Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 7147940, 10 pages
https://doi.org/10.1155/2021/7147940

Research Article

A Metaheuristic Approach to Secure Multimedia Big Data for IoT-Based Smart City Applications

Harsimranjit Singh Gill,[1] **Tarandip Singh**,[2] **Baldeep Kaur**,[2] **Gurjot Singh Gaba**,[3] **Mehedi Masud**,[4] **and Mohammed Baz**[5]

[1]*Department of Electronics and Communication Engineering, Guru Nanak Dev Engineering College, India*
[2]*Department of Electronics Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India*
[3]*School of Computer Science, Mohammed VI Polytechnic University, Ben Guerir 43150, Morocco*
[4]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[5]*Department of Computer Engineering, College of Computer and Information Technology, Taif University, P. O. Box 11099, Taif 21994, Saudi Arabia*

Correspondence should be addressed to Mehedi Masud; mmasud@tu.edu.sa

Received 18 May 2021; Revised 16 June 2021; Accepted 15 September 2021; Published 4 October 2021

Academic Editor: Celestine Iwendi

Media streaming falls into the category of Big Data. Regardless of the video duration, an enormous amount of information is encoded in accordance with standardized algorithms of videos. In the transmission of videos, the intended recipient is allowed to receive a copy of the broadcasted video; however, the adversary also has access to it which poses a serious concern to the data confidentiality and availability. In this paper, a cryptographic algorithm, Advanced Encryption Standard, is used to conceal the information from malicious intruders. However, in order to utilize fewer system resources, video information is compressed before its encryption. Various compression algorithms such as Discrete Cosine Transform, Integer Wavelet transforms, and Huffman coding are employed to reduce the enormous size of videos. moving picture expert group is a standard employed in video broadcasting, and it constitutes of different frame types, viz., I, B, and P frames. Later, two frame types carry similar information as of foremost type. Even I frame is to be processed and compressed with the abovementioned schemes to discard any redundant information from it. However, I frame embraces an abundance of new information; thus, encryption of this frame is sufficient enough to safeguard the whole video. The introduction of various compression algorithms can further increase the encryption time of one frame. The performance parameters such as PSNR and compression ratio are examined to further analyze the proposed model's effectiveness. Therefore, the presented approach has superiority over the other schemes when the speed of encryption and processing of data are taken into consideration. After the reversal of the complete system, we have observed no major impact on the quality of the deciphered video. Simulation results ensure that the presented architecture is an efficient method for enciphering the video information.

1. Introduction

A city becomes smart when the physical objects are transformed into cyberphysical objects. The transformation facilitates real-time monitoring, manages resources, optimizes smart city operations, and improves citizens' quality of life. Few applications of a smart city include garbage van route optimization, automatic irrigation, wearable health network, and smart energy meters. Internet of Things (IoT) is the technology behind this revolution; it associates a sensor integrated into a communication unit with a physical object. Consequently, the cyberphysical object can then be accessed from anywhere using internet access. One of the primary applications of smart cities is monitoring the roads and rushy areas through closed-circuit television (CCTV) cameras for preventing crimes. There are plenty of CCTVs installed in

the smart city, resulting in enormous multimedia big data [1]. The big multimedia data generated by IoT nodes in the smart city contains sensitive information preventing tampering and other cyberthreats [2].

Information security is vital in communication and even while storing multimedia information [3]. The one way to protect the information is by blocking unauthorized access, but such a method is not very secure and reliable [4]. Another method is to encrypt the information in the gibberish form, so an end-user cannot decode it until the encryption method is known. Image and video encryption have various applications like multimedia messaging, military purposes, and internet communication like video calling, video conferencing, and satellite TV broadcasting [5, 6]. There are various encryption methods; AES is one of the most secure methods on which no possible attack is confirmed to date. In traditional approaches, there are two techniques of encryption, first is encrypting the whole data, and in another technique, entire data is compressed first by compression method, and then, it is encrypted, but these techniques take a lot of time and decrease the processing speed [7].

Currently, numerous compression and encryption techniques are proposed. However, these days' encryption techniques attract attention to joint compression and partial encryption techniques for secure video transmission. There are various methods for image and video encryption; for example, Alattar encrypts intracoded macroblocks of all frames of the MPEG video, which reduces the processing time and increases speed over full encryption of video. Another method called encrypting the header information of predicted macroblock and encrypting the whole data in all I-macroblocks is presented [8]. The method of encryption presented here constitutes three sections, i.e., the motion vector difference, intraprediction modes, and the signed bits of the texture data. Only the selected domain is secured according to the scalability types [9]. For encryption of video, the author proposed a different technique based on one-dimensional chaotic map in the DCT domain that uses multiple operations such as scrambling and encryption of I frame and three chaotic maps. In the whole process, five keys have been incorporated, which were not easy to find, and the I frame changes can make it complex [10, 11].

