

Compression of Grayscale Images in DRPE-based Encrypted Domain

Osama S. Faragallah^{1,*}, Ensherah A. Naeem², Hala S. Elsayed³ and Fathi E. Abd El-Samie⁴

¹Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

²Department of Electrical, Faculty of Technology and Education, Suez University, Suez 43527, Egypt

³Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt

⁴Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

*Corresponding Author: Osama S. Faragallah. Email: o.salah@tu.edu.sa

Received: 04 April 2021; Accepted: 05 May 2021

Abstract: Compressing the encrypted images is considered an important issue in many applications such as cloud computing. From this perspective, this paper introduces an efficient approach for compression processing of images in the encrypted domain. The images are optically encrypted using the Double Random Phase Encoding (DRPE). The Joint Photographic Experts Group (JPEG) and the Set Partitioning in Hierarchical Trees (SPIHT) compression schemes have been used to compress the encrypted images. The process starts by converting the original image into an optical signal by an optical emitter like an optical source and encrypting it with DRPE. The DRPE applies two-phase modulations on both time and frequency domains to get the encrypted image. The JPEG and SPIHT compression techniques are utilized with different bit rates. The effect of compressing encrypted images with the DRPE is studied. Security analysis results show that the encrypted images using the DRPE are adequately compressed by SPIHT at a low bit rate, and can be adequately compressed by JPEG at a high bit rate. Also, experimental outcomes and security study prove that the multipurpose encryption and SPIHT compression scheme is more secure and effective.

Keywords: DRPE; image compression; JPEG; SPIHT

1 Introduction

Nowadays, multimedia are around us everywhere, on the Internet, in military applications, in medical images, and multimedia transmission is a daily routine. It is a challenge to find a secure way to transmit them over networks. Encryption is the primary technique for image protection. It transforms the image to ensure security during transmission and storage. Optical encryption and security schemes have witnessed many advantages because of their features of fast processors and parallelism. Optics provides many strategies for optical encryption according to the used encoding method for the optical beam, like polarization-encoding encryption, full phase and amplitude-based encryption [1]. The full phase encryption is the superior one due to its non-linearity and its high security. The DRPE was suggested by



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Refregier and Javidi [2]. It can be considered as an efficient and vastly utilized optical ciphering scheme. In Faragallah et al. [3–4], the fractional Fourier transform (FrFT) is viewed as a generalization of the Fourier transform. In Castro et al. [5–6], the lenses in the DRPE are employed for performing the optical Fourier transform (OFT) of an object. The main issue of lenses is suffering from aberration, which results in errors for estimating the FT. To improve encryption, the compression can be combined with encryption. Furthermore, the processing time is decreased. Traditionally, in the transmission of images, the images are often subjected to compression followed by encryption at the transmitter. For recovering the image data at the receiver, the received images are often subjected to decryption before decompression. However, with some applications, traditional treatment has to be reversed, and the encryption is followed by compression. This may be known as conducting a compression process at an encryption domain, and at the compressor, there is no need for the secret encryption key. The processing of images after encryption in the encrypted domain has obtained much attention. Image processing, such as image compression, has many benefits; it facilitates storage and speeds up data transmission. There exist two compression types: lossy compression, which does not conserve the quality of the image, and lossless compression, which is reversible and does not cause any visual problem. Suppose the compressed image is subjected to encryption. In that case, it may have good security and a faster transmission rate through the network than just only image encryption and transmitting the uncompressed image. However, compressing the image may increase the image overhead size and processing time with certain scenarios. Wavelet transform [7] became common and powerful in the past few decades in digital signal processing due to its efficiency in analyzing signals according to different scales or resolutions and representing data or other functions. One of the typical applications of wavelet transform in digital signal processing is wavelet-based image compression. Wavelet-based image compression techniques like embedded zero-tree wavelet transform (EZW) are appropriate and very quick in execution and they produce an excellent subjective human understanding of the retrieved images. The authors in [8] improved the EZW performance by introducing a superior and speedy implementation termed SPIHT. The SPIHT may be considered an effective method in terms of execution time and visual quality compared to other algorithms. The SPIHT can give an excellent distortion rate, while maintaining lower encoding complexity. A block-based image compression algorithm like JPEG produces characteristic blocking artifacts in the images and blurs fine details when working at low bit rates [9].

