IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 3, 2021, accepted November 25, 2021, date of publication November 30, 2021,
date of current version December 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131566

Joint Crypto-Compression Based on Selective Encryption for WMSNs

IYAD HRAINI[1], MOUSA FARAJALLAH[2], NABIL ARMAN[3], AND WASSIM HAMIDOUCHE[4]

[1]College of Graduate Studies, Palestine Polytechnic University, Hebron 00970, Palestine
[2]Department of Computer Engineering, Palestine Polytechnic University, Hebron 00970, Palestine
[3]Department of Computer Science and Information Technology, Palestine Polytechnic University, Hebron 00970, Palestine
[4]Department of Electrical Engineering, Univ. Rennes, INSA Rennes, CNRS, IETR-UMR 6164, 5700 Rennes, France

Corresponding author: Mousa Farajallah (mousa_math@ppu.edu)

ABSTRACT Wireless Multimedia Sensor Networks (WMSNs) have been widely used in many aspects of life such as monitoring aims, risk environments and medical services. However, WMSNs have many challenges due to resources limitation (e.g., restriction in processing, energy and memory). Moreover, security issues related to WMSNs attract many research efforts. Due to limitations of WMSNs resources and their internal encoding, standard methods of data encryption are inappropriate to be used in order to secure data of WMSNs. In this paper, a compression algorithm named Set Partitioning In Hierarchical Tree (SPIHT), jointly with selective encryption during the compression process cycle, is proposed. Selected bins to be encrypted are analyzed and tested to preserve format compliance and constant bit rate. As a result the decoder will not crash. Moreover, any standard decoder can be used without any modifications. This is of great importance to the encoding companies that use standard Codecs. The proposed approach is suitable and capable to be used in WMSN taking into account their limitations of resources. The obtained results confirm the high performance of the proposed approach with an overhead of less than 1%. The main contribution of this paper is the ability to use selective encryption based on tested and predefined bins that preserve format compliance and constant bit rate requirements during the compression cycle with minimum overhead. Thus, our proposed approach is applicable for real-time applications.

INDEX TERMS Wireless multimedia sensor networks, joint crypto-compression, SPIHT, limited resources.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are small devices that sense scalar data like temperature from different environments as monitoring, health care, industrial and defense applications. An example of security of real-time application in WMSN is surveillance. In this application, the obtained video frames should be transmitted and encrypted in real-time.

As an extension and development to WSN, Wireless Multimedia Sensor Networks (WMSNs) appeared last year [1], [2]. WMSNs devices sense multimedia data (audio, images, and videos) rather than scalar values, which means more resource requirements in these devices. WMSNs are used in environments with limited available power, risky places, and medical applications. In recent years, researchers are focusing on enabling wireless sensors networks to support multimedia data [3]. The devices used in these systems face many challenges because of the limitation of resources such as processing, power consumption, memory size, and bandwidth. The sensors detect and transmit data through wireless channel connections, which have many security threats and vulnerabilities to attacks, to sink nodes using a set of protocols and communication standards. They achieve this goal with many difficulties since transmission is not for scalar data only but audio, images, and video, which means more challenges in processing, memory, and power.

A lot of research efforts were presented to address security threats in WMSNs [4]. As WMSNs are part of the Internet of Things (IoT), they extend more and more in different applications such as military uses, health-care and medical applications. They play a role in surgery, highways traffic monitoring to avoid traffic congestion by giving drivers notifications about that congestion, gaming to sense player actions, wildlife monitoring, energy harvesting sensors, and other life usages [5]–[7]. The sensitivity of transmitted information in WMSNs motivates researchers to propose novel approaches in order to secure this information. The challenge

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

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

is to achieve the encryption in such an environment that has limited resources (memory and processing power). The significant of our proposed approach is its ability to secure real-time applications that use codecs without crashing the decoder during decompression process. In addition, our approach preserves constant bitrate.

Data compression is a process of decreasing the number of bits required to represent data. Compressing data can save storage capacity, speed up file transfer, and reduce costs for storage hardware and network bandwidth [8]. In traditional encryption, all data is encrypted, which means more processing and more power consumption. We should reduce the volume of encrypted data using partial or selective encryption which provides a suitable level of securing data transmission with minimized overhead. SPIHT algorithm takes the strengths of Embedded Zerrotree Wavelet (EZW), as embedded coding of wavelet coefficients and ordered coefficient transmission. Selective encryption, in SPIHT, to sensitive information is the best choice for encrypting to serve the limitation in resources(power, memory, and bandwidth) in WMSNs.

To reduce the time of processing, we combine compression and encryption in a single processing step. Thus, we can save power consumption, which is a critical issue in WMSNs. The standard approaches are not applicable to secure communication between WMSNs devices. The research question is how to secure the transmitted data over WMSNs.

II. LITERATURE REVIEW

In recent years, many approaches have been proposed to overcome the security issues in WMSN. The main aspects of security in these approaches are:

1) Symmetric and Asymmetric Cryptography: most proposed approaches use symmetric cryptography which defines single shared key for encryption and decryption functions. At the same time there are challenges on how to distribute the shared key securely in WMSNs environment. Asymmetric cryptography algorithms are rarely used in WMSNs because they have high computing overhead and require more processing times. Most of the proposed works use compression in order to reduce data transmitted between nodes and sink node especially when multimedia data are transmited.
2) Selective Image Encryption: to reduce the size of data and processing time of encryption, some approaches propose a selective image encryption technique. In traditional encryption (i.e., full encryption), all data is encrypted, which means more processing and more power consumption; instead, in WMSNs, the volume of encrypted data should be minimized. Partial or selective encryption provides a reasonable level of securing data transmission with a minimum overhead [9]. In addition, selective encryption is based on encrypting only part of the compressed data. This part of data has the most significant information of the original data image [10]. Two coding algorithms are the most suitable for selective encryption: quadtree coding and wavelet coding. In wavelet coding, Discrete Wavelet Transform (DWT) decomposes raw(organic) images into smaller parts, called sub-layers, where each sub-layer image has different importance in the process of reconstructing original images. Each sub-layer can be ordered into one or more data packets, where the sub-layer of greatest relevance always has higher priority than remaining sub-layers.
   By using DWT, the sub-layer of primary relevance is necessary for the regeneration of the original image, where the reconstructed image will not be clear in case that layer is missing. However, only with the sub-layer of highest relevance it is possible to reconstruct images of acceptable quality, depending on the application requirements. Proposing a selective encryption combined with a DWT reduces the computational overhead and saving resources [11].
   RC4 (Rivest Cipher 4) is a variable-key-size stream cipher. It is used in large number of presented selective image encryption algorithms. It uses a variable length key from 1 to 256 bytes to initialize a 256-byte array. The array is used for subsequent generation of pseudo-random bytes and then forms a pseudo-random stream that is XOR-ed with the plain-text or cipher-text to produce the cipher-text in the encryption process or the plain-text in the decryption process [12].
3) Compression techniques: DWT is compression technique used in Selective images encryption. Partitioning a space based on a neighborhood relations of places in the space is named as **Voronoi tessellation** [13]. It uses the Voronoi Diagram (VD), which is a set of points in the plane that partitions the plane into polygons, called Voronoi cells. Each cell contains exactly one generated point (called site). As a result, every point in a given cell is closer to its generating point than any other. So at the source side, the Voronoi tessellation is applied on each input image.

TABLE 1. Literature approaches in WMSNs encryption.

Approach	Encryption	Compression	Selective-encryption	Year
Xiang et al. [14]	RC4	DWT	Yes	2013
Goncalves and Costa [15]	AES	DWT	Yes	2016
Mostefaoui et al. [16]	RC4	Voronoi tessellation	No	2015
Tsitsipis et al. [17]	Skipjack	Quadtree	Yes	2011
Taneja et al. [18]	Stream cipher	SPIHT	Yes	2011
Xiang et al. [19]	RC4	SPIHT	Yes	2014

Table 1 presents the most important approaches that have been presented recently regarding WSN security.

