Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 12, December 2016, pg.150 – 159

Encryption of Stereo Images after Estimated the Motion Using Spatially Dependent Algorithms

Marwah Kamil Hussien
Assistant Lecturer
Lava_85K@yahoo.co.uk
Lava85k@gmail.com
Department of Information Systems, College of Computer Sciences and Information Technology, University of Basrah, Basrah, IRAQ

Abstract: ***Recent researches of Modern images encryption algorithms have been increasingly based on permutations systems, so information security is becoming more important in data storage and transmission, Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access.***

This paper focuses mainly on the different kinds of image encryption techniques after estimated the different (the motion) between of stereo images using Spatially Dependent Algorithm. As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time to encrypt the images to make images more secure.

In this paper, a survey of different image encryption techniques that existing is given. It additionally focuses on the functionality of permutation techniques. Firstly we were estimating the disparity between them by Spatially Dependent algorithms (for the purpose of reducing the size of stored image memory). The resulting disparity vector and the remaining image were divided into several parts in order to obtain each part alone , then we change arrange of these parts based on secure key (encryption key) , finally we encrypt these parts by using merge technique.

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.

Keywords: Stereo imaging, stereo image compression, Permutation Systems, Image Encryption, Image Decryption.

1. Introduction

Recent researches of modern images encryption algorithms have been increasingly based on permutations systems, so information security is becoming more important in data storage and transmission, Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access.

This paper focuses mainly on the different kinds of image encryption techniques. As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques which are discovered from time to time to encrypt the images to make images more secure [1],[2].

In this paper, a survey of different image encryption techniques that existing is given. It additionally focuses on the functionality of permutation techniques. Firstly we were estimating the disparity between them by Spatially

Dependent algorithms. The resulting disparity vector and the remaining image were divided into several parts in order to obtain each part alone , then we change arrange of these parts based on secure key (encryption key) , finally we encrypt these parts by using merge technique, As show in Fig.1 .

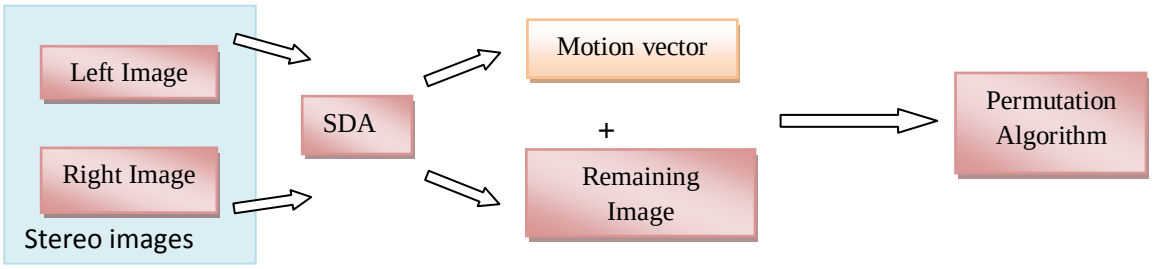


Fig.1: Encryption a Pair of Stereo Images after Compressed.

2. Motion Estimation

Motion Estimation (ME) is the process of analyzing successive frames in a video sequence to identify objects motion. In this paper, motion estimation used to process of analyzing two stereo images by using spatially dependent algorithms.

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].

2.1 Disparity Estimation Using Spatially Dependent Algorithm (SDA)

Spatially dependency checks the correlation between the motion vectors of neighboring blocks to provide a prediction to the previous matching algorithms. Frequently the prediction is formed by taking a weighted average of the neighboring motion vectors. A typical block has eight immediate neighbors. Depending on the order in which target blocks are matched, the motion vectors for some of these neighbors might not been available when a block is being matched [4].

The hierarchical solution used in the previous section has been modified by adding an additional candidate in level 2 based on spatial correlation. In this paper, it was suggested to calculate the spatially dependent motion vector from neighboring motion vectors. Let MVC be the motion vector of the current block, and MV1,MV2 and MV3 be the motion vectors of the neighboring blocks.

