The Optimum Encryption Method for Image Compressed by AES

Marwah Kamil Hussein[1]

[1] University of Basrah, Basrah

Received: 16 December 2019 Accepted: 4 January 2020 Published: 15 January 2020

Abstract

In this paper, the idea of partial encoding has been proposed to use for secure encryption of only a portion of compressed data. Only 10

Index terms— quad tree compression, image processing, compression, encoding, decoding, partial encryption, AES.

1 Introduction

he use of image and video applications such as the World Wide Web and video conferencing has increased dramatically in recent years. When communication bandwidth or storage is limited, data has been often compressed. Especially when a wireless network is used, low bit-rate compression algorithms are needed because of the limited bandwidth. The processing time for encryption and decryption is a major bottleneck in real-time image and video communication and processing. Moreover, we must also take into account the processing time required for compression and decompression.

We propose a novel approach called partial encryption to reduce encryption and decryption time in image communication and processing. In this approach, only part of the compressed data is encrypted. Partial encryption allows the encryption and decryption time to been significantly reduced without affecting the compression performance of the underlying compression algorithm [1].

The aim of the algorithm proposed here is to combine image compression with encryption. Many researchers have examined the possibility of combining compression and encryption. In 1997, Li X., KnipeJ., Cheng H. [2] proposed two separate algorithms to compress and encrypt images. In the first, a Quad treebased algorithm has been used to decompose the image in the spatial domain. In the second, a wavelet transform has been used to decompose the image in the transform domain and a modification of the SPIHT Author: Department of Computer Science, College of Science, University of Basrah, Basrah, Iraq. e-mail: Lava85k@gmail.com algorithm. A partial encryption method in this work takes advantage of the tree structure and simplifies, or even eliminates, the need for secret-key encryption. In 1997, Tang L. [3] proposed the idea of incorporating cryptographic techniques (random algorithms) with digital image processing techniques (image compression algorithms) to achieve compression (decompression) and encryption (decryption) in one step. In 1998, Cheng H. [4] proposed an alternative solution, called partial encryption, in which a secure encryption algorithm has been used to encrypt only part of the compressed data. Partial encryption is applied to quad tree image compression algorithm in this work.

In the present work, only part of the compressed image is encrypted. Some compression algorithms have been important parts that provides a significant amount of information about the original data; partial encryption approach encrypts only it, as illustrated in Figure (1). A significant reduction in encryption and decryption time has been achieved when the relative size of the important part is small.

2 Basic Principles a) Quad tree Compression Algorithm

Quad tree compression partitions the visual data into a structural part (the Quad tree structure) and color information (the leave values). The Quad tree structure shows the location and size of each homogeneous region;

the color information represents the intensity of the corresponding region. The generation of the quad tree follows the splitting strategy well known from the area of image segmentation [5].

A quad tree is a rooted tree in which every node has zero or four children, whereas a 4-arry tree is a rooted tree in which every node has at most four children. Nodes with children have been called internal nodes, whereas those without any children are called leaf nodes. For each node in a tree, we define its level to be the number of edges in the shortest path from the node to the root. The height of the tree is known to be the maximum of the levels of its nodes. Thus, a node at a low level is close to the root.

The quad tree decomposition provides outlines of objects in the original image, as illustrated in Figure (2). In lossless compression, the algorithm starts with a tree with one node. If the image is homogeneous, the root node has been made a leaf, and the gray level describing the image is attached to the leaf. Otherwise, the image has been partitioned into four quadrants, and four corresponding children have been added to the root of the tree. The algorithm then recursively examines each quadrant using each of the four children as the root of a new subtree. The lossy version is similar to the lossless counterpart, but the test for homogeneity of a square block has been replaced by a test for similarity. The similarity of the pixels in a block can been measured by the variance of the pixel values, texture information, and other kinds of statistics. In computer science and information theory, Huffman coding is an entropy encoding algorithm used for lossless data compression. The term refers to the use of a variable-length code table for encoding a source symbol (such as a character in a file) where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It was developed by David A. Huffman while he was a Ph.D. student at MIT and published in the 1952 paper "A Method for the Construction of Minimum-Redundancy Codes" [6].

Huffman coding is a type of variable length entropy coding where each symbol corresponds to a unique binary string of varying length. Huffman coding is uniquely decodable. In other words, when the symbols are encoded by concatenating the binary strings, this concatenated binary string can be decoded uniquely when reading sequentially in the same order that it was written [7].

