IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 1, 2021, accepted February 10, 2021, date of publication February 18, 2021, date of current version March 1, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3060317*

# Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques

**OSAMA FOUAD ABDEL WAHAB[1,2], ASHRAF A. M. KHALAF[1], AZIZA I. HUSSEIN[3], AND HESHAM F. A. HAMED[1,4]**

[1]Faculty of Engineering, Minia University, El-Minia 61111, Egypt
[2]Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3]Department of Electrical and Computer Engineering, Effat University, Jeddah 8482, Saudi Arabia
[4]Department of Telecommunications Engineering, Egyptian Russian University, Badr 11829, Egypt

Corresponding authors: Ashraf A. M. Khalaf (ashkhalaf@yahoo.com) and Osama Fouad Abdel Wahab (osamaf@hotmail.com)

**ABSTRACT** Data compression is an important part of information security because compressed data is more secure and easy to handle. Effective data compression technology creates efficient, secure, and easy-to-connect data. There are two types of compression algorithm techniques, lossy and lossless. These technologies can be used in any data format such as text, audio, video, or image file. The main objective of this study was to reduce the physical space on the various storage media and reduce the time of sending data over the Internet with a complete guarantee of encrypting this data and hiding it from intruders. Two techniques are implemented, with data loss (Lossy) and without data loss (Lossless). In the proposed paper a hybrid data compression algorithm increases the input data to be encrypted by RSA (Rivest–Shamir–Adleman) cryptography method to enhance the security level and it can be used in executing lossy and lossless compacting Steganography methods. This technique can be used to decrease the amount of every transmitted data aiding fast transmission while using slow internet or take a small space on different storage media. The plain text is compressed by the Huffman coding algorithm, and also the cover image is compressed by Discrete wavelet transform DWT based that compacts the cover image through lossy compression in order to reduce the cover image's dimensions. The least significant bit LSB will then be used to implant the encrypted data in the compacted cover image. We evaluated that system on criteria such as percentage Savings percentage, Compression Time, Compression Ratio, Bits per pixel, Mean Squared Error, Peak Signal to Noise Ratio, Structural Similarity Index, and Compression Speed. This system shows a high-level performance and system methodology compared to other systems that use the same methodology.

**INDEX TERMS** Cryptography, data compression, DWT, Huffman coding, LSB, MSE, PSNR, SSIM, RSA, steganography.

## I. INTRODUCTION

In the current scenario, secret messages can be sent by hiding in an image or a text so nobody other than sender and receiver can read or see the message. hiding and unhiding of data are known as steganography. In steganography, the Image which hides the data is known as Cover Image because it covers the secret message and after hiding the data image is known as stego-image. In Steganography LSB insertion is a very popular and commonly applied technique for embedding data in a cover file. The LSB embedding technique suggests that data can be hidden in such a way that even the naked eye is unable to identify the hidden information in the LSBs of the cover file. It is a spatial domain technique. Cryptography is a method that converts the text in codes so that intruder is successful in finding the secret message it can't be readable by an intruder. So, if we apply steganography and cryptography then it will provide a double layer of security. Image compression is used to reduce the size of the message so that message easily hides [1].

Image compression can be described as a vital application in the field of Digital Image Processing. Compacting is

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

generally removing all the unwanted data from the image, therefore enhancing the memory space required without necessarily distorting the image. Consequently, it is simple to use Huffman coding algorithm as it is cheap in implementing. The compression ratio is directly related to the memory space required; that is, the better the compression ratio, the lesser the cache space [2], [3].

Different algorithms can be used to perform the compression ratio; some retain the original information, described as lossless, and some are lossy, and often lose the unique information upon compression. Every compression method is designed for a specific kind of image and cannot work well with unintended images. Many algorithms let you change variables and modify the compression to have a more elegant image [3]. For authenticity, it is better to use the cryptography method before concealing the message. Many known algorithms can be utilized in cryptography. They include Advanced Encryption Standard (AES), Blowfish, Data Encryption Standard (DES), RC4 Rivest-Shamir-Adleman (RSA) [4]–[7].

In this paper, steganography and cryptography are used to send the compressed secret message along with the sender, and the side message in the recipient is decrypted, decompressed, and extracted from the stego-image. Also, in this research, the combination of RSA cryptography and Steganography using Huffman Coding, and DWT can be effective.

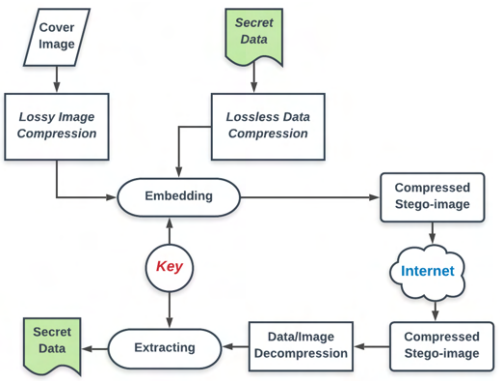


**FIGURE 1.** Block diagram of image compression.

### A. BASIC MODEL

The main purpose of compressing images is to reduce those parts of the image that are not of primary interest to the user. This reduces the image size by reducing the number of pixels and makes it efficient for storing and transmitting data by various means of communication [5]. In Fig. 1, there is the proposed algorithm's basic model shows how a piece of secret information can be done from the sender to the receiver. Fig. 1, illustrates the stages of the image compression process. The secret message is encrypted using RSA cryptography, then compressed by Huffman's algorithm, and the cover-image is compressed by the DWT algorithm. then the cover-image is combined with the secret message via LSB and sent them over the Internet to the destination as a compressed file. These encoded streams (bits) are then sent to a decoder that decodes these streams (bits) and the final output image is retrieved as a decoding file output. Lossy and lossless image decompression [6] is used to reduce the number of bits required to represent an image.

### B. RSA ENCRYPTION

Cryptographic algorithms are broadly classified into two types, namely, symmetric key algorithms and asymmetric key algorithms. Symmetric encryption uses the key for both encryption and decryption. It is very simple and easy to implement, but it does have some major disadvantages. Once the individual key is known, an attacker can easily discover the information [7]. In asymmetric key encryption, two different keys are used for encryption and decryption. The public key is distributed to all senders, and the private key is known only to a specific user (the recipient). But the main disadvantage of this key coding is slower compared to symmetric algorithms [8].

we have two different types of keys: one is the public key and the second is the private key. The public key is publicly known, and the private key is kept secret. The system is called an asymmetric system, if data encrypted by the public key so it can only decrypt by the private key. In a public-key cryptosystem, no need to share secret data between two parties. So, there is less chance of data stolen & manipulated and data is more secure.

