* values for encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with the ECB operation mode are the highest among the obtained *ID* values, which once more ensures that the ECB mode is not good in securing information.

3) HISTOGRAM

In this subsection, the performance of the proposed color image cryptosystem and the cryptosystem of [25] in encrypting RGB components of the tested color images is examined in terms of histogram. For efficient encryption, the histograms of encrypted RGB components should be entirely different from those of the corresponding RGB components of the original color images. The histogram test

TABLE 6. The PSNR in dBs for the decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.

Image	Operation modes		*PSNR* in dB with different *SNRs* in dB				
			10	20	30	40	50
Tux	CBC	R	6.8514	7.0199	15.9267	∞	∞
		G	6.9997	7.1422	16.1529	∞	∞
		B	6.8663	6.9780	15.6282	∞	∞
	CFB	R	4.9781	4.9558	4.9730	4.9842	4.9842
		G	5.0647	5.0681	5.0681	5.0729	5.0729
		B	5.0023	4.9900	4.9982	4.9929	4.9929
	ECB	R	6.8264	6.9772	16.0161	∞	∞
		G	7.0335	7.1130	16.1534	∞	∞
		B	6.8501	6.9831	15.5641	∞	∞
	OFB	R	26.6150	30.1149	48.7316	∞	∞
		G	26.9447	30.3612	50.5186	∞	∞
		B	25.3257	30.8394	43.5756	∞	∞
Bit Map	CBC	R	8.2976	8.5282	14.5728	∞	∞
		G	8.8359	9.0033	13.3191	∞	∞
		B	8.8359	9.0033	13.3191	∞	∞
	CFB	R	5.4718	5.4735	5.4927	5.4816	5.4816
		G	5.7733	5.7810	5.7677	5.7853	5.7853
		B	5.4559	5.4754	5.4571	5.4558	5.4558
	ECB	R	8.3095	8.5723	14.6503	∞	∞
		G	8.8590	8.9743	13.2340	∞	∞
		B	8.1311	8.2577	10.6789	∞	∞
	OFB	R	27.5113	32.5124	42.0278	∞	∞
		G	28.5790	32.7208	45.7523	∞	∞
		B	26.2468	31.2719	38.5739	∞	∞
Medical	CBC	R	4.9951	5.1028	10.6125	∞	∞
		G	4.8393	5.0787	13.1156	∞	∞
		B	4.8659	5.1325	21.3884	∞	∞
	CFB	R	4.9576	4.9952	8.2546	11.1346	11.1346
		G	4.8588	4.9644	9.5530	11.3377	11.3377
		B	4.9242	5.0753	11.3055	11.6550	11.6550
	ECB	R	4.9644	5.0247	10.5072	∞	∞
		G	4.8794	5.0979	21.8958	∞	∞
		B	4.8295	5.0297	12.6927	∞	∞
	OFB	R	21.9109	27.8161	38.0918	∞	∞
		G	22.0205	27.9823	44.3747	∞	∞
		B	23.1365	29.9841	59.4651	∞	∞
Water Lilies	CBC	R	7.3926	7.4572	14.4555	∞	∞
		G	8.1472	8.3594	20.9516	∞	∞
		B	5.9392	5.9507	10.9984	∞	∞
	CFB	R	7.4057	7.4000	7.4270	7.4184	7.4184
		G	8.18965	8.2006	8.1657	8.1691	8.1691
		B	5.9335	5.9637	5.9408	5.9476	5.9476
	ECB	R	7.4356	7.4584	14.5208	∞	∞
		G	8.1656	8.3158	20.8327	∞	∞
		B	5.9147	5.9622	11.0002	∞	∞
	OFB	R	26.1587	31.4688	44.3659	∞	∞
		G	26.1587	31.4688	44.3659	∞	∞
		B	23.2661	28.8714	41.1576	∞	∞

TABLE 7. Decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.