3 c) Advanced Encryption Standard (AES) Cipher

The AES cipher described by Rijndael (also called Rijndael encryption algorithm) [8], it is a block cipher that converts clear text data blocks of 128, 192, or 256 bits into cipher text blocks of the same length. The AES cipher uses a key of selectable length (128, 192, or 256 bits). This encryption algorithm has been organized as a set of iterations called round transformations. In each round, a data block has been transformed a series of operations. The total number of rounds depends on the largest of round r and key length k and equals 10, 12, and 14 for lengths of 128, 192, and 256 bits, respectively. All-round transformations are identical, apart from the final one. The AES algorithm takes the cipher key and transforms a key expansion routine to generate a key schedule. For number of round=10 and key length=128bits, the key expansion generates total of 44 words. The resulting key schedule consists of a linear array of 4-byte words, denoted by [wi], with i in the range 0 ? i $<$ 44.

4 Figure 3: AES Encryption and Decryption

In this scheme, we propose a method for partial encryption (PE) the compressed image. The proposed method consists of Quad tree compression, encryption of important part, then coding the resultant image by using a Huffman coding algorithm. The encryption step in this algorithm can been performed by using an advanced encryption standard algorithm. During the compression step, the Quad tree image compression is used, which can achieve a reasonably good compression rate, Quad tree compression algorithms are computationally simple and outperform JPEG at low bit rates.

In this scheme, only the important part (Quad tree structure) is encrypted, whereas the remaining parts (unimportant parts) are transmitted without encryption. The Quad tree structure has been encrypted with AES.

5 Quad tree-AES-PE-Algorithm:

1. Encryption key selection. 2. Threshold value selection.

6 Decomposition (compression) the image, here

Quad tree compression is applied. 4. Partial encryption, here AES cipher is used. 5. Entropy coding, here the Huffman coding is adopted.

7 III.

8 Experimental Results

In this section, several of experiments that are used to examine our proposed Quad tree based image encryption algorithm will been presented. The algorithms were programmed in MATLAB version 6.5 on a Pentium IV PC (2.00 GHz) using color boys image and grayscale boys image of (256×256) pixels.

To evaluate each of the proposed partial encryption schemes, five aspects are examined [9]: 1. Security. Security in this work means confidentiality and robustness against attacks to break the images. It is that the goal

is not 100% security, but analgorithm is adopted, such as AES cipher that makes them difficult to cryptanalyze. 2. Speed. Less data to encrypt means less CPU time required for encryption. So, general partial encryption algorithms are used to reduce encryption and decryption time.

3. Compression Performance. The compression performance of the selected compression method has been used to reduce the bandwidth required for data transmission. The proposed encryption scheme does not reduce the compression performance of the underlying selected compression method. Peak signal-to-noise ratio (PSNR) measures are estimates of the quality of a reconstructed image compared to an original image. Typical PSNR values ranges 20 and 40 decibels (dB) [10] In this work, several experiments on the proposed partial encryption scheme have been done. Different cases were considered.

In these experiments, three different threshold values have been chosen, which are 0.3, 0.5, and 0.7 in lossy compression. In Table (1), the first column gives the threshold value. The second column gives CR. The third column gives the PSNR of the reconstructed image with the original image for each test image. Lastly, the fourth column gives the time of the operations. The encryption key is "2b 7e 15 16 28 ae d2 a6 abf7 15 88 09 cf 4f 3c". The size of the key spaces is 2 128 . Only part of the output from the image compression algorithm is encrypted.

9 Experiment 1

In this experiment, the AES encryption scheme has been considered only. Figure (4) shows the result obtained for the grayscale boys' images. Figure (5) shows the histograms of the original grayscale boy's image and the cipher-image.

10 Experiment 2

In this method, different threshold values (0.3, 0.5, and 0.7) of grayscale images (lossy compression) have been chosen. The results in this method have been present in Table (1). Figure (6) shows the results obtained for grayscale boys' image. The Optimum Encryption Method for Image Compressed by AES

11 Experiment 3

In this scheme, different threshold values (0.3, 0.5, and 0.7) of color images (lossy compression) have been chosen. The results of this method have been present in Table (2). Figure (7) shows the results obtained for the color boys' image.

12 Experiment 4

In this experiment, the threshold value equal to zero of grayscale images (lossless compression) has been chosen. The results of this method have been present in Table (3). Figure (8) shows the results obtained for grayscale boys' image.