To estimate MVC, The motion vectors of the neighboring are examined and find a proper a group out of five groups given in Fig.2. Then the corresponding shaded block motion vectors are averaged and down-scaled to obtain an estimate of MVC, which is the third candidate beside the other candidates that were driven using the previous algorithm. In the case of group E where no motion similar motion vectors exist, (0,0) is selected as the estimate.

Here, e1=ll MV1-MV2 ll, e2= ll MV2-MV3 ll, and e3= ll MV3-MV1 ll, and D is threshold value to examine similarity between the two MVs. A value of 8 for D has been used in our simulations based on this paper.

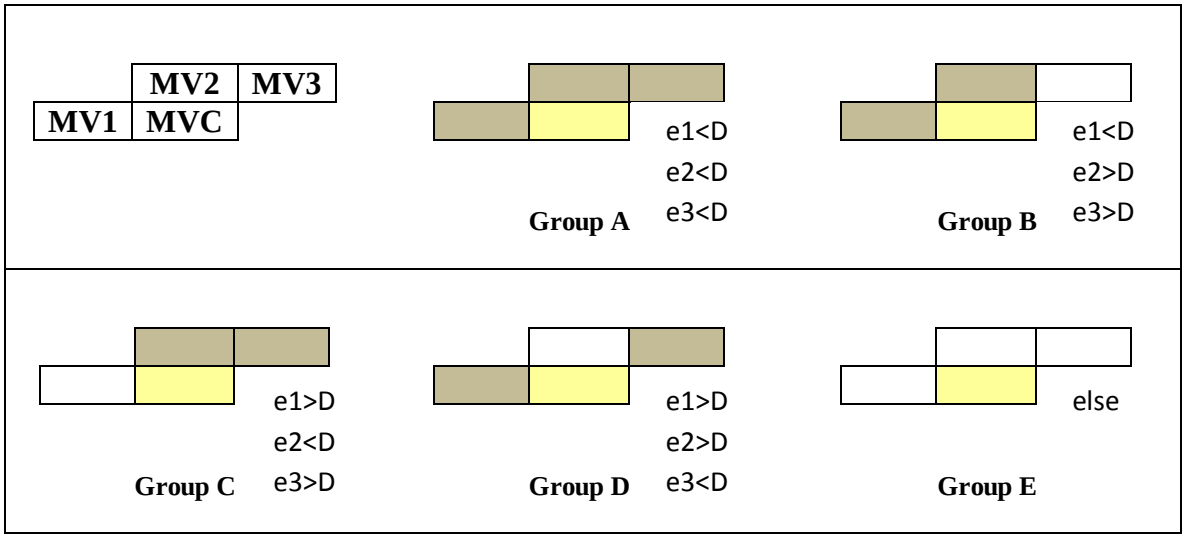


Fig.2: Grouping of Similar Neighboring Motion Vectors (MVs) to Predicate MVC.

3. Permutation Algorithm

The image encryption process consists of three processing:-

1. At first selects image of n*n size (Fig.3). This image is split into number of blocks (we chose 9 in this paper) and numbered (Fig.4). These numbered blocks are changing its arrange using one of Hash or random key ;therefore; the Each sub block is further shuffled as in (Fig.5) .That called Permutation algorithm. A random number is selected which lies in the range of 1 to 9, These rows and columns of the total images are shifted based on the random number that is selected. (in our paper we use the key as the following :-

Number of blokes= [1,2,3,4,5,6,7,8,9]

Key= [4,9,2,6,5,1,7,8,3]

That is mean the bloke(4) in Cipher image is the bloke (1) in Original image, and the bloke (9) is the bloke(2) ,…ect,

Fig.3: The Original Image.

