Grayscale and color images encryption in a DRPE assisted by SPHIT, RLE, QR code and two chaos logistic maps

Abdallah K. Cherri and Ihab B. Dirawieh

Kuwait University, College of Engineering and Petroleum, Electrical Engineering Department, P. O. Box 5969; Safat 13060, Kuwait

Corresponding Author: abdallah.cherri@ku.edu.kw

Submitted: 21-03-2022

Revised: 29-06-2022

Accepted: 05-07-2022

ABSTRACT

A non-linear encryption approach for compressed grayscale and color images is proposed in Double Random Phase Encoding (DRPE) setup using two compression algorithms: Set Partitioning in Hierarchical Trees (SPIHT) and Run-length encoding (RLE). The compressed image is then segmented and embedded in multiple Quick Response (QR) codes, which are combined again into a single image. Further, this single image is scrambled by two-coupled chaos logistic maps, at which the scrambled image is now ready for DRPE encryption. The use of two-coupled chaos logistic increases the security level of this proposed DRPE encryption from various attacks. The proposed DRPE encryption is extended to handed color images, which are segregated into three color-channels (Red, Green and Blue), where each channel is individually encrypted. For grayscale images, the proposed system will have three security key codes while for color images it has nine security key codes. The robustness and invulnerability of the proposed scheme against various attacks is demonstrated through cryptoanalysis and computer simulation results.

Keywords: Optical Encryption; Double random phase encoding; Set Partitioning in Hierarchical Tree; Run-length encoding and QR code.

INTRODUCTION

Nowadays, the huge usage of the internet and computer technologies governs almost every aspect of our daily life. Consequently, the field of information security applications has received growing attention by researchers (Yadav et al., 2021; Oad et al., 2014; Chen et al., 2014; Liu et al., 2014; Javidi et al., 2016) who developed many digital and optical techniques to secure the information transmission. Among the optical techniques, DRPE is one of the earliest proposed systems for image encryption in the field of optical cryptosystem technology (Refregier et al., 1995). DRPE scheme uses a 4-*f* coherent optical set-up where two random-phase masks (RPMs) provide the security keys: the first RPM is used at the input plane and the second RPM is used at the Fourier plane. It has been demonstrated that the security of the DRPE encryption faces various challenges regarding its resistance against various type of attacks (Frauel et al. 2007; Jiao et al., 2018). In the literatures, many methods were proposed to improve the security level of DRPE using non Fourier transform domain for processing the information such as the use of fractional Fourier, Fresnel, and Gyrator domains (Joshi et al., 2009; Sui et al., 2013; Situ et al., 2004; Cuadrado-Laborde et al., 2011). In these encryption techniques, the original image is encoded into a full of noise ciphertext image using an RPM that causes the decrypted image to contain speckle noise, which degrades the quality of the decrypted image. To reduce the effect of the speckle noise, several techniques were proposed such as fully-phase encoding, modifying the encrypted function and using the Quick Response (QR) code. Particularly, the QR code attracts enough popularity as a data container to convert data into optical security images in optical encryption systems and data security applications (Barrera et al., 2013; Qin et al., 2018). However, one of the limitations of the use of QR code is the constraint on the data size that can be embedded.

Nowadays, the growing interest of transmitting and securing information, and in particular for grayscale and color images, pushes researchers forward to develop and employ various image compression techniques aiming at reducing data transmission and increasing the security levels of the data. In this regard, the Set

Partitioning in Hierarchical Tree (SPHIT) (Said et al., 1996) is one of the compression techniques that can achieve both aims (Shapiro et al., 2002). Many publications have tried to enhance the efficiency and the security level of the SPHIT by modifying the compressed data, either by permuting it with the chaos function (Zhang et al., 2013) or by encrypting a partial part of it (Taneja et al., 2009). On the other hand, since the amplitude encryption of DRPE is a linear process, it is vulnerable to various type of attacks such as chosen-plaintext attack (CPA), known-plaintext attack (KPA), and cipher-only attack (COA) (Frauel et al. 2007; Jiao et al. 2018). Therefore, to enhance the security level of the amplitude DRPE scheme, researchers proposed nonlinear encryption methods and used different Transform domains to make the encryption system less vulnerable to break (Joshi et al., 2009).

In this paper, we present a DRPE-based cryptosystem for grayscale and color images. First, the to-be-encrypted image is compressed into a bitstream using the SPIHT and RLE compression algorithms. Second, the resulting compressed data is converted into multiple QR code images which they are combined again into a single image. Note that the two compression techniques (SPHIT and RLE) permit the successful use of the QR code. Third, the combined QR code image is scrambled with two chaos logistic maps where the initial conditions of the chaos functions are kept as the security keys. Finally, the scrambled image is sent to the DRPE setup to complete the encryption process. For decryption, the inverse operations of encryption are performed on the decrypted image, i.e., inverse chaos, inverse QR, inverse RLE, and inverse SPHIT. The proposed cryptosystem achieves both objectives of using less amount of data that are converted to multiple QR codes and improving the security level through scrambling functions. Further, a cryptoanalysis against various attacks is provided and a series of computer simulations are presented to demonstrate the performance and the feasibility of the proposed grayscale/color image cryptosystem.

