Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN: 2521-3520 (online)
Volume 28, Issue 2, 2017
DOI: http://doi.org/10.23851/mjs.v28i2.511

Research Article

Encryption of Stereo Images after Compression by Advanced Encryption Standard (AES)

Marwah K. Hussien, Alyaa J. Jalil
Department of Information Systems, College of Computer Sciences and Information Technology, University of Basrah, IRAQ
*Correspondent Author Email: Lava85K@gmail.com, aliaa. jaber@yahoo.com

ArticleInfo

Received
06/09/2016

Accepted
17/04/2017

Abstract

New partial encryption schemes are proposed, in which a secure encryption algorithm is used to encrypt only part of the compressed data. Partial encryption applied after application of image compression algorithm. Only 0.0244%-25% of the original data isencrypted for two pairs of different grayscale imageswiththe size (256 ´ 256) pixels. As a result, we see a significant reduction of time in the stage of encryption and decryption.

In the compression step, the Orthogonal Search Algorithm (OSA) for motion estimation (the different between stereo images) is used. The resulting disparity vector and the remaining image were compressed by Discrete Cosine Transform (DCT), Quantization and arithmetic encoding. The image compressed was encrypted by Advanced Encryption Standard (AES). The images were then decoded and were compared with the original images.

Experimental results showed good results in terms of Peak Signal-to-Noise Ratio (PSNR), Compression Ratio (CR) and processing time. The proposed partial encryption schemes are fast, secure and do not reduce the compression performance of the underlying selected compression methods.

Keywords: Stereoimaging, Stereoimage compression, Imageencryption, cryptography.

الخلاصة

تم اقتراح طرق جديدة للتشفيرالجزئي،والذي يستخدم خوارزمية التشفيرآمنة لتشفير فقط جزء من البيانات المضغوطة. وشفربحدود 0.0244%-25%))من البيانات الأصلية لزوجين من الصور الرمادية المختلفة بأبعاد (256*256)عنصرصورةللحصول على تقليل مهم في زمن التشفيروفك الشفرة. استخدمت في مرحلة الضغط خوارزمية البحث المتعامد(*OSA*) لتقدير الحركة (الفرق بين الصورتين). متجه الحركة الناتج والجزء المتبقي تتم عملية ضغطه بالتحويل الجيبي المنقطع, التكميم الرقمي والترميز الحسابي. ثم تشفر بعد ذلك الصورة المضغوطة باستخدام طرق تشفيرمتقدمة مثلا لتشفيرالقياسي المتقدم (AES) والصور المشفرة يعاد استرجاعها ثم فك ضغطها واسترجاعها و تقارن مع الصور الاصلية. انظمة التشفير الجزئي المقترحة كانت سريعة وذات سرية عالية كما ان انجازية الضغط لا تقل ضمن طرق الضغط المختارة. النتائج التجريبية بينت نتائج جيدة عند حساب نسبة قمة الإشارة إلى الضوضاء (PSNR) ونسبة الضغط (CR) ووقت المعالجة.

Introduction

As a result of the increase in the use of images in recent years, it must be to have to deal with it (move) safely through the so-called pressure and encryption. For this, the researchers combined compression and encryption together to reduce the overall processing time.

In this research, has been selected a pair of stereo images which are very similar to each other are taken from two different angles (and this is why the pressure of each of the images independently, which means in the efficiency of the stereo image compression). We can get the sequence of these images by film cameras or generated by demand sequentially.compress these pictures is the foundation necessary to reduce this data through the difference between the two images Account (matching), also known as disparity estimation, then squeeze one image independently. This is known as image as a reference, and can either is the right image or the left image, then use the reference image and vector disparity to rebuild the second image [2]. Figure 1 shows flowchart of encryption a pair of stereo image-

safter compressed.

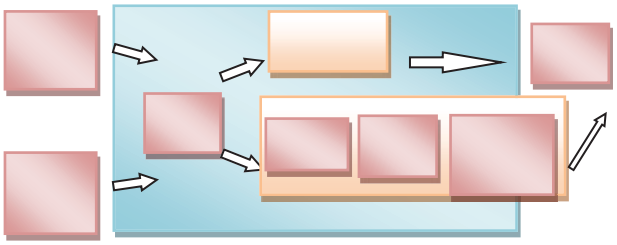


Figure 1: Encryption a pair of stereo images after Compressed.