13 Experiment 5

In this experiment, the threshold value equal to zero of color images (lossless compression) has been chosen. The results of this method have been present in Table (4). Figure (9) shows the results obtained for the color boys' image.

14 Conclusion

In all experiments, the attacker cannot obtain the original image unless he knows the encryption key. So, the proposed method has good security since the key space is very large to make brute-force attack infeasible. Out of the results of experiments (lossy compression), one can notice that as the threshold value increase, the CR will increase (low compression). Figure (10) shows the CR versus the threshold value for the color boys' image. From histograms, one can see that the histogram of the cipher-image is significantly different from that of the original image. By this difference between the two histograms, the positions and the values of the pixels of original image have been rearranged with the user key. As a result, the cipher-image can reach properties of confusion to protect the confidential image data from unauthorized access.

It can been noticed that the execution time required to encrypt the amount of image data (the important) is shorter compared to that of the full image. So partial encryption reduces the CPU time considerably. This time can been further reduced by using an efficient program code and a faster computer.

Also, the execution time lossy compression is less than lossless compression. The PSNR value of lossless compression equal to infinity because of the reconstructed image after compression is numerically identical to the original image on a pixel-by-pixel basis, as shown in Tables (3 and 4). The CR value of lossy compression is less than lossless compression, the reconstructed image contains degradation relative to the original image, because redundant information has been discarded during compression. As a result, much higher compression is achievable, and according to what we will see below, no visible loss has been perceived (visually lossless), as shown in Tables (1 and 3). [1]

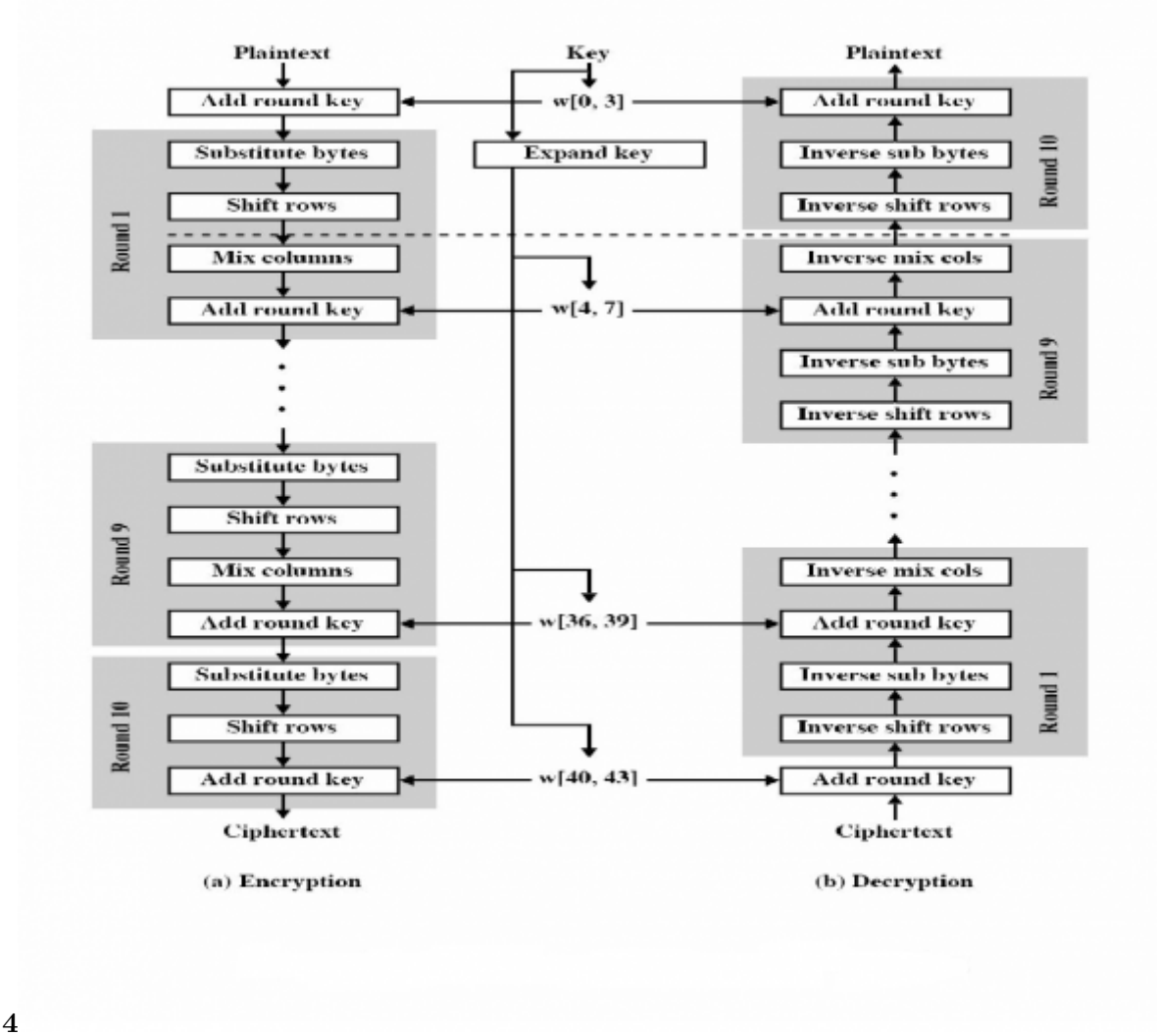
[1]( ) F © 2020 Global JournalsThe Optimum Encryption Method for Image Compressed by AES

