Vol. 5(16) Apr. 2015, PP. 2169-2174

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

A new approach for gray scale image encryption by random grids

J. Vahidi[1,*], M. Riyahi[2] and R. Motevalli[3]

[1]*Department of Mathematics, Iran University of Science and Technology, Tehran, Iran*
[2]*Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran*
[3]*Department of Computer Science, Sari branch, Islamic Azad University, Sari, Iran*

***Corresponding Author's E-mail:** jvahidi@iust.ac.ir

Abstract

A random grid is a two-dimensional array of pixels that are either transparent or opaque. Each pixel in a random grid is produced in a totally random way. In this paper, a new algorithm is designed to carry out the encryption of the gray scale images by using random grids in such way that neither of two shares gives any especial information of original image. The original image can be recognized only when two encrypted shares are combined by XOR operation. In this approach, against others, bit planes are used instead of half toning techniques and also gray scale level will remain after decryption process in decrypted image.

Keywords: *Image encryption, Random Grids, Bit plane*

1. Introduction

With increasing in computer networks, and also, prevalence of multimedia technology, digital images have more important rule than text data. According to these new technologies, image encryption for protecting of digital image from illegal access, has been became one of important issues for many researchers. To fulfill this aim, numerous approaches have been published that one of most important approaches among them is visual secret scheme. Visual secret scheme is divided into two groups: Visual cryptography and Random Grids.

The first idea for image encryption based on visual secrete scheme, was introduces by Kafri and Keren in 1987 [3]. They named their approach Random Grids. In this approach, the binary image is encrypted into two independent random grids that do not show any especial details about origin image. The decrypted image is reconstructed when these two random grids are superimposed together. The striking feature of the approach is that, it does not need any computation in the decryption process because this process is done by human visual system. Later, because of the benefit of visual secrete scheme that does not need to any digital computation, Naor and Shamir introduced their approach that was named visual cryptography, in 1995 [2]. In introduced approach by Naor and Shamir, a binary image is encoded into two shares and the origin image can't be seen unless these two shares are stacked together. Despite of benefits of Naor and Shamir approach, it has two main weak points in comparison with random grids. Firstly, it needs basis matrices and secondly, in this approach the size of decrypted image is increased. This paper is organized as follows: an introduction of random grids and main related researches, are introduces in section 2. Section 3 contains proposed algorithm for encrypting gray-scale images. The results are shown in section 4 and finally, conclusion is proposed in section 5.

Article History:
Received Date: Dec. 04, 2014
Accepted Date: Mar. 19, 2015
Available Online: Apr. 14, 2015

2. Related Works

As it was said before, binary image encryption by random grids was defined by Kafri and Keren in 1987. In fact, each random grid is a two-dimensional array of pixels which each pixel can be either completely dark or completely bright. The process of selecting the darkness and brightness for each pixel, in random grids, is randomly. Consequently, there is no correlation between the values of different pixels in each random grid [3]. For binary image encryption by random grids, three algorithms were introduced by Kafri and Keren. Each introduced algorithms by Kafri and Keren generates two random grids such that don't show any information about original binary image. In decryption process, two produced random grids are superimposed together based on "OR" operation. Algorithms 1, 2, and 3 show the process of encrypting a binary image which introduced by Kafri and Keren.

Algorithm 1

1. Generate R_1 as Random Grid, $T(R_1) = 1/2$

   // for (each pixel $R_1[i, j], 1 \le i \le w, 1 \le j \le h$) do

   // $R_1[i, j] = \text{random\_pixel}(0,1)$

2. for (each pixel $B[i, j], 1 \le i \le w, 1 \le j \le h$) do

2.1 { if $(B[i, j] = 0)$ $R_2[i, j] = R_1[i, j]$

   else $R_2[i, j] = \overline{R_1[i, j]}$

   }

3. output (R_1, R_2)

Algorithm 2

1. Generate R_1 as Random Grid, $T(R_1) = 1/2$

   for (each pixel $B[i, j], 1 \le i \le w, 1 \le j \le h$) do

2 { if $(B[i, j] = 0)$ $R_2[i, j] = R_1[i, j]$

   else $R_2[i, j] = \text{random\_pixel}(0,1)$

   }

3. output (R_1, R_2)

Algorithm 3

1. Generate R_1 as Random Grid, $T(R_1) = 1/2$

   for (each pixel $B[i, j], 1 \le i \le w, 1 \le j \le h$) do

2 { if $(B[i, j] = 0)$ $R_2[i, j] = \text{random\_pixel}(0,1)$

   else $R_2[i, j] = \overline{R_1[i, j]}$

   }

3. output (R_1, R_2)

Note that in above algorithms, B is the origin image, R_1 and R_2 are two random grids, and Random_pixel(0,1) is a function that returns a binary value 0 or 1 by random process which 0 means

the pixel is bright and 1 shows the pixel is dark. Also, $\overline{R_1(i,j)}$ denotes the inverse of $R_1(i,j)$. For more information about introduced algorithms, please see reference [3].