A novel encryption scheme that exploits partial information as an input used a secure encryption algorithm to encipher a part of compressed information through an orthogonal search algorithm. DCT and some other coding like quantization and arithmetic have been used for image compression, and then, the resultant information is encrypted by RSA algorithm [12, 13]. In the encryption techniques for the secure transmission of MPEG video bitstreams, another method was used, which comprised various encrypted I frames and header information of every predicted frame [14]. The encryption method has been presented where only the AC and DC coefficients of the I frame were encrypted. Both coefficients of I frame, AC coefficients of the P frame, and motion vector difference were encrypted [15]. Another approach based on the hash encryption model was demonstrated in [16]. In this approach, intraprediction, the difference of motion vector, and coefficients of quantization were encrypted. A novel key generation process was constructed using a hash function. In [17], Cheng and Li proposed a partial encryption method in which only a part of compressed data was encrypted. The presented scheme of partial encryption technique was later applied in numerous image and video compression algorithms. The encryption and integrated multimedia compression technique were illustrated in [18] based on modified entropy coders with multiple statistical models and selective encryption models.

Firstly, the limitations of selective encryption using cryptanalysis were explored and then processed the information through the selective encryption model. A similar approach based on multiple statistical models has been presented in which entropy coders were used to designing an encryption cipher. Using this technique, multiple encryption schemes were designed which incorporate the Huffman coder and the QM coder [19]. An unlike approach on text file was compressed and encrypted using chaotically mutated Huffman trees. Many Huffman tables were used to encode that text message. With the use of large keyspace, this technique provides robust security to the Brute-force attack. Another scheme employed lossless compression and contourlet transform before the encryption of image's most significant part. This method promised an increase in cipher image security [20, 21].

In [22], Setyaningsih and Wardoyo proposed a dissimilar technique comprised of compression and encryption technique, in which shared encryption occurs between the low- and high-frequency components. These coefficients and initial keys and total pixel values were used as an input to the hash function. The hash function value was used for encryption of the high-frequency components. For the joint compression and encryption of medical images, another author proposed a technique where the image was compressed by Discrete Wavelet Transform (DWT) and then encrypted by Advanced Encryption Algorithm. This scheme was designed to increase protection along with security [23]. A similar technique of joint image compression and encryption using the properties of integer wavelet transform (IWT) and SPHIT was presented where multiple methods were exploited such as hyperchaotic system, secure hash algorithm, nonlinear inverse operation, and plain text-based keystream to improve the security [24].

To enhance the compression ratio, Song et al. [25] presented a system that employs the intrinsic features of input images along with entropy encoding for the encryption process. SHA-256 has also been used to build a secure, chaotic cryptosystem that is resistant to certain common attacks. Another approach based on 3D chaotic maps was presented to decorate the adjacent pixels of an image after successfully implementing the arithmetic compression algorithm. This technique was developed for transfer images over a network for real-time application [26]. To encrypt [27, 28] the large data files and reduce execution time, the authors proposed the most secure and effective grid-based encryption technique. Here, the image is divided into grids and encrypted by AES algorithm [29]. A unique model has been shown

for the encryption of surveillance videos [30]. Numerous methods for image compression such as DWT, DCT, and Huffman encoding compression algorithm were presented. The medical image was compressed by using these methods [31]. Another technique of compression, IWT, was presented. The lifting process was used, which compressed the image by dividing the odd and even coefficients and then generating four subband images [32]. To achieve compression and scramble the pixels data of an image based on set partitioning in hierarchical trees (SPIHT) was suggested by Xiang et al. in [33]. The presented scheme can provide better resistance for different attacks compared to the original SPIHT technique.

For real-time applications [34–36], a new encryption method was proposed. It constitutes three sections: motion vector difference, intraprediction mode, and residual data. The encryption was executed by Network Abstraction Layer and distinguished the enhancement layer spatial scalability and temporal scalability [37]. In the field of compression and encryption, a new method of encryption with the scan pattern was proposed. This technique was based on scan methodology, which creates many scanning paths and space-filling curves. Firstly, lossy compression was applied on the difference of adjacent frames, and then, encryption was performed on compressed frame differences [38]. Another approach illustrates the usage of wavelength division multiplexed systems for end-to-end distribution of compressed video [39]. Moreover, speech signals can be transported between multiple entities of a network, keeping end-to-end encryption into consideration, using chaotic and cryptographic algorithms. The various chaotic maps have been employed to scramble the speech information, and semantic encryption techniques were used to encipher the information [40].

Based on the literature review, it is found that a number of encryption techniques have been applied to the video information, but no scheme has explored the possibility of joint compression technique and encryption technique. Therefore, this work focuses on combining both schemes, and we have tested it on a multimedia file. The proposed model is employed to broadcast video between two ends. Various techniques are explored to provide compression, such as IWT, DCT, Huffman coding, and encryption involved in AES algorithm. For video compression, the information of three frames, which includes I, B, and P frames, has been used. Among three frames, I frame contains the most information of the video. On the other side, P and B frames contain only a small portion of image information. The proposed model includes the following steps: the information of the I frame is extracted first from a MPEG video. In the second step, an IWT is applied to extracted I frame. After that, an image is divided into different subbands such as LL, HL, LH, and HH, respectively. The LL subband is the closest guesstimate of an original image. In the third step, DCT is applied to the LL band, and the resultant image is divided into one DC and various AC coefficients. During encryption, the DC coefficient is partially encrypted using the AES-128 bit, and the rest of AC coefficients are compressed by Huffman coding. AES and Huffman coding output is concatenated in the last step, and a cipher image is obtained.