1 

Figure 1: Figure 1 :

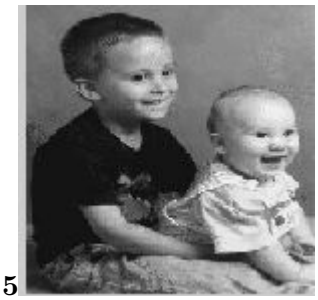
2 

Figure 2: Figure 2 :



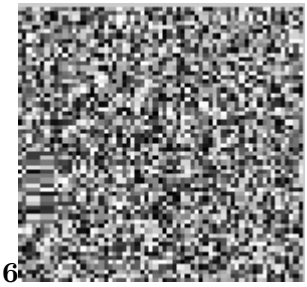
4

Figure 3: Figure 4 :



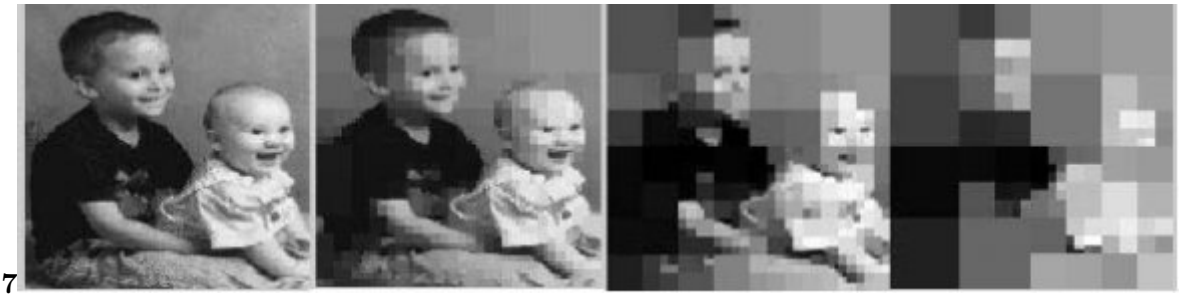
5

Figure 4: Figure 5 :