In this paper, compression of encrypted optical images based on DRPE is employed. The lossy JPEG compression and lossless SPIHT compression are executed on the encrypted images. A comparative study of compressing DRPE encrypted images using JPEG or SPIHT techniques is presented. The original images are encrypted at the transmitter by the content owner with DRPE-based image encryption method. The encrypted images are effectively compressed using JPEG or SPIHT compression techniques without revealing the original content. At the receiver, the original images are recovered using the secret keys. The performance of the proposed encryption-compression schemes is evaluated experimentally on a group of test images and compared to the theoretically realizable compression rates.

The remaining sections of this paper are subdivided as follows. Section 2 summarizes some of the related works. Section 3 displays a background about DRPE as an optical encryption technique, JPEG and SPIHT as compression techniques. In Section 4, the design of the proposed encryption-compression approach is given in details. Section 5 presents simulation analysis and results. The effect of noise on the decryption process is discussed in Section 6. Finally, in Section 7, the concluding remarks are given.

2 Related Works

There have been some related works on image security in the compressed encrypted domain over the past few years. The authors of [10] proposed an encryption-compression method using multiple chaotic

maps to enhance the encrypted data security. The authors of [11] introduced a partial or selective encryption scheme for JPEG images to completely dissimulate the visual image information and produce lower resolution images. The authors in [12] proposed the compression of encrypted images when the underlying resource information is obscure in advance. In Lazzeretti et al. [13], the authors presented several frameworks to compress encrypted grayscale and color images. The type of compression is lossless compression using LDPC codes.

Furthermore, the authors of [14] developed a pixel permutation-based image encryption scheme, and deduced that the cipherimage might be, compressed by dismissing the excessive rough information. With this scheme, most information is transformed into a group of coefficients via the orthogonal transformation. After that, unwanted information in coefficients is eliminated and the amount of data is decreased. In recent days in [15], Zhang et al. proposed a compression technique for encrypted images using multilayer decomposition. Methods of blind encryption of videos were proposed with much effort, but they face poor performance compared with the systems that work on unencrypted output. In Maniccam et al. [16], the authors presented a binary/grayscale lossless compression and encryption scheme depending on SCAN methodology. In You et al. [17], the authors have proposed a compression encryption approach that employs the discrete wavelet transform (DWT) and the advanced encryption standard (AES). In Ito et al. [18], the authors proposed an encryption and compression scheme using the discrete cosine transform (DCT) and independent component analysis (ICA). In Cheng et al. [19], the authors have proposed a Quadtree compression algorithm, and a partial encryption algorithm. In Maheswari et al. [20], the authors have proposed combining Shuffle Encryption Algorithm (SEA) and lossless compression by using XML and JPEG compression. In Keat et al. [21], the authors have proposed a method combining RC4 and wavelet compression by using embedded zero-tree wavelet (EZW) encoder. In Thakur et al. [22], the authors have presented a method combining fractal coding and spiral architecture for lossy compression and encryption. In Kesavaraja et al. [23], the authors have performed a comparative survey of three conventional image compression techniques and their assortment of different features to select the most preferable one for cluster processing. The distributed intrusion detection system (DIDS) is used for cluster node monitoring, and robust intrusion control (RIC) prevention system is used. In Celikel et al. [24], the authors have presented text file compression and encryption schemes based on arithmetic coding, Huffman coding, Lempel-Ziv compression and symmetric key encryption. The prediction process is performed using partial matching and burrows-wheeler.

3 Background

3.1 DRPE

The DRPE was presented by Refregier and Javidi [2]. The optical DRPE encryption technique uses two 2D random phase masks (RPMs) and both encryption and decryption processes use the same Fourier RPMs. Let $I(x, y)$, and $F(x, y)$ be the plainimage, and cipherimage, respectively. $\theta(x, y)$ and $\omega(u, v)$ are the key functions in time/frequency. Their corresponding estimates are in the interval [0–1] with uniformly distributed probability.