The rest of the paper is organized as follows. A review of IWT, DCT, Huffman encoding, and AES is given in Section 2. In Section 3, the proposed approach is presented. Simulation results and discussion are presented in Section 4. Finally, we summarize the paper and present a conclusion in Section 5.

2. Preliminaries

2.1. Integer Wavelet Transform (IWT). When the image is decomposed, it is divided into different groups. The approximated content of an image is further divided into four subbands. The IWT provides a better result of compression prior to which approximate contents of the image are decomposed. It is a form of DWT and has many advantages of DWT, but it also has some functions that DWT cannot perform. It uses round-off values rather than floating-point values. Forward and reverse scheme is shown in Figures 1 and 2. Forward and reverse lifting scheme (LS) is used to perform simple shifting and adding operations. LS is used to divide the odd and even coefficients. This scheme is performed by three steps, i.e., split, predict, and update.

(i) Split: input image or signal is divided into even and odd coefficients

(ii) Predict: combining even values from predicted odd samples and then subtracting it from calculated odd samples to generate prediction error

(iii) Update: add the computed predicted error to update the entire even samples

Forward LS is used to compress the image and reverse LS for the reconstruction of the signal. Every transform by this scheme can be inverted [24, 32].

2.2. Discrete Cosine Transform (DCT). DCT is usually employed in almost all types of multimedia compression schemes. Likewise, in Discrete Fourier Transform, DCT converts a sequence of data or information from spatial-domain to frequency-domain. As DFT is based on complex numbers, DCT uses real numbers. The sequence generated by DCT is the addition of cosine functions that waver at various frequencies decorrelates the image information into different frequency bands. When calculating DCT of an image, the values that are in the high-frequency bands are near to zero, and then, compression occurs after quantization. Initially, the RGB image is translated into the $Y_{Cb}C_r$ color space. After that, each color space is converted into a number of 8×8 blocks which are again converted into DCT domain by using the 2D-DCT formula.

2.3. Huffman Coding. Huffman coding is a type of lossless data compression algorithm. It is the form of statistical coding which is used to reduce the input information bits and gives the strings of symbols. It assigns the dynamic length codes to the input characters. The length of that allocated codes depends on the occurrence of input characters. The

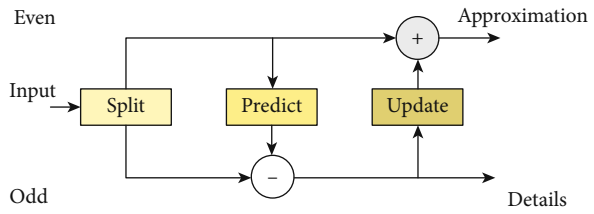


Figure 1: Forward lifting scheme.

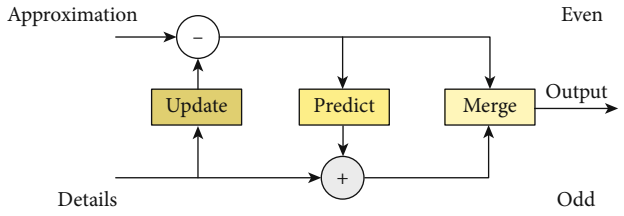


Figure 2: Reverse lifting scheme.

most recurring character is translated to a shorter code, and the character having the opposite frequency gets the longest code. The length of the codeword is not variable. It can reconstruct the original image or data [31].

2.4. Advanced Encryption Standard. AES is an encryption algorithm that is used to encrypt an image over the network. The AES was announced by the National Institute of Standards and Technology in the year 2001. AES falls under the category of an asymmetrical block cipher and was designed and implemented in both software and hardware. The block length varies from 128 bits to 512 bits and has a similar range of key length. Depending upon the size of the block length and key length is to be fixed with a similar size; thus, the number of rounds is selected, which range from 10 to 14 rounds, i.e., 16-byte key to 32-byte key. Each round is designed to perform four similar steps: permutation, arithmetic operations, byte substitution over a finite field, and XOR operation with a key. For the calculation of arithmetic operations, the modular reduction method can be used in Galois fields of mathematics. In AES, representation of each element is done as

$$A(x) = a_7x^7 + \cdots + a_1x + a_0, \tag{1}$$

where $a_i \in GF(2) = \{0, 1\}$. In addition to representation, each polynomial of AES is represented using the following notation of vector

$$A = [a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0]. \tag{2}$$

Modulo reduction plays a vital role in arithmetic operations, and the default irreducible polynomial is given as

$$P(x) = x^8 + x^4 + x^3 + x + 1. \tag{3}$$

This algorithm is applied to the DC coefficients of an image extracted by the compression algorithm and then transferred over the public network in the presented work. The original image can be reconstructed at the receiver side by applying a decryption algorithm on the cipher image. The length of all keys of the AES algorithm is sufficient to protect classified information up to the secret level. Thus, this algorithm gives better security and data confidentiality [14–18]. AES requires small space and low memory for the implementation of both encryption and decryption. An unlike modification in AES algorithm through primitive operations has been shown to mitigate low diffusion rate at the initial stage [41–43].

3. Proposed Approach

This section has provided a detailed description of enciphering and deciphering of I frames extracted from MPEG video.

3.1. Compression and Encryption Approach. The architecture of joint image compression and encryption is illustrated in Figure 3. There are various steps to perform joint image compression and encryption.

