Global Scientific JOURNALS

GSJ: Volume 8, Issue 4, April 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

The optimum encryption method for image compressed by AES

Marwah Kamil Hussein
**Department of Computer Science, College of Science, University of Basrah, Basrah, Iraq.*
Lava85k@gmail.com

ABSTRACT

In this paper, the idea of partial encoding is proposed to be used for secure encryption of only a portion of compressed data. Only 10% -25% of the output is encrypted from the quadtree compression algorithm. As a result, the encryption and decryption time was reduced considerably.Thus, in the compression stage, the quadtree compression algori**thm is used while in the** encoding stage, the Advanced Encryption Standard (AES) algorithm is applied.The proposed partial coding system is fast and safe and does not **reduce the compression** performance of the underlying specific algorithm.

Keywords : *Quadtree , Image Compression, Partial Encryption, AES.*

1. INTRODUCTION

The 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 is 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 timeto be significantly reduced without affectingthe compression performance of the underlying compression algorithm [1].

The aim of algorithm proposed here is to combineimage 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, an quadtree-based algorithm is used to decompose the image in the spatial domain. In the second, a wavelet transform is used to decompose the image in the transform domain and a modification of the SPIHT 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 is used to encrypt only part of the compressed data. Partial encryption is appliedto quadtree image compression algorithm in thiswork.

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

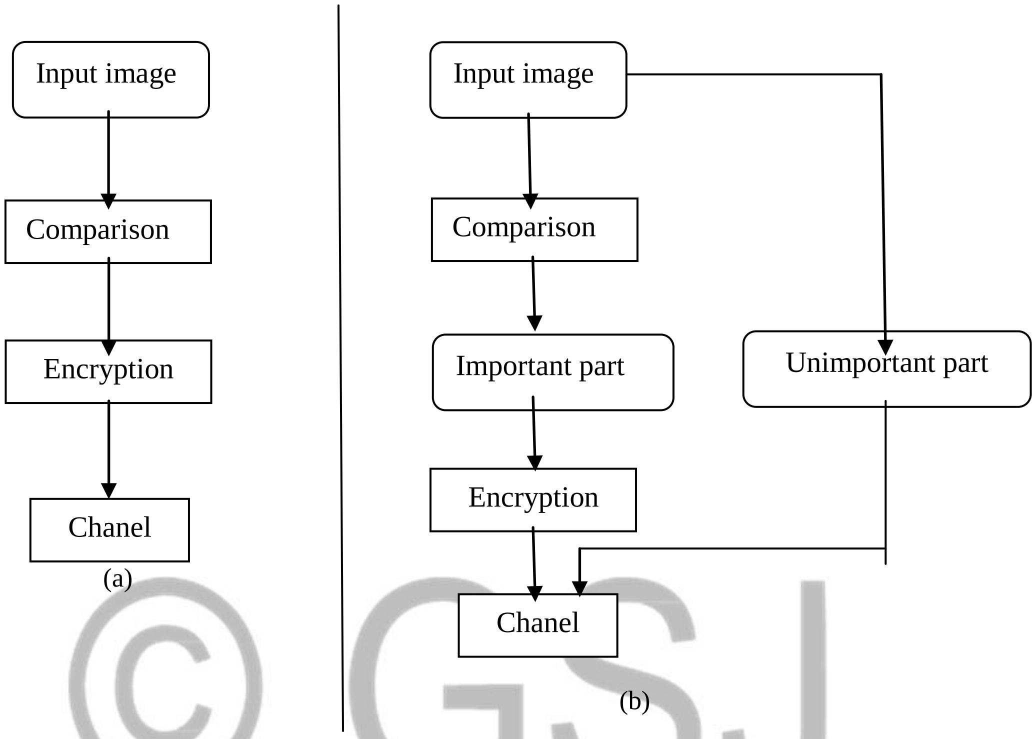


Fig. 1. Comparison of (a) The traditional approach to secure image communication and (b) The proposed approach.