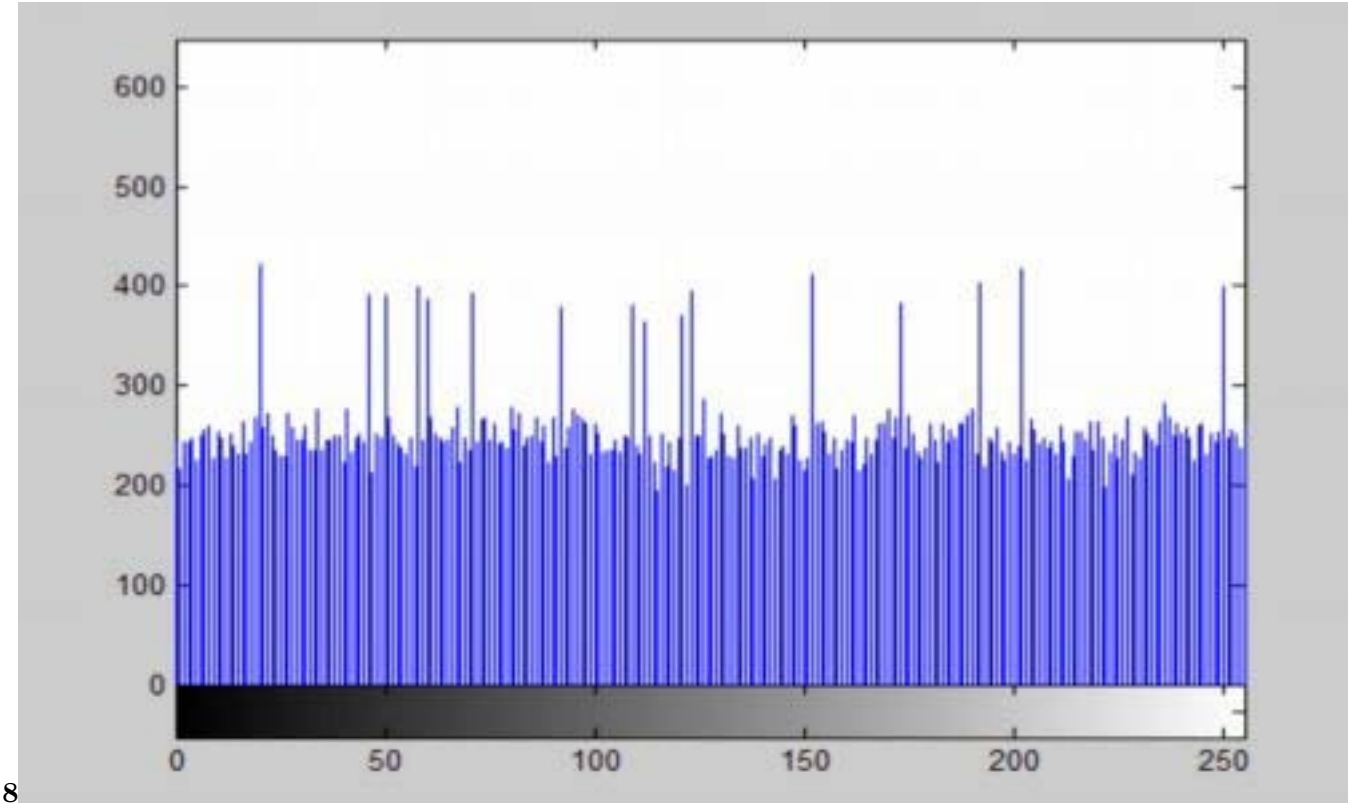
6

Figure 5: Figure 6 :