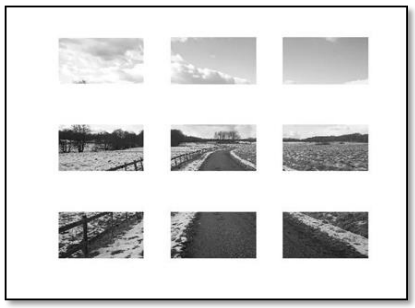


Fig.4: The Image after Clipping

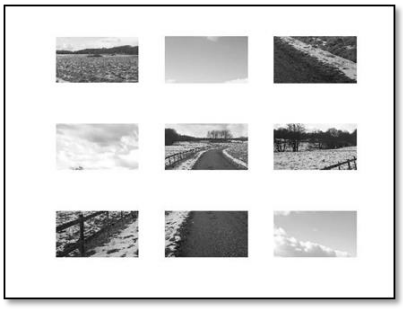


Fig.5: The Image after Permutation

2. To bring about confusion and diffusion in the encryption process each pixel element influences the next row of pixels. Due to this even a slight change in the pixel value results large changes in the cipher image. The encryption takes place in the encryption key by rotating it periodically. Moreover, after the image is divided into nine planes, we added in this stage a little of confusion to make code broken operation is more difficult. We added every two parts and put it in one for example:-

Part1+Part2→ Part1

Part2+Part3→ Part2

…

Part9+Part1→Part9

And the result after this operation is shown in (Fig.6).

Fig.6: The Image after Confusion

Then we returned it one image after this stage to be one bloke as in (Fig.7).

Fig.7: The Image after Combination

3. This is the final stage in encryption , we used the same secret key to change the value of image elements , The key generation algorithm, is randomized. It takes no inputs. When it is run, it flips coins internally and uses these to select a key K. Typically, the key is just a random string of some length, in which case this length is called the key length of the scheme. In this point we Collect key values (4+9+2+6+5+1+7+8+3=45), this value is adding to the image value as in the following equation :-

$$Img=(Img+45) \bmod 225 \quad \ldots (1)$$

We calculate the reminder because the rang of gray image as known 0-255.

The resulting image is cipher as in (Fig.8). [5],[6],[7],[8]

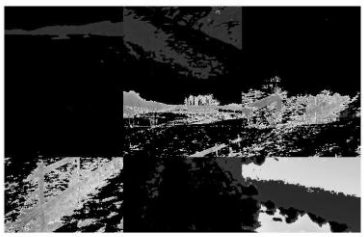


Fig.8: The Cipher Image

B. Decryption Algorithm

The process of decryption involves obtaining the key that is generated and the shares. Once the identification process is done the permutation information and the random number from the key is obtained to implement the inverse of the permutations to reveal the secret. So this phase consider as the inverse of Encryption, we applied the pervious operation on the cipher image to obtain the original image [9],[10],[11].

2.6 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 [12],[13]:

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

where the Mean Square Error (MSE) is defined as [10]:

$$MSE = \frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left[C_{ij}(m,n) - R_{ij}(m,n)\right]^2 \quad \ldots (3)$$

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

4. Experimental Results

This section explains the experiments which have been implemented on two stereo images, each one of them is in size of 256*256 and of QCIF format. MATLAB version 7.4.0.287 (R2007a) 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 Equ. (3). The MSE of the image is the average of the MSE of the left image and the MSE of the right image.

$$MSE = (MSE_L + MSE_R) / 2 \quad \ldots..(4)$$

The MSE was converted into Peak-Signal to Noise Ratio according in the Equ. (2)

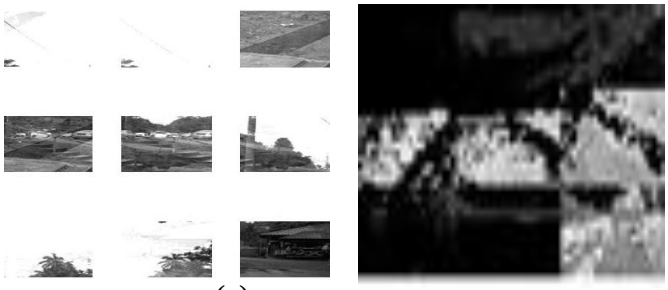
4.1 Results

(a)

(b)

(c)

(d)



(e) (f)

(g) (h)

Fig.9: (a) and (b) Original Left and Right Images.
(c) The image after clipping. (d)The image after permutation
(e) The Image after combination. (f) The cipher image.
(g) and (h) Reconstructed Left and Right images.