It is the most known public-key implementation strategy and it named after MIT scholars that developed the concept in 1977. They were Leonard **A**dleman, Adi **S**hamir, Ronald **R**ivest [9], [5]. RSA, the Advanced Encryption Standard, is a symmetric key encryption standard commonly used to protect data where confidentiality is a critical and important problem. The security of the algorithm is based on the rigidity of the analysis of a large number of compounds and a complex number for a specified odd integer (e) computation of the unit of moral roots. The RSA public key consists of an integer pair (n, e). Typical is the result of multiplying 2 primes. Using the key feature of RSA, a variable key size, and cipher block to improve security [10].

To clarify RSA encryption and decryption as follows:

**Key Generation Procedure:**

Choose two distinct large random prime numbers p & q such that $p \neq q$.

Calculate $n = p \times q$

Calculate $\Phi(n) = (p-1)(q-1)$

Choose an integer e such that $\gcd(\Phi(n), e) = 1$ ;

$1 < e < \Phi(n)$

Compute d to satisfy the congruence relation

$d = e^{-1} \bmod \Phi(n)$; d is kept as private

Public Key KU = {e, n }

Private Key KR = {d, n }

The public key is (n, e) and the private key is (n, d).

Keep d, p, q and $\Phi$ secret.

**Encryption :**
Plaintext Message $<$ n
Ciphertext C $=$ Message$^{e}$ mod n
**Decryption :**
Ciphertext C
Plaintext Message $=$ C$^{d}$ mod n

### C. STEGANOGRAPHY

Steganography is divided into four domains: **1.** The spatial domain: In this type of technology, the bits of confidential messages are directly embedded in the bits of the cover media and they usually have simple algorithms. LSB (least significant bits) is one of the most well-known algorithms in the field which replaces the secret message bits with LSB for the cover media. This change cannot be detected by the human eyes but can be recognized through statistical tests [1], [3]. LSB methods are very fast and simple but have some drawbacks: a) The secure message size is small. B) The secure message bits are damaged in the compression of the cover media. C) With the smallest of changes to the media cover the embedded information can disappear [4]. **2.** Transform domain: This category uses transposition to include secure messages in cover media [5]. These transformations are included: DCT (Discrete Cosine Transform): In this type, the cover media is divided into $8 \times 8$ blocks. These blocks are quantified with a quantization table and then the sensitive bits for the cover media are specified in each block. Embedding is performed in all parts of each particular block in the highly sensitive part of the media cover [2]. DWT (Discrete Wave Switching): In this type, the cover media is divided into 4 major sub-bands (LL, HL, LH, and HH). The main features of cover media are in LL, and if a secret message is included in this part, it will not be destroyed by different compression [6]. DFT (Discrete Fourier Transform): This changes every point of the input signal into two points at the output. The input signal in the DFT is a mixture of samples obtained at regular time intervals [7]. **3.** Spread spectrum: This method embeds the secret message in the noise of the cover media created in the image acquisition process. This method is a blind scheme and there is a payload capacity in this type [8]. **4.** Model-based: This method divides the cover media into two parts. The first part will not be used during the embedding process. The secret message is included in the second part without changing the statistical properties of the cover media. The high modulation capacity is one of the advantages of this method [9]. Increasing the size of the confidential message in the embedding process and being highly resistant against various known attacks are some of the benefits of the transform domain. The high time of embedding and extraction by increasing the volume of cover media or secret message can be considered a defect [11].

### D. COMPRESSION TECHNIQUES

There are two ways in which we can classify the image/data Compression techniques, lossless and lossy image/data compression [12]–[15]. The previous technique involves reconstructing the image as a calculation identical to the original data, thus some data loss is incurred. It beats the latter in terms of achieving a higher compression ratio. The techniques considered on the basis of the literature include discrete wavelet transform (DWT). The last technique and includes Huffman coding involve recreating the original data from the compressed form. Since it uses all the original image/data information while compressing the data/image, the incoming image after decompressing the image is exactly the same as the original image. They are mainly lossless and lossy. In lossless compression, the look for long strings code is done, and also an alternative it with shorter chains is done. The technique is unique as it recreates the whole file as original before compression. On the other hand, lossy compression searches the code and looks for pieces to delete. Although they can be used in a program file, they are useful in multimedia folders where a lot of information kept is hard for the human sense to detect. The data may look similar but different at code state.

### E. HUFFMAN CODING (LOSSLESS DATA COMPRESSION)

Huffman coding has various advantages over the other techniques like the lossless data compression that can be effective and cheap to implement [13]. The implementation involves the occurrence of every data, and then it sorted through ascending. The technique produced a Huffman tree, which can be implemented to restore data to become the original information after compression. Huffman coding is one of the oldest lossless image compression techniques, it was developed to reduce duplication of code while maintaining the quality of the reconstructed image [14]. To understand the algorithm, let's consider using the following example. There are seven source codes for the digital image (B1, B2, B3, B4, B5, B6, B7) with their likelihood values (0.25, 0.25, 0.125, 0.125, 0.125, 0.0625 and 0.0625). The process of obtaining Huffman code is represented in Fig. 2. The probabilities are written in descending order, then two smaller probabilities are added, and the result is written over the probability that is equal to the sum of the last two numbers, and all other probabilities are written under it and thus the process continues [15]–[19]. Table 1 represents the calculation of the codeword length.

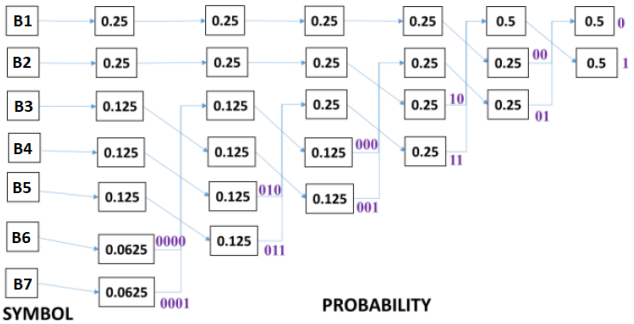


**FIGURE 2.** Huffman encoding: average word length = 2.625 bits, bit assignment process.

**TABLE 1.** Huffman encoding: code word.

| Symbol | Probability | Code Word | Length |
|---|---|---|---|
| B1 | 0.25 | 10 | 2 |
| B2 | 0.25 | 11 | 2 |
| B3 | 0.125 | 1 | 3 |
| B4 | 0.125 | 10 | 3 |
| B5 | 0.125 | 11 | 3 |
| B6 | 0.0625 | 0 | 4 |
| B7 | 0.0625 | 1 | 4 |