The work aims to propose an efficient technique for stereo images compression by estimated the disparity vectors between them (The left and right image) using Orthogonal Search Algorithm *(OSA)*. The remaining image is transformed using Discrete Cosine Transform (DCT). The resulting image is quantized using the scalar quantization and then compressedusing arithmetic coding; we show that in Section 2. The two images are very similar to each other; disparity vectors between the two images are estimated. The resulting disparity vector and image compressed are encryption byAdvanced Encryption Standard (AES), We show that in Section 3. Section 4 gives the experimental results. Finally, the paper has been concluded in Section 5.

Motion Estimation

Motion Estimation (ME) is the process of analyzing successive frames in any image sequence to identify objects motion. In this paper, motion estimation used to process of analyzing two stereo images by using OSA.

The motion of an object is usually described by a two-dimensional motion vector, which is the placement of the co-ordinate of the best similar block in previous frame for the block in current frame. This placement is represented by the length and direction of motion [3] [4].

Disparity Estimation Using Orthogonal Search Algorithm (OSA)

OSA was introduced by Puri. It has a vertical stage followed by a horizontal stage for the search for the optimal block. The algorithm may be described as follows:

Step1- Pick a step size (usually half the maximum displacement in the search window). Take two points at a distance of step size in the horizontal direction from the center of the search window and locate (among these) the point of minimum distortion. Move the center to this point.

Step 2- Take two points at a distance step size from the center in the vertical direction and find the point with the minimum distortion.

Step 3- Halve the step size, if it is greater than one, else halt.

A particular path for the convergence of the algorithm may be shown in the following Figure 2 [5]:

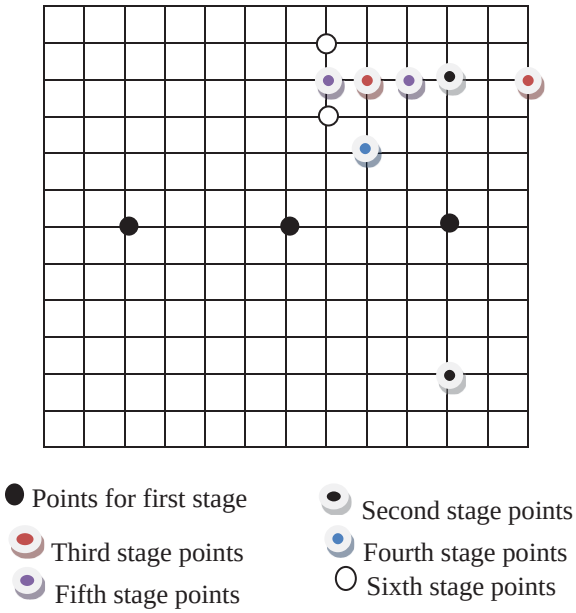


Figure 2: Example of Orthogonal Search Algorithm.

Image Transform

Divide the source image into blocks and apply the transformations to the blocks [6].

Parameter quantization

Quantization is irreversible operation because of its lossy property. The data generated by the transformation are quantized to reduce the amount of information. This step represents the information within the new domain by reducing the amount of data [7] [8].

Arithmetic Encoding

Arithmetic encoding and its derivative technique, Q-coding, is used to overcome some of the limitations of Huffman codes. It is a non-block code, in that a single code word is used to represent an entire sequence of input symbols, in contrast to Huffman coding where a source symbol block corresponds to a code word block. Instead, it uses the real numbers to represent a sequence of symbols by recursively subdividing the interval

between 0 and 1 to specify each successive symbol. The limitation of this technique is the precision required in performing the calculations and arriving at the code word which will represent the entire sequence correctly [9].

Partial Encryption

Partial encryption (also called *selective encryption* or *soft encryption*) is a secure encryption algorithm which is used to encrypt only part of the data. It is used to reduce encryption and decryption time. During our work, only part of the compressed data is encrypted. Some compression algorithms have *important parts* that provide a significant amount of information about the original data, whereas the remaining parts
may not provide much information without the important parts. For simplicity, we consider all the important parts as one unit, and the remaining parts are grouped into one unimportant part. Since it is difficult to obtain information from the unimportant part alone, partial encryption approach encrypts only the important part. A significant reduction in encryption and decryption time is achieved when the relative size of the important part is small.

In some cases, partial encryption allows the important part to be encrypted while the unimportant part is transmitted in parallel so that the encryption time becomes negligible [10]. A secure encryption algorithm is used to encrypt the important part.