Table1: Data for Image.

Quality	Total Size (kb)	Bitrate	PSNR (db)
30	106623	0.432	32.222
40	126190	0.522	33.321
50	143952	0.643	34.411

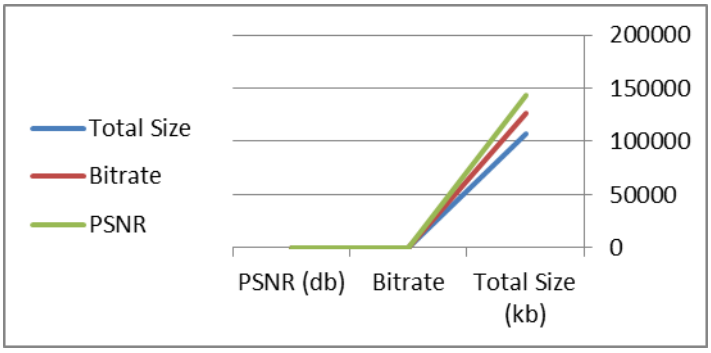


Fig.10: PSNR vs Bitrate for Image.

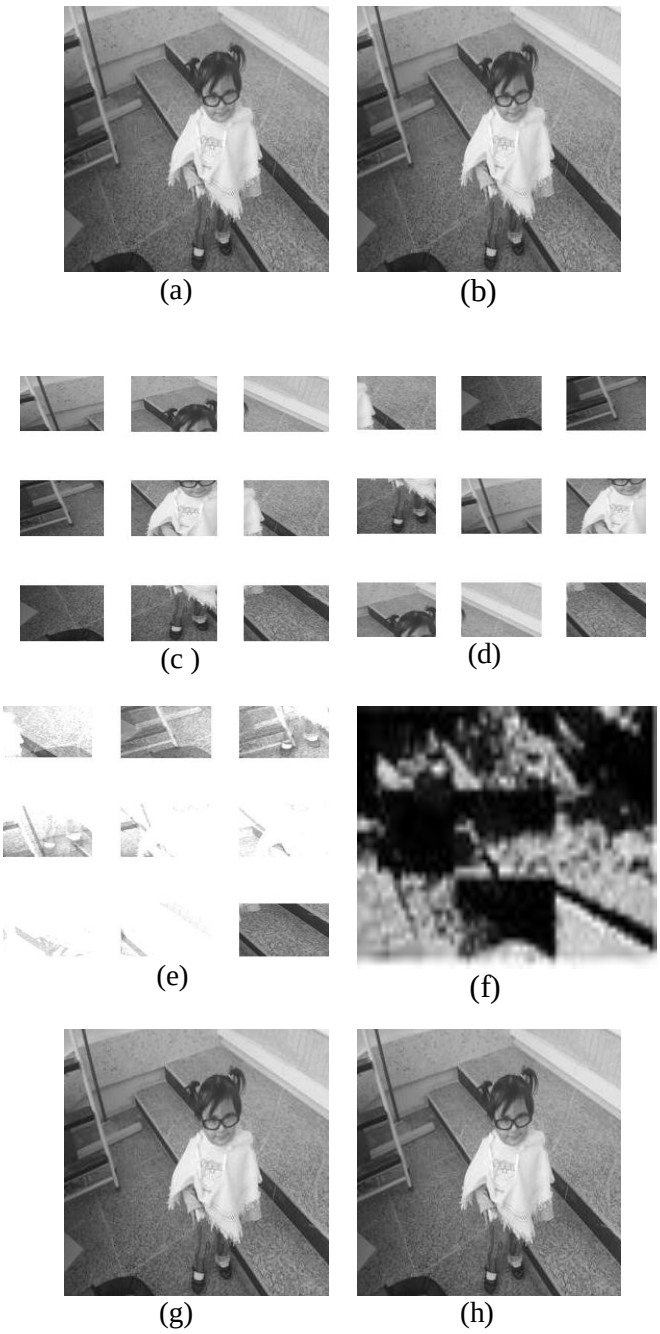


Fig.11: (a) and (b) Original Left and Right Images.
(c) The image after clipping. (d)The image after permutation
(e) The Image after combination. (f) The cipher image.
(g) and (h) Reconstructed Left and Right images.