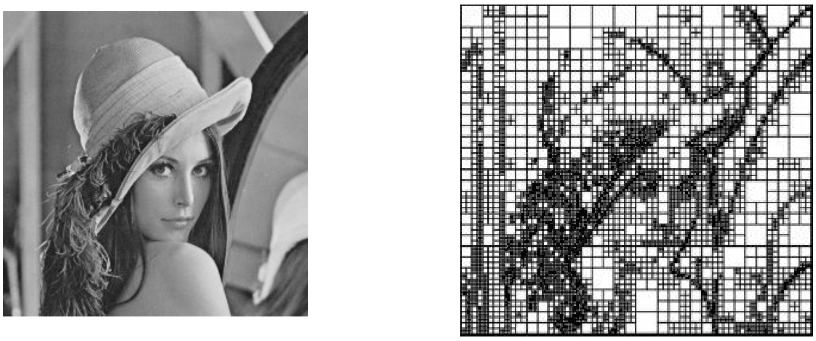
2. BASIC PRINCIPLES

1. Quadtree CompressionAlgorithm

Quadtree compression partitions the visual data into a structural part (the quadtree structure) and color information (the leave values). The quadtree structure shows the location and size of each homogeneous region, the color information represents the intensity of the corresponding region. The generation of the quadtree follows the splittingstrategy well known from the area of image segmentation [5] .

A quadtree is a rooted tree in which every node has zero or four children, whereas a 4-ary tree is a rooted tree in which every node has at most four children. Nodes with children are 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 defined to be the maximum of the levels of its nodes. Thus, a node at a low level is close to theroot.

The quadtree 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 entire image is homogeneous, the root node is made a leaf, and the gray level describing the entire image is attached to the leaf. Otherwise, the image is partitioned into four quadrants, and four corresponding children are 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 lossyversion is similar to the lossless counterpart, but the test for homogeneity of a square block is replaced by a test for similarity. The similarity of the pixels in a block can be measured by the variance ofthe pixel values, texture information, and other kinds of statistics.



(a) (b)

Fig. 2. Quadtree decomposition ofan image (a) Original image. (b) Quadtreedecomposition.

2. Huffman Coding

In computer science and information theory, Huffman coding is an entropyencoding 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. Huffmanwhile he was a Ph.D. student at MIT, and publishedinthe 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 read sequentially in the same order that it was written [7] .

3. ADVANCED ENCRYPTION STANDARD (AES)CIPHER

The AES cipher described by Rijndael(called also *Rijndael encryption algorithm*)[8] , it is a block cipher that converts cleartext data blocks of 128, 192, or 256 bits into ciphertextblocks of the same length. The AES cipher uses a key of selectable length (128, 192, or 256 bits). This encryption algorithm is organized as a set of iterations called *round transformations*. In each round, a data block is transformed by 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 numberofround=10andkeylength=128bits,thekeyexpansiongeneratesa