The average password length is as follows:

$$L_{avg} = \sum_{i=1}^{L} B(r_i)P(r_i) \tag{1}$$

where B($r_i$) is the total bits that represent grey level, $P(r_i)$ is the respective probability value, and ($r_i$), i = 1, 2, L represents the i[th] grey level of an (L-grey level) image especially L-grey level [16]. Thus, when analyzing Table 1, we can come to the conclusion that the average length of the password can be calculated, in this example as follows:

$$\begin{aligned} L_{avg} &= 0.25 * 2 + 0.25 * 2 + 0.125 * 3 + 0.125 * 3 \\ &\quad + 0.125 * 3 + 0.0625 * 4 + 0.0625 * 4 \\ L_{avg} &= 2.625\ bits \end{aligned} \tag{2}$$

From the above example, it is clear that the average number of bits shrinks to 2,625 bits for variable-length coding. However, the algorithm is optimal, if the source of the probability distribution is known in advance and each bit of the source symbol bits are encoded in the form of an integral number.

### F. DISCRETE WAVELET TRANSFORM (DWT) (LOSSY DATA COMPRESSION)

The discrete wavelet transforms [17] is a powerful technique in image processing, in which the wavelet converts the image into a series of wavelets that are stored more efficiently compared to blocks of pixels. For one dimension, the signals are divided into two parts: high and low frequencies. The low pass and high pass filters for DWT are expressed as in [18]. DWT is an important technique that plays a vital role in compressing the image while ensuring that no information of the picture is lost. DWT is under lossless image compression. The method to transforms discrete-time signals to separate wavelength representation.

It situated on a time scale depiction that can provide multiresolution. It is better to use wavelets than to compress signals and considered one of the most useful and advantageous computational tools to be used in the multiplicity of processing applications and messages. They are chiefly used in images to minimize noise and even to blur. Wavelet transformation is emerging to be one of the most useful and powerful tools that can be used for image and data compression [19].

In DWT there are several filters that can be implemented to process the signal and Haar is the simplest filter that mostly used. The implementation of DWT in the 2D image is by dividing the image into four subbands, such as LL–LH–HL–HH [7], [8], which can be seen in Fig. 3.

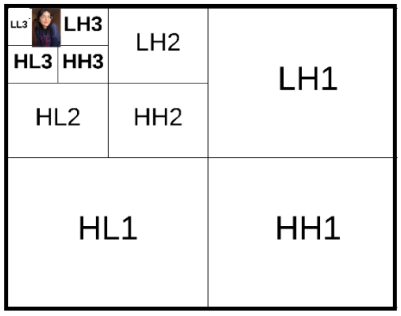


**FIGURE 3.** DWT subbands.

To gain the coefficient of every subband can be used the Haar filter calculation below [1], [10]:

$$\begin{aligned} LL(x, y) &= [p(x, y) + p(x, y + 1) + p(x + 1, y) \\ &\quad + p(x + 1, y + 1)]/2 \end{aligned} \tag{3}$$

$$\begin{aligned} LH(x, y) &= [p(x, y) + p(x, y + 1) - p(x + 1, y) \\ &\quad - p(x + 1, y + 1)]/2 \end{aligned} \tag{4}$$

$$\begin{aligned} HL(x, y) &= [p(x, y) - p(x, y + 1) + p(x + 1, y) \\ &\quad - p(x + 1, y + 1)]/2 \end{aligned} \tag{5}$$

$$\begin{aligned} HH(x, y) &= [p(x, y) - p(x, y + 1) - p(x + 1, y) \\ &\quad + p(x + 1, y + 1)]/2 \end{aligned} \tag{6}$$

where, p = the image pixel, x = row number, and y = column number.

A total of four sub-bands numbers (LL1, LH1, HL1, and HH1) were obtained for the Level 1 decomposition [13].

By repeating a similar procedure in the sub-bands called LL1, we obtain LL2, LH2, HL2, HH2, and so on.

## II. RELATED WORK

The main goal that image compression accomplishes is that it helps reduce the space requirements for storing digital images. There are many uses for digital images, and sometimes they are used in some applications and sometimes in some important areas. The use of image compression technologies meets the application requirements. The idea here is to reduce the largest number of bits possible while preserving the authenticity of the reconstructed image.

In [11], Reza Jafari and *et al.* presented a transform domain steganography. The proposed method used DWT for embedding and extracting the secret message. This algorithm first applies DWT to the cover image and then selects the LL part of the transform. Then, the LL part is split into 2 × 2 blocks and the embedding secret message process begins on

these blocks. Experimental results show that the algorithm has good resistance against image compressing.

In [20], Cheng, H. and *et al.* discuss different compression techniques that rely on traditional sensing and compression theories for color medical images. Some switching techniques such as DCT / DWT and hybridization-based transforms are used for compression.

Traditional techniques take a higher processing time compared to techniques based on CS theory. Performance is measured in terms of peak-to-noise ratio, reconstruction error, and time taken to perform the reconstruction. For many decades, image compression has been the most researched area Because transporting and storing photos is a real tough job. In [21], Hiremath and *et al.* discussed various image compression algorithms such as JPEG, JPEG 2000, BWT, and sparse coding methods.

Comparison of compressed file with DWT gives better results and good image quality than file compression with DCT. Also, compressed files that use DWT take less time to reach the destination node compare the proposed algorithm with Huffman coding.

In [22], Setiadi, and *et al.* evaluated the Burrows-Wheeler transformations-based image compression algorithm with computational coding in conjunction with Huffman coding schematics and noted that the results obtained from the hybrid schema exceeded those obtained from the single schema. Lossless compression methods are analyzed [23] based on compression ratio and elapsed time. The compression algorithms that the authors studied are Huffman and DWT encoding on multimedia data.

The segment will be introducing the relevant information and the background of the concept of image compacting. There are several claims that craft image compression techniques are already available, like Discrete Wavelet Transform and Wavelet Compression Technique, being some of the examples. The methods are vital for a lot of image processing implementations. RSA can be described as renowned asymmetric cryptographic algorithms. Montgomery representation can be used and is outlined [24] that plays an essential role in RSA implementation and even in ovoid curve cryptography.

In [25], Rawat, Abhishek, *et al.* have granted their insights on different applications of the Montgomery multiplication algorithm that is forming the base of an optimization program useful in standard exponentiation.

