

# A Hybrid Approach for Enhancing the Security of Information Content of an Image

Kumar Jalesh and S. Nirmala

**Abstract** Recent advancements in communication technologies have resulted in sharing of most multimedia information through internet. Securing such information from eavesdroppers during communication is still challenging task. In this paper, a hybrid approach is proposed for securing the contents of an image. This hybrid approach is a combination of edge detection and encryption process. The proposed approach comprises three stages. In first stage, the input image is divided into two sub images, image with edges and image without edge information. Canny edge detection algorithm is used for detecting edges in the input image. In second stage, sub images obtained from previous stage are encrypted separately using crossover and mutation operations. The encrypted images are fused in the final stage. The performance of the proposed method is measured in terms of correlation coefficient and histogram. The results obtained are compared with method [1]. The comparative study reveals that the image processing technique can be combined with encryption process to provide different levels of security.

**Keywords** Hybrid approach • Edge detection • Selection • Crossover • Mutation • Levels of security

---

K. Jalesh (✉)

Department of Computer Science and Engineering, J.N.N.C.E, Shimoga, Karnataka 577204, INDIA

e-mail: jalesh\_k@yahoo.com

S. Nirmala

Department of Information Science and Engineering, J.N.N.C.E, Shimoga, Karnataka 577204, INDIA

e-mail: nir\_shiv\_2002@yahoo.co.in

## 1 Introduction

From time immemorial, people have been trying to exchange messages without letting others to know about it. In modern times, messages are increasingly being exchanged over computer networks. Secure storage and transmission of digital images are needed in many applications such as medical imaging systems, pay-per-view TV, satellite images, image based document management and confidential video conferencing [2, 3]. Generally, two levels of security for digital image encryption could be considered: low level and high level security encryption [4]. In low level security encryption, the encrypted image has degraded visual quality compared to that of the original one. However, the contents of the image are still visible and understandable to the viewers. In the high level security case, the content is completely scrambled and the image just looks like random noise. Different approaches have been evolved to provide more security for image contents. Security based on edge information is a new approach. Edge information is used in image enhancement, compression, segmentation and recognition [5].

Many encryption techniques are proposed in the past to secure the image contents. But, some of them have been known to be insecure [6]. Evolutionary computation algorithms represent a range of problem solving techniques based on principles of biological evolution, like natural selection and genetic inheritance. Such algorithms can be used to solve a variety of difficult problems, among which are those from the area of cryptography.

In this paper, a hybrid approach is proposed which is a combination of image processing and encryption techniques. In Sect. 2, a related literature survey is carried out. In Sect. 3, the proposed method is described. Experimental results are discussed in Sect. 4. Statistical analysis of the results is presented in Sect. 5. In Sect. 6, comparative study is carried out. Conclusions drawn are summarized in Sect. 7.

## 2 Literature Survey

The security of digital images has become increasingly more important in today's highly computerized and interconnected world. In recent past different techniques have been analyzed on image security. Mitra et al. [7] used a random combination of bit or pixels or permutation of blocks. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. To extract an image, a combinational sequence of permutations and permutation keys using pseudo random index generators should be known. In this investigation the combination of block, bit and pixel permutation are used respectively. Permutation techniques are attractive, but lacks in generated key and security. A block based transformation algorithm based on the combination of image transformation and Blowfish algorithm is discussed in [8]. The original

image was divided into uniform blocks which were rearranged into a transformed image using any transformation algorithm. Blowfish algorithm is used for encryption. Transformation process adds additional processing overhead in this technique.

A survey of cryptographic applications that can be developed with the help of evolutionary computation methods are discussed in [9, 10]. Kumar [11] proposed a new approach based on genetic algorithms with pseudorandom sequence to encrypt the data stream. The approach ensures high data security and feasibility for easy integration with commercial multimedia transmission applications. The properties of chaos are used for encryption along with genetic algorithm. Enayatifar [12] described a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. Genetic approach is used to get the best encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels. Husainy [2] discuss a new image encryption technique using genetic algorithm based on mutation and crossover. Security of this method depends on the use of different vector lengths and number of crossover and mutation operations. In Ref. [3], a new effective method for image encryption which employs magnitude and phase manipulation using differential evolution approach is discussed. Linear feedback shift register is used to select the crossover points. In this approach, discrete fourier transform followed by differential evolution are used for image encryption.