Xiao *et al.* [20] presented a low-cost and high-efficient privacy-protection scheme for distributed compressed video sensing in WMSNs. A scrambling technique is used in order to achieve the required substitution and diffusion effects to resist potential attacks. The presented results confirm that the scheme is suitable for real-time applications and restricted resources.

Kong *et al.* [21] presented a good survey and comparison using one hundred symmetric ciphers for restricted resources and real-time applications. The evaluated algorithms are classified into:modern block ciphers, involution ciphers, lightweight block ciphers and stream ciphers. The research concludes that any symmetric cipher for WMSN should be evaluated and addressed on real-time environment and using the same variables and parameters to identify the most suitable one.

Xiang *et al.* [14] presented a quick, lightweight image encryption algorithm in (WMSN) for protecting JPEG 2000 images. The encryption algorithm uses the idea of selective encryption based on RC4 algorithm.

Goncalves and Costa [15] presented a system that can keep the energy while assuring acceptable levels of protection.

Mostefaoui *et al.* [16] presented an image encryption algorithm, without using any of traditional compression techniques and security standards. A new method, based on a simple algebraic rule, to construct a dynamic Voronoi diagram had been presented. Also, the stream cipher RC4 layer is used to produce a set of points (x, y) that are used to build the Voronoi tessellation.

A system for secured sequential image transmissions in a WMSN is designed in Tsitsipis *et al.* [17], where a Quad Tree Decomposition (QTD) algorithm that is able to compress the images before transmission is used. Skipjack algorithm is used to encrypt data which is a relatively lightweight symmetric cipher, using an 80–bit key to encrypt and decrypt 64–bit data blocks.

Taneja *et al.* [18] presented a selective encryption of high probably significant bits of the SPIHT bitstream output. A decision criterion was developed for identifying the significance bits. Selection of significant bits is obtained using two stages: in the first stage, a random vector R is generated using logistic map, and in the second stage a deciding criterion is enforced for vector R for selection of significant bits which have high probability. Security in this approach is attained by encrypting the significant bits and encrypting the bits locations.

Xiang *et al.* [19] presented a Joint compression and selective encryption based on SPIHT(JCSE-SPIHT). The basic idea of JCSE-SPIHT method is to perform a Fast Random Insertion(FRI) on the List of Insignificant Pixels(LIP) and List of Insignificant Sets(LIS) on selected numbers of iteration coding of SPIHT. Therefore, selective node randomization of LIP and LIS by FRI is in the first round (r) of iteration; the parameter r is used to control the required security level. A selection of r represents a trade-off between security demand and computational overhead. The testing result finds that when $r = 6$, a suitable configuration as the plain image is well secured while 1-4 percent of data is needed to be encrypted. The proposed method generates keystream plain text that is dependent on JCSE-SPIHT compression algorithm that resists the chosen-plaintext attacks. According to this approach it is concluded that a lot of processing required regarding the scrambling ordering of lists position and mod operations. Also six rounds for encryption($r = 6$) consume more processing, memory and power. It is essential to have a real-time secure image encryption that considers the limitation in WMSNs and require less computational resources.

According to the previous approaches joint compression and selective encryption is the only solution to secure WMSNs. The compression is used to reduce the amount of transmitted data, which serves a limited bandwidth in WMSNs environment; while the selective encryption is also implemented to minimize the amount of encrypted data while satisfying a suitable level of security. The best compression algorithm that is suitable to be used in WMSNs to assist the required constrained in compression was discussed in [22]. SPIHT is the best solution among all compression algorithm in WMSNs; so, this algorithm is selected to be integrated in the proposed approach.

III. PROPOSED SOLUTION

The proposed solution is shown in Figure 1. First of all, an image is read and converted to the coefficient array. Then, using Discrete Wavelet Transform (DWT), the coefficient array is converted to a wavelet coefficients array. The SPIHT algorithm depends on the wavelet coefficients array to perform compression and encryption jointly. The encrypted output bitstream is sent through the insecure wireless channel to the receiver side. However, the used secret key can be transmit-ted using asymmetric key cryptography or a trusted-server schemes. Figure 1 shows in detail all processes of SPIHT, which include compression, encryption, and bitstream output. On the receiver side (sink node), the encrypted bitstream arrives, and the algorithm receives bitstream and performs decryption and decompression in the same step (jointly). The output of this process is the wavelet coefficient array. By using the inverse of DWT, the wavelet coefficient array is converted to a coefficient array. Finally, the decrypted and decompressed image is reconstructed.

Figure 1 shows the core function of the SPIHT, which is joint compression and encryption. The coding process that includes the compression algorithm on the sender side and also the decoding process and decompression process on the receiver side is analyzed and implemented. More details about this algorithm are presented in subsection A. A joint encryption and compression solution in the same cycle used the Pseudo-Random Number Generator (PRNG) to construct session keys and stream ciphers. The used generator is initially proposed in [23]. It is based on a modified chaotic map and a proposed lookup table, which is created in such a way that the stored numbers will not be duplicated in the same row, column, or diameter. The proposed map and lookup table are used to produce non-linear and non-invertible functions, which are the primary targets of any secure PRNG. The used PRNG secret key length is 299 bits [23]. The proposed solution in this paper should follow the standard requirements of the real-time video streaming, where presented security solutions for WMSN in the literature to the best of our knowledge did not consider all of the following:

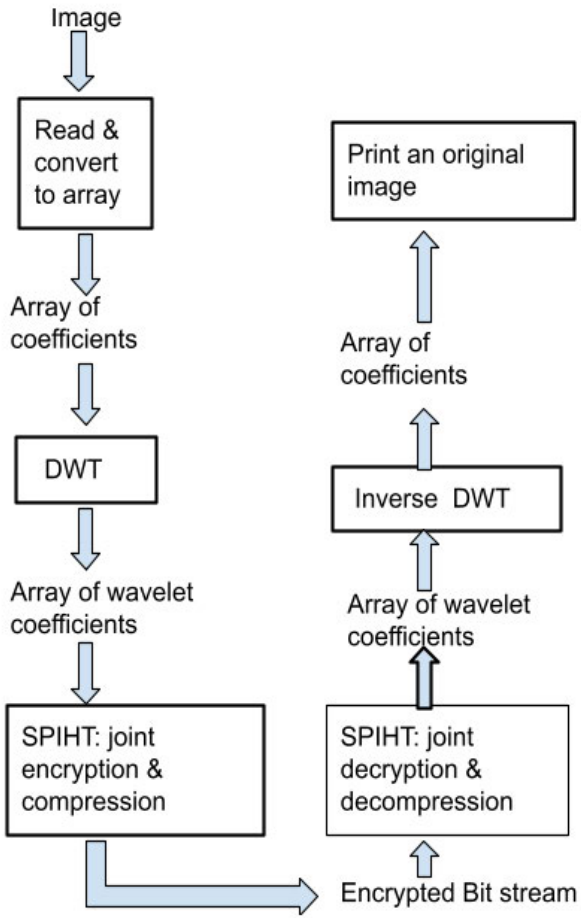

FIGURE 1. Proposed solution diagram.

1) Any solution should be format compliance.
2) The compression ratio including the encryption algorithm should be close to the compression function only (before joint compression and selective encryption).
3) Security level should be suitable for WMSN applications.
4) The limitation of resources(power, RAM, and CPU) should be considered.
5) The speed of compression and selective encryption approach should be close to compression without encryption.