The following equation can achieve the DRPE encryption process:

$$F(x, y) = FT\{FT[I(x, y) \exp(j2\pi\theta(x, y))] \exp(j2\pi\omega(u, v))\} \quad (1)$$

The following equation can achieve the DRPE decryption process:

$$I(x, y) = \{FT^{-1}[FT^{-1}(F(x, y)) \exp(-j2\pi\omega(u, v))]\} \exp(-j2\pi\theta(x, y)) \quad (2)$$

Here, $\exp(j2\pi\theta(x, y))$ and $\exp(-j2\pi\omega(u, v))$ denote the two secret keys. The FT is the Fourier transform, and the FT^{-1} is the reverse process.

3.2 JPEG – Joint Picture Expert Group

Fig. 1 shows the JPEG lossy compression scheme. The image is firstly divided into 8×8 blocks with 8-bit values. After that, we apply the 2-D DCT for each block individually, which leads to the transformed matrix F . The element in the upper left represents the DC coefficient, and the others are 63 AC coefficients [25–26]. The next step is the quantization process. We select a quantization matrix Q with items q_{ij} according to JPEG recommendation and quantify DCT coefficients using the following equation [26]:

$$F(u, v)_{Quantization} = \text{round}\left(\frac{F(u, v)}{Q(u, v)}\right) \quad (3)$$

where $F(u, v)$ and $Q(u, v)$ are the transformed and the quantization matrices.

The reverse process is represented as [26]:

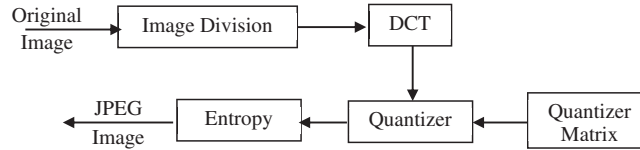


Figure 1: The JPEG lossy compression scheme

$$F(u, v)_{deQ} = F(u, v)_{Quantization} \times Q(u, v) \quad (4)$$

The Q matrix is defined in Eq. 3

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 18 & 12 & 14 & 19 & 20 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 54 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} \quad (5)$$

The DC quantized coefficients may be encoded based on the former block DC term, as shown in Fig. 2.

$$\text{Diff}_i = DC_i - DC_{i-1} \quad (6)$$

where $DC_0 = 0$. The first coefficient, which is the difference of DC coefficients, and the AC coefficients are encoded with the Huffman coding algorithm. After quantization and zigzag scanning for AC coefficients, the zero run-length coding is applied on the obtained vectors using the Huffman table for encoding coefficients, and finally, we get the bitstream.

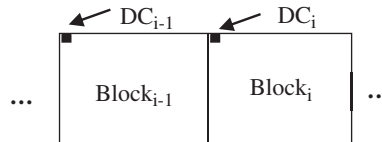


Figure 2: The differential coding

3.3 SPIHT – Set Partitioning In Hierarchical Trees

The SPIHT was presented in Mitra et al. [27–28]. It may be considered a simple, fast wavelet-based image compression and an efficient refinement of EZW coding. It gives a better image quality with lower bit rates and a higher PSNR than the conventional image compressing schemes such as JPEG.

In SPIHT, the coefficients are ordered by magnitude, and the most significant bits are transmitted first. The SPIHT encoder consists of a DWT transformation, two passes of quantization, the sorting and the refinement passes, and a coder. There are three linked lists (LIP, LIS and LSP) that are used in the sorting pass. The LSP represents a list of significant pixels with coefficients of magnitudes above or equal to some threshold. The LIP represents a list of insignificant pixels, which has coefficients of magnitudes below the threshold. This list maintains the pixels that have to be estimated. The LIS is the list of insignificant sets. The pixels in those sets are below some certain threshold. The enhancement pass provides additional quantization precision bit entries in the LSP, excluding those generated in the sorting pass of this iteration. Better quality of reconstructed images is obtained by iterating the quantization process, and bisectioning the threshold every time. The encoding procedure creates a completely scalable bitstream and can be blocked if a target bit rate or a quality demand is achieved.