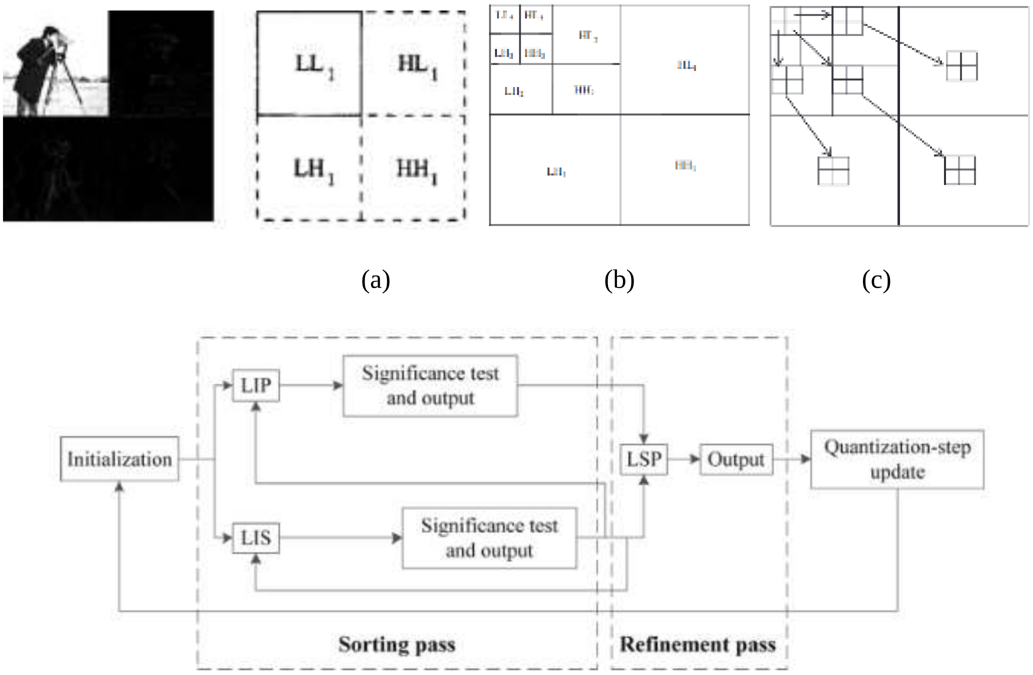
IMAGE COMPRESSION AND CHAOS MAPS

The overgrowing demand of real-time information transmission and processing in data-processing networks and communication systems lead to the considerable efforts that are devoted to data encryption and secure transmission. Over the years, to achieve this goal, the data processing researchers exercise intensive efforts for data compressing, encoding, and securing techniques to reduce the images size. In this regard, SPHIT algorithm (Said et al., 1996) is considered as one of the most efficient compression techniques that reconstructs images with high quality. SPIHT algorithm is based on the Discrete Wavelet Transform (DWT) where an image passes first through a DWT block decomposition to obtain the wavelet coefficients of the image, which are organized into a spatial treelike structure, as shown in Figure 1. In Fig. 1a, the image is decomposed first, using one level of the wavelet transform, into four sub-bands: *LL*, *HL*, *LH*, and *HH*. The upper-left sub-band *LL* approximates the original image whereas the sub-bands *HL*, *LH*, and *HH* preserve the vertical edge details, horizontal edge details, and diagonal details, respectively. Each sub-band will be recursively decomposed into multiple level and produces sets of wavelet coefficients as shown in Fig. 1(b).

Next, the resulting coefficients are arranged into a Spatial Orientation Tree (SOT) as displayed in Fig. 1(c). The SPIHT algorithm go through four main steps: initialization, sorting, refinement, and quantization, as illustrated in Fig. 1(d). The SPHIT program works on the wavelet coefficients and generates three significant lists according to a significant test which is defined as:

$$S_n(X) = \begin{cases} 1, & max_{(i,j)\in X}\{|c_{i,j}| \geq 2^n\} \\ 0, & Otherwise \end{cases} \tag{1}$$

where $c_{i,j}$ denotes the coefficient at (i,j) coordinates; X indicates the coordinate step; n denotes an integer number; and 2^n is the threshold for the test. Note that SPIHT algorithm starts by testing the significant bits of the coefficients as presented in Eq. (1) where $S_n(X) = 1$ if the significant bit X value is higher than the threshold 2^n; otherwise $S_n(X) = 0$. Thus, the SPIHT scheme groups the coefficients into three ordered lists: (i) LIP for the list of insignificant pixels, (ii) LIS for the list of insignificant sets, and (iii) LSP for the list of significant pixels. References (Zhang et al., 2017; Xiang et al., 2014) have well summarized descriptions of the SPIHT algorithm. In summary, SPIHT algorithm delivers an excellent compression which can be applied to 1D, 2D, and 3D signals (Laiphrakpam et al., 2021; Devi et al., 2021).



(a) (b) (c)

(d)

Figure 1. One level of DWT image decomposition: (b) Three-level DTW decomposition, (c) Spatial orientation tree in SPIHT algorithm, (d) the four steps of the algorithm (After References (Zhang et al., 2017; Xiang et al., 2014

Being a lossless data compression and due to its simplicity in encoding/decoding data, the RLE technique has been employed in many cryptosystem applications (Qin et al., 2018; Zea et al., 2016). The RLE generates a bitstream which contains individual data value and the length (or counts or runs) of the data instead of the original image value. The RLE appears in the compressed sequence data as $[v_{RLE}(i)\ \ r_{RLE}(i)]$, where $v_{RLE}(i)$ denotes the value on a single pixel and $r_{RLE}(i)$ is the count for the repeated value of $v_{RLE}(i)$. For example, if the bitstream contains 'bbbbbccccaaaaaaaeeeeee' the RLE format is [b5 c4 a7 e6]. Obviously, the RLE string can be significantly shorter than the original string representation. For binary images, the compression ratio would be very high. For instance, the binary sequence [11111110000011111111] is compressed into RLE format as [71 50 81]. Fortunately, RLE compression is very helpful for the kind of image that has many runs such as cartoon images, construction sketches, and binary images. Unfortunately, sometimes the RLE does not efficiently compress an image that does not include many runs.

Chaos-based cryptosystem is regarded as one of the safe methods to transmit and protect data due to its many attractive features such as high sensitivity and dependence on initial conditions, control parameters, unpredictable behavior, and randomness (Trujillo-Toledo et al., 2021; Cun et al., 2021). However, to improve security and also to offer good resistance to external attacks, developers propose chaotic systems with higher dimensions such as 2D, 3D, 4D (Sahari et al., 2018; Norouzi, 2014) where the dynamic structure and multiple parameters of these multi-dimensional chaotic functions made it difficult to incorporate into hardware/software, and consequently, the computational complexity have increased. Therefore, due to its simplicity for implementation as well as its low computational complexity, 1D chaos encryption system might be preferred over multi-dimensional methods for real-time image encryption.

The nonlinear formula of a chaos logistic map for one-dimension data can be presented as:

$$f(x) = p \cdot x \cdot (1 - x) \tag{2}$$

Where p is a control parameter known as a system parameter and it is restricted in the intervals $0 < p \leq 4$. The logistic chaos map can be written for the generated pattern as follows:

$$x_{n+1} = p \cdot x_n \cdot (1 - x_n) \tag{3}$$

In Eq. (3), the iteration value is restricted for $x_n \in [0,1]$ and x_o denotes the initial value. In addition, we have selected the control parameter value in the range $p \in [3.5699456,\ 4]$. A slight change of the initial chaos value leads to huge different random sequence pattern values, which are non-convergent and non-periodic. When scrambling an image with this logistic map, the encrypted image has low security due to its simplicity (such as the small key space as well as vulnerability to various attacks) (Sui et al., 2013). To alleviate this drawback, practically, some methods combined two 1-D logistic maps of nonlinear chaos functions where each function has its own tuning on its parameters. Accordingly, we can combine two logistic maps of chaos function to produce a series of random patterns:

$$\begin{aligned} x_{n+1} &= p \cdot x_n \cdot (1 - x_n) \\ y_{n+1} &= p \cdot y_n \cdot (1 - y_n) \end{aligned} \tag{4}$$