A. SPIHT ALGORITHM

SPIHT is an algorithm that combines the strengths of EZW as embedded coding of wavelet coefficients and ordered coefficient transmission. SPIHT algorithm can exploit the grouping of insignificant coefficients. Also, an encoder and the decoder follow the same execution path. The decoder can recover the ordering information from the execution path [24]. In SPIHT, for a given value of n, the coefficients are examined according to equation 1, where n is calculated as in equation 3.

$$\left|C_{i,j}\right| \geqslant 2^n \tag{1}$$

where C is the value of coefficient at i,j location, and 2^n is the threshold. For a subset of coefficients T_m, they are examined to determine if the subset is significant or not according to equation 2

$$max_{(i,j)\epsilon T_m}\left\{|X_{i,j}|\right\} \geq 2^n \tag{2}$$

where X is the maximum value of coefficient in set T_m, i, j is the coordinate location and T_m is a subset of pixels. If the condition is true, the subset T_m is significant, and the subset is further partitioned to determine insignificant and significant subsets. If the condition is false, then the subset T_m is insignificant. The significant subsets are repetitively partitioned till single significant coefficients are identified.

SPIHT Encoding and Decoding: The SPIHT algorithm applies the above rules to the subband coefficients. Both encoder and decoder are identical, and no direct transmission of ordering information needed in other progressive transmission algorithms for embedded coding is necessary. The encoder and decoder continuously update the following lists:

1) List of Insignificant Pixels (LIP).
2) List of Significant Pixels (LSP).
3) List of Insignificant Sets (LIS).

The entry is identified by a coordinate(i,j). In LIP and LSP, the entry represents individual pixels, whereas, in LIS, the entry represents a set of sets. The number n is determined from the maximum magnitude of the coefficients as in equation 3.

$$n = \left\lfloor log_2(max_{(i,j)}\left|C_{i,j}\right|)\right\rfloor \tag{3}$$

$|C_{i,j}|$ is the maximum coefficients value, and n is the initial value of n^{th} threshold. So n equals the low magnitude of the binary logarithm of the value of the maximum coefficients.

B. JOINT CRYPTO-COMPRESSION IN SPIHT ALGORITHM

The SPIHT algorithm has four stages: initialization, sorting, refinement, and quantization. The proposed solution performs encryption jointly in the sorting pass. The selection of the position of the proposed selective encryption is proposed after many experiments to identify the position that satisfies the WMSN encryption requirements mentioned previously. This pass is presented in detail to show how the joint compression and selective encryption in the single process of the SPIHT algorithm are achieved. Algorithm 1 presents our proposed solution algorithm. Algorithm 1 begins with an initialization step, which includes finding n as in equation 3, which is the first threshold. Setting LSP, to be $\{\phi\}$ and setting LIP list, which entry represents individual pixels in LL subband. Three steps follow the initialization step: sorting, refinement, and quantization; the algorithm updates its passes, which are iteratively repeated in this order until the least significant refinement bits are transmitted. During the sorting pass, if it is the first pass (max threshold) as in equation 4: If we have a coefficient value X, then we compare this value with threshold T, if X less than T its declared as insignificant and output '0'; and if X is greater than or equal to T its declared

as significant and output '1'.

$$S(X) = \begin{cases} 1\,(significant), & if\ X \geq T \\ 0\,(insignificant), & Otherwise \end{cases} \quad (4)$$

If $S_n(i, j)$ significant then move (i,j) coordinate from LIP to LSP. Output the sign of significant coefficient '1' if it is positive, '0' otherwise. Encrypt the output for all bit-stream representing the LIP coefficients (Only in the first pass) and the sign of significant coefficients using PRNG.

C. ENCRYPT THE SIGN OF COEFFICIENTS AND FIRST LIP LIST

Any change in the output bitstream of the encoder will distort the image through the decoding process; because each bit of the stream has an impact in encoding and decoding side; some bits represent significant coefficients, and others represent their sign, whereas others represent the significant set.

The ordering of bitstream depending on LIP and LIS is shown in SPIHT Algorithm 1. First, the algorithm searches LIP for capable significant coefficients, and then the algorithm searches the LIS list for the significant set. The structure of the bitstream is as follows: the first position in the bitstream represent the size of the matrix (number of rows); the second position represents the maximum coefficient in the matrix of image; where the third position in the bitstream represents the level of decomposition; the reset values of the bitstream are 0 or 1 representing the following cases:

1) 0's may indicate that the determined LIP coefficient is insignificant. It may also refer to insignificant sets, or the sign of the LIP coefficients(negative sign).
2) 1's may refer to the significant LIP coefficients or the set in the LIS list is significant, or refer to the sign of coefficients (positive sign).

The big challenge, in this case, is to find a strategy to encrypt part of the bitstream and decrypt this bitstream without any violations that crash the decoder to accept its format. So, the bitstream is analyzed and investigated carefully. The sign of the significant coefficients can be encrypted without crashing the decoder, and it reconstructs the encrypted and compressed images again. Moreover, extra encryption is formed to increase the security level by encrypting the first LIP list of coefficients, which is sensitive and has the most information about the image. The sign of significant coefficients is encrypted as presented in equation 5.

$$sign_{new} = sign_{old} \oplus PRNG_i \quad (5)$$

where $sign_{old}$ represents the old value of the significant coefficient's sign, $sign_{new}$ represents the new value of the significant coefficient's sign after performing the XOR operation with $PRNG_i$ bit. $PRNG_i$ is the i^{th} bit of generated bits from PRNG bitstream. Also, the coefficients of the first LIP list are encrypted as presented in equation 6.

$$LIPcoeff_{new} = LIPcoeff_{old} \oplus PRNG_i \quad (6)$$

where $LIPcoeff_{old}$ is the coefficient's old value from the first LIP list, $LIPcoeff_{new}$ is the coefficient's new value of the first LIP list after performing XOR operation with $PRNG_i$.

Our proposed algorithm differs from the existing algorithm (SPIHT) in the selective encryption process, which is performed during compression cycle (joint encryption and compression), mainly preserving format compliance, constant bit rate and taking into account the limited resources(memory and power consumption) of these types of devices. A comparison between our algorithm and the standard algorithm is presented in Table 2. It is clear that the proposed approach doesn't violate the format compliance and at the same time it maintains constant bit rate requirement of the standard algorithm. Moreover, in our proposed approach, compression and encryption are achievable without any information losses, where the total overhead is less than 1%, making it appropriate for real-time applications.

IV. EXPERIMENTS AND RESULTS

The proposed approach is utilized to secure multimedia data transmission in WMSNs, considering wireless sensors network limitation, hardware resources, and bandwidth. The proposed algorithm is simulated using MATLABR2017a. Gray-level images in the USC-SIPI image database [25] are used. Our proposed approach encrypts the most sensitive information, which exists in the first LIP list, and the sign of significant coefficients to evaluate the security and performance parameters of the proposed approach.

Our proposed approach was evaluated using standard metrics: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index(SSIM), Visual Quality(VQ), Edge Detection (ED). Other statistical metrics have also be considered, such as Histogram Analysis, Encryption Quality (EQ), and Key Space Analysis to check the robustness of the proposed approach against different types of attack. Time overhead will be measured, and constant bitrate will also be assessed.

A. TIME OVERHEAD AND CONSTANT BITRATE

The encryption time of the proposed approach on the gray level images is 36 ms. Also the measured decryption time is close to 36 ms. While the compression time without encryption on the same image Lena with size of 512 × 512 is $Tcomp = 12.66s$. Thus, the overhead time is calculated as in equation 7, the key generated time (Tkey) equal to $72.2789\mu s$.

$$overhead = \frac{Tencrypt + Tkey}{Tcomp}$$
$$overhead = \frac{0.036 + 0.0000722789}{12.664} = 0.0028484111576 \quad (7)$$

The encryption overhead is 0.2848%, which means that it's less than 1% and so it's suitable for all real-time applications.