4 The Proposed Encryption-Compression Scheme

For encrypting an image, it is split into equivalent segments and transformed into an optical signal using an optical emitter like an optical source. Then, it is encrypted by the DRPE, which employs two phases modulation; one in the spatial domain and one in the FT. Finally, the optical encrypted image is revealed by the CCD digital camera, which converts it back to a digital format.

The decryption process works by applying the conjugate of the two random phase modulations to decrypt the encrypted image. After that, the optical encrypted image is converted to an electrical signal by an optical detector. Finally, the blocks are collected to obtain the original image. Fig. 3 depicts the proposed encryption-compression scheme. The process is as follows:

- 1- Apply the DRPE on different images.
- 2- Apply JPEG or SPIHT compression on the encrypted images with different bitrates.

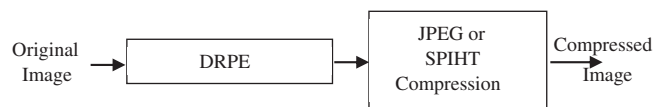




Figure 3: Scheme to compress encrypted images

5 Simulation Results

The 512×512 grayscale Lena and 512×512 grayscale Cameraman images, shown in Tab. 1, are used to evaluate the proposed scheme. Evaluation of the obtained results depends on the visual quality of decrypted images, entropy values, histogram graphs, encryption quality, differential analysis, and noise immunity.

















Table 1: Lena and Cameraman original images

Name	Lena	Cameraman
Image		

5.1 Visual Inspection

The decrypted images are shown in [Tab. 2](#) for JPEG and SPIHT compression. The visual appearance of the decrypted images ensures the superiority of the proposed encryption-compression scheme. In addition, the decrypted Lena and Cameraman images for JPEG and SPIHT compression schemes indicate that the SPIHT is more appropriate for a low bit rate than the JPEG.

Table 2: Decrypted images with different bitrates

Compression	Image	Decrypted images			
		bitrate: 1	3	5	7
JPEG	Lena				
	Cameraman				
SPIHT	Lena				
	Cameraman				

5.2 Entropy Analysis

An efficient cryptosystem must conceal all structural features of the source plainimage. Concealing structural features ensures the unpredictability of the information included in the plainimage. The unpredictability can be computed using the entropy measure. The entropy $E(x)$ of a cipherimage x can be calculated by [29–30]:

$$E(x) = - \sum_{i=0}^{2^N-1} p(x_i) \log_2 p(x_i) \quad (7)$$

where $p(x_i)$ denotes the symbol x_i occurrence probability in the ciphered image, N defines the number of bits to represent the x_i symbol, and \log_2 expresses entropy in bits. The entropy estimate for an ideally encrypted image equals 8. The entropy measurements of the compressed images at different bitrates are tabulated in [Tab. 3](#).

From these results, it can be seen that the entropy estimates of SPIHT compressed images are close to the standard value of 8, which indicates that the information leakage in the encryption and SPIHT compression may be neglected. Hence, the proposed scheme is secure for entropy attacks.

5.3 Histograms Analysis

Image histogram demonstrates pixels distribution within the image. The histogram is represented by graphing the number of pixels for every gray level. The histograms of the compressed and encrypted images and their corresponding original images are estimated and analyzed. The original plainimages

histograms are illustrated in Tab. 4. The histograms of encrypted JPEG and SPHIT compressed images at different bitrates are shown in Tab. 5. The results show that the histograms of the encrypted images after compression are distinguishable from their corresponding original plainimages histograms and significantly different from those of the encrypted images without compression.