The two control parameters for generating random values are chosen according to the following equation:

$$\begin{aligned} p_x &= \begin{cases} 3.9111, & 0 < x_i \le 0.5 \\ 3.9666, & 0.5 < x_i \end{cases} \\ p_y &= \begin{cases} 3.9222, & 0 < y_i \le 0.5 \\ 4.0000, & 0.5 < y_i \end{cases} \end{aligned} \tag{5}$$

For an $M \times N$ image, we use Eqs. (4) and (5) to create sequences of random values $X = \{x_1, x_2, \dots, x_{M+K}\}$, $x_i \in [0, 1]$ and $Y = \{y_1, y_2, \dots, y_{N+K}\}$, $y_i \in [0, 1]$ with various initial values x_o and y_o and any integer K. In the encryption and decryption processes, the initial values x_o, y_o can serve as security keys.

DRPE-BASED CRYPTOSYSTEM FOR GRAYSCALE AND COLORED IMAGES

Figure 2 illustrates the optical DRPE-based encryption and decryption approaches. Let x and u denote the spatial and the Fourier domain coordinates, respectively, $f(x)$ and $e(x)$ represent the to-be-encrypted original image and the encrypted image, respectively. We use two RPMs $r(x) = exp[\, i2\pi\varphi_r(x)]$ and $h(x) = exp[\, i2\pi\varphi_h(x)]$, where both functions $\varphi_r(x)$ and $\varphi_h(x)$ are statically independent and uniformly distributed in the interval [0, 1]. The amplitude encryption of the original image $f(x)$ is obtained by two steps. In the first step, the original image $f(x)$ is bounded by the first RPM $r(x)$. In the second step, the bounded image $\{f(x)r(x)\}$ is convolved by the second RPM $h(x)$, which is the inverse Fourier transform (FT^{-1}) of the phase only function $H(u) = exp[\, i2\pi\Phi_h(u)]$. In Fig. 2(a) the original image $f(x)$ and $r(x)$ are displayed at the input plane of the DRPE. The first lens produces the FT of the input image $FT[f(x)r(x)]$ at its rear focal plane (the Fourier plane) at which we place the second RPM $H(u)$. After that, the second lens performs the FT^{-1} to obtain the encrypted image $e(x)$ at the output plane. Therefore, the encrypted image can be expressed as:

$$e(x) = FT^{-1}\{FT\{f(x)r(x)\}.H(u)\} = \{f(x)r(x)\} * h(x) \tag{6}$$

Where " $*$ " indicates the convolution operation. $e(x)$ can be processed either optically or digitally.

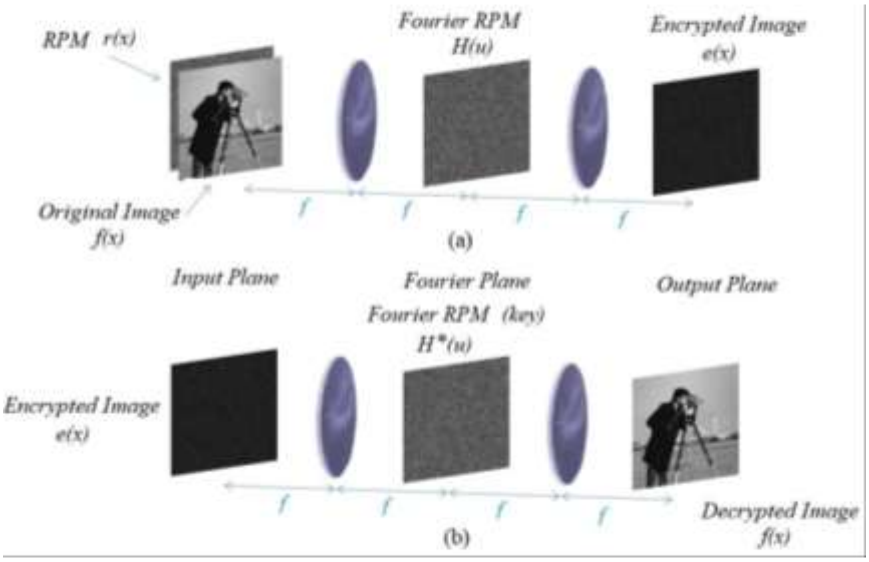


Figure 2. The optical DRPE scheme: (a) The encryption process, (b) The decryption process.

In the same way, Fig. 2(b) illustrates the optical decryption setup. The ciphertext or the encrypted image $e(x)$ is optically FT by the first lens as $e(u) = FT\{f(x)r(x)\}.H(u)$. At the Fourier plane, this signal is bounded by the complex conjugate of the second RPM $H^*(u)$ as $e(u).H^*(u) = FT\{f(x)r(x)\}.H(u).H^*(u) = FT\{f(x)r(x)\}$. At the focal point of the second lens (at the output plane) the function $FT^{-1}\{FT\{f(x)r(x)\}\} = f(x)r(x)$ is displayed. The phase function $r(x)$ is eliminated by using a CCD camera (square law or intensity device) to obtain the decrypted image $f(x)$. Note that The original image $f(x)$ can be retrieved only when the complex conjugate of the second RPM is available, i.e., $H^*(u) = exp[-i2\pi\Phi_h(u)]$, which represents the security code in the decryption process of Fig. 2(b).

Figure 3 illustrates the grayscale image encryption-decryption proposal where the sequential operations of SPIHT, RLE, QR code, and two logistic chaos maps are performed on $f(x)$ and set it ready for DRPE encryption. The SPIHT algorithm first converts the original image from two-dimensional data into a single bitstream shaped like binary data. After that, the bitstream is encoded by the RLE to achieve higher compressed data. Next, this compressed data is converted to multi QR code images and then these images are recombined into a single image. Finally, this new QR coded image is scrambled by two logistic chaos maps and is delivered to the DRPE scheme to complete the encryption process. For decryption, we just reverse the encryption process. The inverse chaos functions are applied to the decrypted image followed by the sequential applications of inverse QR, inverse RLE, inverse SPIHT algorithms to retrieve the original image $f(x)$. This proposed cryptosystem of grayscale images can be easily extended to handle color images. Three separate channels are generated to handle the color image which is decomposed into its three basic components: red (R), green (G), and blue (B). The three RGB images can now be considered as grayscale images and the encryption-decryption operations of Fig. 3 will be applied individually for each color. Practically, depending on the computational speed or the system size, we may have three individual channels to handle the three images in parallel, or we may use a single channel and send the RGB images sequentially to the encryption/decryption process.