The bitrate of the proposed approach is evaluated. The number of bits that is used to represent the image in the case of using compression without encryption is identical to the number of bits in the case of joint crypto-compression for

Algorithm 1 Our Proposed Approach/Algorithm

Step-1: Initialization:
  Output $n = \lfloor log_2(max_{(i,j)} |C_{i,j}|) \rfloor$
  Set the LSP to ϕ.
  Set the LIP to individual pixels in the LL subband.
Step-2: Sorting pass:
  Step-2.1: For each entry in LIP
    If the first pass (when $n = n_{max}$) then:
      A) As in equation 4 output '1' if $S_n(i, j)$ significant, '0' otherwise;
       If $S_n(i, j)$ significant then move (i,j) coordinate from LIP to LSP
      B) Output the sign of significant coefficient only;
       '1' if it is positive, '0' otherwise.
      C) Encrypt the output for all bit-stream
       that represents the LIP coefficients and
       the sign of significant coefficients using PRNG
    Else (if it is not the first pass)
      A) As in equation 4 output '1' if Sn(i,j) significant, '0' otherwise.
       If $Sn(i, j)$ significant then move (i,j) coordinates from LIP to LSP list
      B) Output the sign of significant coefficient only; '1' if it is positive, '0' otherwise
      C) Encrypt the sign of significant coefficients only
  Step-2.2: For each entry (i, j) in the LIS do:
    Step-2.2.1: if entry of type A then:
      output $S_n(i, j)$; i.e., '1' if it is significant, '0' otherwise.
      if $S_n(D(i, j)) = 1$ (significant) then:
        for each $(k, l) \epsilon O_{(i,j)}$ do
          output $S_n(k, l)$; i.e., '1' if it is significant, '0' otherwise.
          if $S_n(k, l) = 1$ then add k,l to LSP and output the sign of coefficient (k,l)
          if $S_n(k, l) = 0$ then add k,l to LIP
        if $L_{(i,j)} \neq \phi$ then move (i,j) to the end of LIS as entry of type B, go to step 2.2.2;
        otherwise remove entry (i,j) from the LIS
    Step-2.2.2: If the entry of type B then
      output $S_n(L_{(i,j)})$, i.e., 1 if it is significant, 0 otherwise
      if $S_n(L(i, j)) = 1$ (significant) then
        add each $(k, l) \epsilon O_{(i,j)}$ to end of the LIS as type A
        remove (i,j) from the LIS
Step-3: Refinement pass: For each entry in the LSP, except those which are added
  during the sorting pass with the same n, output the n^{th} most significant bit
Step-4: Quantization-step update pass In this pass, n is decremented by 1 and the steps-2,
  3 and 4 are repeated until n

TABLE 2. Comparison of our proposed approach with the standard algorithm (SPIHT).

Comparison criteria	SPIHT	Proposed approach	Comments
Compression time	12.6648 s	12.7001 s	<1%
PSNR	39.85	39.85	Loss of info is zero
SSIM	0.9489	0.9489	Loss of info is zero
Encryption	No	Yes: selective	–
Format Compliance	Yes	Yes	–
Constant bitrat	Yes	Yes	–

different Lena image sizes. This concludes that the proposed approach solution is constant bitrate.

B. OBJECTIVES QUALITY

Objectives quality evaluation assessment includes: PSNR, and SSMI [23]. PSNR is the ratio between the maximum possible power of a signal to the power of corrupting noise. PSNR is defined by the Mean Squared Error (MSE).

$$MSE = \frac{1}{n \times m} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [x(i, j) - y(i, j)]^2.$$

PSNR can be calculated using equation 8:

$$PSNR = 10 \times log(\frac{255^2}{MSE}) \quad (8)$$

where $n \times m$ is the image size; x(i,j) is the value of the original image, and y(i,j) is the value of the image at the same position in the corresponding distorted image.

SSIM measures the perceptual difference between two similar images. For a good encrypted image, the value of PSNR must be low. For the decrypted image, the PSNR value must be high. Typical values for the PSNR in the lossy image and video compression are between 30 and 50 dB for valid decrypted images, provided the bit depth is 8 bits, for encrypted image PSNR above 28 dB indicates no perceptual degradation achieved [18].

SSIM is defined as in equation 9:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{9}$$

where x and y are the windows of two images of size $m \times m$; μ_x and μ_y are the average of x and y respectively; σ_x^2 and σ_y^2 are the variance of x and y respectively; σ_{xy} is the covariance of x and y; $C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$, where $k_1 = 0.01$, $k_2 = 0.03$, and L is the gray level of pixel value. For a good encrypted image the value of SSIM must be closed to zero since zero indicates the ratio of similarity between the original and ciphered image is very low. For the valid decrypted image, the value must be closed to 1. According to the above visual quality parameters, the proposed approach with different Lena image sizes is evaluated. Table 3 presents PSNR and SSIM in case that the selected encrypted bins include the sign of all significant coefficients and the first LIP list.

The obtained PSNR and SSIM values of the encrypted and compressed image of the proposed approach confirm a high degradation in all benchmark images. The obtained PSNR values are between (2.46 db and 4 db), which means a high degradation and scrambling. Therefore a large difference between a plain image and its cipher. Moreover, the obtained SSIM values are between (0.016 and 0.142), which indicates the ratio of similarity between the original and ciphered image is very low, confirming the obtained result of PSNR regarding objective assessment. The bitrate of the proposed approach To evaluate the proposed approach, a valid decrypted image is evaluated. Table 3 presents PSNR and SSIM values, which are exactly the same as values of the SPIHT algorithm without encryption and decryption; thus, the proposed encryption algorithm approach confirms that it does not violate the format compliance does not destroy any compression steps. The high SSIM ratio (when it's close to 1) indicates that the proposed approach provides good similarity between the original and the reconstructed image after correct decryption. The values of SSIM are between (0.97 and 0.98). The obtained results prove the robustness of the proposed approach regarding objectives quality metrics compared to previous approaches.

Image degradation measures the perceptual distortion of the encrypted image related to its plain image. For sensitive data, a high visual degradation, it desirable to hide the visual content completely. The PSNR is used to measure visual degradation. Figures 2-7 show the degradation of the plain image for the different sizes of images.

C. HISTOGRAM

A histogram is a quantitative tool that graphically displays a data set. It's a type of graph that represents the frequency of occurrence of continuous data. The histogram of an image shows the frequency of pixel intensity values. The X-axis is the gray level intensity, and it values range from zero(black) to 255 (white); Y-axis is the frequency of these intensities. Figures 8-13 show histograms of original Lena images and its encrypted ones at different sizes: 512×512, 256×256, 128×128, and 32×32. Histogram of Lena plain images are nonuniform and can provide a lot of information about the image. However, the encrypted one is fairly uniform, which means it does not reveal any information about the plain image.

D. EDGE DETECTION

Many image processing applications use edge detection, which includes methods that identified a point in the image when the brightness changes sharply. Edge detection is used to indicate the boundaries of objects, surface marking, or curves. In robust encryption systems, the edges or contours of an object are incomprehensibly presented. The degradation of an image can effectively be evaluated by measuring troubles in the edges. Figures 14-17 show the degradation results of the proposed joint-selective encryption. The two edge dependent evaluations parameters used are Edge Ratio (ER) and Edge Deferential Ratio (EDR). ER is the ratio of several Edge formation Contributing Pixels (ECPs) in the encrypted image to a number of ECPs in the original image. EDR reveals the difference in the location of ECPs in the original image and its encrypted counterpart [18].

