Stereo Images Encryption by OSA & RSA Algorithms

IOP Conf. Series: Journal of Physics: Conf. Series **1279** (2019) 012045 doi:10.1088/1742-6596/1279/1/012045

Stereo Images Encryption by OSA & RSA Algorithms

Asaad A. Alhijaj and Marwah Kamil Hussein

University of Basra, Basra, Iraq

lava85k@gmail.com

Abstract: The proposed new partial encryption schemes use a secure encryption algorithm to encrypt only part of the compressed data. After application of image compression algorithm the partial encryption will applied. For two pairs of different gray scale images with the size (256 ´ 256) pixels, only 0.0244%-25% of the original data is encrypted. 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 RSA algorithm. The decoded images then compared with the original images.Good results showed in the experimental results of Peak Signal-to-Noise Ratio (PSNR), Compression Ratio (CR) and processing time. The proposed schemes of partial encryption are fast, secure and not be reducing in compression performance of the selected compression methods.

.

1 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 techniques and encryption algorithms together to reduce the total processing time.

In this research, the pair images selected from stereo images are fully similar to each other which taken from different angles (for this reason 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 two images differences. Disparity estimation (or match accounting), then squeeze one of the images independently. This is called as image as a reference, and can either be the right or left image, then use the disparity vector and reference image to rebuild the second image [1]. Figure 1 shows flowchart of 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). Scalar quantization used for the resulting image and then compressed using arithmetic coding; we show that in Section III. The two images are fully similar to each other; disparity vectors are estimated between the two images. The compressed image and resulting disparity vector are encryption by RSA algorithm. We show that in Section IV. Section V gives the experimental results. Finally, the paper has been concluded in Section VI.

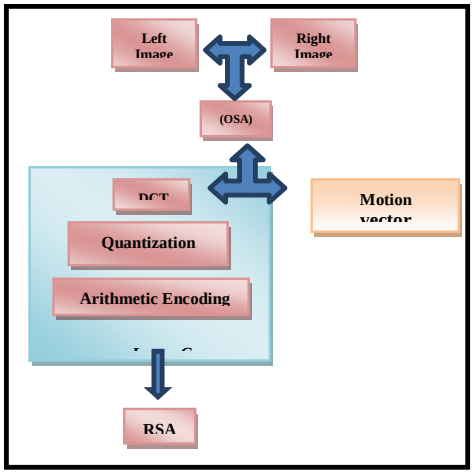


Figure1: Encryption a pair of stereo images after Compressed Using RSA algorithm.

2. Related Work

DAN Boneh, Glenn Durfee, and Yair Frankel [2] we show that for law public exponent RSA, given a quarter of the bits of the private key an adversary can recover the entire private key. Similar results are obtained for larger values of e. For instance, when e is prime in the range [$N^{-1/4}$,$N^{-1/2}$], half the bits of the private key suffice to reconstruct the entire private key. Our results point out the danger of partial key exposure in the RSA public key system. [3] used the algorithm SDA in working , In the compression step. The image compressed was encrypted by permutation techniques. The images were then decoded and were compared with the original images.

3 Motion Estimation

Analyzing process of successive frames of any image sequence for identify objects motion is called Motion Estimation (ME). This paper use motion estimation to process of analyzing two stereo images by using OSA.[3].

3.1 Disparity Estimation Using Orthogonal Search Algorithm (OSA)

OSA
was introduced by Puri. The search for the optimal block in two stages; a vertical stage followed by a horizontal stage. The algorithm described in following three steps:

1. Pick a step_size (in the search window step size= maximum displacement/2).
   a. Take 2 points at a distance of step size in the horizontal direction from the center of the search window.
   b. Locate the point of minimum distortion.
   c. Move the center to this point.
2. Take 2 points at a distance step_size from the center in the vertical direction and find the point with the minimum distortion.
3. If (step size is greater than one) Halve the step_ size, Else halt.