In [26], Minnen, D. and *et al.* have explained the importance of eliminating the transfer of two random numbers as a way of implementing RSA securely. The Huffman coding depends on the discrete cosine in integers form, transformation and novel, entropy encoder, an efficient and low complexity, therefore, making utilizing the adaptive Golomb-Rice Algorithm instead of Huffman tables. Quantization is an essential module in Wavelet transform-rooted codec and minimizes visual redundancy. It is also the only operating which introduces distortion. PSNR is used to give the standards of images, and the DWT algorithm is essential in providing a better compression ratio [27]. DWT might be computed through sub-sampling and also by convolution with several filters producing a low pass gauze outcome and also a specific high pass filter outcome. Multiresolution decomposition can be achieved by recapitulating the subsampling and convolution of the two filters in the approximation component. For two dimensional prompts, some wavelets are separable where the computation decomposes to parallel processing, which is then followed by vertical operations using only the 1D gauze.

According to Patel *et al.* [28], image compression with the Huffman coding is more comfortable and more straightforward. Compression of images is vital since its implementation gets less memory and also convenient. The main aim of the essay is to have an insight at Huffman coding, and how it helps in removing redundancy in a piece of information through examining several parameters like the Peak signal to noise ratio, Bits per Pixel, compression ratio and mean square error for several inputs image in various sizes and also new ways of splitting such photos will provide excellent results and the data content also will be secure. There are many advantages of the compression technique in image analysis, which contains the security of the image.

In [29], Nixon, K. W. and *et al.* present an image compression technique that uses several inserted Wavelet-based image coding together with the Huffman Coding technique to aid in further compression. They have utilized the EZW with SPHIT algorithms accompanied by Huffman encoding through the use of different wavelength families and also differentiate the PSNRs, rating the families. We tested the algorithms using several images, and the results obtained through the technique had an incredible quality and also gives a very high compression ratio in comparison to the previously used lossless model compacting method.

This planned way produces excellent rated performance, bend plane other than all the different access ways. Therefore, the proposed algorithm uses fixed-length bit codes. It shows a high compression ratio, more saving percentage values, and also ensures greater data security.

## III. PROPOSED ALGORITHMS

The proposed algorithm, in this case, is combining RSA and Huffman coding, or DWT with the intention of reducing the information's bit in steganography. Two key processes are involved, embedding the information process, and also getting or extracting the message process as in fig. 4.

### A. EMBEDDING ALGORITHM

In this process, several steps have followed that include:

- Firstly, the secret message is processed aided by RSA with turns and keys giving encrypted information.
- Next step is compressing the secret message using the Huffman Coding, and
- Next step is decomposing the cover image using DWT to get four subbands which are LL, LH, HL, and HH.
- From an already obtained compressed encoded message image, include it in the selected subbands

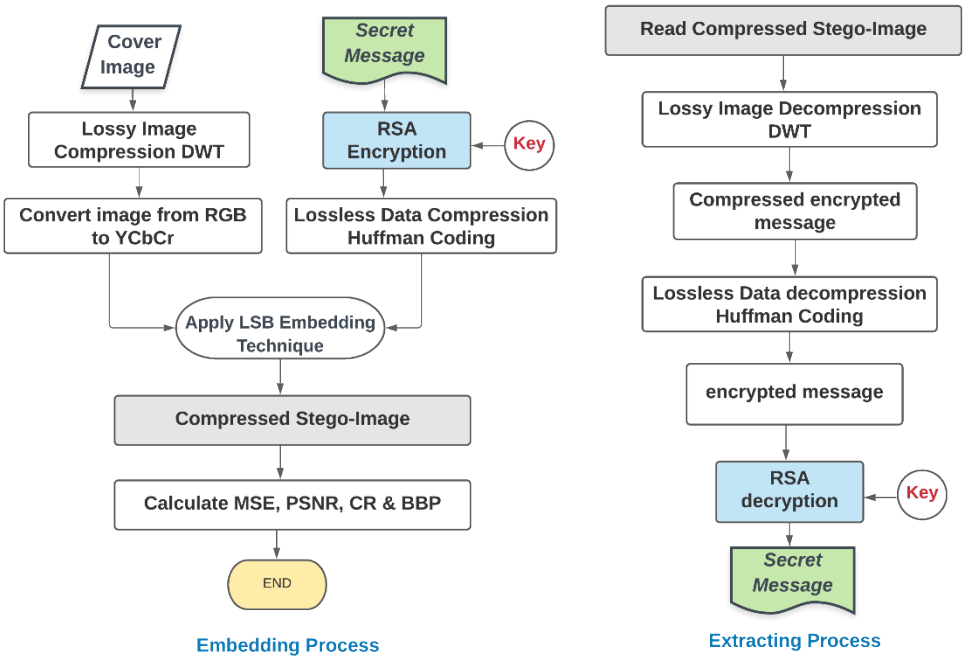


**FIGURE 4.** Process of embedding and extracting the secret message.

(LH, HL, and HH) and produce the enclosing subbands of the cover image.
- Using LSB embedding cover image with the encrypted secret message and getting compressed stego-image.
- The last step calculates CR, BPP, SP, MSE, and PSNR.

### B. EXTRACTING ALGORITHM

To get the secret message, the following steps must be followed:

- Firstly, decompress the already compressed stego-image using Huffman Coding and DWT in order to produce an uncompressed stego-image.
- Extract a message from the selected subbands (LH, HL, and HH) and produce a compressed encrypted message image.
- The next step is to use the Huffman tree file and implement Huffman encoding, decompress a compressed encrypted message image and produce an encrypted message image.
- Extracting the message using LSB from each pixel will help in retrieving stego-image binaries.
- Finally, decrypt the RSA-encrypted message using a key and output the secret message.

It is crucial to know the rate of adulteration available between the original cover image as well as the stego-image. In order to assess the distortion resulting from the proposed algorithm, objective measures are used. These are Peak Signal to Noise Ratio (PSNR), Mean Square Root (MSR), Compression Ratio (CR), Bits per Pixel (BPP), Saving Percentage and compression time.

## IV. MEASURING COMPRESSION PERFORMANCES

Several criteria can be used to evaluate the performance of the compressed algorithm. The following parameters can be used between compressed and uncompressed image:

#### 1) COMPRESSION RATIO (CR)

Compression ratio (CR) is vital in measuring pressure efficiency [3]. It is the ratio of the original and the compressed image. Image quality increases with increasing compression ratio (Higher the CR better the compression) and is mathematically expressed in Eq. (7)

$$\text{CR} = \text{Size of original image}/\text{Size of the compressed image}. \tag{7}$$

#### 2) COMPRESSION TIME

This factor specifies the amount of time that compression technology will require to compress and rebuild the original file [1]. Lower the value is considered as best for usage.