The ER value can be calculated using equation 10:

$$ER = \frac{\sum_{i,j=0}^{N-1} E(i,j)}{\sum_{i,j=0}^{N-1} P(i,j)} \tag{10}$$

where E(i,j) is a bit value in the edge detected binary matrix of encrypted image, and P(i,j) is a bit value in the edge detected binary matrix of the original image. The binary matrix contains '0' or '1' regarding edge existence. When the edge exists then the matrix value at that position is 1, otherwise the value is 0. The binary matrix is produced using the thresholding technique as in equation 11 [26].

$$g(i,j) = \begin{cases} 1, & f(i,j) \geq T \\ 0, & f(i,j) < T \end{cases} \tag{11}$$

where $g(i,j)$ is the location of bit, $f(i,j)$ is the value of the bit, and T is the threshold. ER is tested for different image sizes, and results are presented in Table 4. An encrypted image should have a lower number of edges when compared to its original one. The low ER value reflects the ability to hide edges that help to show the original image. The optimal result of ER is about 0.50. It is clear form Table 4 that the obtained values of ER are between 0.54 and 0.59, and these values indicate that the encrypted images have fewer edges

TABLE 3. Encryption used the sign and first LIP list.

	Our approach				SPIHT- Compression-decompression without encryption-decryption	
	Encrypted image		Decrypted image			
Image size	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
512 X 512	2.468	0.14237	39.85	0.9489	39.85	0.9489
256 X 256	4.08	0.07808	36.47	0.943	36.47	0.943
128 X 128	3.274	0.04772	32.23	0.932	32.23	0.932
32 X 32	2.49	0.0162	25.55	0.883	25.55	0.883

FIGURE 2. 512 × 512 the original image.

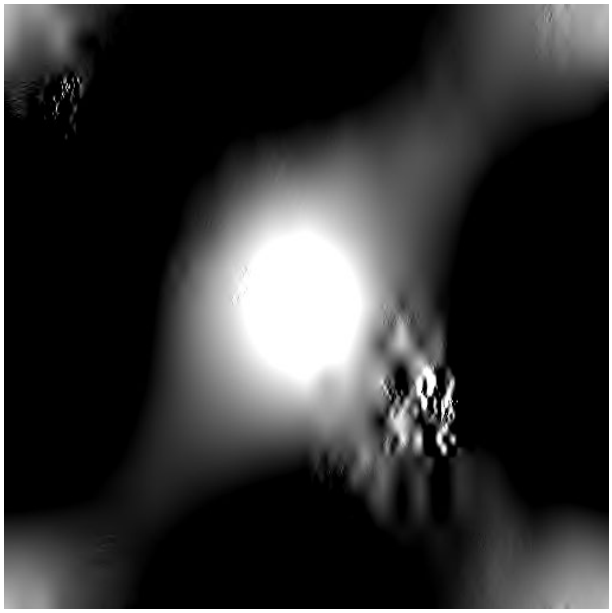

FIGURE 3. 512 × 512 image degradation after encryption.

than originals images, which means a better crypto-system achieved regarding the ER measure.

EDR can be calculated as in equation 12.

$$EDR = \frac{\sum_{i,j=0}^{N-1} |P(i,j) - E(i,j)|}{\sum_{i,j=0}^{N-1} |P(i,j) + E(i,j)|} \tag{12}$$

When the EDR is close to '0', the edges are wholly matched; and no degradation has taken. When the EDR value is bigger than 0.90, then it means a high-security level achieved [18]. Table 5 presents the EDR values for different Lena image sizes, and the average of many experiments readings is calculated. The EDR values are between 0.905 and 0.938, which are close to the required EDR secure values. The obtained results of the EDR confirm that the proposed approach has a high-security level regarding this assessment parameter.

E. KNOWN PLAINTEXT ATTACK

A known-plaintext attack is an attack type of crypt-analysis. The attacker knows some parts of plaintext and its corresponding ciphertext and uses this information to partially or completely crypt-analyze the encrypted data or get any information regarding the used secret key. This is done using mathematical or statistical analysis [27]. In image and video

TABLE 4. ER for different Lena image sizes (plain and cipher).

Image size/ER	512 X 512	256 X 256	128 X 128
	0.4452	0.6359	0.5487
	0.841	0.6725	0.4405
	0.4125	0.9668	0.6042
	0.8275	0.4269	0.4082
	0.4378	0.6807	0.6651
	0.5469	0.6158	0.6085
	0.4601	0.6463	0.5369
	0.6531	0.4185	0.5078
	0.6715	0.9764	0.6107
	0.6927	0.9398	0.5218
Average	0.59883	0.69796	0.54524

encryption algorithms, known-plaintext attacks are evaluated using the error concealment attack, and format compliance test analyzed below.

F. ERROR CONCEALMENT ATTACKS

Error concealment attacks are formed by replacing all encrypted bits with a predefined values (0 or 1), which is a type of known plaint text attack. The Error concealment attack is evaluated using PSNR and SSIM of the replacement image bits. Table 6 presents the average of PSNR and SSIM of the encrypted image after replacing the encrypted bits

FIGURE 4. 256 × 256 original image.

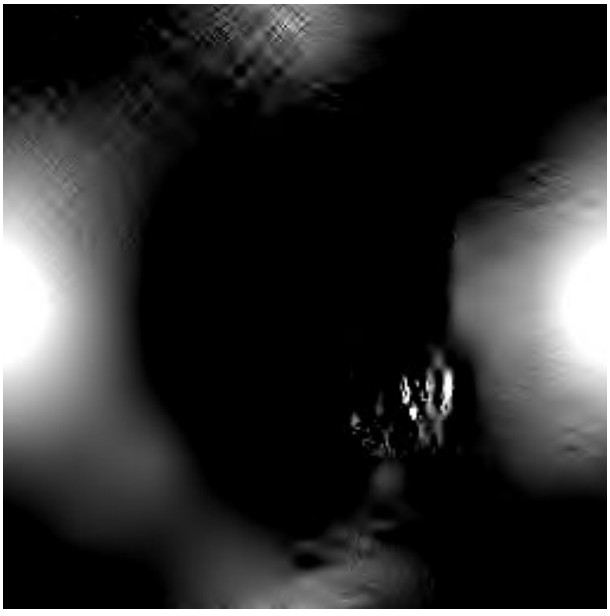

FIGURE 5. 256 × 256 image degradation after encryption.

FIGURE 6. 128 × 128 the original image.

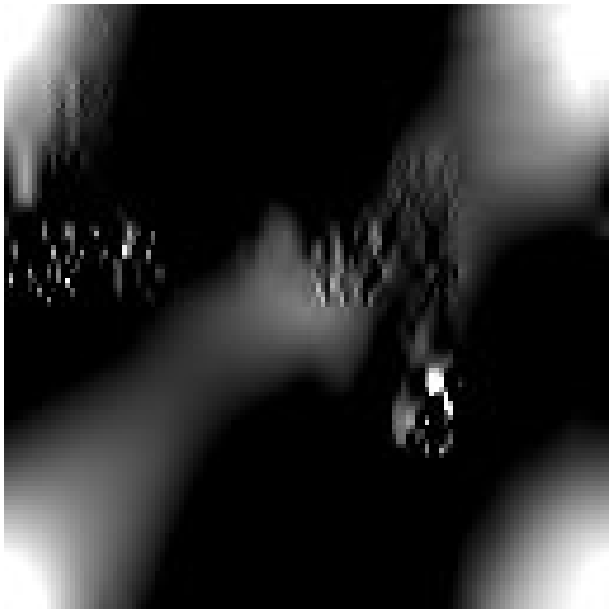

FIGURE 7. 128 × 128 image degradation after encryption.

by zeros. The obtained PSNR and SSIM values remain low and confirm the robustness of the proposed approach against this scenario of attacks.