The following Fig.2, showing a particular path for the convergence of the algorithm:

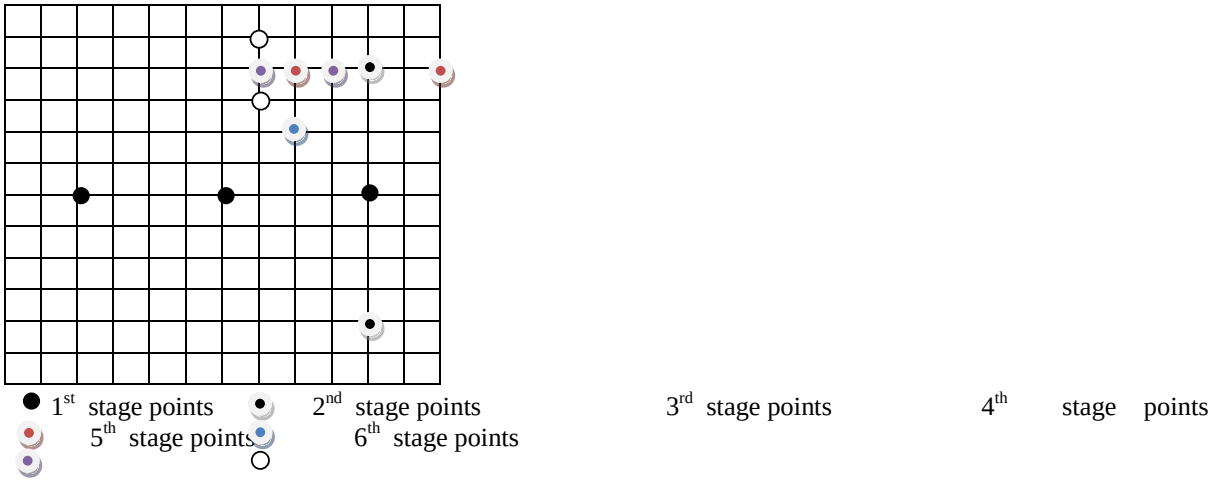


Fig.2: Example of Orthogonal Search Algorithm.

3.2 Image Transformation

The source image divided into blocks and applies the transformations to the blocks [4].

3.3 Parameter Quantization

Quantization is irreversible operation because of its loss property. To reduce the amount of information, the data generated by the transformation must be quantized. In this step the information represented within the new domain by reducing the amount of data [5].

3.4 Arithmetic Encoding

Overcome some of the limitations of Huffman codes, require to use the arithmetic encoding with its derivative technique; Q-coding. To represent an entire sequence of input symbols, via this non-block code, a single code word is used, in associate to Huffman coding where a source symbol block matches to a code word block. Instead of that, the real numbers is used to represent a sequence of symbols. The interval between 0 and 1 subdivided recursively to specify each successive symbol. This technique has limitation in the precision needed to perform the calculations and arriving at the code word which will correctly represent the entire sequence.

4 Partial Encryption

A secure encryption algorithm; ***partial encryption*** (also known *soft encryption* or *selective encryption*) is used to encrypt only part of the data. The algorithm used to reduce the time of encryption and decryption. There are *important parts* in some compression algorithms which provide a significant amount of information about the original data. The *remaining parts* may not provide enough information without the *important parts*. We consider that all the important parts as one unit and grouping part all remaining parts into one unimportant. Partial encryption approach encrypts only the important part because the difficulty to obtain information from the unimportant part alone. A significant reduction in encryption and decryption time is achieved when the size of the relative important part is small.

In some cases, the encryption time becomes negligible because the partial encryption allows in parallel, to encrypt the important part while the unimportant part is transmitted [6]. So that, we use secure encryption algorithm to encrypt the important part.

4.1 RSA Cipher

RSA cipher was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman (Computer Science and Mathematics Department of MIT Laboratory), the Initials of their names are the RSA characters. In 1973, a mathematician Clifford Cox, (GCHQ in UK intelligence agency), in an internal document suggest an equivalent cipher system. This system was considered only curious, and has never been published, because the computers needed to implement that relatively system was very expensive at the time. But this discovery was

not bringing to light until 1997 because of his highly classified classification. Rivest, Shamir and Adelman inherited or completed their RSA algorithm from Clifford Cox [7].
RSA Encryption and Decryption algorithm for gray image.

1. Read the grayscale of digital image file.

To open or read an image from a computer as follows:

```
X= imread (filename, format);
Imshow (X);
```

Where the filename is read with the format and then stored in the X matrix.