Step 1. Firstly, an I frame is selected from a MPEG video which contains more image information. I frame is an intra-coded completely specified picture and has a large amount of image information selected for compression.

Step 2. In the second step, the single-level decomposition of IWT is performed on I frame. IWT is based on the subband coding and lifting scheme. After transformation, four subbands LL, HL, LH, and HH are extracted. The LL subband is the closest estimation of the original image, HL subband signifies the detail about verticals, LH subband denotes the detail about the horizontal edge, and HH subband represents the detail about diagonal. Therefore, the LL subband is compressed because it has greater image information.

Step 3. In the third step, DCT is performed on LL subband according to the mathematical formula given as:

$$V_{pq} = \delta_p\delta_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} U_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, 1 \le p \le M-1, /1 \le q \le N-1, \tag{4}$$

where V_{pq} is known as DCT coefficients of U. The variables δ_p and δ_q are calculated as

$$\delta_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0, \\ \sqrt{2/M}, & 1 \le p \le M-1, \end{cases} \qquad \delta_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0, \\ \sqrt{2/N}, & 1 \le q \le N-1. \end{cases} \tag{5}$$

DCT is primarily used in the various types of multimedia compression schemes. It gives a finite sequence of data in

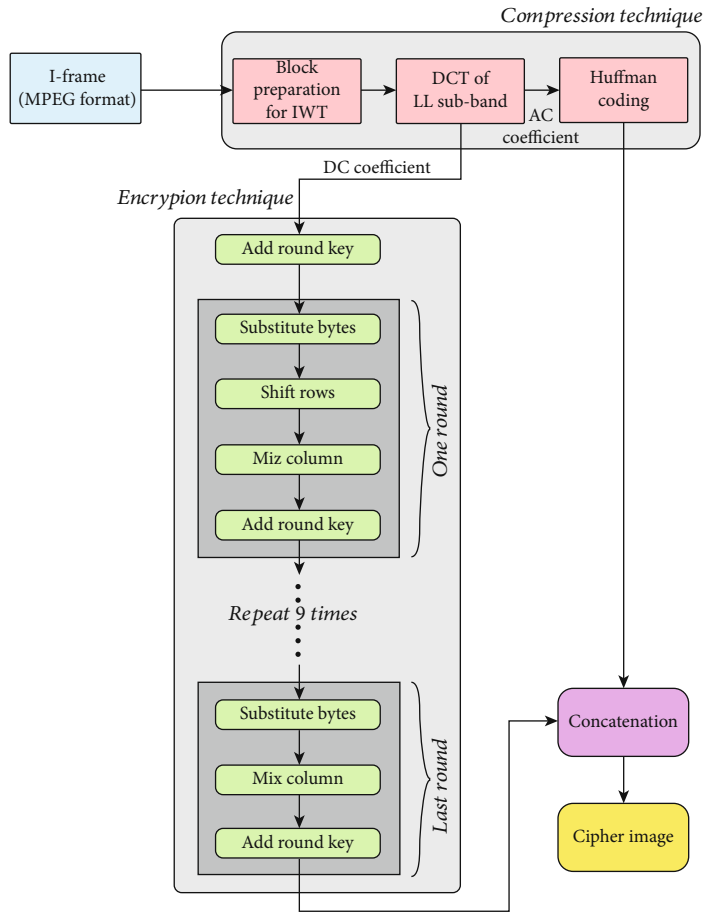


Figure 3: The basic building block of joint image compression and encryption.

terms of a cosine function. It alters an input image to the frequency domain from the spatial domain. When DCT is applied to the LL band, an image is obtained with one DC constant, and others are AC values. The DC coefficient is a low-frequency component with a huge value, and AC constants are high-frequency components close to zero.

Step 4. In this step, partial encryption is performed. The DC coefficient, which occurs after DCT compression, is partially encrypted by using the AES-128 bit. It performs 10 rounds on input data for the purpose of more confusion and diffusion. More rounds mean more security against the cryptanalysis attack. The detailed algorithm used for enciphering DC coefficient is presented in Algorithm 1.

Step 5. There are numerous tools used for compression purposes like Huffman coding, run-length encoding, entropy encoding, and arithmetic encoding. In this scheme, Huffman encoding is used, which is lossless data compression algorithm. The rest of AC coefficients obtained from DCT is further compressed by using Huffman encoding. It reduces the information bits to fewer bits, and the compressed image is obtained.

Step 6. In the final step, concatenation involves the output of the AES-128 bit and Huffman encoder. As a result, the cipher image is obtained, which is totally different from the original image. Moreover, if someone can access the AC coefficients of data, even then, the adversary may not be able to decrypt the image, owing to the robustness of the encryption model.

To address the issue of processing the data, we have incorporated the compression algorithms before preparing and presenting the data for encryption. In this way, the proposed architecture can be used to save a lot of system resources while still concealing the information and getting a plausible result from the presented system. In comparison to approaches discussed in [10, 15], the presented model shown in Figure 3 has superiority in terms of the time taken to process one frame of data. Since the data has already been compressed tremendously before the application of encryption, thereby, this approach is considered higher performance in terms of speed.