In 2007, a new approach for gray-scale images and color images was presented based on Kafri and Keren's algorithms by Shyong Jian Shyu [7]. The main idea in Shyu's approach is that gray-scale images and also color images be transformed into equivalent black and white images. For transferring images into black and white, halftoning techniques are used. In this approach, to encrypt the gray-scale images, firstly, the origin image is transformed into halftone image by Error diffusion algorithm [1,5], and in the next step, the result image is encrypted by Kafri and Keren's algorithms. In Shyu's approach, for encrypting color images, the image is decomposed into three primarily color components at first. Then, each primarily image is encrypted by encryption ability of gray-scale images.

To improve Kafri and Keren's approach, a new approach was introduced by Kumar and Sharma, in 2012 [4]. In fact, with changing the decryption process, the quality of the decrypted image is increased. As it said, the OR was used in decryption process in Kafri and Keren's approach while in Kumar and Sharma's approach, for improving the quality of recomposed image, XOR is used. Also, other approaches were introduced using random grids for encrypting different kind of images [8, 9, 10, 11].

3. Proposed Algorithm

According to previous researches, different gray-scale image encryption methods based on random grids have been used halftoning techniques. The considerable weak point of using halftoning techniques is that, by transforming the gray-scale image into halftoning image, some main details of origin image will be removed. With regard to this point that the main aim of all different approaches in this subject is increasing the quality of the decrypted image, in this paper a new approach is designed based on bit plan technique for encrypting gray-scale images. In fact, bit planes are eight binary images that with combine all of them the original gray-scale image will be produced [6]. Algorithm 4 shows process of the proposed algorithm. Encryption and decryption process are descripted separately in sub-sections 3.1 and 3.2.

3.1. Encryption process

This process is composed of four phases. The first phase is decomposition phase. In this phase, the origin gray-scale image is decomposed to eight bit plane. In the second phase, that is selection phase, three valuable bit planes are selected. The valuable bit planes have more details of origin image. The third phase is encode phase. In this phase, each selected valuable bit plane is encrypted by algorithm 1. Finally, in the fourth phase or combination phase, six produced random grids in third phase are combined to create two gray-scale random grids. For creating the first gray-scale random grids, three first random grids are combined and also for creating the second one, other random grids are combined.

3.2. Decryption process

After encrypting the original gray-scale image, two random grids RG_1 and RG_2 will be sent on network. None particular information won't be explored of two gray-scale random grids. The decryption process is in reverse of encryption process. In this process, firstly, two gray-scale random grids RG_1 and RG_2 are decomposed to RG_{61}, RG_{62}, RG_{71}, RG_{72}, RG_{81}, and RG_{82}. Then, XOR operation is applied on (RG_{61}, RG_{62}), (RG_{71}, RG_{72}), and (RG_{81}, RG_{82}) for creating bit planes 6, 7, and 8. Finally, to create decrypted image, bit planes are combined.

Algorithm 4

Encryption phase

Decompose the gray-scale image

\\ Producing bit plane 1 to bit plane 8

Select valuable bit planes

\\ Bit planes 6, 7, and 8 are selected

Encode the valuable bit planes by algorithm 1

\\ Six random grids RG_{61}, RG_{62}, RG_{71}, RG_{72}, RG_{81}, and RG_{82} are produced

Create gray-scale random grids RG_1 and RG_2

\\ RG_1 is composed by combining RG_{61}, RG_{71}, and RG_{81}

\\ RG_2 is composed by combining RG_{62}, RG_{72}, and RG_{82}

Decryption phase

Decompose the gray-scale random grids RG_1 and RG_2

XOR pairs (RG_{61}, RG_{62}), (RG_{71}, RG_{72}), and (RG_{81}, RG_{82})

Combine bit planes 6, 7, and 8

4. Results

In this section, the result of implementation of proposed approach is shown. Figure 1 illustrates first phase of encryption process. In this figure, the origin gray-scale image is transformed to eight equal bit planes.