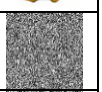
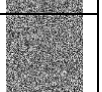
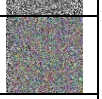
Image	Operation modes		Decrypted images with different *SNRs* in dB				
			10	20	30	40	50
Tux	CBC	R					
		G					
		B					
		Deciphered image					
	CFB	R					
		G					
		B					
		Deciphered image					
	ECB	R					
		G					
		B					
		Deciphered image					
	OFB	R					
		G					
		B					
		Deciphered image					
	CBC	R					
		G					
		B					
		Deciphered image					

TABLE 7. *(Continued.)* **Decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.**

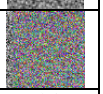
Image	Operation modes		Decrypted images with different *SNRs* in dB				
			10	20	30	40	50
Bit Map	CFB	R					
		G					
		B					
		Deciphered image					
	ECB	R					
		G					
		B					
		Deciphered image					
	OFB	R					
		G					
		B					
		Deciphered image					
Medical	CBC	R					
		G					
		B					
		Deciphered image					
	CFB	R					
		G					
		B					
		Deciphered image					

TABLE 7. ***(Continued.)*** **Decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.**

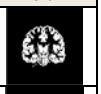
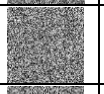
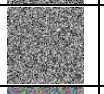
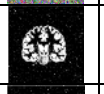
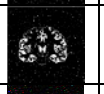
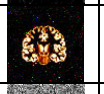
Image	Operation modes		Decrypted images with different *SNRs* in dB				
			10	20	30	40	50
	ECB	R					
		G					
		B					
		Deciphered image					
	OFB	R					
		G					
		B					
		Deciphered image					
Water Lilies	CBC	R					
		G					
		B					
		Deciphered image					
	CFB	R					
		G					
		B					
		Deciphered image					
	ECB	R					
		G					
		B					
		Deciphered image					

TABLE 7. *(Continued.)* **Decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.**

Image	Operation modes		Decrypted images with different *SNRs* in dB				
			10	20	30	40	50
	OFB	R					
		G					
		B					
		Deciphered image					

results for the encrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images and their corresponding RGB components of the original images using the proposed color image cryptosystem with CBC, CFB, ECB, and OFB operation modes and the cryptosystem of [25] are shown in Figures 7 to 10, respectively.

According to the histogram results, it is easy to notice that the proposed color image cryptosystem and the cryptosystem of [25] do not change the histograms of the decrypted RGB components for all of the tested Medical, Bit Map, Tux and Water Lilies color images from those of their corresponding original ones. It is also easy to realize that the histograms of the encrypted RGB components for all of the tested Medical, Bit Map, Tux and Water Lilies color images using either the proposed cryptosystem with different operation modes or the cryptosystem of [25] are entirely dissimilar to those of the original ones. These results indicate that even if the original color image has some similar input data blocks, the proposed color image cryptosystem can encrypt such blocks efficiently to entirely different enciphered blocks, which reflects the high encryption quality. A final notable point is that the histograms of encrypted RGB components for all of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with ECB operation mode are not homogeneous, which reflects the inapplicability of this operation mode in securing information.

D. EXPERIMENT 4

The performance of the proposed cryptosystem with different operation modes and the cryptosystem of [25] is investigated using various differential test metrics in this section. The differential tests were employed to check the effect of one-pixel modification on the entire encrypted image using the proposed cryptosystem and the cryptosystem of [25]. The following two indicators are employed: the NPCR and UACI. The NPCR computes the percentage of dissimilar pixels to the entire pixels in each of the two encrypted images E_1 and E_2 of similar original images with just a single difference in one pixel, while the UACI measures the mean intensity of the difference between the two enciphered color images E_1 and E_2. Table 5 lists the *NPCR* and *UACI* values between two encrypted RGB components for the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem and the cryptosystem of [25] with one-pixel change in the original RGB components. As it could be seen from the *NPCR* and *UACI* results in Table 5, the proposed color image cryptosystem with different operation modes gives the best results compared with the cryptosystem of [25]. This proves that the proposed cryptosystem is very sensitive to small modifications in RGB components of the original color images, which reflects a high encryption quality.