Table 3: Entropy results of compressed images at different bitrates

Compression	Image	Compressed images			
		bitrate: 1	3	5	7
JPEG	Lena	5.8150	5.8150	5.8482	6.2543
	Cameraman	5.8973	5.8973	5.9194	6.3191
SPIHT	Lena	7.4680	7.4756	7.3265	7.2456
	Cameraman	7.4688	7.4728	7.3233	7.2391

Table 4: Histogram results of images

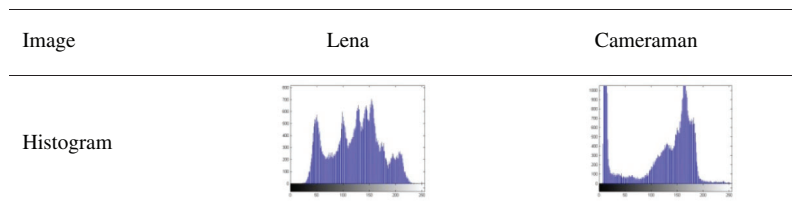
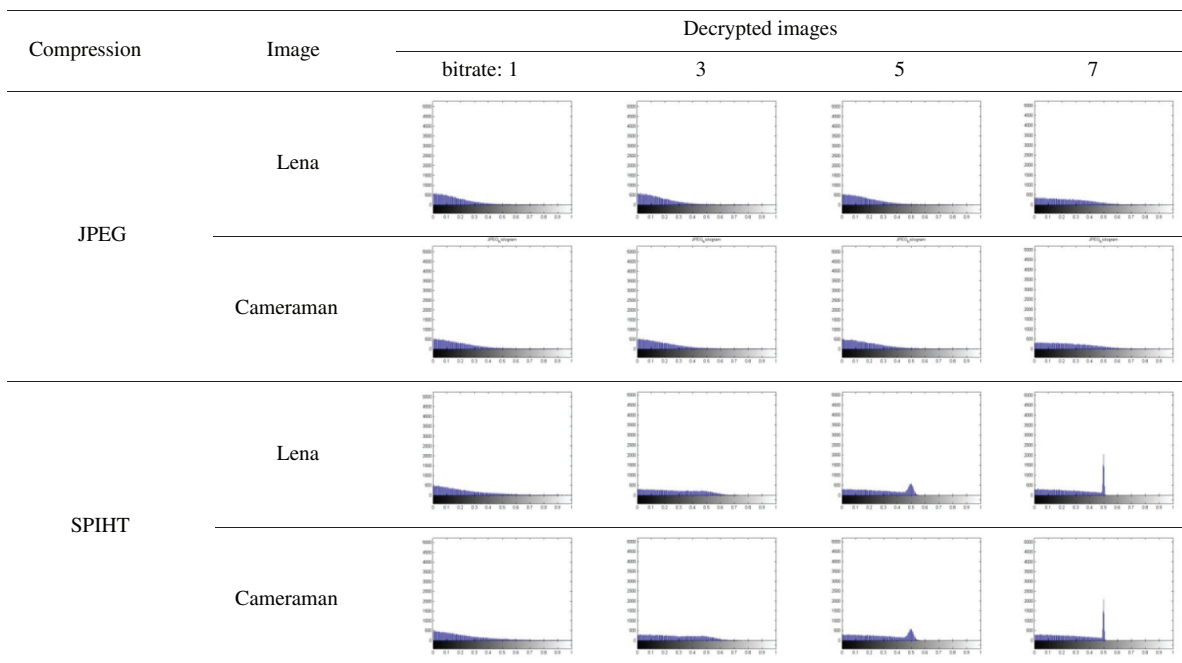


Table 5: Histogram results of encrypted, compressed images at different bitrates



5.4 Compression/Encryption Quality

The proposed compression encryption module quality is studied and evaluated in terms of the correlation coefficient r_{xy} among the plainimages and the cipherimages, histogram deviation D_H , and irregular deviation D_I . The correlation coefficient r_{xy} can be evaluated among the plainimage x and cipherimage y as follows [31]:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (8)$$

where $\text{cov}(x, y) = \frac{1}{L} \sum_{l=1}^L (x(l) - E(x))(y(l) - E(y))$, $D(x) = \frac{1}{L} \sum_{l=1}^L (x(l) - E(x))^2$, $E(x) = \frac{1}{L} \sum_{l=1}^L x(l)$, and L is the number of image pixels.