Advanced Encryption Standard (AES) Cipher

The AES cipher described by Rijndael (called also *Rijndael encryption algorithm*). It was chosen in 1977 by the International Institute of Technological Standards As an international standard for encryption, And on the basis development in the types of encryption that are of class as Symmetric Encryption.

This algorithm is a widely accepted in the world; it is considered a safe method of encryption, and because of the length of the encryption key [10]. Encryption algorithm blocks which supports keys lengths and lengths of multiple texts. Encryption $\boldsymbol{k}$ key is a matrix with dimensions $\boldsymbol{N_k \times 4}$ (any key length is $\boldsymbol{N_k \times 4}$):

$$\underline{k} = \begin{pmatrix} k_{0,0} & k_{0,1} & \cdots & k_{0,N_{k-1}} \\ k_{1,0} & k_{1,1} & \cdots & k_{1,N_{k-1}} \\ k_{2,0} & k_{2,1} & \cdots & k_{2,N_{k-1}} \\ k_{3,0} & k_{3,1} & \cdots & k_{3,N_{k-1}} \end{pmatrix}$$

Where each $\boldsymbol{k_{i,j}}$ can be considered:

- 8-bit or 1 byte that any number in the group $\boldsymbol{Z_{2,8}}$
- Integer in the group $\boldsymbol{Z_{256}}$
  the key length of the AES algorithm can be $\boldsymbol{N_k = 4, 6, 8\ (128, 192, 256)}$ bytes.
  Read the encryption key from the matrix be according to each column from left to right any:

$$\underline{k} = \left(k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, \cdots, k_{0,N_{k-1}}, k_{1,N_{k-1}}, k_{2,N_{k-1}}, k_{3,N_{k-1}}\right)$$

Block or text that you want to encrypt_$\boldsymbol{x}$ is a matrix with lengths of $\boldsymbol{N_b \times 4}$ (any key length is $\boldsymbol{N_b \times 4}$ bytes):

$$\underline{x} = \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N_{b-1}} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N_{b-1}} \\ x_{2,0} & x_{2,1} & \cdots & x_{2,N_{b-1}} \\ x_{3,0} & x_{3,1} & \cdots & x_{3,N_{b-1}} \end{pmatrix}$$

Where each $\boldsymbol{x_{i,j}}$ can be considered:

- 8-bit or 1 byte that any number in the group $\boldsymbol{Z_{2,8}}$
- Integer in the group $\boldsymbol{Z_{256}}$
  Block in Raendaul algorithm can be $\boldsymbol{N_b = 4, 6, 8\ (128, 192, 256)}$ bytes.
  Read the block of the matrix be according to each column from left to right any: $\underline{x} = \left(x_{0,0}, x_{1,0}, x_{2,0}, x_{3,0}, \cdots, x_{0,N_{k-1}}, x_{1,N_{k-1}}, x_{2,N_{k-1}}, x_{3,N_{k-1}}\right)$

  Status Raendall $\boldsymbol{\omega}$ is the matrix:

$$\underline{\omega} = \begin{pmatrix} \omega_{0,0} & \omega_{0,1} & \cdots & \omega_{0,N_{b-1}} \\ \omega_{1,0} & \omega_{1,1} & \cdots & \omega_{1,N_{b-1}} \\ \omega_{2,0} & \omega_{2,1} & \cdots & \omega_{2,N_{b-1}} \\ \omega_{3,0} & \omega_{3,1} & \cdots & \omega_{3,N_{b-1}} \end{pmatrix}$$

Where each $\boldsymbol{\omega_{i,j}}$ is an integer in the $\boldsymbol{Z_{256}}$ Raendaul is installing transfers (Transformation), The positions RaendaulThese transfers called cycles (iterations) ie:

$\boldsymbol{R\ I\ J\ (\underline{x}) = \underline{y} = (T_{N\,r} \circ T_{N\,r-1} \circ \cdots \circ T_{N\,1} \circ T_{N\,0})}$

Each T_i: $\omega \rightarrow \omega$ie the field and is long positions Raendaul, the number of cycles ($N_r$respect to the key length (N_k) and the length of the text (N_b): Raendaul number (N_r) courses
First Session of T_0 is XOR between the text (the first position) and any encryption key:

$$T_0(x) = \begin{pmatrix} k_{0,0} & k_{0,1} & \cdots & k_{0,N_{k-1}} \\ k_{1,0} & k_{1,1} & \cdots & k_{1,N_{k-1}} \\ k_{2,0} & k_{2,1} & \cdots & k_{2,N_{k-1}} \\ k_{3,0} & k_{3,1} & \cdots & k_{3,N_{k-1}} \end{pmatrix} \oplus \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N_{k-1}} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N_{k-1}} \\ x_{2,0} & x_{2,1} & \cdots & x_{2,N_{k-1}} \\ x_{3,0} & x_{3,1} & \cdots & x_{3,N_{k-1}} \end{pmatrix}$$