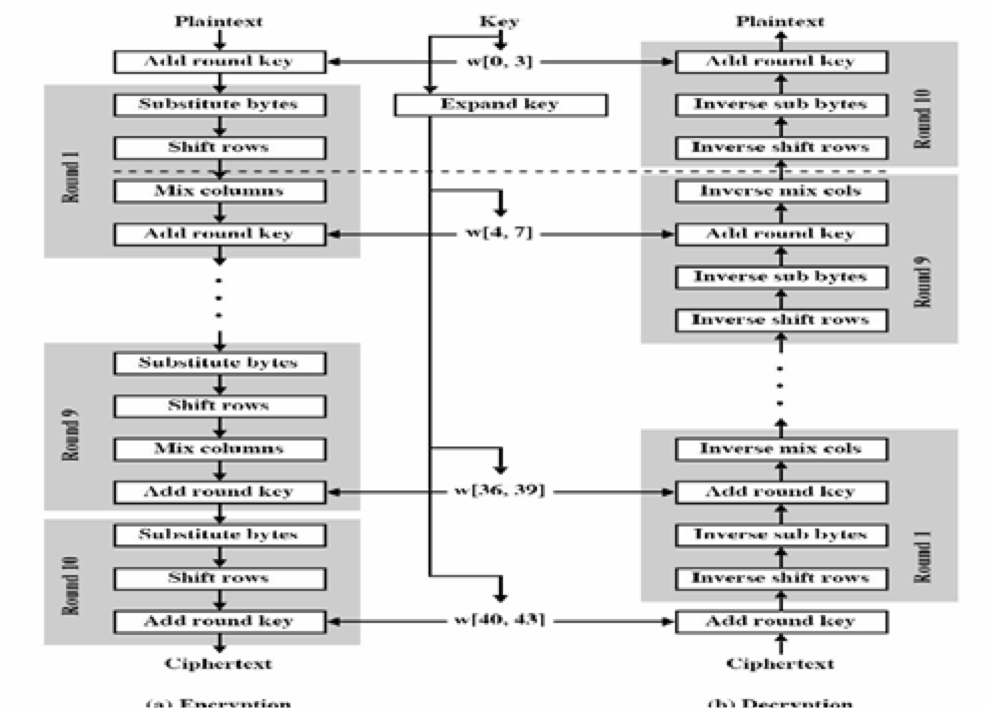


Fig. 3. AES Encryption and decryption.

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

In this scheme, only the important part (quadtree structure) is encrypted whereas the remaining parts (unimportant parts) are transmitted without encryption. The quadtree structure is encrypted withAES.

Quadtree–AES–PE-Algorithm:

1. Encryption keyselection.
2. Threshold valueselection.
3. Decomposition (compression) the image, here quadtree compression is applied.
4. Partial encryption, here AES cipher isused.
5. Entropy coding, here the Huffman coding isadopted.

4. EXPERIMENTAL RESULTS

In this section, a number of experiments which are used to examine our proposed quadtree based imageencryption algorithm will be 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 scheme, five aspects are examined [9]:

1. **Security.** Security in this work means confidentiality and robustness against attacks to break the images. It is obvious that the goal is not 100% security, but a good algorithm is adopted, such as AES cipher that make them difficult tocryptanalyze.
2. **Speed.** Less data (important part) to encrypt means less CPU time required for encryption. So, in general partial encryption algorithms are used to reduce encryption and decryption time.
3. **Compression Performance.** Compression performance of the selected compression method is used to reduce bandwidth required for data transmission. The proposed encryption scheme do not

reduce 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].

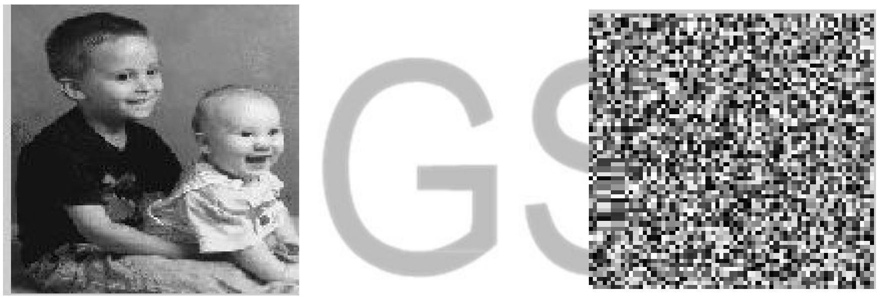
4. **Keyspace Analysis.** A good image encryption algorithm should be sensitive to cipher key, and the keyspace should be large enough to make brute-force attackinfeasible.
5. **Histograms of Encrypted Images.** Select several 256 gray-level images with size of 256×256 that have different contents, to calculate their histograms. One can see that the histogram of the cipher-image is significantly uniform and different from that of the originalimage.

In this work, several experiments on the proposed partial encryption scheme are done. Different cases wereconsidered.

In these experiments, three different threshold values are chosen which are 0.3, 0.5, and 0.7 in lossycompression. In Table (1), the first column gives the threshold value. The second column gives CR. The third column givesthe PSNR of the reconstructed image with the original image for each test images. 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 keyspaceis 2^{128}. Only part of the output from image compression algorithm isencrypted..