The histogram deviation is utilized to measure encryption quality by calculating the deviation amount between the original plainimage and its corresponding cipherimage [31]. The histogram deviation D_H is determined by estimating the area under the curve of histogram differences [31]:

$$D_H = \frac{\left(\frac{d(0)+d(255)}{2} + \sum_{i=1}^{254} d(i) \right)}{W \times H} \quad (9)$$

where $d(i)$ defines the absolute difference amplitude among the plainimage and cipherimage histograms at pixel intensity value i . W and H represent image dimensions.

The irregular deviation is utilized as a measure of encryption quality through calculating the irregular deviation amount on the cipherimage [32]. The irregular deviation D_I is can be expressed as [32]:

$$D_I = \frac{\sum_{i=0}^{255} h_D(i)}{W \times H} \quad (10)$$

$$h_D(i) = |h(i) - M_H| \quad (11)$$

where $h(i)$ and M_H denote the cipherimage histogram at pixel intensity value i and the uniform histogram mean for an ideal cipherimage.

The correlation coefficient results for compressed images at different bit rate are given in Tab. 6, and the correlation coefficient results for decrypted images at different bit rates are given in Tab. 7. All results indicate a good performance of encryption with SPIHT compared to JPEG, where the correlation is low among the plainimage and the cipherimage pixels. The histogram deviation results for compressed images at different bit rates are given in Tab. 8. All results indicate a good performance of the encryption algorithm with SPIHT and JPEG, where the correlation is low among the plainimage and the cipherimage pixels. Finally, the irregular deviation results for compressed images at different bit rates are given in Tab. 9. All results indicate a good performance of the encryption with SPIHT and JPEG, where the correlation is low among the plainimage and the cipherimage pixels.

Table 6: The correlation coefficient results for compressed images at different bitrates

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	-0.0010	-0.0010	-0.0009	0.0018
	Cameraman	0.0035	0.0035	0.0034	-0.0017
SPIHT	Lena	0.0053	-0.0088	-0.0088	-0.0082
	Cameraman	-0.0103	-0.0042	-0.0038	-0.0036

Table 7: The correlation coefficient results for decrypted images at different bitrates

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	0.1122	0.1122	0.1178	0.2529
	Cameraman	0.1196	0.1196	0.1258	0.2658
SPIHT	Lena	0.3149	0.8226	0.9044	0.9092
	Cameraman	0.3289	0.8682	0.9367	0.9402

Table 8: Histogram deviation results for compressed images at different bitrates

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	0.3299	0.3299	0.3254	0.2748
	Cameraman	0.3308	0.3308	0.3313	0.3082
SPIHT	Lena	0.3059	0.2621	0.2639	0.2873
	Cameraman	0.3180	0.2939	0.2982	0.3215

Table 9: The irregular deviation results for compressed images at different bitrates

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	0.1639	0.1639	0.1639	0.1639
	Cameraman	0.2464	0.2464	0.2464	0.2463
SPIHT	Lena	0.1638	0.1640	0.1639	0.1638
	Cameraman	0.2461	0.2460	0.2458	0.2458

6 Effect of Noise

The robustness of the proposed encryption-compression module against noise in the decryption process is a significant factor for the success of our module. Therefore, the *PSNR* can be used to evaluate the decrypted images visual quality in the existence of noise. The effectiveness of the decryption procedure is computed using the *PSNR*. It can be defined as [33]:

$$PSNR = 10 \log \frac{W \times H (255)^2}{\sum_{i=0}^{H-1} \sum_{j=0}^{W-1} (f1(i,j) - f2(i,j))^2} \quad (12)$$

where $f1(i,j)$ and $f2(i,j)$ represent the pixels grayscale level at position (i,j) of the plainimage and decrypted cipherimage, respectively.

As the *PSNR* value becomes high, the algorithm becomes better for noise immunity. The *PSNR* is increased as the bit rate is increased at a specific *SNR* for JPEG and SPIHT compression schemes. The decrypted images and the *PSNR* results for JPEG compared with SPIHT compression at different compression rates and different *SNR* are tabulated in [Tabs 10, 11, 12](#) and [13](#). The obtained results prove that the SPIHT compression is more efficient than JPEG, particularly at all bit rates.