Table 2: Data for Image.

Quality	Total Size (kb)	Bitrate	PSNR (db)
30	823115	0.367	31.302
40	108673	0.477	32.421
50	100243	0.543	32.981

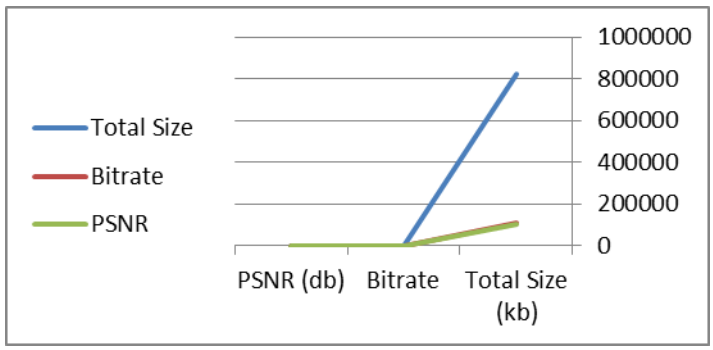


Fig.12: PSNR vs Bitrate for Image.

5. Conclusions

A method for matching of stereo images is spatially dependent algorithm to reduce the number of images, then encryption the results by Permutation Cipher.

The reconstructed images were compared with the original images.

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data Now, in order to achieve these goals various cryptographic algorithms are developed by various people. We must ensure the image or the details be secure and protect to prevent the authorize person to know or to change the information.

Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm. But as public key cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper. All the techniques are useful for Real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. Newly proposed image encryption techniques and also enhance the security level by introducing more than one scheme for image encryption algorithms. A new algorithm for encrypting gray images was also analyzed.

References

[1]. Patel D., Belani S. (November 2011). Image Encryption Using Different Techniques. (ISSN 2250-2459, Volume 1, Issue 1).
[2]. Krishnan K., (Mar 8-11 2004), Computer Networks and Computer Security.
[3]. Turaga D., Alkanhal M., ” Search of Block Matching Algorithms in Motion Estimation”, International Journal of advanced Science and Technology, Vol. 32, July, 2011.
[4]. Beil W. and Carlsen I., “ Surface reconstruction from stereoscopy and “shape from shading” in SEM images in Machine Vision and Applications, pp281-295, 2010.
[5]. Indrakanti S. P., Avadhani P.S. ,(August 2011) Permutation based Image Encryption Technique (Volume 28– No.8).
[6]. Ayushi,(2010), A Symmetric Key cryptographic algorithm, Volume 1 – No. 15.
[7]. Nandeesh G.S. , Vijaya[2] P.A., Sathyanarayana[3] M.V. , (May 2013), An Image Encryption Using Bit Level Permutation And Dependent Diffusion.
[8]. Dixit A., Dhruve P.k. , Bhagwan D.,(1-9-2012), Image Encryption Using Permutation And Rotational Xor Technique.

[9]. Sakthidasan K., Krishna B. V. Santhosh,(June 2011) , A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images, Vol. 1, No. 2.

[10]. Acharya B., Panigrahy S., Patra S., Panda G.,(Jan 2010), Image Encryption Using Advanced Hill Cipher Algorithm , Vol 1, No. 1.

[11]. Abdulla S. , (April 2010), New Visual Cryptography Algorithm For Colored Image, VOLUME 2, ISSUE 4, ISSN 2151-9617.

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

[13]. 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.