#### 3) COMPRESSION SPEED

Compression speed is based on adopted compression technology and parameter results depend on memory size. Lossy compression techniques increase computational and storage complexity. It is measured as a percentage of the size of the compressed output file per unit time required to compress the file in seconds [4] and is mathematically expressed in Eq. (8):

$$\text{Compression Speed} = \text{compressed file size}/\text{Compression} \times \text{time}. \tag{8}$$

**TABLE 2.** Proposed algorithm results.

| Cover images | Message size | Proposed Algorithm | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | SSIM | CR | CT | CS | SP% | BPP | MSE | PSNR |
| **Man** | **38278** | 0.9433 | 37.08 | 0.228 | 124571 | 25.8 | 1.11 | 2.54 | 39.71 |
| **Boy** | **25000** | 0.9421 | 36.77 | 0.244 | 77254 | 24.6 | 1.51 | 2.44 | 40.105 |
| **Girl** | **30178** | 0.9500 | 37.45 | 0.1552 | 153029 | 21.3 | 1.35 | 2.21 | 41.015 |
| **Apple** | **33145** | 0.9404 | 37.39 | 0.1744 | 146720 | 22.8 | 1.47 | 3.2 | 40.61 |
| **Bear** | **43123** | 0.9488 | 38.42 | 0.1696 | 195274 | 23.2 | 1.41 | 2.96 | 40.4 |
| **Lena** | **22652** | 0.9462 | 38.11 | 0.2248 | 79907 | 20.7 | 1.06 | 2.95 | 40.02 |
| **Average** | **32063** | **0.9451** | **37.53** | **0.1993** | **129459** | **23.1** | **1.32** | **2.72** | **40.31** |

#### 4) SAVING PERCENTAGE

Defined as in Eq. (9) the size reduction of size in compressed file compared to the uncompressed value [6]. Higher the percentage is considered as best for usage.

$$\begin{aligned}\text{Saving Percentage in(in\%)} &= (\text{original file size} - \text{compressed file size})/\text{original} \\ &\quad \times \text{file size}. \end{aligned} \tag{9}$$

#### 5) BITS PER PIXEL (BPP)

These are the information (bits) stored per pixel in a given image. As in Eq. (10), The total number of bits in the compressed image by that of the original image [2].

$$\begin{aligned}\mathbf{BPP} &= \text{number of bits in compressed image/total} \\ &\quad \times \text{number of pixels inthe image}. \end{aligned} \tag{10}$$

If the BPP is large, then a large memory is required to store the stego-image and vice versa.

#### 6) MEAN SQUARED ERROR (MSE)

This is the difference between the compressed image data and the original one as in Eq. (11). It is used mainly to analyze the quality of our image. It should be as less as possible where if it is 0, it means that the compressed and the original image are similar and is called the lossless image compression technique [2].

$$\mathbf{MSE} = \frac{1}{\boldsymbol{MxN}} \sum_{X=1}^{M} \sum_{Y=1}^{N} (\boldsymbol{f}(\boldsymbol{X}, \boldsymbol{Y}) - \boldsymbol{f}'(\boldsymbol{X}, \boldsymbol{Y}))^2 \tag{11}$$

where f (x, y) is the original input image, f′(x, y) is compressed image, and M, N are the dimensions of the images.

#### 7) PEAK SIGNAL TO NOISE RATIO (PSNR)

This is the ratio between the signal strength and the noise that appears in the signals. It all depends on the quality of the image. The higher the PSNR, the higher the image quality. It depends on the MSE of the selected image. When there is less difference between the two images, the PSNR is high, and so is the image quality and is mathematically expressed in Eq. (12)

$$\mathbf{PSNR} = 10\log_{10}(\text{MAX}^2/\text{MSE}) \tag{12}$$

where $\text{MAX}^2$ is $255^2$ is the maximum intensity of pixels in the ideal image. The quality of steganography will be tested using PSNR [2], [8], [10]. The higher PSNR's result and that achieved more than 40 dB indicated that the Stego-Image has good cognition as will be shown in experiments results.

#### 8) STRUCTURAL SIMILARITY (SSIM) INDEX

SSIM actually measures the perceptual difference between two identical images. It is not possible to judge which is better: this must be inferred from knowing which one is ''original'' and which has undergone additional treatment such as data compression [30]. The SSIM index defined as in Eq. (13):

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + \text{C}_1)(2\sigma_x\sigma_y + \text{C}_2)}{(\mu_x^2 + \mu_y^2 + \text{C}_1)(\sigma_x^2 + \sigma_y^2 + \text{C}_2)} \tag{13}$$

where $\mu_x$ and $\mu_y$ are defined by illuminating each image in the $x$ and $y$ directions, $\sigma_x$ and $\sigma_y$ are the standard deviations and the contrast estimation of the signal, and $\text{C}_1$ and $\text{C}_2$ are very small constants involved in controlling instability when either $(\mu_x^2 + \mu_y^2)$ or $(\sigma_x^2 + \sigma_y^2)$ is very close to zero. However, while respecting the standards of the global quality index, these constants are ignored and equal to zero. Therefore, the closer the SSIM is to the unity, the better the image performance it can reach [31].

## V. EXPERIMENTAL RESULTS

This proposed methodology is stimulated with the help of MATLAB 2012b software used on the Windows 7 platform as it offers efficient performance in much numerical computation, data analysis, visualization capabilities, and also acts as a tool for developing applications. MATLAB provides efficiency in using the functions as its interface helps the user through the processes of encryption and decryption, from and into cover [32]–[37].