3.2. Extraction and Decryption Approach. To retrieve I frame from the cipher text or encrypted image, all the blocks presented in Figure 3 can be reversed. Primarily, the received data is segregated into two blocks, the former block is given to the Huffman decoder, and the latter block is fed for AES decryption. The Huffman decoder is used to retrieve actual AC coefficients for I-DCT; however, AES decryption is employed to recover the values of DC coefficients of

Data: An input of DC coefficient calculated after application of forward DCT
Result: Ciphertext
1 for *key_expansion*
2 $W = [W_0 W_1 \cdots W_s]$where $W \in K_{AB}$ and $W_s = W_3/W_5/W_7$
3 *initialize* k_r
4 for $i = s + 1$ to 43
5 $temp = sbox(W_{i-1} \lll 8, 8)$
6 $g = temp \bigoplus rcon(k_r + 1)$
7 $W_i = W_{i-s-1} \bigoplus g$
8 $W_{i+1} = W_{i-s} \bigoplus W_i$
9 $W_{i+2} = W_{i-s+1} \bigoplus W_{i+1}$
10 $i = i + s + 1$
11 *increment* k_r
12 *update* W and ***go*** to *line* 3
13 ***while*** *encryption*
14 ***prepare*** *DCT data* in *blocks* of 128 *bits* in 4 *X* 4 *matrix*
15 $intialphase = block_{1\_input} \bigoplus block_{first\_subkey}$
16 for *round* 9/*downto* 1
17 $bytesubs = sbox(intialphase)$
18 for *shiftrow*
19 *circular* − *shift row* 1/2/3/4 *right with* 0/3/2/1 *bytes*
20 for *mixcolumn*
21 for *each_row* and *each_column*
22 $mcol = constants * shiftrow$**where***constants* is *a* 4 *X* 4 *matrix*
23 $addrk = mcol \bigoplus block_{round\_subkey}$
24 for *lastround*
25 *repeat line* 17 to 19
26 out = *line* 25 ⊕ $block_{last\_subkey}$
27 *Ciphertext* = out
28 ***go*** to *line* 14

Algorithm 1: Algorithm used for enciphering the data.

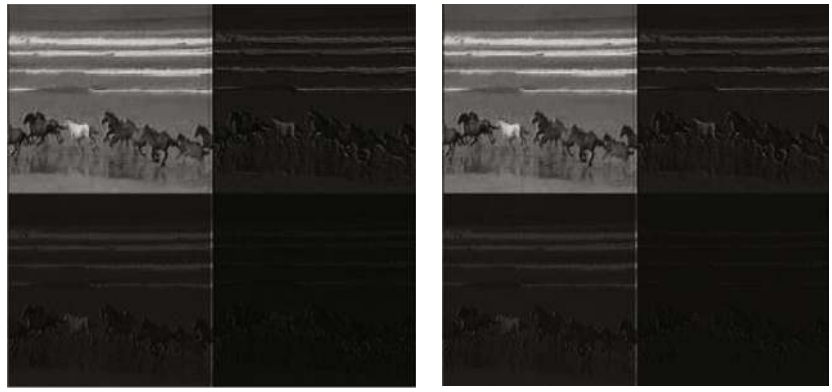
different macroblocks of the image. AES decryption process is an exact replica of AES encryption model, but only a reversal of the key schedule. This means DC coefficients are evaluated through the similar and symmetric key used for enciphering purposes. The evaluated coefficients are then processed through the inverse DCT stage and then given to inverse IWT block to construct the I frame of the transmitted video. To conclude, it is assessed that the extraction process of the I frame includes similar but reversal blocks and functions employed at the sender side.

4. Results and Discussions

The simulation of the proposed technique is performed on MATLAB with an Intel-core-5 i5 processor and 1 TB memory. The video is played in MATLAB video reader from where I, B, and P frames are extracted from MPEG video. Among these frames, a random I frame is selected from a video (as shown in Figure 4).

After selecting I frame, IWT is applied to transform the image, which divides the image into four subbands shown in Figure 5. Forward and reverse lifting scheme is also applied in which simple shifting and adding operations are performed. The data can be recovered by reverse lifting scheme without any loss. LS is used to divide the odd and even coefficients. Three stages perform the presented scheme: split, predict, and update. The split function divides the input image or signal into even and odd coefficients. Predict function forecasts the odd sample as a linear mixture of

Figure 4: Original I frame extracted from a MPEG video.



(a) (b)

Figure 5: Image after subband coding. (a) Operation is performed on 200×200. (b) Operation is performed on 256×256.

(a) (b)

Figure 6: DCT on LL subband. (a) Operation is performed on 200×200. (b) Operation is performed on 256×256.

even portions. Formerly, it is subtracted from the odd portion to generate a prediction error. Update function updates the even portion by totaling them to the previously generated value, i.e., prediction error. The same operation is performed on 200×200 (represented in Figure 5(a)) and 256×256 images (shown in Figure 5(b)).

The first band after decomposition is the LL band. LL band is the approximation of the original image, which contains more information. So, it is selected for compression purposes. After IWT, DCT is applied on the LL subband to compress the image. The image obtained after DCT is shown in Figure 6. When DCT is performed on an image, it divides into DC and AC coefficients. The DC coefficients are low-frequency components and have the highest value, and the AC coefficients in the high-frequency bands have a value close to zero, and then, compression occurs after quantization.