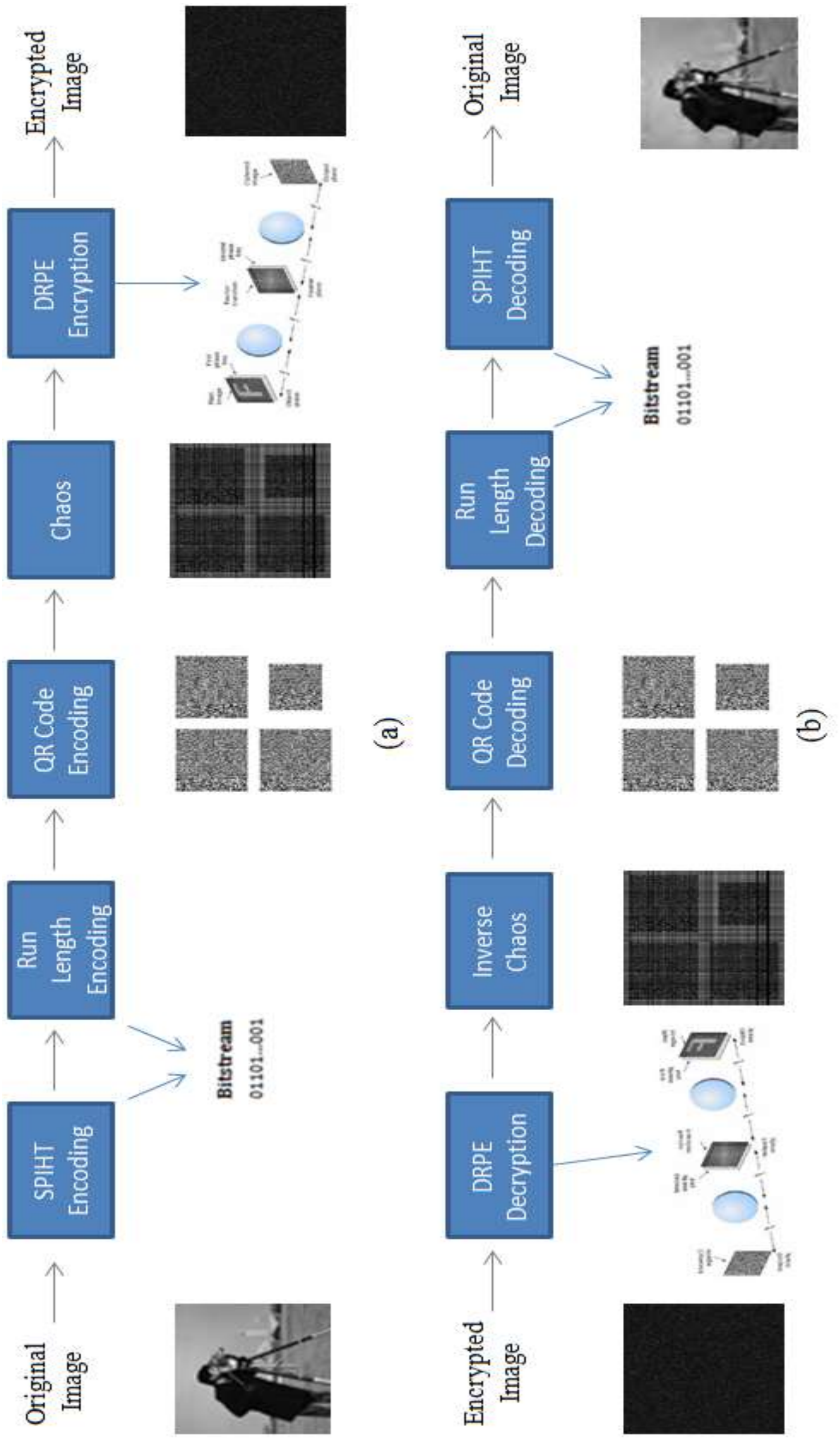


Figure 3. The proposed encryption/decryption system for grayscale images: (a) The encryption steps, (b) The decryption steps.

Figure 4 shows the encryption-decryption steps for each *R*, *G* and *B* channel individually, where for each channel the image goes through SPHIT and RLE compressions followed by multiple QR coding and combing and scrambling by two chaos logistic maps and then sending to the DRPE setup. Note that the security level of this encryption/decryption process is very high since that each color channel may have its own initial conditions in the chaos logistic maps as well its individual RPM for each channel.

To assess the quality of the decrypted grayscale image for the proposed encryption system, we will use the following correlation coefficients (*CC*) formula to measure the similarity between the original $f(x)$ and the decrypted $\hat{f}(x)$ images:

$$CC = \frac{\sum_{x=1}^{M}\left(f(x) - \overline{f(x)}\right)\left(\left(\hat{f}(x) - \overline{\hat{f}(x)}\right)\right.}{\sqrt{\left(\sum_{x=1}^{M}(f(x) - \overline{f(x)})^2\right)\ \left(\sum_{x=1}^{M}(\hat{f}(x) - \overline{\hat{f}(x)})^2\right)}} \tag{7}$$

The values of $\overline{f(x)}$ and $\overline{\hat{f}(x)}$ denote the sample means for the $f(x)$ and $\hat{f}(x)$, respectively. When handling color images, the *CC* expression Eq. (7) is modified to:

$$CC = \frac{CC_R + CC_G + CC_B}{3} \tag{8}$$

Where CC_R, CC_G, and CC_B indicate the *CC* for the *R*, *G* and *B* channels and they are calculated separately using Eq. (7).

COMPUTER SIMULATIONS AND DISCUSSION

A series of computer simulations have been carried out to present the performance and the feasibility of the proposed grayscale and color image encryption. Note that the control parameters of the two logistic chaos maps are sets according to Eq. (5).