In Ref. [5], a new concept of image encryption which is based on edge information is discussed. The basic idea is to separate the image into the edges and the image without edges, and encrypt them using any existing or new encryption algorithm. The user has the flexibility to encrypt the edges or the image without edges or both of them. Algorithm based on 3D Cat Map is used for encryption process. The type of the edge detection method and its threshold value, the parameters and iteration times of the cat map transform can act as the security keys. The encrypted edges and encrypted image without edges for each 2D component is combines into a format of the complex number to get the encrypted image. Hou [13] have proposed three methods for visual cryptography. Gray-level visual cryptography method first transforms the gray-level image into a halftone image and then generates two transparencies of visual cryptography. We proposed a genetic algorithm for encryption of image contents in [6]. In this work pseudorandom generator, crossover and mutation operation, along with feedback function is used for encryption.

From the literature survey, it is evident that different techniques are evolved for image encryption. Evolution algorithms, visual cryptography and encryption based on image processing techniques provide a new dimension in encryption process. In this paper, a hybrid approach is proposed for securing the contents of an image which is a combination of image processing technique and genetic algorithm. Images are encrypted after dividing into with and without edge information based on genetic process. Two encrypted images are fused using simple exclusive OR function. The encrypted image with or without edge information acts as a key image to retrieve the original image.

### 3 Proposed Method

The proposed approach composes three stages. The block diagram of the proposed method is shown in Fig. 1. In first stage, the input image is divided into two sub images, image with edges and image without edge information. Canny edge detection algorithm is used for detecting edges in the input image. In second stage, sub images obtained from previous stage are encrypted separately. The encryption process used is elaborated in Fig. 2. Encryption process uses key stream generator, crossover and mutation operations as discussed in [1]. In the proposed approach three different cases are considered for securing the contents of source image.

Case 1: Encrypting only the structural information of an image

Case 2: Encrypting the image after removal of structural information

Case 3: Fusion of the information obtained from both the case 1 and case 2

The algorithm of the proposed approach is as given below.

#### Algorithm:

##### Stage 1: Division of input image into two sub images

Input: A color image 'I' of dimension  $3 \times M \times N$

Output: Two images with and without edge information

Step 1: Apply canny edge detection algorithm on the input color image

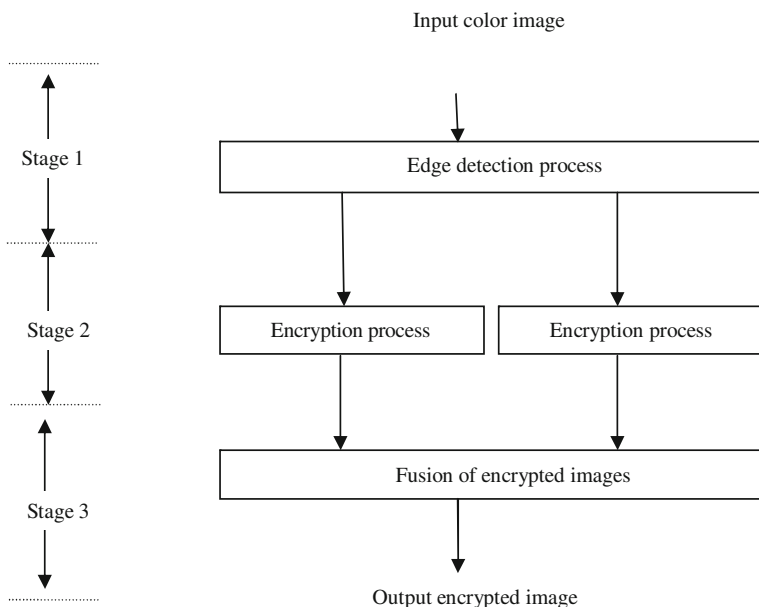
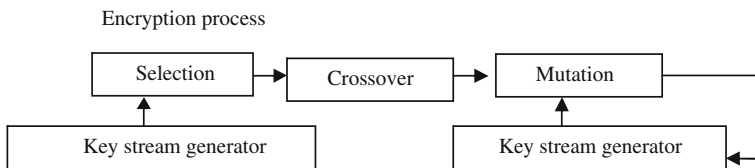


Fig. 1 Stages in proposed approach



**Fig. 2** Encryption process

Step 2: Obtain two sub images ‘A’ and ‘B’ where ‘A’ contain only edge information and ‘B’ without edge information.