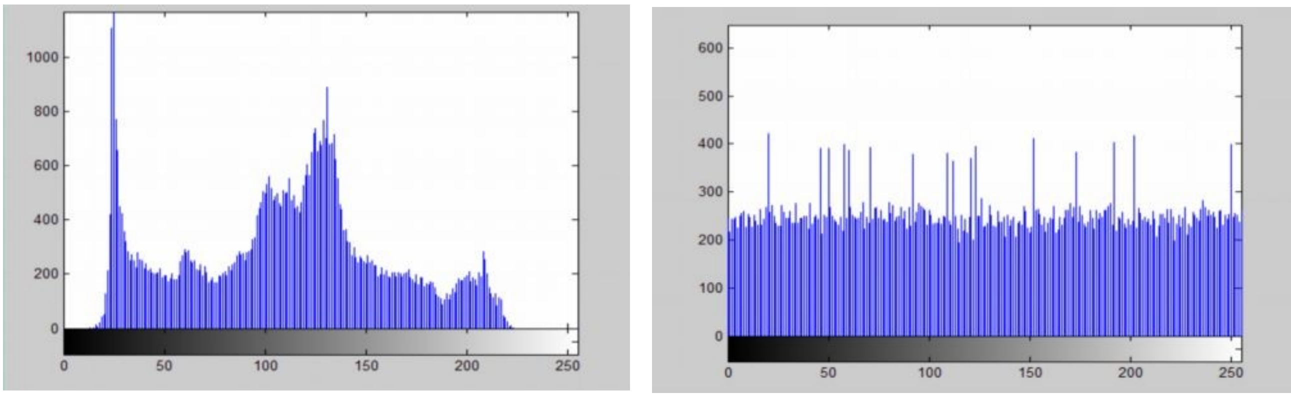
5.1 Experiment 1

In this experiment, AES encryption scheme is considered only. Figure (4) shows the result obtained for grayscale boys image. Figure (5) shows histograms of the original grayscale boys image and thecipher-image.



(a) (b)

Fig. 4. Results of experiment 1 using AES encryption scheme:
a) Original grayscale boys ima ge. b) Image resulting fromencryption.



(a) (b)

Fig. 5. Histogram of experiment 1 using AES (a) The original gray scale boysimage.
(b) Thecipher-image.

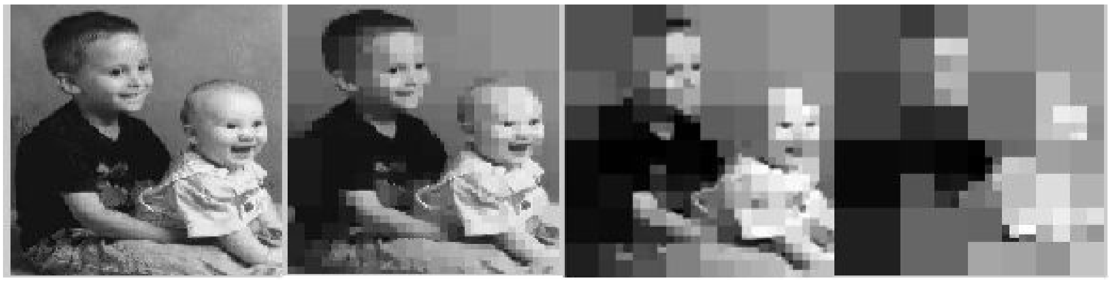
5.2 Experiment 2

In this method, different threshold values (0.3, 0.5, and 0.7) of grayscaleimages (lossy compression) are chosen. Results of this method are present in Table (1). Figure (6) shows the results obtained for grayscaleboysimage.

TABLE 1

RESULTING OF EXPERIMENT 2.

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



(a) (b) (c) (d)

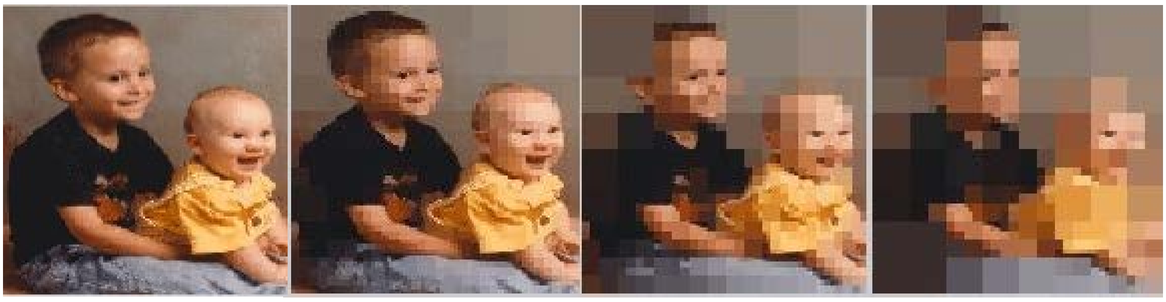
Fig. 6. Results of experiment2:
(a) Original grayscale boysimage.
(b) Reconstructed image at threshold =0.3.
(c) Reconstructed image at threshold =0.5.
(d) Reconstructed image at threshold =0.7.