G. FORMAT COMPLIANCE

The proposed approach encrypts selected bits of the bitstream which are compliant with the compressor. As in Table 3, PSNR and SSIM of the proposed approach after decryption are the same as the PSNR and SSIM of compression without decryption (standard codec). This means that the proposed encryption doesn't change, violate or destroy any compression steps. These results show that the proposed approach is robust against this type of attack and doesn't crash the decoder.

H. MEASUREMENT OF ENCRYPTION QUALITY

EQ is a mathematical measure used to evaluate the degree of encryption quality. The degree of encryption quality can be expressed by the total changes in pixels values(bytes) between the original and encrypted image. The EQ is defined in equation 13 as in [28].

$$EQ = \frac{\sum_{i=0}^{255} |P_i - C_i|}{255} \tag{13}$$

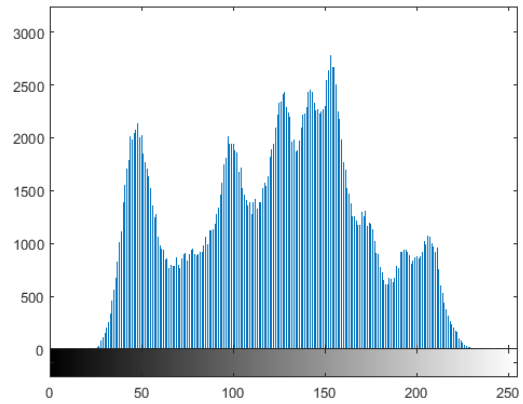

FIGURE 8. Histogram of Lena plain image with size of 512 × 512.

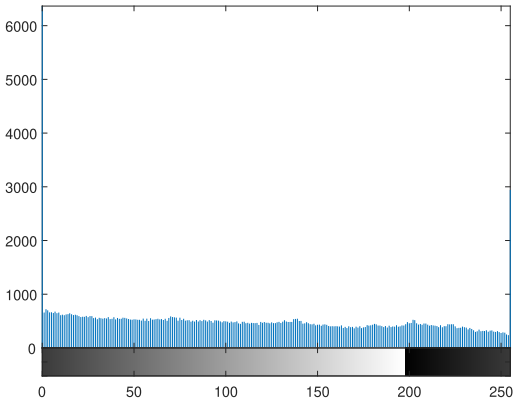

FIGURE 9. Histogram of Lena selective encrypted image with size of 512 × 512.

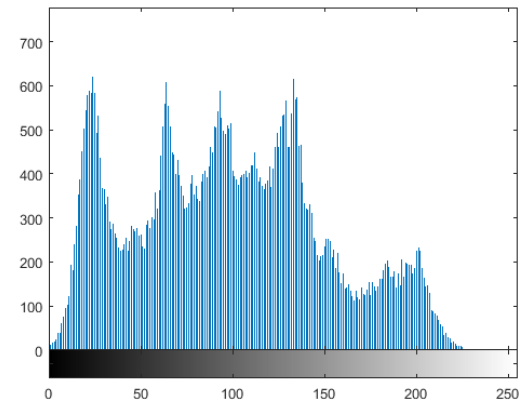

FIGURE 10. Histogram of Lena plain image with size of 256 × 256.

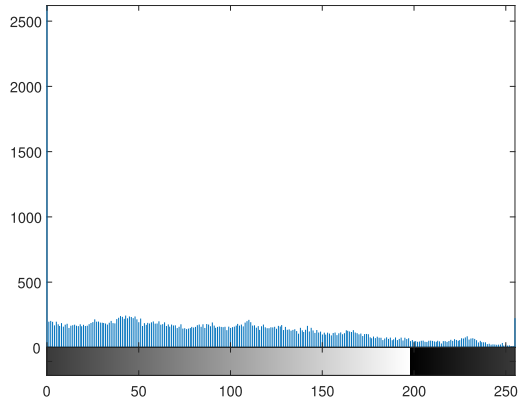

FIGURE 11. Histogram of Lena selective encrypted image with size of 256 × 256.

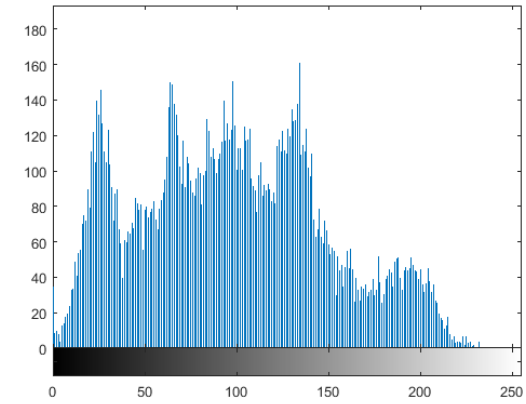

FIGURE 12. Histogram of Lena plain image with size of 128 × 128.

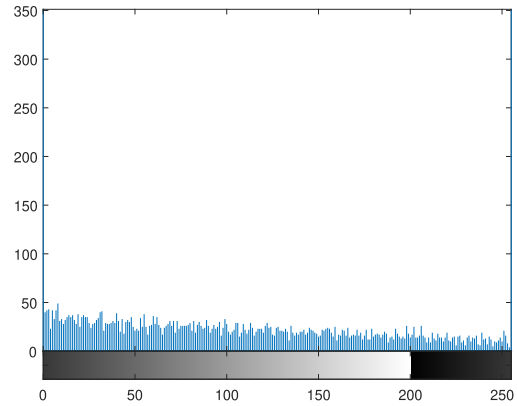

FIGURE 13. Histogram of Lena selective encrypted image with size of 128 × 128.

where P_i is the number of appearance of gray level in the plain image, C_i is the number of appearance of gray level in the encrypted image, and 255 is the total gray levels number. Also, the maximum EQ value is calculated using equation 14 as in [23].

$$EQ_{max} = \frac{510 \times L \times C}{256^2} \tag{14}$$

where L and C is the columns and rows sizes receptively. Using equation 13, an average EQ was calculated of the proposed approach. Using Lena gray image with size 512×512, the obtained value is 1447.

Also, the EQ_{max} was calculated using equation 14, and its value equals to 2040.

$EQ_{max} = \frac{510 \times 512 \times 512}{256^2} = 2040$. The ratio of EQ to EQ_{max} is calculated as:

FIGURE 14. 512 × 512 edge detected of original image.

FIGURE 15. 512 × 512 edge detected of encrypted image.

FIGURE 16. 256 × 256 edge detected of original image.

$ratio = \frac{EQ}{EQ_{max}} = \frac{1447}{2040} = 0.70$ The obtained results are more than 50% which confirm the robustness of the proposed solution.

FIGURE 17. 256 × 256 edge detected of encrypted image.

TABLE 5. EDR for different sizes of Lena image.

Image size/EDR	512 X 512	256 X 256	128 X 128
10*	0.9242	0.9403	0.9085
	0.923	0.946	0.8885
	0.9534	0.9388	0.9305
	0.9319	0.9508	0.8944
	0.9616	0.8949	0.9264
	0.9243	0.9322	0.9234
	0.9373	0.9372	0.8964
	0.919	0.9112	0.9298
	0.9602	0.9257	0.8939
	0.9513	0.9496	0.868
Average	0.93862	0.93267	0.90598

TABLE 6. Average PSNR and SSIM for replacing encrypted bits by zero.

Image size	PSNR	SSIM
512 X 512	2.881	0.0534
256 X 256	5.46	0.0413
128 X 128	5.49	0.0206
32 X 32	3.566	0.01224

I. KEY SPACE ANALYSIS

The keyspace should be large enough to prevent such comprehensive searching that tries to guess the key. In the proposed approach, the used key generator has been proposed in [29]. The key has 299 bits which means that the keyspace size is in the range $(0, 2^{299})$. Thus the proposed approach is robust against brute force attacks.