The sequence generated by DCT is the summation of cosine functions that oscillate at various frequencies or we can say that it decorrelates the image information into multiple frequency bands. Firstly, the color image of RGB pattern is converted into the YC_b C_r color space. After that, individual color space is separated into several 8×8 blocks, which are again converted into DCT domain by using the 2D-DCT formula in Equation (4). The white portion of the image is DC coefficient, and the other black portion of the image is AC coefficient. The operation is performed on 200×200 is shown in Figure 6(a) and on 256×256 pixel image is shown in Figure 6(b). After DCT, DC coefficients have the highest value selected for encryption purposes. To encrypt the DC coefficient through network's highest secure symmetric encryption algorithm, Advanced Encryption Algorithm is used. In the presented scheme, 128-bit AES algorithm is used. Here, the algorithm constitutes the following parameters: size of the key is 128 bits, block size of plain text is 128 bits, and ciphertext block size is similar to the size of plain text.

Some tests have been carried out to evaluate the effectiveness of the proposed system. The I frame extracted in Figure 4 is presented for the computation of the Average Peak Signal to Noise Ratio (PSNR) and compression ratio. Both of these parameters are observed to measure the quality of compressed, encrypted, and transmitted frames. The higher value of PSNR depicts higher fidelity or better reconstruction of the transmitted image. PSNR values in the range of 25-30 dB represent the decent quality of the reconstructed image; however, higher values indicate better visual quality. To calculate PSNR of an individual frame, the mean square error is observed beforehand, and then, the logarithmic value of PSNR is measured. The mathematical expressions

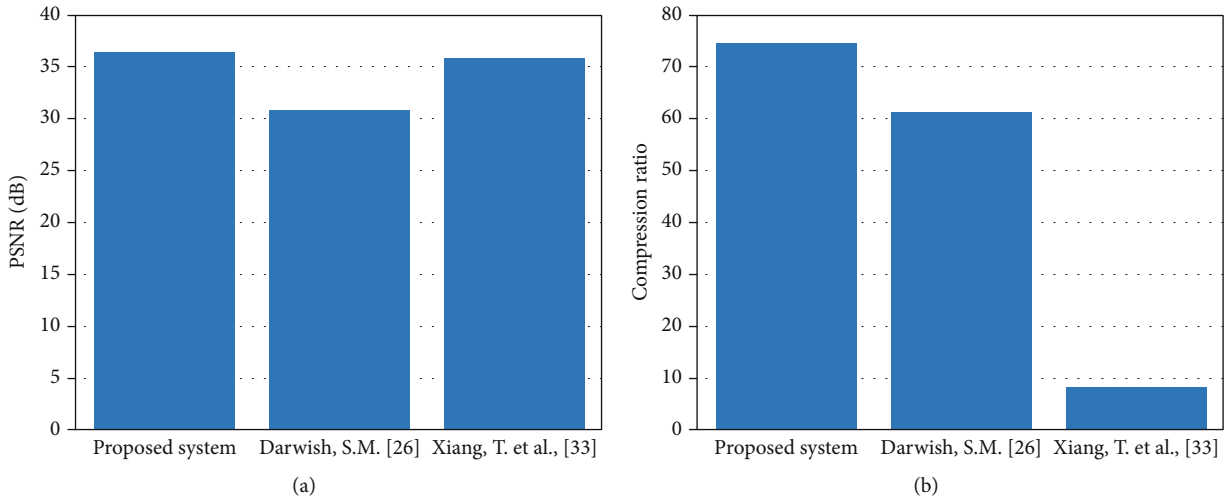


Figure 7: Performance analysis. (a) Calculated PSNR for 256×256 image. (b) Computed compression ratio for different techniques.

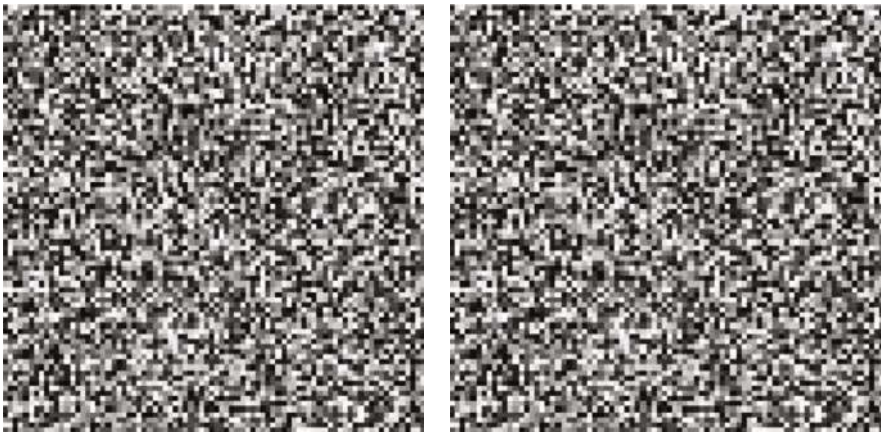


Figure 8: Cipher image. (a) Operation performed on 200×200. (b) Operation is performed on 256×256.

to evaluate PSNR and compression ratio are expressed as

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{\text{MSE}}\right),$$
$$\text{Compression ratio} = \frac{\text{Size of original I} - \text{frame}}{\text{Size of encoded frame}}. \quad (6)$$

Both of the mentioned parameters are shown in Figures 7(a) and 7(b). The proposed technique is compared with models presented by Darwish [26] and Xiang et al. [33]. It is clear from Figure 7(a) that PSNR value of each of the models is higher than 30 dB, which means the perceived frames at the receiver end are of high quality. Moreover, the calculated percentage of the compression ratio of individual I frame is close to 75% in comparison to 65% and 8% of techniques presented in [8, 26], respectively. After the analysis of compression ratio, it is examined that each pixel of I frame is represented by 0.107 bit as compared to 0.123 bit and 1 bit, respectively. Thus, the observations made demonstrate the effectiveness and efficiency of the proposed system.