**TABLE 3.** Huffman coding algorithm results.

| Cover images | Message size | Huffman coding (Lossless) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | SSIM | CR | CT | CS | SP% | BPP | MSE | PSNR |
| Man | 38278 | 0.8832 | 35.76 | 0.277 | 113452 | 17.9 | 1.51 | 1.3 | 38.91 |
| Boy | 25000 | 0.7832 | 34.73 | 0.287 | 71864 | 17.5 | 1.67 | 1.37 | 38.88 |
| Girl | 30178 | 0.7965 | 35.12 | 0.185 | 135067 | 17.2 | 1.75 | 1.39 | 39.68 |
| Apple | 33145 | 0.8743 | 34.52 | 0.197 | 140824 | 16.3 | 1.73 | 1.4 | 34.52 |
| Bear | 43123 | 0.8503 | 34.95 | 0.201 | 179786 | 16.2 | 1.66 | 1.42 | 34.93 |
| Lena | 22652 | 0.8827 | 35.01 | 0.266 | 69574 | 18.3 | 1.15 | 1.27 | 36.13 |
| Average | 32063 | **0.8450** | **35.02** | **0.236** | **118428** | **17.2** | **1.58** | **1.36** | **37.18** |

**TABLE 4.** DWT algorithm results.

| Cover images | Message size | DWT (Lossy) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | SSIM | CR | CT | CS | SP% | BPP | MSE | PSNR |
| Man | 38278 | 0.9288 | 28.17 | 0.008 | 3933065 | 17.8 | 0.98 | 0.25 | 40.51 |
| Boy | 25000 | 0.9295 | 28.66 | 0.018 | 1127778 | 18.8 | 0.89 | 0.08 | 41.33 |
| Girl | 30178 | 0.9277 | 29.45 | 0.009 | 2729432 | 18.6 | 0.88 | 0.23 | 42.35 |
| Apple | 33145 | 0.9243 | 29.94 | 0.021 | 1295812 | 17.9 | 0.95 | 0.05 | 46.7 |
| Bear | 43123 | 0.9311 | 31.29 | 0.011 | 3155820 | 19.5 | 0.86 | 0.19 | 45.87 |
| Lena | 22652 | 0.9151 | 30.69 | 0.015 | 1218678 | 19.3 | 0.97 | 0.13 | 43.91 |
| Average | 32063 | **0.9261** | **29.70** | **0.0137** | **2243431** | **18.7** | **0.92** | **0.16** | **43.45** |

**TABLE 5.** Comparison between the proposed method with the other existing methods.

| Average Values | SSIM | CR | CT | SP% | BPP | MSE | PSNR |
|---|---|---|---|---|---|---|---|
| Proposed Algorithm | 0.9451 | 37.535 | 0.199 | 23.067 | 1.318 | 2.717 | 40.310 |
| [3] | - | 0.0101 | 0.277 | - | - | 9.155 | 38.175 |
| [7] | 0.9704 | - | 1.314 | 15.325 | 0.087 | - | 25.331 |
| [31] | 0.9462 | - | - | 16.033 | - | 1.321 | 37.781 |

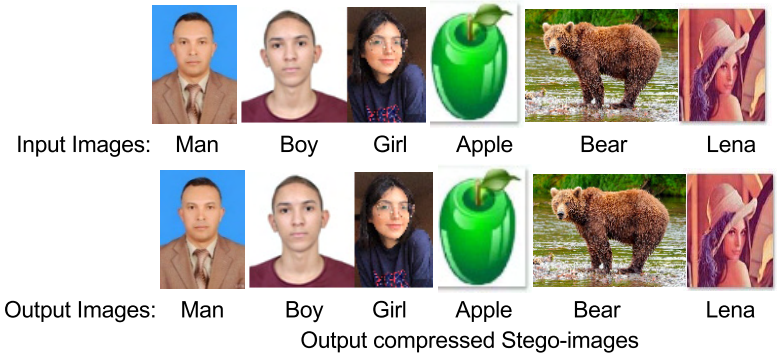


**FIGURE 5.** Input/output of images.

Based on Tables 2, 3, and 4 also Fig. 5 and Fig. 6, show the subjective analysis of the images and represent the output of the images using lossy/lossless compression techniques. In the implementation part, the color image of any format (like jpeg, png, and bmp) is taken into consideration. While using the Huffman coding, the stego-image produced gives