**Step 2: Apply the encryption algorithm on both the sub images separately**

Input: Images with and without edge information

Output: Two encrypted images as described in Case 1 and Case 2 of the proposed approach

Step 1: Let each value of pixel in each color channel be in the range 0 to  $((M \times N) - 1)$

For  $C = 0$  to  $((M \times N) - 1)/2$ , perform the following operations

1.  $v1 = V[i]$ ,  $v2 = V [((M \times N) - 1) - C]$  where ‘v1’ and ‘v2’ are variables to store pixel values.
2. Use a linear congruential pseudorandom generator for the selection of the crossover point, say ‘s’. According to selection point ‘s’, divide ‘v1’ into ‘v11’ and ‘v12’, where  $v11 = s$  and  $v12 = v1 - s$  divide ‘v2’ into ‘v21’ and ‘v22’, where  $v21 = s$  and  $v22 = v2 - s$
3. Apply the crossover operation between ‘v1’ and ‘v2’, New generation obtained after crossover is stored in position

$$V[i] = v1 \text{ and } V [((M \times N) - 1) - i] = v2$$

Step 2: Generate initial value using a congruential pseudorandom generator, say ‘K’. For  $C = 0$  to  $(M \times N) - 1$

$$V[i] = V[i] \oplus K$$

$$K = V[i]$$

Step 3: Write an encrypted image on the basis of vector ‘V’ obtained after Step 1 and 2.

### Stage 3: Fusion of encrypted images

Input: Encrypted images from Case 1 and Case 2

Output: Encrypted image

Step 1: Let 'C1' and 'C2' are encrypted images using Case 1 and Case 2. Each value of pixel in each color channel be in the range 0 to  $((M \times N) - 1)$  in both images.

Step 2: For each  $i = 0$  to  $((M \times N) - 1)$  in 'C1'  
 For each  $j = 0$  to  $((M \times N) - 1)$  in 'C2'

$$D[i] = C1[i] \oplus C2[(M \times N) - 1 - i]$$

Step 3: Write an encrypted image on the basis of vector 'D' obtained after Step 2.

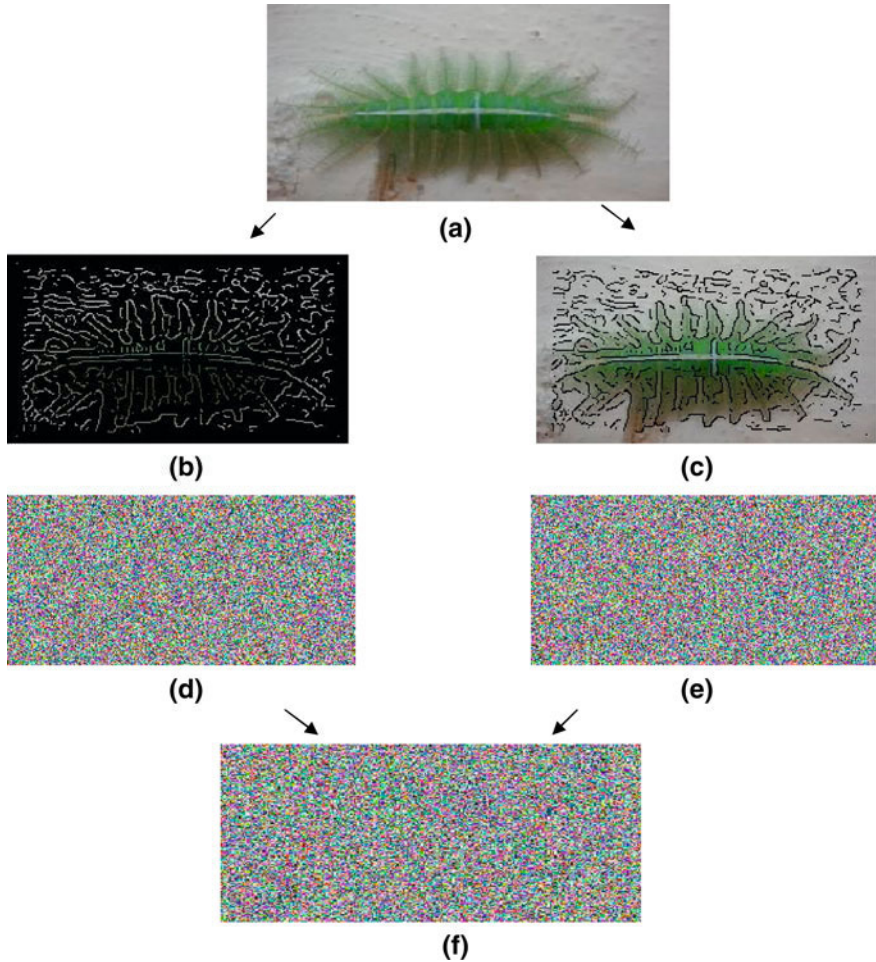
The proposed approach is as shown in Fig. 3.