Excluding the last round in every case, all other rounds are identical. Every round of operation includes one substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. DC coefficients after DCT are encrypted. The rest of the AC coefficients are further compressed by Huffman encoding. It is a type of lossless data compression algorithm. It assigns the variable-length codes to the input characters that are AC coefficients. The most frequent character gets the smallest code, and the character which is least frequent gets the largest code. When Huffman coding is applied to the AC coefficients, it reduces the bits into fewer bits and gives output. After Huffman encoding, concatenation combines the output of Huffman encoder and AES, which results in cipher image shown in Figure 8. The same operation is performed on 200×200 shown in Figure 8(a) and on 256×256 pixel image shown in Figure 8(b). It is a scrambled form of the original image; it can only be decrypt by a person who has a secret key called a decryption key.

5. Conclusions and Future Directions

A joint image compression and encryption scheme for video broadcasting is proposed. The proposed technique includes two key operations: extracting I frame and encrypting that frame. I frame is selected from a MPEG video for the purpose of compression. IWT is performed on I frame, and images are divided into four subbands, then DCT is applied on LL band. After that, compression image is divided into DC and AC coefficients. After that, partial encryption is performed on the DC coefficient. AC coefficients are compressed further with Huffman coding. Finally, the compressed AC coefficients and encrypted data concatenate to form a cipher image. The simulation results and evaluated PSNR and compression ratio values show that the presented technique is efficient and gives proper security. The encryption process does not modify the compressed data and does not change the quality of the video. The results show that the frame encryption method is secure, and the proposed scheme fits the multimedia system and Internet communication or secret communication. The prospect of this research work includes the incorporation of Artificial Intelligence and Machine Learning to secure big multimedia data from cyberabuses.

Data Availability

The data that support the findings of this study are available upon request.

Conflicts of Interest

The authors declare that they have no competing interests.

Acknowledgments

The authors would like to thank the Taif University Researchers Supporting Project number (TURSP-2020/239), Taif University, Taif, Saudi Arabia, for the support.

References

[1] C. Iwendi, S. Ponnan, R. Munirathinam, K. Srinivasan, and C.-Y. Chang, "An efficient and unique TF/IDF algorithmic model-based data analysis for handling applications with big data streaming," *Electronics*, vol. 8, no. 11, p. 1331, 2019.

[2] M. Mohit, L. K. Saraswat, C. Iwendi, and J. H. Anajemba, "A neuro-fuzzy approach for intrusion detection in energy efficient sensor routing," in *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–5, Ghaziabad, India, 2019.

[3] A. Rehman, S. U. Rehman, M. Khan, M. Alazab, and G. Thippa Reddy, "CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1456–1466, 2021.

[4] N. Deepa, Q.-V. Pham, D. C. Nguyen et al., "A survey on blockchain for big data: approaches, opportunities, and future directions," 2020, https://arxiv.org/abs/2009.00858.

[5] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, "The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems," *Sensors*, vol. 20, no. 9, p. 2559, 2020.

[6] G. T. Reddy, M. P. K. Reddy, K. Lakshmanna et al., "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, pp. 54776–54788, 2020.

[7] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, *A Metaheuristic Optimization Approach for Energy Efficiency in the IoT Networks*, Software: Practice and Experience, 2020.

[8] A. M. Alattar and G. I. Al-Regib, "Evaluation of selective encryption techniques for secure transmission of MPEG compressed bit streams," in *1999 IEEE International Symposium on Circuits and Systems (ISCAS)*, Orlando, FL, USA, 1999.

[9] S. W. Park and S. U. Shin, "Efficient selective encryption scheme for the H.264/scalable video coding (SVC)," in *International Conference on Networked Computing and Advanced Information Management*, Gyeongju, South Korea, 2008.

[10] S. Yang and S. Sun, *A Video Encryption Method Based on Chaotic Maps in DCT Domain*, Progress in Natural Science, China, 2008.

[11] S. A. Aliesawi, D. S. Alani, and A. M. Awad, "Secure image transmission over wireless network," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 2758–2764, 2018.

[12] A. A. Alhijaj and M. K. Hussein, "Stereo images encryption by OSA & RSA algorithms," *Journal of Physics: Conference Series*, vol. 1279, article 012045, 2019.

[13] S. SerElkhetm and S. Heshmat, "A survey study on joint image compression - encryption methods," in *International Conference on Innovative Trends in Communication and Computer Engineering*, Aswan, Egypt, 2020.