For grayscale images, the initial condition values of the two-coupled chaos logistic maps are sets to x_o= 0.3202 and y_o= 0.5000. Fig. 5(a) shows a 64×64 pixels original image and Figs. 5(b) and 5(c) display the first RPM $r(x)$ and the second RPM $h(x)$, respectively, where each RPM is 512×512 pixels generated randomly by the computer's software. Fig. 5(d) is the combined four generated QR coded images after converting them from the bitstream characters. Note that we have used QR version 25 which has a maximum window size of 117×117 pixels and a maximum character length of 1269. The 64×64 pixels original image characters length is 3686, which is divided into three parts of 1000 characters each and one part of 686 characters. The four generated QR coded images are combined into an image of size 512x512 pixels. Fig. 5(e) shows the scrambled QR code images with the two logistic chaos maps. Fig. 5(f) shows the final encrypted image after sending the scrambled image to be encrypted by the DRPE scheme. Fig. 5(g) displays the decrypted image after employing the sequence of operations of the decryption process shown in Fig. 3(b), i.e., inverse chaos scrambling, QR decoding, and decompressing process for RLE and SPIHT algorithms, respectively. The calculated *CC* value is 0.991. It worth mentioning that the main source of the slight reduction in the quality of the decrypted image is due to the quantizing operation in the SPIHT compression technique.

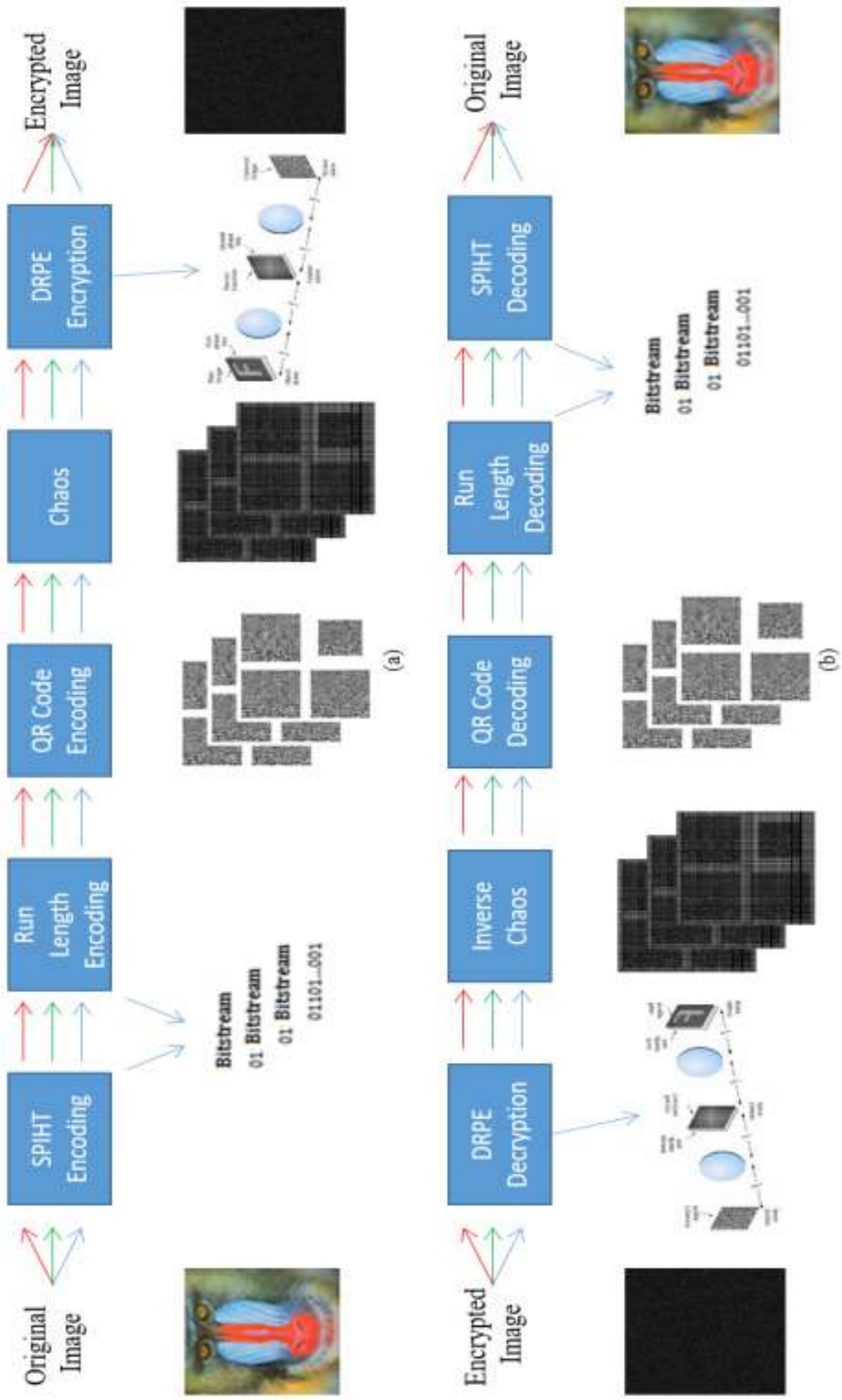


Figure 4. The encryption/decryption system for color images: (a) The encryption steps, (b) The decryption steps.