Table 10: Decrypted images for compression with different bitrates and *SNR* = 20 dB









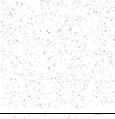
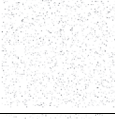

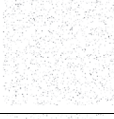




Compression	Image	Decrypted images			
		bitrate: 1	3	5	7
JPEG	Lena				
	Cameraman				
SPIHT	Lena				
	Cameraman				

Table 11: The *PSNR* for the decrypted images for JPEG and SPIHT compression schemes at different bitrates and *SNR* = 20 dB

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	5.8873	5.8873	5.8874	5.8884
	Cameraman	5.8461	5.8461	5.8461	5.8477
SPIHT	Lena	5.8864	5.8870	5.8870	5.8870
	Cameraman	5.8445	5.8452	5.8451	5.8451

Table 12: Decrypted images for compression with different bitrates and $SNR = 30$ dB

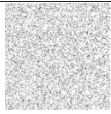
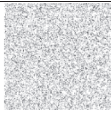

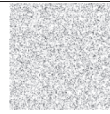





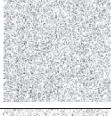
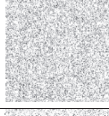
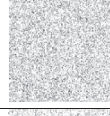
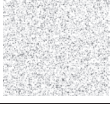

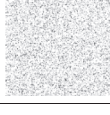

Compression	Image	Decrypted images			
		bitrate: 1	3	5	7
JPEG	Lena				
	Cameraman				
SPIHT	Lena				
	Cameraman				

Table 13: The $PSNR$ for the decrypted images for JPEG and SPIHT compression schemes at different bitrates and $SNR = 30$ dB

Compression	Image	Encrypted images			
		bitrate: 1	3	5	7
JPEG	Lena	5.7623	5.7623	5.7624	5.7644
	Cameraman	5.6917	5.6917	5.6918	5.6941
SPIHT	Lena	5.7626	5.7649	5.7647	5.7647
	Cameraman	5.6916	5.6935	5.6933	5.6933

7 Conclusions

This paper introduced a superior compression processing approach in the DRPE-based encrypted domain. First, the image is optically encrypted with the DRPE. Then, either the JPEG or the SPIHT compression technique is employed for compressing the encrypted image. Both simulation results and security analysis show that the decrypted images for JPEG and SPIHT compression schemes indicate that the SPIHT is more appropriate for all bit rates than the JPEG. Furthermore, the SPIHT compression of encrypted images is not significantly affected by noise. So, it can work efficiently in a noisy environment.