[14] A. M. Alattar and G. I. Al-Regib, "Improved selective encryption techniques for secure transmission of MPEG video bit streams," in *IEEE International Conference on Image Processing*, Kobe, Japan, 1999.

[15] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, 2003.

[16] X. Wang, N. Zheng, and L. Tian, "Hash key-based video encryption scheme for H.264/AVC," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 427–437, 2010.

[17] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[18] Chung-Ping Wu and C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828–839, 2005.

[19] H. Hermassi, R. Rhouma, and S. Belghith, "Joint compression and encryption using chaotically mutated Huffman trees," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 10, pp. 2987–2999, 2010.

[20] S. Qiu, Y. Cui, and X. Meng, "A Data Encryption and Fast Transmission Algorithm Based on Surveillance Video," *Wireless Communications and Mobile Computing*, vol. 2020, no. - Article ID 8842412, p. 12, 2020.

[21] A. T. Hashim and B. D. Jalil, "Color image encryption based on chaotic shit keying with lossless compression," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, p. 5736, 2020.

[22] E. Setyaningsih and R. Wardoyo, "Review of image compression and encryption techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 2, 2017.

[23] S. Ajili, M. A. Hajjaji, and A. Mtibaa, "Hybrid SVD-DWT watermarking technique using AES algorithm for medical image safe transfer," in *International Conference on Sciences and Techniques of Automatic Control and Computer Engineering*, Monastir, Tunisia, 2015.

[24] M. Zhang and X. Tong, "Joint image encryption and compression scheme based on IWT and SPIHT," *Optics and Lasers in Engineering*, vol. 90, pp. 254–274, 2017.

[25] Y. Song, Z. Zhu, W. Zhang, L. Guo, X. Yang, and H. Yu, "Joint image compression–encryption scheme using entropy coding and compressive sensing," *NNonlinear Dynamics*, vol. 95, no. 3, pp. 2235–2261, 2019.

[26] S. M. Darwish, "A modified image selective encryption-compression technique based on 3D chaotic maps and arithmetic coding," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 19229–19252, 2019.

[27] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, 2021, https://ieeexplore.ieee.org/document/9430932.

[28] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim, M. Liyanage, and P. Kumar, "Robust and lightweight key exchange (LKE) protocol for industry 4.0," *IEEE Access*, vol. 8, pp. 132808–132824, 2020.

[29] N. B. Rad and H. Shah-Hosseini, "Grid-based cryptography with AES algorithm," in *International Conference on Computer and Electrical Engineering*, Phuket, Thailand, 2008.

[30] X. Cao, M. Ma, X. Guo, L. Du, and D. Lin, "A new encryption scheme for surveillance videos," *Frontiers of Computer Science*, vol. 9, no. 5, pp. 765–777, 2015.

[31] T. Kumar and R. Kumar, "Medical image compression using hybrid techniques of DWT, DCT and Huffman coding," *International Journal of Innovative research in Electrical, Electronics, Instrumentation and Control Engineering*, vol. 3, no. 3, pp. 54–60, 2015.

[32] T. Mukherjee, B. Y. V. N. R. Swamy, and M. V. L. Bhavani, "Robust image compression using integer wavelet transform exploiting lifting scheme," *International Journal of Engineering Trends and Technology*, vol. 7, no. 5, pp. 217–220, 2014.

[33] T. Xiang, J. Qu, and D. Xiao, "Joint SPIHT compression and selective encryption," *Applied Soft Computing*, vol. 21, pp. 159–170, 2014.

[34] M. Masud, M. Alazab, K. Choudhary, and G. S. Gaba, "3P-SAKE: privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks," *Computer Communications*, vol. 175, pp. 82–90, 2021.

[35] G. S. Gaba, G. Kumar, H. Monga, T.-H. Kim, and P. Kumar, "Robust and lightweight mutual authentication scheme in distributed smart environments," *IEEE Access*, vol. 8, pp. 69722–69733, 2020.

[36] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, "A robust and lightweight secure access scheme for cloud based E-healthcare services," *Peer-to-peer Networking and Applications*, vol. 14, no. 5, pp. 3043–3057, 2021.

[37] L. M. Varlakshmi, G. F. Sudha, and G. Jaikishan, "An efficient scalable video encryption scheme for real time applications," *Procedia Engineering*, vol. 30, pp. 852–860, 2012.

[38] S. S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns," *Journal of Pattern Recognition*, vol. 37, no. 4, pp. 725–737, 2004.

[39] Y.-T. Chang, Y.-C. Lin, and W.-H. Wang, "Intelligent shuffling cryptography with dynamic AWG/switch matrix for video transmission in WDM-PON network," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 2, pp. 1009–1022, 2019.

[40] G. Kaur, K. Singh, and H. S. Gill, "Chaos-based joint speech encryption scheme using SHA-1," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10927–10947, 2021.

[41] E. M. de Los Reyes, A. M. Sison, and R. Medina, "Modified AES cipher round and key schedule," *Indonesian Journal of Electrical Engineering and Informatics*, vol. 7, no. 1, 2019.

[42] M. Masud, G. S. Gaba, S. Alqahtani et al., "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet of Things Journal*, 2021.

[43] S. Ibrahim, H. Alhumyani, M. Masud et al., "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.