## 4 Experimental Results

We have created an image corpus for the experimental study. The image corpus consists 60 color images of different sizes. Some images in the corpus are downloaded from web [14]. Image samples in the corpus are of multi colors. Images in the corpus contain text information and non text/graphical information. The results of the proposed approach on sample images in image corpus are shown in Fig. 4.

Three different types of images with uniform color, random textured and complex background are considered. The results obtained after Case 1, Case 2 and Case 3 are shown in Fig. 4. Case 1 shows the sub image contains only edge information for the corresponding input image along with the encrypted image. Further, the results obtained after encrypting the image without edge information are shown in Case 2. As described in Sect. 3, encrypted images obtained in Case 1 and Case 2 are fused together and result is shown in Case 3. From results it is observed that the encrypted images will not reveal any identity of the original image. Encrypted images obtained are completely different from the original images. Image after decryption process is also shown in Fig. 4.

In this work, the decryption is the reverse process of encryption. The result obtained after decryption is shown in Fig. 5. Original input image is retrieved without any loss of information. Two encrypted images are received by the receiver. By performing reverse process of encryption original input image would be obtained. For example, Fig. 5a and b are encrypted images from Case 3 and Case 1 respectively. Figure 5c is obtained after fusion of two encrypted images. Decryption process is applied on the images in Fig. 5b and c to obtain image with and without edge information Fig. 5d and e. From These two images the original input image could be constructed Fig. 5f.



**Fig. 3** The outcomes of all the three stages of the proposed approach for a sample input *color image*. **a** Input color image. **b** Image with only edge information. **c** Image without edge information. **d** Encrypted image with *Case 1*. **e** Encrypted image with *Case 2*. **f** Encrypted image with *Case 3*

### 5 Statistical Analysis

From the literature, it is known that many ciphers have been successfully analyzed with the help of statistical analysis. Several statistical attacks are proposed on images [3]. To prove the robustness of the proposed method, statistical analysis is performed by plotting the histograms of the original and encrypted images. Correlation coefficients between original and encrypted images are also measured.






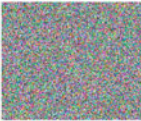










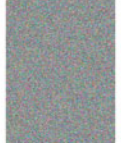




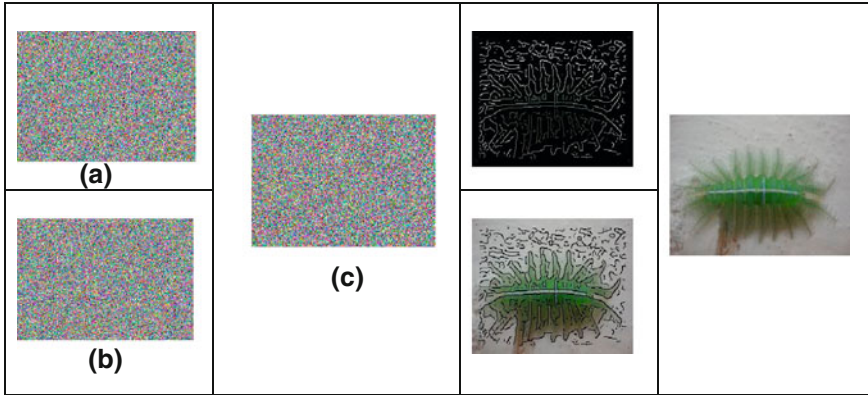
Input color image	Case 1	Case 2	Case 3	Image after Decryption
 <p>(a)</p>	 	 		
 <p>(b)</p>	 	 		
 <p>(c)</p>	 	 		