Acknowledgement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Funding Statement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] R. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Optical Engineering*, vol. 33, pp. 1752–1756, 1994.
- [2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, pp. 767–769, 1995.
- [3] O. S. Faragallah, H. S. El-sayed, A. Afifi and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 137, pp. 106333, Feb. 2021.
- [4] O. S. Faragallah, M. A. AlZain, H. S. El-sayed, J. F. Al-Amri, W. El-Shafai *et al.*, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.
- [5] J. M. Castro, I. B. Djordjevic and D. F. Geraghty, "Novel super structure bragg gratings for optical encryption," *Journal of Lightwave Technology*, vol. 24, pp. 1875–1885, 2006.
- [6] T. K. Hazra, N. Kumari, S. Priya and A. K. Chakraborty, "Image encryption and decryption using phase mask over sinusoidal single and cross grating," in *IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, pp. 1–6, 2016.
- [7] E. Kofidisi, N. Kolokotronis, A. Vassilarakou, S. Theodoridis and D. Cavouras, "Wavelet-based medical image compression," *Future Generation Computer Systems*, vol. 15, no. 2, pp. 223–243, 1999.
- [8] S. Amir and A. P. William, "A new fast and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions On Circuits and Systems For Video Technology*, vol. 6, pp. 243–250, 1996.
- [9] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey level and color images," in *Proc. 16th Eur. Signal Processing Conf. (EUSIPCO 2008)*, Lausanne, Switzerland, pp. 1–5, 2008.
- [10] B. Prasad and K. Mishra, "A combined encryption compression scheme using chaotic map," *Cybernetics and Information Technologies*, vol. 13, no. 2, pp. 75–81, 2016.
- [11] W. Puech and J. M. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT," in *13th European Signal Processing Conference*, Antalya, Turkey, pp. 1–4, 2005.
- [12] D. Schonberg, S. C. Draper and K. Ramchandran, "On compression of encrypted images," in *Proc. IEEE Int. Conf. Image Proces*, Atlanta, GA, USA, pp. 269–272, 2006.
- [13] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey level and color images," in *Proc. 16th Eur. Signal Process. Conf.*, Lausanne, Switzerland, pp. 1–5, 2008.
- [14] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58, Mar. 2011.
- [15] X. Zhang, G. Sun, L. Shen and C. Qin, "Compression of encrypted images with multilayer decomposition," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 1–13, 2013.
- [16] S. S. Maniccam and N. G. Bourbakis, "SCAN based lossless image compression and encryption," in *Proc. of Int. Conf. on Information Intelligence and Systems*, Bethesda, MD, USA, pp. 490–499, 1999.
- [17] Y. You and H. Kim, "Endoscopy image compression and encryption under fault tolerant ubiquitous environment," in *Proc. of IEEE Biomedical Circuits and Systems Conf.*, Beijing, China, pp. 165–168, 2009.
- [18] M. Ito, N. Ohnishi, A. Alfalou and A. Mansour, "New image encryption and compression method based on independent component analysis," in *Proc. of the 3rd Int. Conf. on Information and Communication Technologies: From Theory to Applications*, Damascus, Syria, pp. 1–6, 2008.
- [19] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions On Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.
- [20] D. Maheswari and V. Radha, "Secure layer based compound image compression using xml compression," in *2010 IEEE Computational Intelligence and Computing Research*, Coimbatore, India, pp. 1–5, 2010.
- [21] G. H. Keat, A. Samsudin and Z. Zainol, *Enhanced Performance of Secure Image using Wavelet Compression*. Malaysia: World Academy of Science, Engineering and Technology, pp. 633–636, 2007.

- [22] N. V. Thakur and O. G. Kakde, "Compression mechanism for multimedia system in consideration of information security," in *Proceeding of International Workshop on Machine Intelligence Research*, Nagpur, India, pp. 87–96, 2009.
- [23] D. Kesavaraja, R. Balasubramanian, D. Jeyabharathi and D. Sasireka, "Secure and faster clustering environment for advanced image compression," *International Journal of Advanced Networking and Applications*, vol. 2, no. 3, pp. 671–678, 2010.
- [24] E. Celikel and M. E. Dalkilic, "Experiments on a secure compression algorithm," *Proceedings of the International Conference on Information Technology: Coding and Computing*, vol. 2, pp. 150–152, 2004.
- [25] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk and T. Rabin, "On compression of data encrypted with block ciphers," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6989–7001, 2012.
- [26] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58, 2011.
- [27] S. K. Mitra, C. A. Murthy and M. K. Kundu, "Partitioned iterated function system: a new tool for digital imaging," *IETE Journal of Research*, vol. 16, no. 5, pp. 279–298, 2000.
- [28] E. Kofidisi, N. Kolokotronis, A. Vassilarakou, S. Theodoridis and D. Cavouras, "Wavelet-based medical image compression," *Future Generation Computer Systems*, vol. 15, no. 2, pp. 223–243, 1999.
- [29] I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas *et al.*, "Efficient chaotic-based image cryptosystem with different modes of operation," *Multimedia Tools and Applications*, vol. 79, pp. 20665–20687, 2020.
- [30] M. Alajmi, I. Elashry, H. S. El-Sayed and O. S. Faragallah, "A Password-based authentication system based on the CAPTCHA AI problem," *IEEE Access*, vol. 8, pp. 153914–153928, 2020.
- [31] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem *et al.*, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
- [32] M. Alajmi, I. Elashry, H. S. El-Sayed and O. S. Faragallah, "Steganography of encrypted messages inside valid QR codes," *IEEE Access*, vol. 8, pp. 27861–27873, 2020.
- [33] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain *et al.*, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.