Courses that come after this will mean transforming the current situation, but this algorithm are doing this in stages:

1. confused linear - Remittances are ***ShiftRow***and***MixColumn;***
2. non-linear - a crossover ***ByteSub***;
3. Add the key - Shunt ***AddRoundKey.*** So blinded show is enough to turn the transfers, namely:

$$RIJ^{-1}(\underline{y}) = \underline{x} = (T_{N_0}^{-1} \circ T_{N_1}^{-1} \circ \cdots \circ T_{N_{r-1}}^{-1} \circ T_{N_r}^{-1})$$

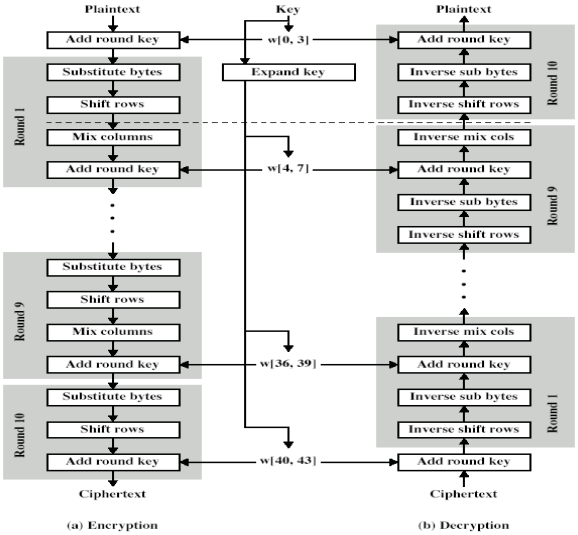


Figure 3: AES Encryption and Decryption Steps

PSNR and CR

Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a compressed image with the original. For an 8-bit grayscale image, the peak signal value is 255. Hence, the PSNR of an M×N 8-bit grayscale image C_{ij} and its reconstruction R_{ij} is calculated as [11] [12]:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (1)$$

Where the Mean Square Error (MSE) is defined as [11]:

$$MSE = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left[C_{ij}(m,n) - R_{ij}(m,n)\right]^2 \qquad (2)$$

PSNR is measured in decibels (dB), M: height of the image, N: width of the image.

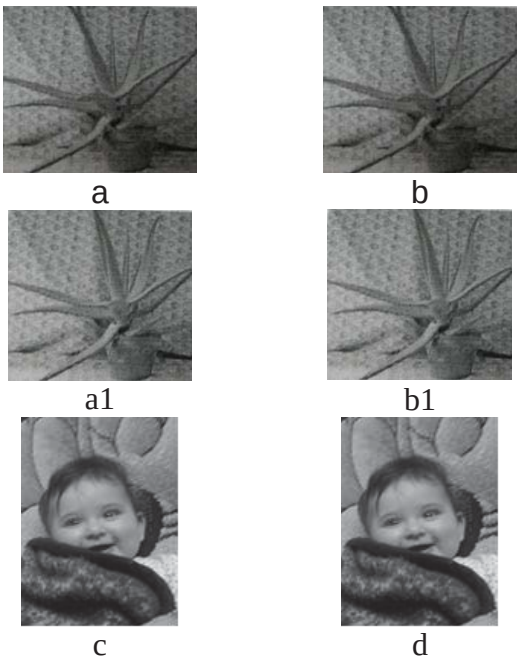
Experimental Results

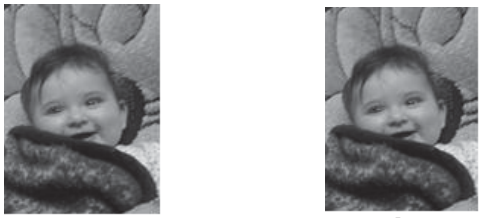
This section explains the experiments which have been implemented on two stereo images, Aloe and child image from personal camera as test images, each one of them is in size of 256*256 and of JPEG format. MATLAB version 7.4.0.287 (R2012a) was used as a work environment to carry out these experiments. The decoded left and right images were compared with the original left and right images. The Mean Square Error (MSE) between the original and decoded left and right images was referred in Equation 2. The MSE of the image is the average of the MSE of the left image and the MSE of the right image.

$$MSE=(MSE_L+MSE_R)/2 \qquad (3)$$

The MSE was converted into Peak-Signal to Noise Ratio according in the Equation (1)

Results for Aloe and Child Images





c1 d1

Figure 4: (a), (b), (c) and (d) Original Left and Right Images. (a1), (b1), (c1) and (d1) Reconstructed Left and Right Images.