E. EXPERIMENT 5

In this experiment, the resistance of the proposed cryptosystem with different operation modes to the presence of AWGN is examined during the decryption phase. The following noise immunity metrics are utilized in conducting such task.

1) PSNR

The *PSNR* is utilized for examining the quality of decrypted RGB components. The higher the *PSNR* values are, the stronger the noise immunity. Table 6 presents the evaluated *PSNR* values in dB for the decrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances for the encrypted RGB components. Form this table, one can notice that the *PSNR* values of the decrypted RGB components for the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed color image cryptosystem with different operation modes increase as the noise variances in the encrypted RGB components increase. It is also noticed generally that the highest and lowest *PSNR* values for all decrypted RGB components of the tested color images are obtained with the proposed cryptosystem with the OFB and CFB operation modes, respectively. This means that the OFB is the best

TABLE 8. The *SSIM* estimations of decrypted RGB components of medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.

Image	Operation modes		*SSIM* with different *SNRs* in dB				
			10	20	30	40	50
Tux	CBC	R	0.2195	0.2268	0.6750	1	1
		G	0.2180	0.2247	0.6721	1	1
		B	0.2180	0.2236	0.6803	1	1
	CFB	R	0.0077	0.0084	0.0079	0.0082	0.0082
		G	0.0080	0.0077	0.0082	0.0079	0.0079
		B	0.0070	0.0079	0.0077	0.0081	0.0081
	ECB	R	0.2259	0.2282	0.5532	1	1
		G	0.2271	0.2284	0.5268	1	1
		B	0.2277	0.2296	0.5217	1	1
	OFB	R	0.7582	0.8680	0.9962	1	1
		G	0.7607	0.8728	0.9967	1	1
		B	0.6927	0.8734	0.9932	1	1
Bit Map	CBC	R	0.2671	0.2775	0.4915	1	1
		G	0.2639	0.2756	0.4307	1	1
		B	0.2618	0.2742	0.3757	1	1
	CFB	R	0.0090	0.0066	0.0098	0.0097	0.0097
		G	0.0095	0.0100	0.0076	0.0080	0.0080
		B	0.0077	0.0097	0.0078	0.0084	0.0084
	ECB	R	0.2752	0.2845	0.4942	1	1
		G	0.2766	0.2828	0.4288	1	1
		B	0.2742	0.2795	0.3768	1	1
	OFB	R	0.7907	0.9178	0.9876	1	1
		G	0.8306	0.9254	0.9894	1	1
		B	0.7961	0.9027	0.9828	1	1
Medical	CBC	R	0.0069	0.0248	0.2237	1	1
		G	0.0043	0.0141	0.4175	1	1
		B	0.0046	0.0892	0.8393	1	1
	CFB	R	0.0026	0.0035	0.0276	0.5904	0.5904
		G	0.0038	0.0032	0.1007	0.6079	0.6079
		B	0.0012	0.0040	0.5310	0.6133	0.6133
	ECB	R	0.0051	0.0183	0.2481	1	1
		G	0.0050	0.0248	0.3312	1	1
		B	0.0021	0.0146	0.8222	1	1
	OFB	R	0.3954	0.6997	0.9719	1	1
		G	0.4110	0.7300	0.9869	1	1
		B	0.4456	0.7822	0.9988	1	1
Water Lilies	CBC	R	0.0079	0.0065	0.3341	1	1
		G	0.0081	0.0140	0.7261	1	1
		B	0.0036	0.0048	0.1737	1	1
	CFB	R	0.0073	0.0093	0.0072	0.0075	0.0075
		G	0.0097	0.0105	0.0088	0.0087	0.0087
		B	0.0047	0.0053	0.0058	0.0070	0.0070
	ECB	R	0.0089	0.0086	0.3396	1	1
		G	0.0087	0.0139	0.7247	1	1
		B	0.0013	0.0067	0.1776	1	1
	OFB	R	0.7554	0.9112	0.9952	1	1
		G	0.7995	0.9368	0.9993	1	1
		B	0.6142	0.8511	0.9873	1	1