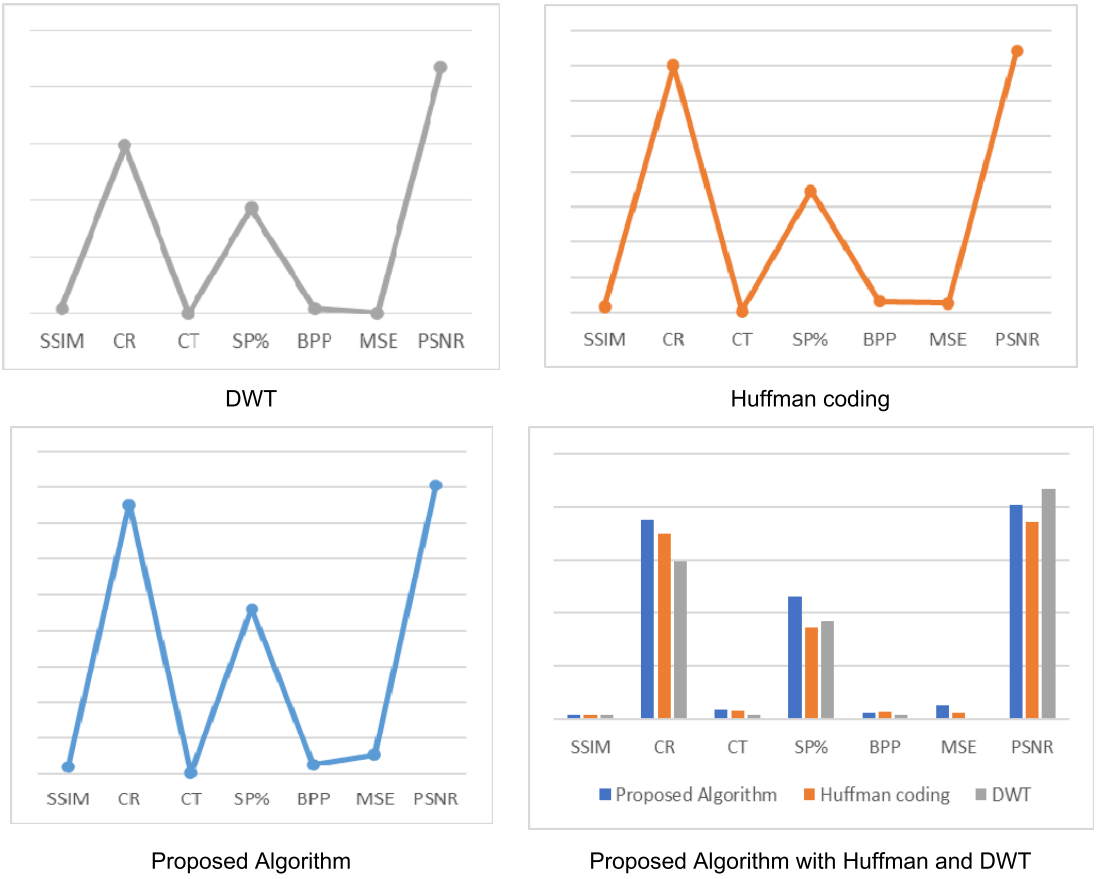


**FIGURE 6.** Proposed paper with Huffman and DWT results.

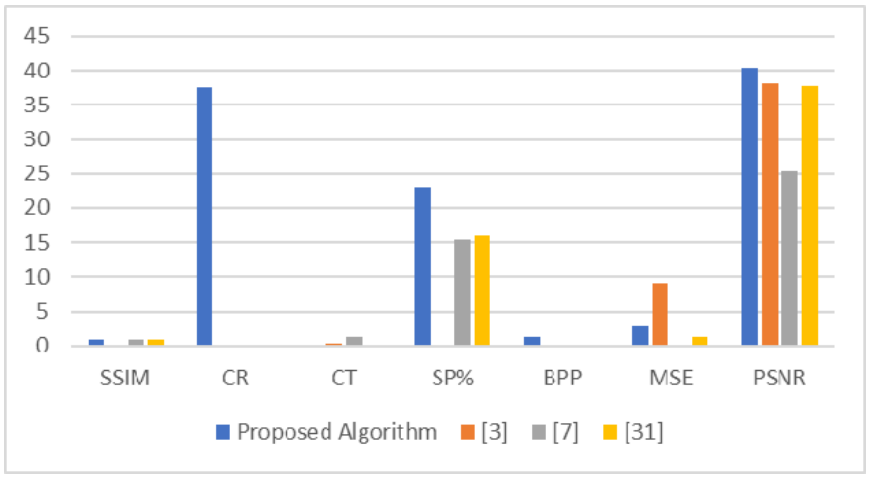


**FIGURE 7.** Comparison between the proposed method with other similar methods.

the effect in a decreasing pixel other than when not using the coding, so that in human visualization, the image still looks original to the cover image. In the proposed research, we concealed a 128 × 128 pixel image to 512 × 512 pixel producing a high-quality stego-image.

In this paper, we calculate several image quality properties, i.e. CR, PSNR, MSE, BPP, Saving Percentage, SSIM, and Compression Time. These properties are calculated for six images and the results projected into the corresponding tables 2, 3, and 4, also, we compared the proposed algorithm results with other results obtained in the relevant work sector especially from papers [3], [7], and [31], as shown in table 5 and Fig.7.

## VI. CONCLUSION

Image compression is a useful technology that helps save memory space and time while transferring images over a network. This helps to increase storage capacity as well as

transfer speed. In this paper, a combination of RSA, Huffman coding, and DWT has been carefully proposed as a method of securing and compressing messages, and even masking messages in the cover image, with the aim of producing a high-quality image with a small size. In our paper, we evaluated and discussed the RSA algorithm for encrypting and decoding the secret file with two different algorithms that can be used for image compression. We have also reviewed and discussed the two algorithms that can be used to compress images for both lossy and lossless techniques. In this paper, the distinct types of image compression techniques are evaluated on the basis of certain criteria such as compression ratio, compression time, compression speed, Saving Percentage, MSE, PSNR, Structural Similarity Index, and saving ratio.

A combination of RSA - Huffman Coding - DWT to secure a message and hide it in the cover image, produced compacted size with good image quality. Provide higher capacity by reducing the total message bits by up to 25% of the original message bits. Good stego-image quality is demonstrated by achieving an average PSNR score of over 40db and, also an average SSIM closest to the unit.

The results were compared with other results obtained in the relevant work sector. The experimental results indicate that the proposed mechanism has the more effective visual quality and storage capacity, and it has high security and acceptable durability against attacks than the existing techniques.