Table1: Results for Stereo Images.

Images	PSNR (db)	CR	Time (sec)
Aloe	45.32	0.566	50.32
Child	47.45	0.6.98	59.44

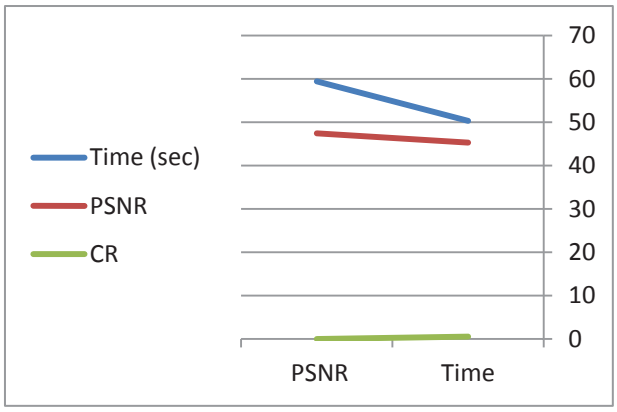


Figure 5: PSNR vs Bitrate for Stereo Images.

Conclusions

Pair stereo images in this research through phases are, DCT, quantization, arithmetic encoding and OSA was proposed in this paper with advanced encryption standard in the encryption step. The two images are very similar to each other; disparity vectors between the two images are estimated in OSA. The resulting disparity vector and image compressed are encryption byAdvanced Encryption Standard (AES). Two pairs of images were encrypted after being compressed them and then reconstructed by reversing the steps followed to encrypt and compress the images.

The proposed partial encryption schemes are fast, secure and do not reduce the compression performance of the underlying compression selected methods. The proposed algorithms contain high level of security due to the size of the keyspace. A good image encryption algorithm should be sensitive to the cipher key and PSNR which are good as shown in Table 1.

The reconstructed images were then compared with the original images.

References

[1] Karthik A., Chandra S. and Das S. ,"3D Tool Wear Measurement and Visualization Using Stereo Imaging" in International Journal of Machine Tools and Manufacture, pp 1531-1522, 2005.

[2] Beil W. and Carlsen I., "Surface reconstruction from stereoscopy and "shape from shading" in SEM images in Machine Vision and Applications, pp281-295, 2010.

[3] Shi Q. and Sun H., "Image and Video Compression for Multimedia Engineering", 2000.

[4] Turaga D., Alkanhal M. ," Search of Block Matching Algorithms in Motion Estimation", International Journal of advanced Science and Technology, Vol.32, July, 2011.

[5] Wang Y., OstermannJ. ,"Video Processing and Communications", Prentice Hall, Upper Saddle River, 2001.

[6] Fisch M. M., Stgner H., Uhl A., "Layered Encryption Techniques for DCT-Coded Visual Data", In Proceedings (CD-ROM) of the European Signal Processing Conference, EUSIPCO '04, Vienna, Austria, September 2004.

[7] SahaS. ,"Image Compression-From DCT to Wavelet: A Review", ACM Crossroads Student Magazine, The ACM's First Electronic Publication, 2001.

[8] Salomon D., "Data Compression" second edition, 2002.

[9] Watson J., "Image Compression Using Discrete Cosine Transform" Mathematic journal, 2007.

[10] *Hameed A. Y., "*New Techniques for Partial Encryptionof Wavelet-based Compressed, May 2012.

[11] Beegan A. P., "Wavelet-based Image Compression Using Human Visual System Models" M. Sc. Thesis, Electrical Engineering Department, Virginia Polytechnic

Institute and State University, Blacksburg, Virginia, May 2001.

[12] Marwa K., "Video Compression by Wavelet Technique", M. Sc. Thesis, *Department of Information Systems, College of Computer Sciences and Information Technology, University of Basrah, IRAQ*, April 2013.