operation mode in terms of noise immunity and the CFB is the worst one. These results reflect the immunity of the proposed cryptosystem to noise, which reveals high encryption quality. Table 7 gives the decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances. Form this table, one can visually see that the decryption quality increases as the noise variances on the encrypted RGB components decrease. Also, form these results, it is easy to notice visually that the best and worst decrypted RGB components of the tested color images are obtained with the proposed cryptosystem with OFB and CFB operation modes, respectively. Consequently, one can conclude that the OFB operation mode is superior to the other examined operation modes in terms of noise immunity and the CFB is the worst one, which again ensures the results obtained in Table 6.

2) STRUCTURAL SIMILARITY (*SSIM*)

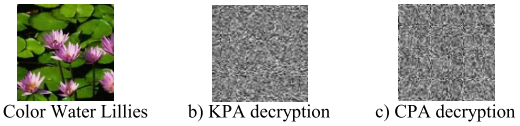
The *SSIM* is utilized to assess the quality of decrypted images. Generally, the *SSIM* values are between zero and one. If the *SSIM* value is high, this means good immunity to noise. Table 7 lists the calculated *SSIM* values for the decrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances. From Table 8, one can notice that the highest and lowest *SSIM* values are obtained with the OFB and CFB operation modes, respectively, and the other operation modes yield intermediate *SSIM* values. This again goes in line with the results listed in Tables VI and VII, which reveal that the OFB operation mode is the optimal one to utilize in terms of noise immunity.

3) FEATURE SIMILARITY INDEX (*FSIM*)

The *FSIM* is employed to assess the decrypted image quality. It is known that the *FSIM* values are between zero and one. Higher values of *FSIM* indicate that the proposed color image cryptosystem immunity to noise is high. In Table 9, the obtained *FSIM* values for the decrypted RGB components of the tested Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances are listed. Again, it is easy to note that the OFB and CFB operation modes yield the highest and lowest *FSIM* values, respectively. These results confirm the results presented in Tables 6, 7 and 8. It is clear that the OFB mode is superior to other operation modes in terms of noise immunity.

4) EXPERIMENT 5

In this experiment, the immunity of the proposed color image cryptosystem to two types of attacks is tested. The first is the plaintext attack (KPA), while the second is the chosen plaintext attack (CPA). The tests are performed on Barbra image shown in Figure 11(a). Figure 11(b) gives the decryption result of KPA, while Figure 11(c) gives the



a) Color Water Lillies plainimage | b) KPA decryption result, CC=0.0031 | c) CPA decryption result, CC=0.0027

FIGURE 11. Robustness of the proposed color image cryptosystem to KPA and CPA.

TABLE 9. The *FSIM* estimations of decrypted RGB components of Medical, Bit Map, Tux and Water Lilies color images using the proposed cryptosystem with different operation modes under different noise variances.