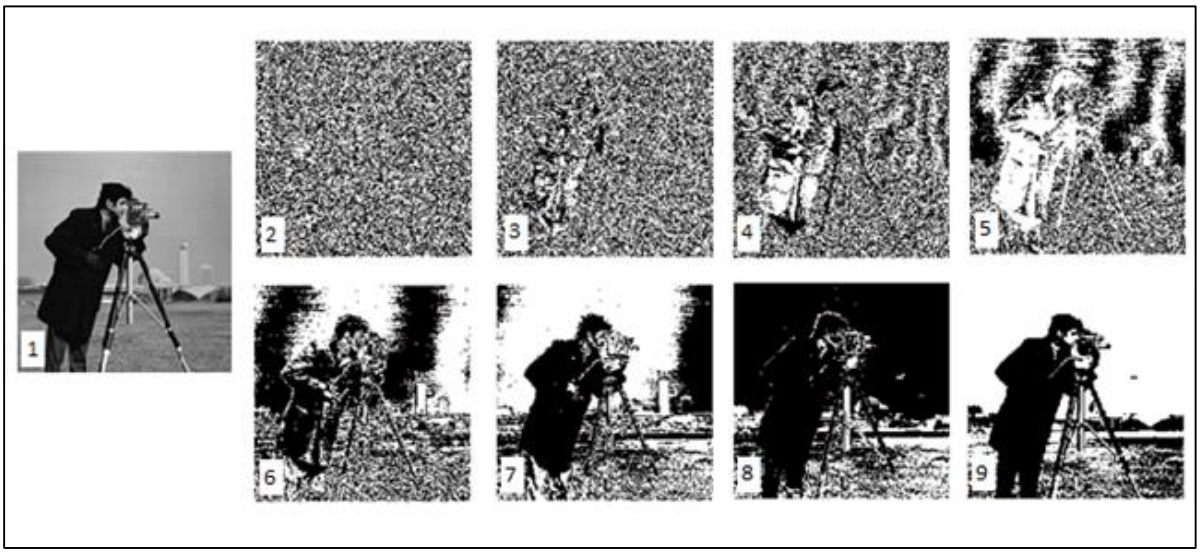

Fig.1. implementation results of phase 1: (1) origin image, and (2) to (9) eight equal bit planes

The result of implementation of phases 2 and 3 are shown in figure 2. In this figure, three valuable bit planes are selected, then, are encoded by algorithm 1. As it was said, the last phase of encryption process is combination six random grids. Figure 3 shows the result of implementation of this phase. As it can be seen, two gray-scale random grids are the outcome of this phase.

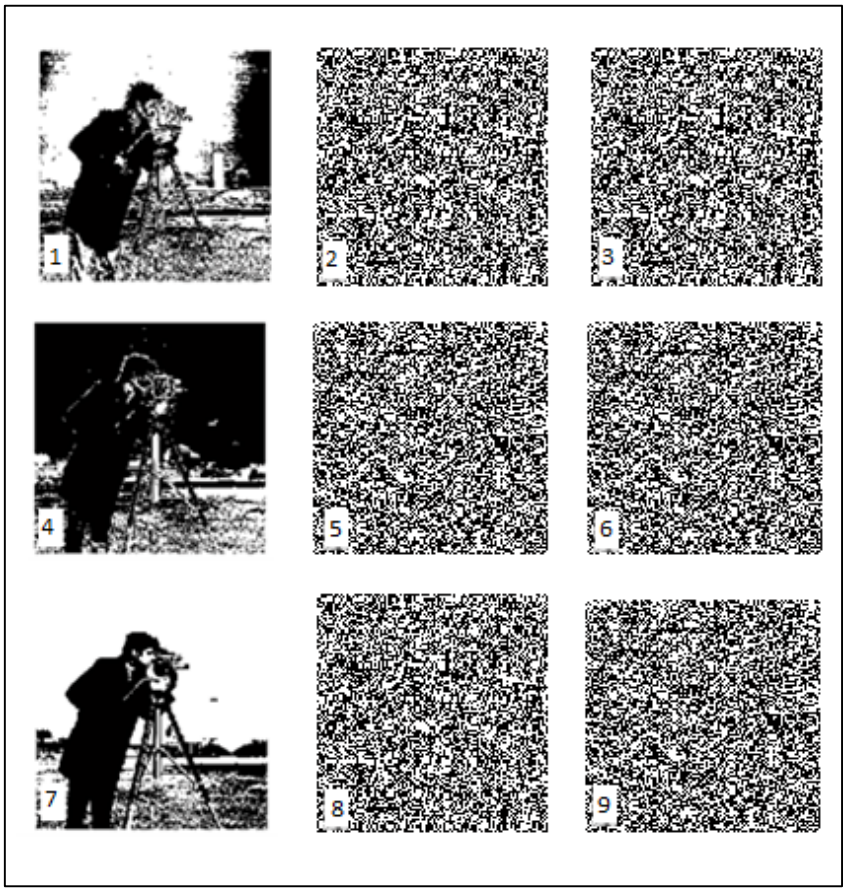

Fig.2. implementation results of phases 2, 3: (1) bit plane 6, (2) RG_{61}, (3) RG_{62}, (4) bit plane 7, (5) RG_{71}, (6) RG_{72}, (7) bit plane 8, (8) RG_{81}, and (9) RG_{82}