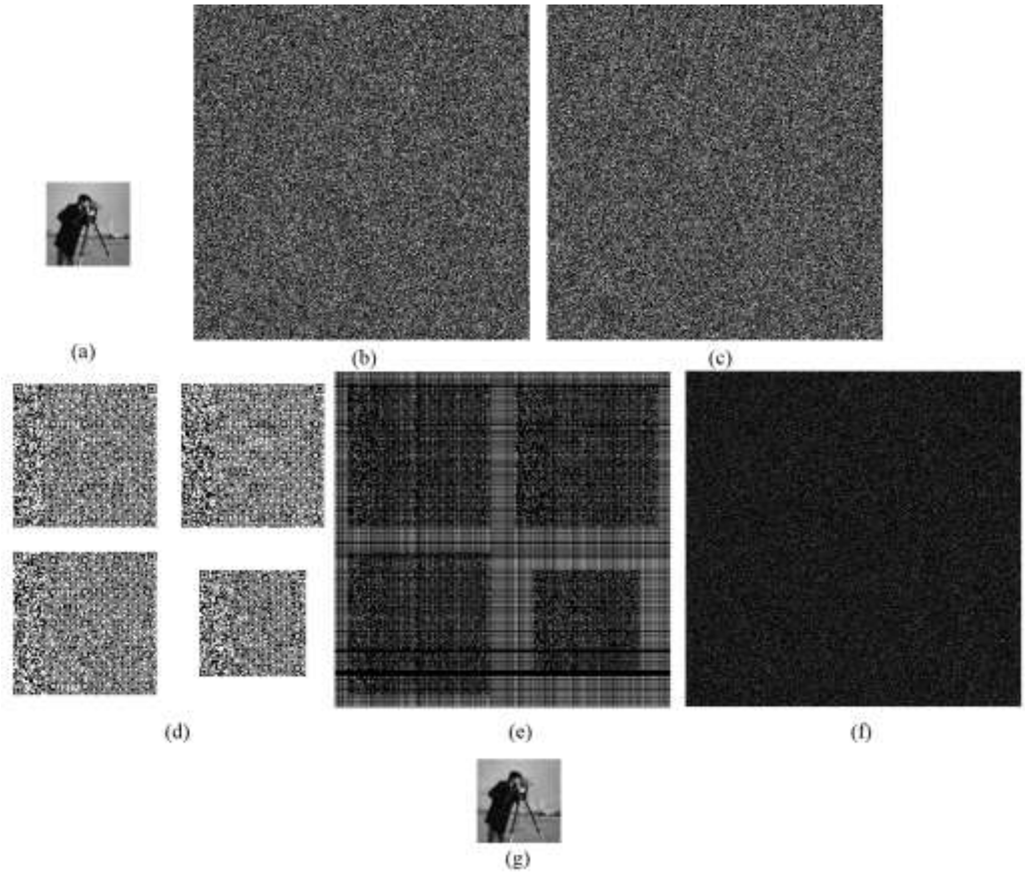


Figure 5. Simulation results for the proposed grayscale cryptosystem: (a) The 64×64 pixels original image, (b) The 512×512 pixels first RPM, (c) The 512×512 pixels second RPM (security key code), (d) The 512×512 pixels QR coded images, (e) The scrambled images related to (d), (f) The encrypted image, (g) The final decrypted image having $CC = 0.991$.

Figure 6 illustrates three tested images that have different image formats. The size of each image is 128×128 pixels and they are translated into 15 QR coded images using version 25 QR code. After compression, the length of decimal number sequence of the bitstream is 14752 characters. Again, we have split this bitstream characters into many parts (fourteen parts with 1000 characters and one part with 752 characters), then we combined them into a single 1280×1280 pixel*s* QR coded image.

For color images, we simulate a 64×64 pixels "Baboon.tif" image (Fig. 7(a)) to demonstrate the performance and effectiveness of the proposed cryptosystem. In this part, we applied the same initial conditions of the two chaos logistic maps of the grayscale encryption proposal, as presented in Eq. (5). We have chosen the six initial conditions (six security keys) for each channel separately as: (i) for R-channel x_{Ro}= 0.3202 and y_{Ro}= 0.5000, (ii) for G-channel x_{Go}= 0.3405 and y_{Go}= 0.4900, and (iii) for B-channel x_{Bo}= 0.3507 and y_{Bo}= 0.4800. In addition, we have selected three different RPMs and applied each one of them as a security key for each channel. Therefore, this proposed cryptosystem has nine security keys, which make the system strongly invulnerable to hack. Fig. 7(b) shows the encrypted image and Fig. 7(c) displays the decrypted image with *CC* = 0.9836 when all the correct security keys are used.

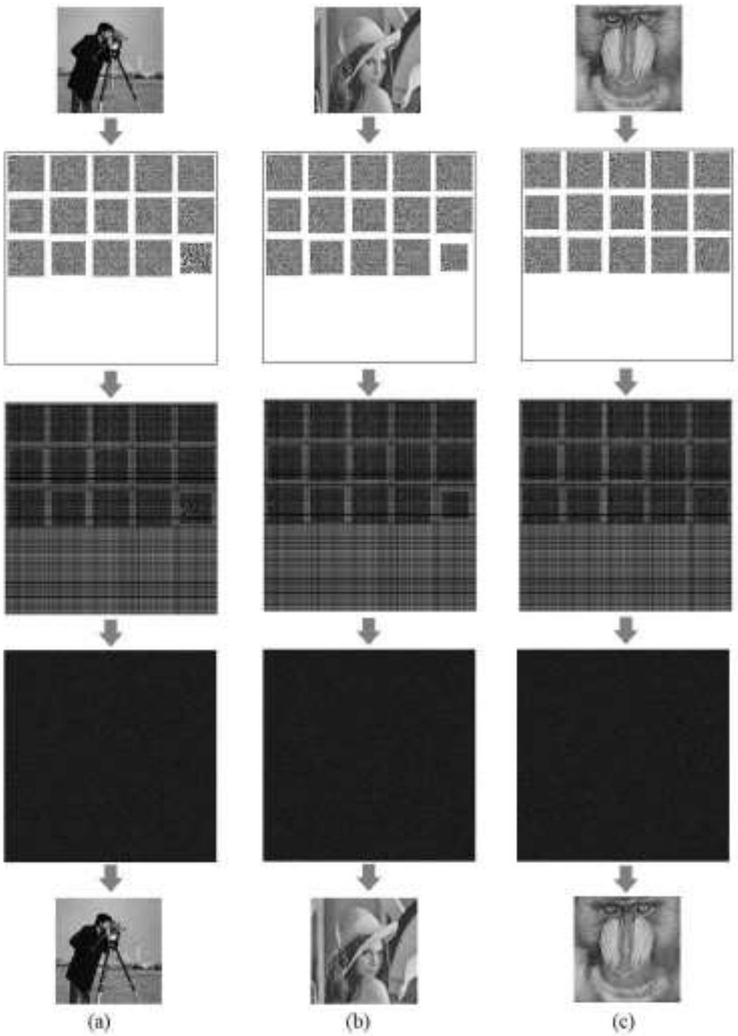


Figure 6. From top to bottom: (a) The original image “cameraman.png”, QR coded image, scrambled image, ciphertext and the decrypted image with *CC* = 0.9962, (b) The original image “lena.jpeg”, QR coded image, scrambled image, ciphertext and the decrypted image with *CC* = 0.9937, (c) The original image “Baboon.tif”, QR coded image, scrambled image, ciphertext and the decrypted image with *CC* = 0.9725. (All the original images and decrypted images in this Figure are 128×128 pixels and all QR coded image, scrambled image are 1280×1280 pixels)

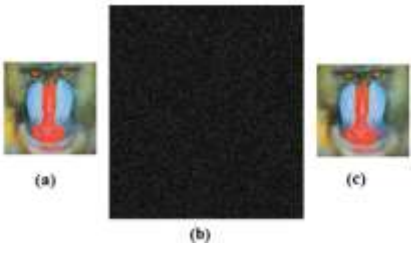


Figure 7. (a) The original 64×64 pixels “Baboon.tif” image, (b) The 512×512 pixels encrypted image, (c) The 64×64 pixels decrypted image with *CC* = 0.9836.

Security and Performance Analysis

In this section, for both grayscale and color images, we analyze the availability of the space of the security key $h(x)$, in addition to the sensitivity of the initial value of the two chaos functions, and the resistance against various attacks such as CPA, KPA and COA of the proposed encryption.