5.3 Experiment 3

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

TABLE 2.
RESULTING OF EXPERIMENT 3.

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



(a) (b) (c) (d)

Fig. 7. Results of experiment 3: (a) Original color boys image.
(b) Reconstructed image at threshold =0.3.
(c) Reconstructed image at threshold =0.3.
(d) Reconstructed image at threshold =0.5.

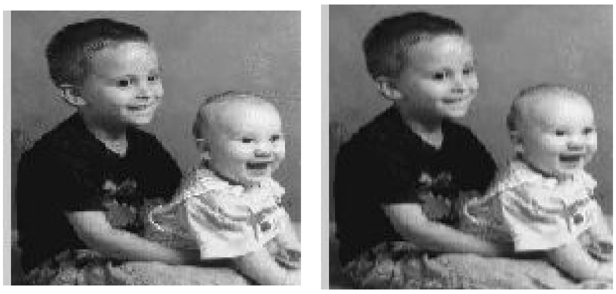
5.4 Experiment 4

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

TABLE 3

RESULTING OF EXPERIMENT 4.

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



(b) (b)

Fig. 8. Results of experiment 4:
(b) Original grayscale boys image.
(b) Reconstructed image.

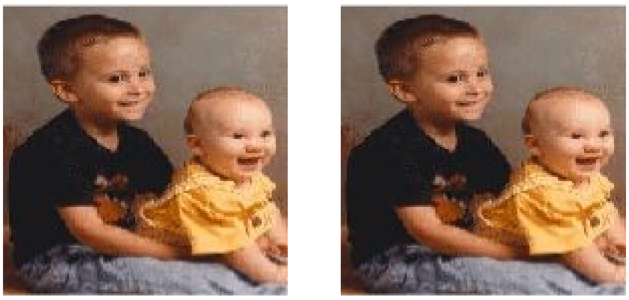
5.5 Experiment 5

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

TABLE 4

RESULTING OF EXPERIMENT 5.

Threshold value	CR	PSNR (dB)	Time (sec)
0	0.1071	infinity	556.7190



(a) (b)

Fig. 9. Results of experiment 4:
(a) Original color boysimage.
(b) Reconstructedimage.

5. CONCLUSION

In all experiment, the attacker cannot obtain the original image unless he knows the encryption key. So, the proposed method have good security since the key space is very large to make brute-force attackinfeasible.Out of the results of experiments (lossy compression), one can notice that as the threshold value increase, the CR will increase (low compression). Figure (9) shows the CR versus the threshold value for color boys image.

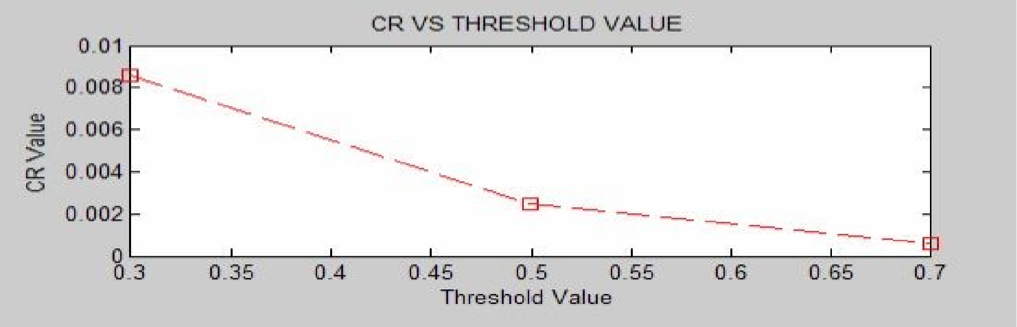


Fig. 10. CR versus threshold for color boys image.

Out of experiments, we conclude that as the threshold value is increased, both the PSNR and the execution time are decreased. Figures (10 and 11) show the PSNR and the execution time versus the threshold value for color boys image, respectively.