Image		Operation modes	*FSIM* with different *SNRs* in dB				
			10	20	30	40	50
Tux	CBC	R	0.2195	0.2268	0.6750	1	1
		G	0.2180	0.2247	0.6721	1	1
		B	0.2180	0.2236	0.6803	1	1
	CFB	R	0.0077	0.0084	0.0079	0.0082	0.0082
		G	0.0080	0.0077	0.0082	0.0079	0.0079
		B	0.0070	0.0079	0.0077	0.0081	0.0081
	ECB	R	0.2259	0.2282	0.5532	1	1
		G	0.2271	0.2284	0.5268	1	1
		B	0.2277	0.2296	0.5217	1	1
	OFB	R	0.7582	0.8680	0.9962	1	1
		G	0.7607	0.8728	0.9967	1	1
		B	0.6927	0.8734	0.9932	1	1
Bit Map	CBC	R	0.2671	0.2775	0.4915	1	1
		G	0.2639	0.2756	0.4307	1	1
		B	0.2618	0.2742	0.3757	1	1
	CFB	R	0.0090	0.0066	0.0098	0.0097	0.0097
		G	0.0095	0.0100	0.0076	0.0080	0.0080
		B	0.0077	0.0097	0.0078	0.0084	0.0084
	ECB	R	0.2752	0.2845	0.4942	1	1
		G	0.2766	0.2828	0.4288	1	1
		B	0.2742	0.2795	0.3768	1	1
	OFB	R	0.8932	0.9602	0.9957	1	1
		G	0.9051	0.9689	0.9967	1	1
		B	0.9061	0.9639	0.9950	1	1
Medical	CBC	R	0.1841	0.1882	0.444	1	1
		G	0.1725	0.1741	0.6404	1	1
		B	0.1570	0.1624	0.8600	1	1
	CFB	R	0.1846	0.1848	0.3070	0.7520	0.7520
		G	0.1716	0.1708	0.4633	0.7557	0.7557
		B	0.1578	0.1544	0.6327	0.7686	0.7686
	ECB	R	0.0051	0.0183	0.2481	1	1
		G	-0.005	0.0248	0.3312	1	1
		B	0.0021	0.0146	0.8222	1	1
	OFB	R	0.3954	0.6997	0.9719	1	1
		G	0.4110	0.7300	0.9869	1	1
		B	0.4456	0.7822	0.9988	1	1
Water Lilies	CBC	R	0.0079	0.0065	0.3341	1	1
		G	0.0081	0.0140	0.7261	1	1
		B	0.0036	0.0048	0.1737	1	1
	CFB	R	0.0073	0.0093	0.0072	0.0075	0.0075
		G	0.0097	0.0105	0.0088	0.0087	0.0087
		B	0.0047	0.0053	0.0058	0.0070	0.0070
	ECB	R	0.0089	0.0086	0.3396	1	1
		G	0.0087	0.0139	0.7247	1	1
		B	0.0013	0.0067	0.1776	1	1
	OFB	R	0.7554	0.9112	0.9952	1	1
		G	0.7995	0.9368	0.9993	1	1
		B	0.6142	0.8511	0.9873	1	1

decryption result of CPA. The obtained *CC* value for KPA is 0.0031, while that for CPA is 0.0027. These results ensure that the proposed cryptosystem is robust to both types of attacks.

VI. CONCLUSION

This paper presented an efficient color image cryptosystem that employs RC6 with different operation modes to encrypt color images with few details. A simulation model has been

built to assess the performance of the proposed color image cryptosystem with different operation modes using various encryption quality metrics. The simulation results show that the utilization of CBC, CFB, and OFB operation modes with the proposed color image cryptosystem is effective in hiding all information within the tested color images, even if the source color images have some similar blocks. On the other hand, the results also reveal that utilizing the ECB mode is not appropriate as it cannot efficiently hide the information in the examined color images with few details. Moreover, the results ensure the superiority of the OFB operation mode from the noise immunity perspective. The attained results ensure the applicability of the proposed color image cryptosystem and its efficiency in terms of security, encryption quality, and immunity to noise.

REFERENCES

[1] J. S. Fouda, A. Eyebe, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014.

[2] K. M. Ali and M. Khan, "A new construction of confusion component of block ciphers," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32585–32604, Nov. 2019.

[3] O. S. Faragallah, "Digital image encryption based on the RC5 block cipher algorithm," *Sens. Imag., Int. J.*, vol. 12, nos. 3–4, pp. 73–94, Dec. 2011.

[4] C. B. B. Aguila, A. M. Sison, and R. P. Medina, "Enhanced RC6 permutation-diffusion operation for image encryption," in *Proc. Int. Conf. Data Sci. Inf. Technol. (DSIT)*, 2018, pp. 64–68.

[5] A. M. Elshamy, A. N. Z. Rashed, A. E.-N.-A. Mohamed, O. S. Faragalla, Y. Mu, S. A. Alshebeili, and F. E. El-Samie, "Optical image encryption based on chaotic baker map and double random phase encoding," *J. Lightw. Technol.*, vol. 31, no. 15, pp. 2533–2539, Aug. 1, 2013.