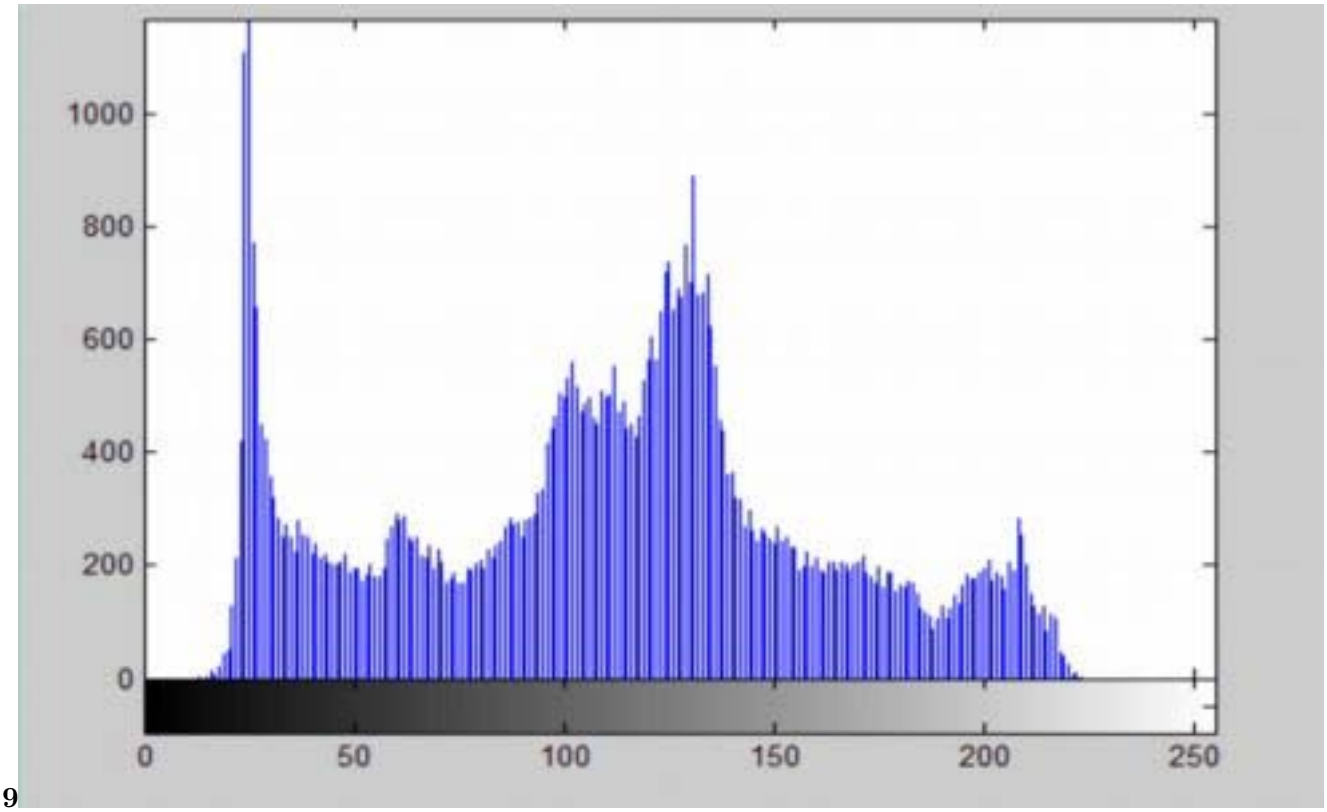
7

Figure 6: Figure 7 :



8

Figure 7: Figure 8 :



9

Figure 8: Figure 9 :

10

Figure 9: Figure 10 :

11

Figure 10: Figure 11 :

12 

Figure 11: Figure 12 :

Figure 12:

1

Threshold value	CR	PSNR (dB)	Time (sec)
0.3	0.0198	27.1229	16.9070
0.5	0.0041	21.6693	10.4840
0.7	0.0005	18.5871	8.7660

Figure 13: Table 1 :

2

Threshold value	CR	PSNR (dB)	Time (sec)
0.3	0.0086	28.0000	20.8280
0.5	0.0025	22.6112	12.3750
0.7	0.0006	20.0000	9.4690

Figure 14: Table 2 :

3

Threshold value	CR	PSNR (dB)	Time (sec)
0	0.3196	infinity	353.0940

Figure 15: Table 3 :

4

Figure 16: Table 4 :

[David ()] *A Method for the Construction of Minimum-Redundancy Codes*, A David . 1952. (Ph.D. student at MIT)

[CarlS ()] *Color Image Compression Using Wavelet Transform*, CarlS , BS E . 1997. Master of Science in Electrical Engineering

[Hussien] *Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES)*, M K Hussien . p. .

[Li et al. ()] 'Image Compression and Encryption Using Tree Structures'. X Li , J Knipe , H Cheng . *Pattern Recognition Letters* 1997. 18 (11) p. .

[Tang ()] 'Methods for encrypting and decrypting MPEG video data efficiently'. L Tang . *Proceedings of the fourth ACM international conference on Multimedia*, (the fourth ACM international conference on Multimedia) 1997. p. .

[Tang ()] 'Methods for Encryption and Decryption MPEG Video Data Efficiently'. L Tang . *Proceedings of the Fourth ACM International Conference on Multimedia*, (the Fourth ACM International Conference on Multimedia) 1997. p. .

[Hussien] *Multi-Frame Video Compression Scheme Using Three Step Search (TSS) Matching Algorithm*, M K Hussien .

[Cheng ()] *Partial Encryption for Image and Video Communication*, H Cheng . 1998. Alberta. Department of Computing Science, University of Alberta (M.Sc. Thesis)

[Alhijaj and Hussein ()] 'Stereo Images Encryption by OSA & RSA Algorithms'. A A Alhijaj , M Hussein . *J. Phys. Conf. Ser* 2019. 1279 (1) .

[Hussein and Alhijaj ()] 'TDL and ron rivest, adi shamir and leonard adleman in stereo images encrypt'. M K Hussein , A A Alhijaj . *J. Adv. Res. Dyn. Control Syst* 2019. 11 (1) p. . (Special Issue)