Key space Analysis and Sensitivity of the Initial Conditions

In DRPE encryption, hackers use the brute force attack to completely recover the second RPM $h(x)$ which has a size of $M \times N$ pixels, and each pixel has L possible outcomes. This means that the attackers need to exhaust L^{MN} attempts to regenerate $h(x)$. In our grayscale image simulation, $M = N = 512$ and $L = 256$, which yields 256^{262144} attempts to recover $h(x)$ while for color images the number of attempts is 3×256^{262144}. With this huge number of attempts, the brute force attack will fail to completely recover $h(x)$. Figure 8 shows examples of failure attempts to recover the QR coded images for incorrect use of the security key code $h(x)$.

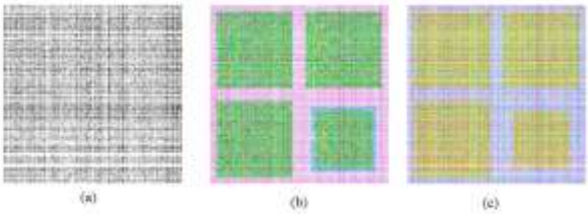


Figure 8. The decrypted QR coded images using wrong $h(x)$: (a) for grayscale image, (b) for the G-channel, (c) for the R & G-channels.

The variation of the initial value x_o of the first chaos function is up to 10^{-15} while the variation of the initial value y_o of the second chaos function is up to 10^{-16}. This means that the sensitivity of the chaos functions' initial values to variation is showing up to 15 (x_o) and 16 (y_o) digits after the decimal digit. For grayscale images and color images, the huge key paces are calculated as $256^{262144} \times 10^{15} \times 10^{16}$ and $3 \times 256^{262144} \times 10^{15} \times 10^{16}$, respectively. These huge key spaces will prevent any brute force attacks (Frauel et al., 2007; Jiao et al., 2018). The proposed encryption scheme has nine security keys. We have randomly tested the use of one or two incorrect security keys as demonstrated in Figure 9, which is a sample of some simulation results for both grayscale and color images. Fig. 9(a) displays the recovered image after adding 10^{-15} to x_o ($x_o = 0.3202 + 1 \times 10^{-15}$) while Fig. 9(b) shows the recovered image after adding 10^{-16} to y_o ($y_o = 0.5 + 1 \times 10^{-16}$). Figs. 9(c) and 9(d) display the retrieved QR codes when using incorrect initial chaos values for one channel only, i.e., for R-channel $x_{Ro} = 0.3202 + 1.0 \times 10^{-15}$ and B-channel $y_{Bo} = 0.4800 + 1.0 \times 10^{-16}$, respectively. Moreover, Fig. 9(e) is a simulation when using two incorrect chaos key values for different channels as G-channel $x_{Go} = 0.3405 + 1.0 \times 10^{-15}$ and B-channel $y_{Bo} = 0.4800 + 1.0 \times 10^{-16}$. Finally, Fig. 9(f) illustrates the use of two incorrect initial chaos values for the same channel G-channel $x_{Go} = 0.3405 + 1.0 \times 10^{-16}$ and $y_{Go} = 0.4900 \times 10^{-15}$.

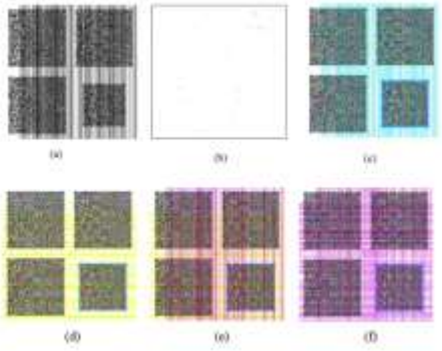


Figure 9. The retrieved grayscale images when using: (a) wrong $x_o = 0.3202 + 1 \times 10^{-15}$ and (b) wrong $y_o = 0.5 + 1 \times 10^{-16}$. (c)-(f) The retrieved QR codes for color images when using wrong initial chaos value: (c) for R-channel $x_{Ro} = 0.3202 + 1.0 \times 10^{-15}$, (d) for B-channel $y_{Bo} = 0.4800 + 1.0 \times 10^{-16}$, (e) for G-channel $x_{Go} = 0.3405 + 1.0 \times 10^{-15}$ & B-channel $y_{Bo} = 0.4800 + 1.0 \times 10^{-16}$, (f) for G-channel $x_{Go} = 0.3405 + 1.0 \times 10^{-16}$ & $y_{Go} = 0.4900 \times 10^{-15}$. (All images in this Figure are 512×512 pixels).

Chosen plaintext (CPA), known plaintext (KPA) and ciphertext only (COA) attacks.

The classical DRPE cryptosystem is vulnerable to various attacks such as CPA, KPA and COA (Jiao et al., 2018). Both CPA and KPA main target is to find the security key $h(x)$ by having a full knowledge of the structure of the DRPE cryptosystem, which is basically a linear process. Both attacks employ a plaintext (original image) and its corresponding ciphertext at the Fourier plane of the DRPE scheme by applying an iterative phase algorithm to retrieve $h(x)$.

In our cryptosystem proposal, the encryption/decryption is achieved through a series of steps starting with SPHIT, RLE, QR code, and logistic chaos maps. These steps break the linearity between the original image and the encrypted image, and eventually making the cryptosystem resistant to CPA & KPA (Qin et al., 2018).

COA hackers try to crack the DRPE by using two approaches. First, the COA technique requires that the original (plain) image to be the same size as the ciphertext, which is not the case in our proposal, as demonstrated in Fig. 5. Second, the attackers may also try to retrieve the permutated chaos function sequence, which is almost impossible due to the huge key space generated by the initial values of the chaos maps as it was demonstrated earlier. Thus, the proposed cryptosystem has significantly improved the security level compared with the traditional DRPE setup and can easily resist the COA.

Moreover, we have generated the histograms for four different grayscale ciphertext images as shown in Figure 10 (Baboon.tif, barbara.bmp, cameraman.tif and Lena.jpg). The four ciphertexts have almost the same histograms after the encryption process. Consequently, the hackers cannot obtain any visible information from these statistical results.