V. COMPARING OUR APPROACH WITH PREVIOUS APPROACHES

This section presents the comparison between the proposed approach and the previous approaches. Xiang *et al.* in [14] is selected because that proposed method is related and has a close environment regarding the proposed approach. Table 7 presents the PSNR and SSIM comparison between our proposed approach and the previous approach. Gray-level images in the USC-SIPI image database [25] are used in these experiments.

It is clear from Table 7 that in the case of encrypted images, the proposed approach presents better PSNR results than

TABLE 7. Comparing presented approach with previous approach (xiang2014joint).

		Ciphered image				Decrypted image			
		Our approach		xiang2014joint		Our approach		xiang2014joint	
File/image	Size	PSNR	MSSIM	PSNR	MSSIM	PSNR	SSIM	PSNR	SSIM
Lena	15 X 512	3.26	0.132	11.35	0.092	39.85	0.9489	-	-
5.1.09	256 X 256	2.75	0.107	15.09	0.134	34.07	0.853	33.28	0.828
5.1.10	256 X256	1.145	0.086	11.32	0.025	28.89	0.9009	25.71	0.891
7.1.01	512 X 512	3.87	0.118	16.005	0.133	36.66	0.924	35.62	0.905
7.1.02	521 X512	2	0.198	13.94	0.224	43.18	0.962	38.55	0.92

TABLE 8. Testing information loss during compression in our proposed approach.

CR_1	MSE_1	$PSNR_1$	$SSIM_1$	CR_2	MSE_2	$PSNR_2$	$SSIM_2$
0	6.72	39.85	0.9489	0	6.72	39.85	0.9489
4	6.72	39.85	0.9489	4	6.72	39.85	0.9489
16	6.73	39.85	0.9488	16	6.73	39.85	0.9488
64	6.76	39.83	0.9486	64	6.76	39.83	0.9486
256	6.89	39.75	0.9476	256	6.89	39.75	0.9476
1024	7.84	39.19	0.9431	1024	7.84	39.19	0.9431
4096	17.20	35.78	0.9086	4096	17.20	35.78	0.9086

TABLE 9. Comparative study of different models that secure WMSN.

Approch	PSNR_DD	SSIM_DD	EDR_DD	ER_DD	PSNR_EC	SSIM_EC	Overhead	CR	Format compliance	Key size
Our approach	39.85	0.9489	0.9242	0.4452	2.881	0.0534	<1%	16	Yes	299
Hamdi et al. [34]	39.67	NA	NA	NA	NA	NA	1.40%	NA	NA	NA
lahdir et al. [33]	35.51	NA	NA	NA	NA	NA	NA	NA	NA	NA
Taneja et al. [18]	NA	NA	0.93862	0.59881	NA	NA	NA	NA	NA	NA
zhang et al. [31]	NA	NA	NA	NA	9.83	0.18	36%	6.22	NA	NA
Xiang et al. [19]	33.28	0.84	NA	NA	11.035	0.092	3%	NA	Yes	NA
Nasrullah et al. [32]	39.85	NA	NA	NA	9.52	0.147	>100%	8.19	NA	1024

the Xing *et al.* approach. For example, in the Lena image, the proposed approach introduces more image degradation (3.26 dB), where a previous approach produced less image degradation (11.35 dB). The lower PSNR values indicate more degradation. Also, Table 7 presents lower PSNR values than the previous approach, which means more security level is achieved. In the case of decrypted images, the higher value of PSNR gives better image quality which means that the proposed encryption algorithm does not violate or destroy any compression step. For all tested images, the proposed approach introduces higher PSNR values than the previous approach, which means good results for the image quality that is reconstructed after decryption and confirms the format compliance of the proposed approach. For SSIM, in the case of encrypted images, the proposed approach and previous approach have nearly the same results, with some little differences, for example, the proposed approach gives 0.118 SSIM value for the image in file 7.1.01, while the previous approach gives the value of 0.133, and so on. For SSIM, in decrypted images, the higher SSIM values, which are close to '1', are better than lower, which means that SSIM reflects the similarity measures between the original image and the reconstructed one. All SSIM results show that the proposed approach has better results than the previous approach. After the comparison, we can conclude that the proposed approach has a high-security level and better results than Xiang's approach. Also, our proposed approach encryption overhead is less than 1%, so it is suitable for all real-time applications. Moreover, our approach achieving format compliance and constant bit rate. The proposed image compression is achievable without any loss of information. To this aim, we calculate some parameters that confirm this fact as presented in Table 8, which includes CR_1, MSE_1, $PSNR_1$ and $SSIM_1$ for SPIHT algorithm without encryption, while CR_2, MSE_2, $PSNR_2$ and $SSIM_2$ refer to our proposed approach, including compression and encryption. It is clear that $PSNR_1$ and $PSNR_2$ are exactly the same. Moreover, $SSIM_1$ and $SSIM_2$ are the same. Finally, the difference between MSE of the original image and the corresponding reconstructed image is zero, which confirms that our proposed approach has lossless properties. This means that the proposed encryption process is achievable without any loss of information due to the encryption cycle. A comparative study and analysis of different existing models for the WMSNs are presented in Table 9, in which PSNR_DD, SSIM_DD, EDR_DD and ER_DD refer to parameters that evaluate the decrypted and decompressed images, while PSNR_EC and SSIM_EC refer to parameters that evaluate the encrypted and compressed images. Our proposed approach and Nasrullah *et al.* approach [32] avoid information loss during the decompression and decryption process. Moreover, our proposed approach has high degradation (see PSNR_EC and SSIM_EC in Table 9) compared

to the existing models for the ciphered and compressed images. Our proposed approach and Xiang *et al.* [19] approach preserve the format compliance. Finally, the overhead of our proposed approach is minimal compared to other approaches.

VI. CONCLUSION

In this paper, a joint crypto-compression based on a selective encryption algorithm is proposed. Our approach challenge is to secure data communication at wireless multimedia sensor networks (WMSNs). Encrypting the first LIP list and the sign of significant coefficients are presented. The proposed approach achieves good results in terms of security and performance based on the standard metrics PSNR, SSIM, EDR, and ER. Our approach has a low computational time and less power consumption comparing to Xiang *et al.* [14]. Xiang *et al.* used the Advanced Encryption Standard (AES) scheme, requiring more complex computation and energy consumption. The proposed approach satisfies our research objectives: Data confidentiality in WMSNs, sensors hardware limitations (CPU, Memory, and power), bandwidth restriction, and the vulnerability of attacks in wireless communications have been considered. Also, the proposed approach satisfies the format compliance, which increases the reliability of our method and constant bitrate. The speed of our approach is close to the speed of compression without encryption function, which is appropriate for real-time applications.

REFERENCES

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Netw.*, vol. 51, no. 4, pp. 921–960, Mar. 2007.

[2] I. Akyildiz, T. Melodia, and K. Chowdury, "Wireless multimedia sensor networks: A survey," *IEEE Wireless Commun.*, vol. 14, no. 6, pp. 32–39, Dec. 2007.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.

[4] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Comput. Surv.*, vol. 47, no. 1, pp. 1–42, Jul. 2014.

[5] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 6–28, Dec. 2004.

[6] M. Farajallah, S. Assad, and M. Chetto, "Dynamic adjustment of the chaos-based security in real-time energy harvesting sensors," in *Proc. IEEE Int. Conf. Green Comput. Commun.*, Aug. 2013, pp. 282–289.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[8] K. Sayood, *Introduction to Data Compression*. Burlington, MA, USA: Morgan Kaufmann, 2017.

[9] J.-L. Liu, "Efficient selective encryption for JPEG 2000 images using private initial table," *Pattern Recognit.*, vol. 39, no. 8, pp. 1509–1517, 2006.