[6] H. M. Elhoseny, H. E. H. Ahmed, A. M. Abbas, H. B. Kazemian, O. S. Faragallah, S. M. El-Rabaie, and F. E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," *Signal, Image Video Process.*, vol. 9, no. 3, pp. 611–622, Mar. 2015.

[7] E. A. Naeem, M. M. Abd Elnaby, N. F. Soliman, A. M. Abbas, O. S. Faragallah, N. Semary, M. M. Hadhoud, S. A. Alshebeili, and F. E. A. El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *J. Syst. Softw.*, vol. 97, pp. 118–127, Nov. 2014.

[8] Y. Naito and T. Sugawara, "Lightweight authenticated encryption mode of operation for tweakable block ciphers," in *Proc. IACR Trans. Cryptograph. Hardw. Embedded Syst.*, 2020, pp. 66–94.

[9] Z. Shao, X. Liu, Q. Yao, N. Qi, Y. Shang, and J. Zhang, "Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyrator domain," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115662.

[10] A. M. Elshamy, F. E. A. El-Samie, O. S. Faragallah, E. M. Elshamy, H. S. El-Sayed, S. F. El-Zoghdy, A. N. Z. Rashed, A. El-Naser, A. Mohamed, and A. Q. Alhamad, "Optical image cryptosystem using double random phase encoding and Arnold's cat map," *Opt. Quantum Electron.*, vol. 48, no. 3, 2016, Art. no. 212.

[11] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105816.

[12] S. Rana, "A survey paper of lightweight block ciphers based on their different design architectures and performance metrics," *Int. J. Comput. Eng. Inf. Technol.*, vol. 11, no. 6, pp. 119–129, 2019.

[13] H. M. Elhoseny, O. S. Faragallah, H. E. H. Ahmed, H. B. Kazemian, H. S. El-Sayed, and F. E. A. El-Samie, "The effect of fractional Fourier transform angle in encryption quality for digital images," *Optik*, vol. 127, no. 1, pp. 315–319, 2016.

[14] J. Mahalakshmi and K. Kuppusamy, "An efficient image encryption method based on improved cipher block chaining in cloud computing as a security service," *Austral. J. Basic Appl. Sci.*, vol. 10, no. 2, pp. 297–306, 2016.

[15] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Cybersecurity and Secure Information Systems*. Cham, Switzerland: Springer, 2019, pp. 31–42.

[16] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[17] H. R. Nematis, Ed., *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering: Information Encryption and Cyphering*. Hershey, PA, USA: IGI Global, 2010.

[18] F. Elgendy, A. M. Sarhan, T. E. Eltobely, S. F. El-Zoghdy, H. S. El-sayed, and O. S. Faragallah, "Chaos-based model for encryption and decryption of digital images," *Multimedia Tools Appl.*, vol. 75, no. 18, pp. 11529–11553, Sep. 2016.

[19] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Inf. Secur. J., Global Perspective*, vol. 29, no. 2, pp. 91–101, Mar. 2020.

[20] H. E.-D.-H. Ahmed, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," *Opt. Eng.*, vol. 45, no. 10, Oct. 2006, Art. no. 107003.

[21] R. E. J. Paje, A. M. Sison, and R. P. Medina, "Multidimensional key RC6 algorithm," in *Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy (ICCSP)*, 2019, pp. 33–38.

[22] S. Banik, A. Bogdanov, and F. Regazzoni, "Compact circuits for combined AES encryption/decryption," *J. Cryptograph. Eng.*, vol. 9, no. 1, pp. 69–83, Apr. 2019.

[23] A. Subandi, M. S. Lydia, R. W. Sembiring, M. Zarlis, and S. Efendi, "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, Oct. 2018, Art. no. 012119.

[24] R. Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)," *J. Phys., Conf. Ser.*, vol. 954, Jan. 2018, Art. no. 012009.