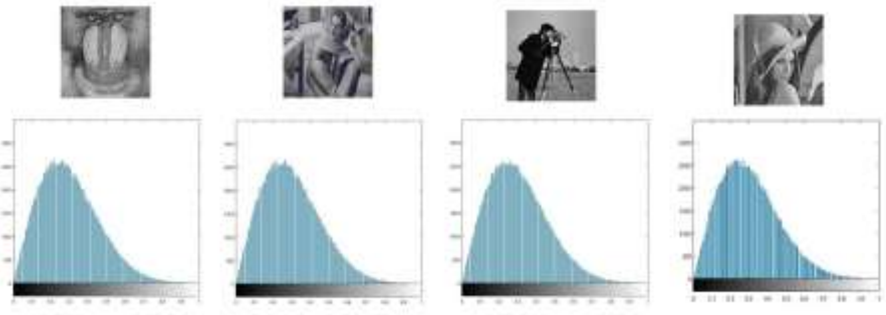


Figure 10. Histograms of various ciphertexts (Baboon.tif, barbara.bmp, cameraman.tif and Lena.jpg).

CONCLUSION

We have presented a very secure cryptosystem for grayscale and color images based on DRPE architecture. The original image is recorded into a single compressed bitstream using the SPIHT and the RLE compression algorithms. Then, the compressed bitstream is converted into multiple QR coded images and then they are combined into one single image. After that, this single image is scrambled by two chaos logistic maps and sent to the DRPE processor for encryption. We were able to successfully embedded grayscale and color images into QR coded images because SPIHT and RLE compression algorithms reduce the size of data, in contrast to the work in Reference (Qin et al., 2018) that deals with binary images only. Cryptoanalysis is performed that shows the huge space key and demonstrates the resistance of the proposed scheme against brute force, CPA, KPA and COA. The security level of the proposed system is very invulnerable due to the use of nonlinear operations. The proposed system achieved a very high decrypted image quality.

REFERENCES

Barrera, J.F., Mira, A. and Torroba, R. 2013. Optical encryption and QR codes: secure and noise-free information retrieval. Optics express, 21(5), pp.5373-5378.

Chen, W., Javidi, B. and Chen, X. 2014. Advances in optical security systems. Advances in Optics and Photonics, 6(2), pp.120-155.

Cuadrado-Laborde, C. and Lancis, J. 2011. The space-bandwidth product in the joint transform correlator optical encryption setup. Optics Communications, 284(19), pp.4316-4320.

Cun, Q., Tong, X., Wang, Z. and Zhang, M. 2021. Selective image encryption method based on dynamic DNA coding and new chaotic map. Optik, 243, p.167286.

Devi, N.K., Mahendran, G., Murugeswari, S., Washburn, S.P.S., Devi, D.A., Saravanan, B., Bharathi, G. and Begam, N.M. 2021. A new lossless compression method using Direction Adaptive-Discrete wavelet transform and Modified SPIHT coding. Materials Today: Proceedings.

Frauel, Y., Castro, A., Naughton, T.J. and Javidi, B. 2007. Resistance of the double random phase encryption against various attacks. Optics Express, 15(16), pp.10253-10265.

Javidi, B., Carnicer, A., Yamaguchi, M., Nomura, T., Pérez-Cabré, E., Millán, M.S., Nishchal, N.K., Torroba, R., Barrera, J.F., He, W. and Peng, X. 2016. Roadmap on optical security. Journal of Optics, 18(8), p.083001.

Jiao, S., Zhuang, Z., Zhou, C., Zou, W. and Li, X. 2018. Security enhancement of double random phase encryption with a hidden key against ciphertext only attack. Optics Communications, 418, pp.106-114.

Joshi, M., Shakher, C. and Singh, K. 2009. Logarithms-based RGB image encryption in the fractional Fourier domain: a non-linear approach. Optics and Lasers in Engineering, 47(6), pp.721-727.

Laiphrakpam, D.S., Waikhom, L.S., Brahma, D., Baruah, P. and Biswas, S. 2021. Image compression–encryption scheme using SPIHT and chaotic systems. Journal of Information Security and Applications, 63, p.103010.

Liu, S., Guo, C. and Sheridan, J.T. 2014. A review of optical image encryption techniques. Optics & Laser Technology, 57, pp.327-342.

Norouzi, B. and Mirzakuchaki, S. 2014. A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dynamics, 78(2), pp.995-1015.

Oad, A., Yadav, H. and Jain, A. 2014. A review: image encryption techniques and its terminologies. International Journal of Engineering and Advanced Technology (IJEAT) ISSN, pp.2249-8958.

Qin, Y., Wang, Z., Wang, H. and Gong, Q. 2018. Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code. Optics & Laser Technology, 103, pp.93-98.

Refregier, P. and Javidi, B. 1995. Optical image encryption based on input plane and Fourier plane random encoding. Optics letters, 20(7), pp.767-769.

Sahari, M.L. and Boukemara, I. 2018. A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. Nonlinear Dynamics, 94(1), pp.723-744.

Said, A. and Pearlman, W.A. 1996. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on circuits and systems for video technology, 6(3), pp.243-250.

Shapiro, J.M. 2002. Embedded image coding using zerotrees of wavelet coefficients. In Wavelet Image and Video Compression (pp. 123-155). Springer, Boston, MA.

Situ, G. and Zhang, J. 2004. Double random-phase encoding in the Fresnel domain. Optics Letters, 29(14), pp.1584-1586.

Sui, L., Xin, M., Tian, A. and Jin, H. 2013. Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain. Optics and Lasers in Engineering, 51(12), pp.1297-1309.

Taneja, N., Raman, B. and Gupta, I. 2009. Partial encryption on SPIHT compressed images. In International Conference on Pattern Recognition and Machine Intelligence (pp. 426-431). Springer, Berlin, Heidelberg.

Trujillo-Toledo, D.A., López-Bonilla, O.R., García-Guerrero, E.E., Tlelo-Cuautle, E., López-Mancilla, D., Guillén-Fernández, O. and Inzunza-González, E. 2021. Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. Chaos, Solitons & Fractals, 153, p.111506.

Xiang, T., Qu, J. and Xiao, D. 2014. Joint SPIHT compression and selective encryption. Applied Soft Computing, 21, pp.159-170.

Yadav, P., Singh, H. and Khanna, K. 2021. A review of optical image encryption techniques based on Cloud computing biometric and multiple image processing. Available at SSRN 3833823.

Zea, A.V., Barrera, J.F. and Torroba, R. 2016. Customized data container for improved performance in optical cryptosystems. Journal of Optics, 18(12), p.125702.

Zhang, M. and Tong, X. 2017. Joint image encryption and compression scheme based on IWT and SPIHT. Optics and Lasers in Engineering, 90, pp.254-274.

Zhang, X. and Wang, X. 2013. Chaos-based partial encryption of SPIHT coded color images. Signal Processing, 93(9), pp.2422-2431.