[10] S. K. Naveenkumar, H. T. Panduranga, and Kiran, "Partial image encryption for smart camera," in *Proc. Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Jul. 2013, pp. 126–132.

[11] D. G. Costa and L. A. Guedes, "A discrete wavelet transform (DWT)-based energy-efficient selective retransmission mechanism for wireless image sensor networks," *J. Sensor Actuator Netw.*, vol. 1, no. 1, pp. 3–35, Feb. 2012.

[12] P. Kitsos, G. Kostopoulos, N. Sklavos, and O. Koufopavlou, "Hardware implementation of the RC4 stream cipher," in *Proc. IEEE 46th Midwest Symp. Circuits Syst.*, vol. 3, Dec. 2003, pp. 1363–1366.

[13] M. Bock, A. K. Tyagi, J.-U. Kreft, and W. Alt, "Generalized Voronoi tessellation as a model of two-dimensional cell tissue dynamics," *Bull. Math. Biol.*, vol. 72, no. 7, pp. 1696–1731, Oct. 2010.

[14] T. Xiang, C. Yu, and F. Chen, "Fast encryption of JPEG 2000 images in wireless multimedia sensor networks," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, 2013, pp. 196–205.

[15] D. De Oliveira Gonçalves and D. G. Costa, "Energy-efficient adaptive encryption for wireless visual sensor networks," in *Proc. Brazilian Symp. Comput. Netw. Distrib. Syst.*, Salvador, Brazil, vol. 30, 2016, pp. 1–14.

[16] A. Mostefaoui, H. Noura, and Z. Fawaz, "Efficient and secure visual data transmission approach for wireless multimedia sensor networks," in *Proc. IEEE 22nd Int. Symp. Model., Anal. Simulation Comput. Telecommun. Syst.*, Sep. 2014, pp. 463–472.

[17] D. Tsitsipis, G. Nikolakopoulos, A. Tzes, and S. Koubias, "A dual scheme for secured multimedia wireless sensor network," in *Proc. 19th Medit. Conf. Control Autom. (MED)*, Jun. 2011, pp. 1160–1165.

[18] N. Taneja, B. Raman, and I. Gupta, "Chaos based partial encryption of SPIHT compressed images," *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 9, no. 2, pp. 317–331, Mar. 2011.

[19] T. Xiang, J. Qu, and D. Xiao, "Joint SPIHT compression and selective encryption," *Appl. Soft Comput.*, vol. 21, pp. 159–170, Aug. 2014.

[20] D. Xiao, M. Li, M. Wang, J. Liang, and R. Liu, "Low-cost and high-efficiency privacy-protection scheme for distributed compressive video sensing in wireless multimedia sensor networks," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102654.

[21] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *J. Netw. Comput. Appl.*, vol. 49, pp. 15–50, Mar. 2015.

[22] H. Z. Eldin, M. A. Elhosseini, and H. A. AliAuthor, "Image compression algorithms in wireless multimedia sensor networks: A survey," *Ain Shams Eng. J.*, vol. 6, no. 2, pp. 481–490, 2015.

[23] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos," Ph.D. dissertation, Dept. Eng. Sci., Univ. Nantes, Nantes, France, 2015.

[24] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, no. 3, pp. 243–250, Jun. 1996.

[25] University of Southern California. *The USC-SIPI Image Database*. Accessed: Jan. 1, 2021. [Online]. Available: http://sipi.usc.edu/database/

[26] M. Kumar Ray, D. Mitra, and S. Saha, "Simplified novel method for edge detection in digital images," in *Proc. Int. Conf. Signal Process., Commun., Comput. Netw. Technol.*, Jul. 2011, pp. 197–202.

[27] M. Farajallah, S. E. Assad, and O. Deforges, "Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28225–28248, Nov. 2018.

[28] H. E. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images," in *Proc. Int. Conf. Electr. Eng.*, Apr. 2007, pp. 1–7.

[29] O. Salahb, N. Jweihan, M. A. Jodeh, M. A. Taha, and M. Farajallah, "Survey paper: Pseudo random number generators and security tests," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 7, pp. 1951–1970, 2018.

[30] I. Hraini, "Joint crypto-compression based on selective encryption for WMSNs," M.S. thesis, College Graduate Stud., Palestine Polytechnic Univ., 2019.

[31] M. Zhang and X. Tong, "Joint image encryption compression scheme based on IWT SPIHT," *Opt. Lasers In Eng.*, vol. 90, pp. 254–274, Oct. 2017.

[32] J. Sang, M. A. Akbar, B. Cai, H. Xiang, and H. Hu, "Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps," *Appl. Sci.*, vol. 8, p. 1963, Oct. 2018.

[33] M. Lahdir, H. Hamiche, S. Kassim, M. Tahanout, K. Kemih, and S.-A. Addouche, "A novel robust compression-encryption of images based on SPIHT coding and fractional-order discrete-time chaotic system," *Opt. Laser Technol.*, vol. 109, pp. 534–546, Oct. 2019.

[34] M. Hamdi, R. Rhouma, and S. Belghith, "A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map," *Signal Process.*, vol. 131, pp. 514–526, Feb. 2017.

IYAD HRAINI received the B.S. degree in computer systems engineering and the M.S. degree in informatics from Palestine Polytechnic University, Palestine. His M.S. thesis was directed in crypto-compression solutions. He is a Researcher at Palestine Polytechnic University. His research interests include networking, cryptography, and information security.

MOUSA FARAJALLAH received the B.Eng. degree in computer systems engineering from Palestine Polytechnic University (PPU), in 2006, with highest rating in PPU systems, the Master of Electronics and Computer Engineering degree (Hons.) from AL-Quds University, Jerusalem, in 2010, with highest rating in AL-Quds University systems, and the joint Ph.D. degree (Hons.) in computer engineering from the University of Nantes and the INSA of Rennes University, France, in 2015, with highest rating in France systems. Previously, he studied cryptography course at Saarland University, Germany, as a Pre-Ph.D. course for cryptography filed, in 2012. His Ph.D. thesis was directed in crypto-compression solutions of high-efficiency video coding (HEVC) and crypto solutions for real-time applications. Currently, he is an Assistant Professor with PPU. He has served more than 12 master's students, 40 graduation projects, and since 2015, he published five ISI papers, five Scopus papers, and three high rank conferences, also he is an active reviewer for high ranking ISI journals. His research interests include cryptography, cryptanalysis, and crypto-compression solutions. He is an active member of many international conferences and workshops.

NABIL ARMAN received the B.S. degree (Hons.) in computer science from Yarmouk University, Jordan, in 1990, the M.S. degree in computer science from American University, Washington, DC, USA, in 1997, and the Ph.D. degree from the Department of Computer Science, School of Information Technology and Engineering, George Mason University, VA, USA, in 2000. He is a Professor of computer science with Palestine Polytechnic University. His research interests include database and knowledge-based systems, algorithms, automated software engineering, and database and multimedia security.

WASSIM HAMIDOUCHE received the master's and Ph.D. degrees in image processing from the University of Poitiers, France, in 2007 and 2010, respectively. From 2011 to 2013, he was the Junior Scientist with the Video Coding Team, Canon Research Center, Rennes, France. He was a Postdoctoral Researcher with the VAADER Team, IETR, from April 2013 to August 2015, where he worked under collaborative project on HEVC video standardization. Since September 2015, he has been an Associate Professor with INSA Rennes and a Member of the VAADER Team, IETR Lab. He has joined the Advanced Media Content Lab of b<>com IRT Research Institute as an Academic Member in September 2017. He is the author/coauthor of more than 140 papers at journals and conferences in image processing, two MPEG standards, three patents, several MPEG contributions, public datasets, and open source software projects. His research interests include video coding and multimedia security.