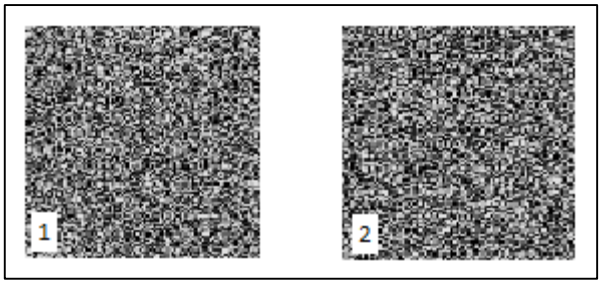

Fig.3. implementation results of combination phase: (1) RG_1, and (2) RG_2

In fact, RG_1 and RG_2 are sent on network and there is no information neither in RG_1 nor RG_2. Because of this reason, the proposed approach is secure. In fact, with regard to this point that in encryption phase, the first algorithm of Kafri and Keren is used, therefore the proposed algorithm has good security level.

In receiver side, firstly two gray-scale random grids are decomposed, then, valuable bit planes are recreated, and finally, the decrypted image is made by valuable bit planes. Figure 4 shows the reconstructed image. As it can be seen, due to the fact that decrypted image is gray-scale, it has good visual quality that it is a striking feature of proposed algorithm.

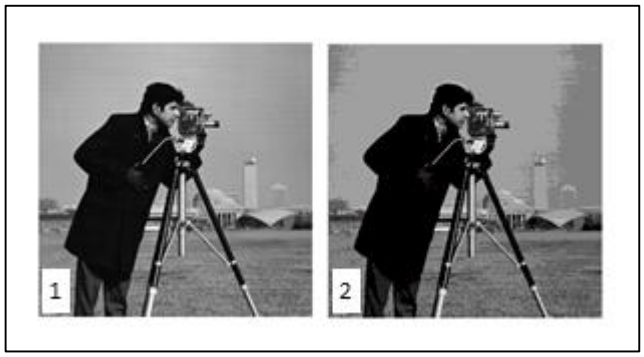

Fig.4. implementation of decryption process: (1) origin image, (2) reconstructed image

5. CONCLUSION

Many different approaches have been proposed for gray-scale image encryption by random grids. The reconstructed image in all algorithms is binary image; consequently, some important details of origin image are lost. For solving this problem, in this paper, a new approach is proposed based on bit plane theory that the constructed image is a gray-scale image and the visual similarity between origin and reconstructed image is high.

References

[1] A. K. Sahoo, “Development of digital halftoning techniques for gray scale image”, Thesis submitted to National institute of technology, Rourkela, 2014.

[2] M. Naor and A. Shamir, “Visual Cryptography”, in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, vol. 950, p.p. 1-12, 1995.

[3] O. Kafri and E. Keren, “Encryption of pictures and shapes by random Grids”, opt, vol. 12, p.p. 377-379, 1987.

[4] S. Kumar and R. K. Sharma, “Improving contrast in random grids based visual secret sharing”, international journal of security and its Application, vol.6, No.1, p.p. 9-27, 2012.

[5] S. Ekdemir and X. Wu, “Digital Halftoning”, Project report UPPSALA Universitet, 2011.

[6] S. Lian, "Multimedia Content Encryption: Techniques and Applications", Auerbach Publication, Taylor & Francis Group, 2008.

[7] S. J. Shyu, “Image encryption by random grids”, Journal of Pattern Recognition, vol. 40, p.p. 1014-1031, 2007.

[8] S. J. Shyu, “Image encryption by multiple random grids”, Journal of Pattern Recognition, vol. 42, p.p. 1582-1596, 2009.

[9] S. J. Shyu, “Visual cryptograms of random grids for threshold access structures”, Journal of Theoretical computer science, vol. 565, p.p. 30-49, 2015.

[10] T. Guo, F. Liu and C. Wu, “K out of K extended visual cryptography scheme by random grids”, Journal of Signal processing, vol. 94, p.p. 90-101, 2014.

[11] Y. C. Hou, Wei and C. Y. Lin, “Random-grids-based visual cryptography scheme”, Journal of Circuits and systems for video technology, vol. 24, p.p. 733-744, 2014.