[25] E. A. Naeem, M. M. A. Elnaby, H. S. El-Sayed, F. E. A. El-Samie, and O. S. Faragallah, "Wavelet fusion for encrypting images with a few details," *Comput. Elect. Eng.*, vol. 54, pp. 450–470, Aug. 2016.

[26] V. K. Pachghare, *Cryptography and Information Security*. New Delhi, India: PHI Learning, 2019.

[27] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[28] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[29] N. Jiang, X. Dong, H. Hu, Z. Ji, and W. Zhang, "Quantum image encryption based on henon mapping," *Int. J. Theor. Phys.*, vol. 58, no. 3, pp. 979–991, Mar. 2019.

[30] Q. Zhang and L. Liu, "DNA coding and chaos-based image encryption algorithm," *J. Comput. Theor. Nanoscience*, vol. 10, no. 2, pp. 341–346, Feb. 2013.

[31] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.

[32] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *Int. J. Bifurcation Chaos*, vol. 29, no. 9, Aug. 2019, Art. no. 1950115.

[33] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.

[34] A. U. Rehman and X. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on chaos, DNA and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 2105–2133, Jan. 2019.

[35] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, "Image encryption using finite-precision error," *Chaos, Solitons Fractals*, vol. 123, pp. 69–78, Jun. 2019.

[36] Ü. Çavu oğlu, S. Panahi, A. Akgül, S. Jafari, and S. Kaçar, "A new chaotic system with hidden attractor and its engineering applications: Analog circuit realization and image encryption," *Anal. Integr. Circuits Signal Process.*, vol. 98, no. 1, pp. 85–99, Jan. 2019.

[37] A. H. M. Ragab, O. S. F. Allah, and A. Y. Noaman, "Encryption quality analysis of the RCBC block cipher compared with RC6 and RC5 algorithms," *IACR Cryptol. ePrint Arch.*, vol. 2014, no. 169, pp. 1–13, 2014.
[38] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014.
[39] T. Sivakumar and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos," *Opt. Laser Technol.*, vol. 111, pp. 196–204, Apr. 2019.
[40] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Process.*, vol. 109, pp. 119–131, Apr. 2015.
[41] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, 2019.
[42] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

OSAMA S. FARAGALLAH received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently a Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator, from 1997 to 2002, and has been an Assistant Lecturer, from 2002 to 2007. Since 2007, he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. His current research interests include network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.

ASHRAF AFIFI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electronic and communication engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently an Associate Professor with the Department of Computer Engineering, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include communication security, image processing, and image encryption.

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. He is currently working as a Lecturer and an Assistant Professor with the ECE Department FEE, Menoufia University. His research interests include wireless mobile and multimedia communications systems, image and video signal processing, efficient 2d video/3d multi-view video coding, multi-view video plus depth coding, 3d multi-view video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3d video watermarking, steganography, and encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software defined networks, the internet of things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, deep learning in signal processing, and communication systems applications.

HALA S. EL-SAYED received the B.Sc.(Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-Kom, Egypt, in 2000, 2004, and 2010, respectively. She is currently an Assistant Professor with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was a Demonstrator, from 2002 to 2004, and has been an Assistant Lecturer, from 2004 to 2010. Since 2010, she has been a Teaching Staff Member with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University. Her research interests include database security, network security, data hiding, image encryption, wireless sensor network, secure building automation systems, medical image processing, and biometrics.

MOHAMMED A. ALZAIN received the Bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, the master's degree in information technology from La Trobe University, in 2010, and the Ph.D. degree from the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia, in September 2014. His Ph.D. research is in cloud computing security. He is currently an Associate Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include cloud computing security, multimedia security, image encryption, steganography, and medical image processing.

JEHAD F. AL-AMRI is currently an Associate Professor in computer informatics. He has graduated from the Centre for Computing and Social Responsibility, De Montfort University. He is currently an Associate Professor with the Department of Information Technology, Faculty of Computers and Information Technology, Taif University, Saudi Arabia.

FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the *Digital Signal Processing Journal, in 2008.*