## REFERENCES

[1] C. A. Sari, G. Ardiansyah, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *Telkomnika*, vol. 17, no. 5, pp. 2400–2409, 2019.
[2] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, and H. M. Kelash, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika*, vol. 17, no. 3, pp. 1168–1175, 2019.
[3] N. Sharma and U. Batra, "Performance analysis of compression algorithms for information security: A review," *ICST Trans. Scalable Inf. Syst.*, vol. 7, no. 27, Jul. 2018, Art. no. 163503.
[4] Z. Ning and Z. Jinfu, "Study on image compression and fusion based on the wavelet transform technology," *Int. J. Smart Sens. Intell. Syst.*, vol. 8, no. 1, pp. 480–496, 2015.
[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[6] R. M. Thanki and A. Kothari, "Data compression and its application in medical imaging," in *Hybrid and Advanced Compression Techniques for Medical Images*. Cham, Switzerland: Springer, 2019, pp. 1–15.
[7] A. Jeromel and B. Žalik, "An efficient lossy cartoon image compression method," *Multimedia Tools Appl.*, vol. 79, nos. 1–2, pp. 433–451, Jan. 2020.
[8] F. Adhanadi, L. Novamizanti, and G. Budiman, "DWT-SMM-based audio steganography with RSA encryption and compressive sampling," *Telkomnika*, vol. 18, no. 2, pp. 1095–1104, 2020.
[9] R. Praisline Jasmi, B. Perumal, and M. Pallikonda Rajasekaran, "Comparison of image compression techniques using Huffman coding, DWT and fractal algorithm," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2015, pp. 1–5.
[10] E. Setyaningsih, R. Wardoyo, and A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 486–503, Nov. 2020.
[11] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, Jun. 2017.
[12] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 9971–9989, Apr. 2019.
[13] H. Anada, T. Yasuda, J. Kawamoto, J. Weng, and K. Sakurai, "RSA public keys with inside structure: Proofs of key generation and identities for Web-of-trust," *J. Inf. Secur. Appl.*, vol. 45, pp. 10–19, Apr. 2019.
[14] Y. Barrios, A. Rodríguez, A. Sáchez, A. Pérez, S. López, A. Otero, E. de la Torre, and R. Sarmiento, "Lossy hyperspectral image compression on a reconfigurable and fault-tolerant FPGA-based adaptive computing platform," *Electronics*, vol. 9, no. 10, p. 1576, 2020.
[15] C. Chen, L. Zhang, and R. L. K. Tiong, "A new lossy compression algorithm for wireless sensor networks using Bayesian predictive coding," *Wireless Netw.*, vol. 26, no. 8, pp. 5981–5995, Nov. 2020.
[16] S. Singh and R. Devgon, "Analysis of encryption and lossless compression techniques for secure data transmission," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Feb. 2019, pp. 1–5.
[17] G. Zhang, J. Wang, C. Yan, and S. Wang, "Application research of image compression and wireless network traffic video streaming," *J. Vis. Commun. Image Represent.*, vol. 59, pp. 168–175, Feb. 2019.
[18] N. Dhawale, "Implementation of Huffman algorithm and study for optimization," in *Proc. Int. Conf. Adv. Commun. Comput. Technol. (ICACACT)*, Jun. 2014, pp. 1–6.
[19] A. K. Pal, K. Naik, and R. Agrawal, "A steganography scheme on JPEG compressed cover image with high embedding capacity," *Int. Arab J. Inf. Technol.*, vol. 16, no. 1, pp. 116–124, 2019.
[20] H. C. C. Lerner, "Rate distortion approach to bit in lossy image set compression," in *Proc. Int. Conf. Syst. Signal Image Process.*, 2014, pp. 227–230.
[21] H. Sunil and S. G. Hiremath, "A combined scheme of pixel and block level splitting for medical image compression and reconstruction," *Alexandria Eng. J.*, vol. 57, no. 2, pp. 767–772, Jun. 2018.
[22] D. R. I. M. Setiadi, "Payload enhancement on least significant bit image steganography using edge area dilation," *Int. J. Electron. Telecommun.*, vol. 65, no. 2, pp. 287–292, Apr. 2019, doi: 10.24425/ijet.2019.126312.
[23] M. R. D. Farahani and A. Pourmohammad, "A DWT based perfect secure and high capacity image steganography method," in *Proc. Int. Conf. Parallel Distrib. Comput., Appl. Technol.*, Dec. 2013, pp. 314–317.
[24] C.-L. Hsu, Y.-S. Huang, M.-D. Chang, and H.-Y. Huang, "Design of an error-tolerance scheme for discrete wavelet transform in JPEG 2000 encoder," *IEEE Trans. Comput.*, vol. 60, no. 5, pp. 628–638, May 2011.
[25] A. Rawat, K. Sehgal, A. Tiwari, A. Sharma, and A. Joshi, "A novel accelerated implementation of RSA using parallel processing," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 309–322, Feb. 2019.
[26] D. Minnen and S. Singh, "Channel-wise autoregressive entropy models for learned image compression," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2020, pp. 3339–3343.
[27] Y. Yang, R. Bamler, and S. Mandt, "Improving inference for neural image compression," 2020, *arXiv:2006.04240*. [Online]. Available: http://arxiv.org/abs/2006.04240
[28] R. Patel, V. Kumar, V. Tyagi, and V. Asthana, "A fast and improved image compression technique using Huffman coding," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 2283–2286.
[29] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105837.
[30] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[31] M. Dehshiri, S. G. Sabouri, and A. Khorsandi, "Structural similarity assessment of an optical coherence tomographic image enhanced using the wavelet transform technique," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 38, no. 1, pp. 1–9, 2021.
[32] C. Tsai, W.-Y. Shih, Y.-S. Lu, J.-L. Huang, and L.-Y. Yeh, "Design of a data collection system with data compression for small manufacturers in industrial IoT environments," in *Proc. 20th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Sep. 2019, pp. 1–4.
[33] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Comput. Commun.*, vol. 152, pp. 72–80, Feb. 2020.
[34] P. Li and K.-T. Lo, "Joint image encryption and compression schemes based on 16×16 DCT," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 12–24, Jan. 2019.

[35] S. Yuan and J. Hu, "Research on image compression technology based on Huffman coding," *J. Vis. Commun. Image Represent.*, vol. 59, pp. 33–38, Feb. 2019.
[36] H. M. Fadhil and M. I. Younis, "Parallelizing RSA algorithm on multicore CPU and GPU," *Int. J. Comput. Appl.*, vol. 87, no. 6, pp. 15–22, 2014.
[37] R. Starosolski, "New simple and efficient color space transformations for lossless image compression," *J. Vis. Commun. Image Represent.*, vol. 25, no. 5, pp. 1056–1063, Jul. 2014.

**OSAMA FOUAD ABDEL WAHAB** received the B.Sc. and M.Sc. degrees in computer science and engineering from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1991 and 2015, respectively, and the Ph.D. degree in electrical and computer engineering from the Faculty of Engineering, Minia University, El-Minia, Egypt. He is currently working as an ICT Consultant and a Lecturer at Kuwait University. His research interests include information, networks, internet and multimedia security, cryptography, steganography, and steganographic algorithms for multimedia applications.

**ASHRAF A. M. KHALAF** received the B.Sc. and M.Sc. degrees in electrical engineering from Minia University, Egypt, in 1989 and 1994, respectively, and the Ph.D. degree in system science and engineering from the Graduate School of Natural Science and Technology, Kanazawa University, Japan, in March 22, 2000. He is currently a Professor of DSP and the Head of the Department Electronics and Communications Engineering, Faculty of Engineering, Minia University.

**AZIZA I. HUSSEIN** received the B.Sc. and M.Sc. degrees from Assiut University, Egypt, in 1983 and 1989, respectively, and the Ph.D. degree in electrical and computer engineering from Kansas State University, USA, in 2001.

She joined Effat University, Saudi Arabia, in 2004, where she established the first Electrical and Computer Engineering program for women in the country and taught related courses. She was the Head of the Department of the Electrical and Computer Engineering, Effat University, from 2007 to 2010. She was the Head of the Department of the Computer and Systems Engineering, Faculty of Engineering, Minia University, Egypt, from 2011 to 2016. She is currently a Professor and the Chair of the Department of the Electrical and Computer Engineering, Effat University. Her research interests include microelectronics, analog-to-digital VLSI system design, RF circuit design, high-speed analog-to-digital converters design, and wireless communications.

**HESHAM F. A. HAMED** was born in Giza, Egypt, in 1966. He received the B.Sc. degree in electrical engineering, and the M.Sc. and Ph.D. degrees in electronics and communications engineering from Minia University, EL-Minia, Egypt, in 1989, 1993, and 1997, respectively. He was the Dean of the Faculty of Engineering, Minia University. He was a Visiting Researcher with Ohio University, Athens, Ohio. From 1989 to 1993, he worked as a Teacher Assistant with Department of the Electrical Engineering, Minia University. From 1993 to 1995, he was a Visiting Scholar with Cairo University, Cairo, Egypt. From 1995 to 1997, he was a Visiting Scholar with Texas A&M University, College Station, TX (with the group of VLSI). From 1997 to 2003, he was an Assistant Professor with the Department of the Electrical Engineering, Minia University. From 2003 to 2005, he was Associate Professor Minia University. He has published more than 120 articles. His research interests include analog and mixed-mode circuit design, low voltage low power analog circuits, current mode circuits, nano-scale circuits design, and FPGA.