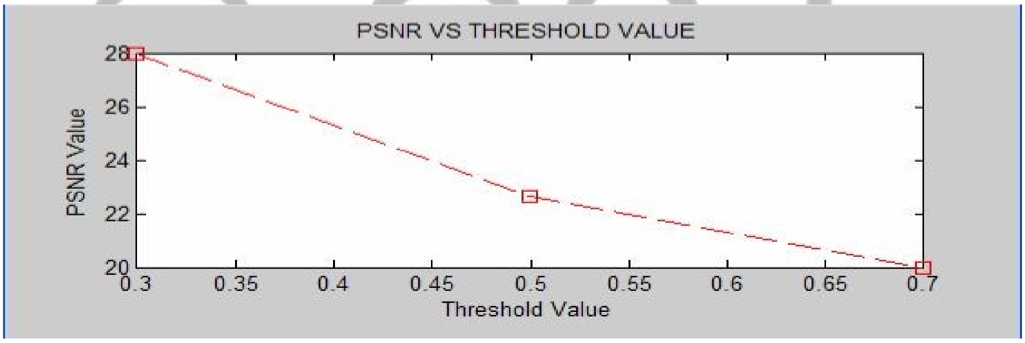


Fig .11. PSNR versus threshold for color boys image

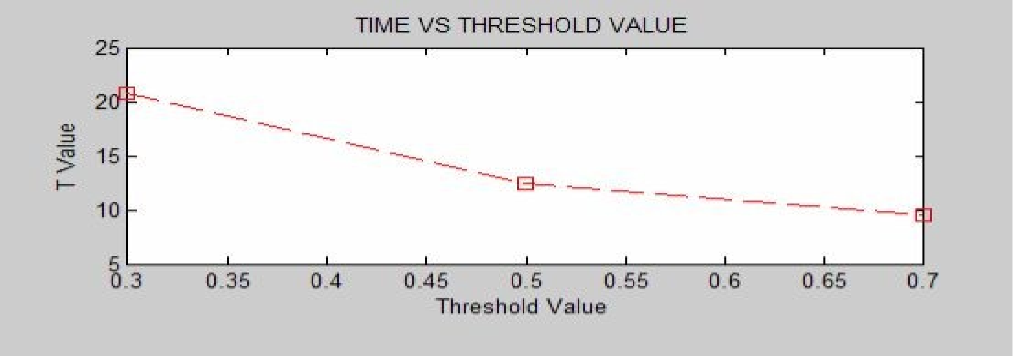


Fig. 12. Time versus threshold for color boys image

rom 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 are rearranged with the user key. As a result, the cipher-image is able to reach good properties of confusion to protect the confidential image data from unauthorized access.

It can be noticed that the execution time required to encrypt the amount of image data (important part) is very short comparing to that of the full image. So partial encryption reduce the CPU time considerably. This time can be further reduced by using an efficient program code and a faster computer.

Also, the execution time of lossy compression is shorter 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 isless than lossless compression, the reconstructed image contains degradation relative to the original image, because redundant information is discarded during compression. As a result, much higher compression is achievable, and under normal viewing condition, no visible loss is perceived (visually lossless), as shown in Tables (1 and3).

REFERENCES

[1] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” in*Proceedings of the fourth ACM international conference on Multimedia*, 1997, pp. 219–229.

[2] Li X., Knipe J., and Cheng H., (1997), “*Image Compression and Encryption UsingTree Structures*”, Pattern Recognition Letters, Vol. 18, No. 11-13, pp. 1253-1259.

[3] Tang L., (1997), “*Methods for Encryption and Decryption MPEG VideoData Efficiently”,* Proceedings of the Fourth ACM International Conferenceon Multimedia, pp.219-229.

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

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

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

[7] Carl S., B.S.E.E, (1997), "*Color Image Compression Using Wavelet Transform"*,Master ofScience in Electrical Engineering.

[8] M. K. Hussien, “Encryption of Stereo Images after Compression by Advanced EncryptionStandard (AES),” pp. 1–6.

[9] M. K. Hussein and A. A. Alhijaj, “TDL and ron rivest, adi shamir and leonard adlemanin stereo images encrypt,” *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1 Special Issue, pp. 1811–1817, 2019.

[10] A. A. Alhijaj and M. Kamil Hussein, “Stereo Images Encryption by OSA & RSA Algorithms,” *J. Phys. Conf. Ser.*, vol. 1279, no. 1, 2019.