2. To find two relatively large initial numbers that are difficult to predict: P, Q.
3. We find the product of the first two numbers.
   N=P*Q
4- Find the value of the ∅ word which is:
   ∅ = (P-1) (q-1)
5. Suppose the value of the public key is e so that:
   1 < e < ∅
6. Calculate the private key, d, value :
   e * d mod ∅ = 1

So we have the value of the public key {e, n}
The value of the private key {d, n}.
7. We apply the coding equation
   C = 〖 p〗 ^ (e) mod N where e is the public key
8. Then decrypt the equation with the following inverse equation: $P = c \wedge d \ mod \ N$ where d is the private key.

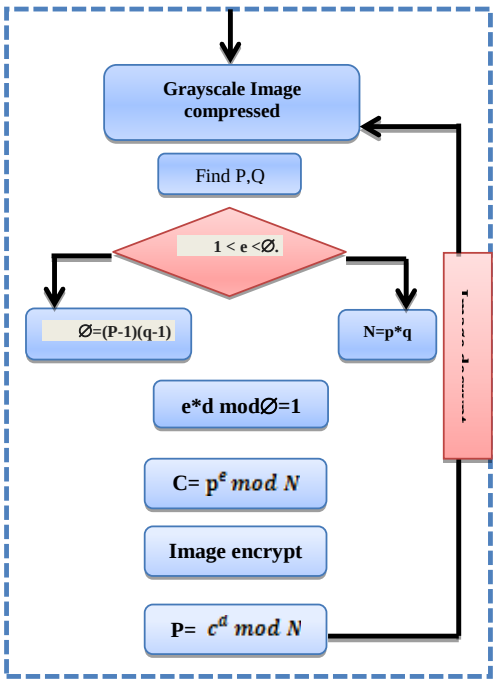


Figure 3: RSA Encryption and Decryption Steps

4.2 PSNR and CR
For quantitatively comparing a compressed image with the original, the standard method is Peak Signal-to-Noise Ratio (PSNR). The value of peak signal is 255 for an 8-bit grayscale image. Therefore, for M×N 8-bit grayscale image C_{ij} and its reconstruction R_{ij} the PSNR is calculated as [8]:

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

where the Mean Square Error (MSE) is defined as [8]:

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

PSNR is measured in decibels (dB), where *m: height* and *n: width* of the image.

5 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 images were compared with the original images, left with left and right with right. In Equ. (2), we referred to MSE between the decoded and original left and right images. The average of the MSE of the left image MSE_L and the MSE of the right image MSE_R is the MSE of the image.

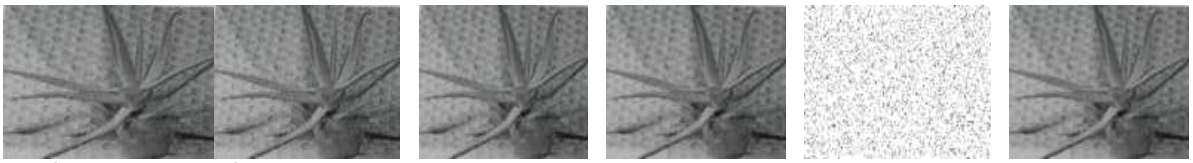
$$MSE=(MSE_L+MSE_R)/2 \quad \ldots(3)$$

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

5.1 Results for Aloe and Child Images

(a)Left and Right Stereo of Images1 (b) OSA Result (c) Image Compressed (d) Encrypt by RSA (e) Reconstructed Image

Figure 4: Results for Stereo of Images1



(a)Left and Right Stereo of Images1 (b) OSA Result (c) Image Compressed (d) Encrypt by RSA (e) Reconstructed Image

Figure 5: Results for Stereo of Images2

(a)Left and Right Stereo of Images3. (b) OSA Result (c) Image Compressed (d) Encrypt by RSA (e)Reconstructed Image

Figure 6: Results for Stereo of Images3.

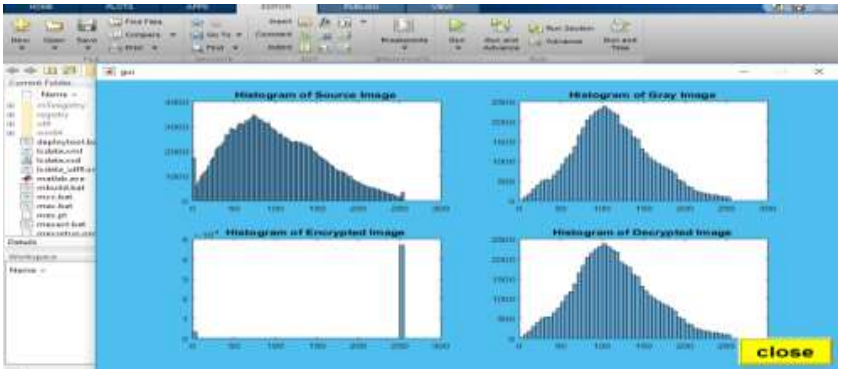


Figure 7: Histogram for Stereo of Images1

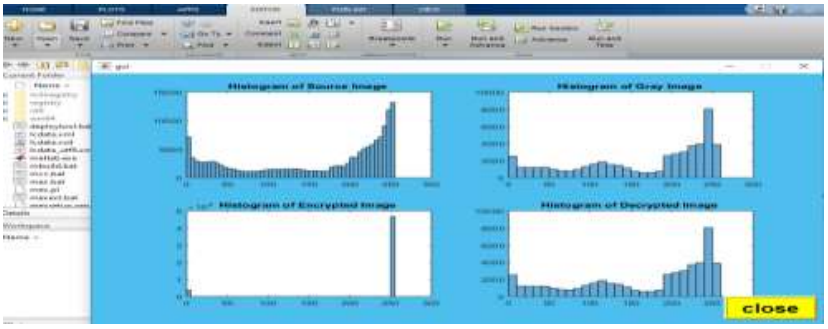


Figure 8: Histogram for Stereo of Images2.

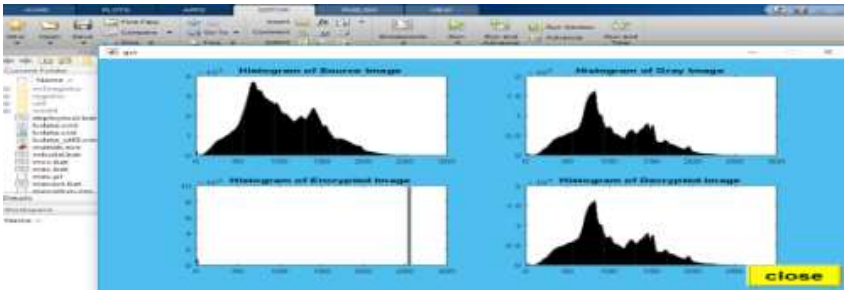


Figure 9: Histogram for Stereo of Images2.

Table1: Results for Stereo Images

Images	PSNR (db)	CR	Time (sec)
Image1	45.32	0.566	50.32
Image2	47.45	0.698	59.44
Image3	47.55	0.799	59.49

6 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 closing similar each other, and disparity vectors between the two images are estimated in OSA. The resulting disparity vector and compressed image are encrypted by RSA. Two pairs of images were encrypted after being compressed them and then reconstructed by reversing the steps followed to compress and encrypt the images.
The proposed schemes of partial encryption are fast, secure and not be reducing the compression performance of the selected compression methods. The proposed algorithms include a high level security through the size of the key space. A good algorithm of image encryption should be sensitive to the cipher key and PSNR which are good as shown in Table (1). Finally, compares the reconstructed images with the original images.

References

[1] H. Hirschmuller and D. Scharstein, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 9, pp. 1582–1599, 2009.
[2] M. Kamil H., International Journal of Computer Science and Mobile Computing, Vol.5, No. 12, PP. 150-159, Indian, December 2016.
[3] S. Sahu, J. Singh, and J. Ashraf,
[4] M. Kamil H. A. Jaber J., Al-Mustansiriyah Journal of Science, Volume 28, Issue 2, 2017DOI: http://doi.org/10.23851/mjs.v28i2.511.
[5] R. L. Joshi, V. J. Crump, and T. R. Fischer, *IEEE Trans. Circuits Syst. Video Technol.*, vol. 5, no. 6, pp. 515–523, 1995.
[6] L. Tang, in *Proceedings of the fourth ACM international conference on Multimedia*, 1997, pp. 219–229.
[7] H. Cheng and X. Li, *IEEE Trans. signal Process.*, vol. 48, no. 8, pp. 2439–2451, 2000.
[8] V. V. Yap, Middlesex University, 2005.