Fig. 4 Results of the proposed method on sample *color images* in image corpus. **a** Uniform color. **b** Random textured. **c** Complex background

### 5.1 Histogram Analysis

To prevent the leakage of information from an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image [3]. The histogram is a graphical representation showing a visual impression of the distribution of data. To prevent an attack, the cipher obtained should not give any clue





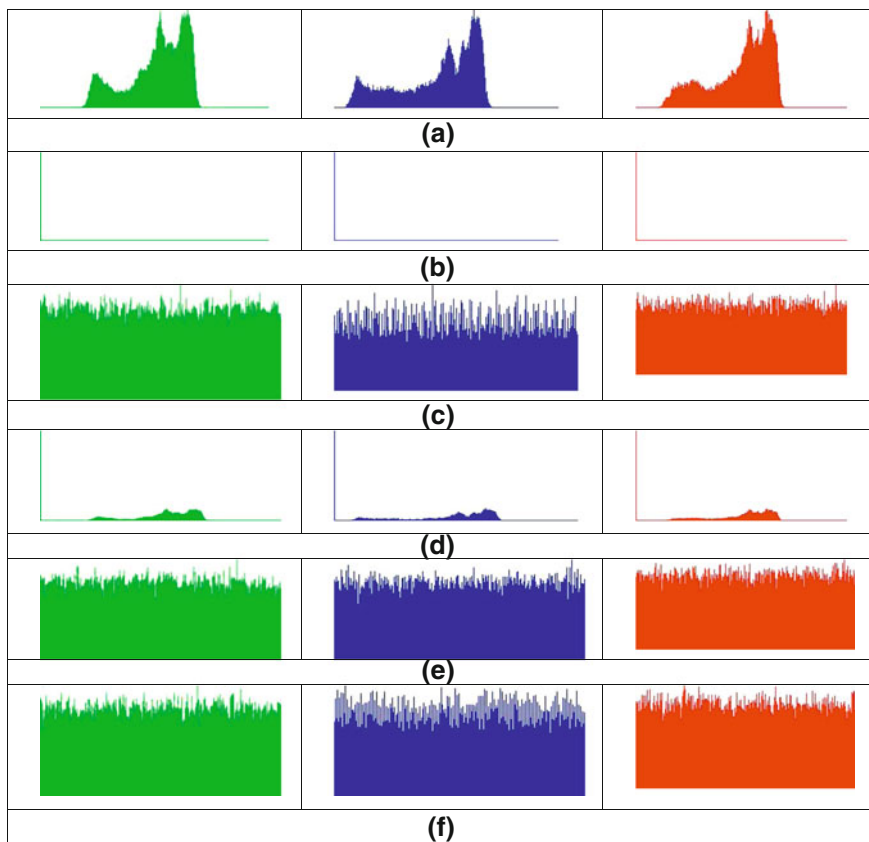
**Fig. 5** Decryption process

about the original image. In the proposed approach, the cipher obtained does not give any clue about the original image which is analyzed through histograms. For sample image and corresponding encrypted images in Fig. 3a–f the histograms are as shown in Fig. 6a–f, respectively. Levels of RGB channels of original image are unequally distributed which is shown in Fig. 6a. Further, Fig. 6b and c represents a histogram for the image with edge and without edge information. Histograms obtained after Case 1 and 2 operations are in Fig. 6d and e, which shows that all pixels are uniformly distributed. Histogram in Fig. 6f represents the encrypted image obtained after fusion operation (Case 3). It is revealed from the histogram that all pixels in R, G and B channels of sample image are distributed uniformly. Hence, the cipher image does not provide any clue to statistical attack in all the cases.

### 5.2 Correlation Coefficient Analysis

Correlation coefficient factor is used to measure the relationship between two variables: the image and its encryption. This factor demonstrates to what extent the proposed encryption algorithm strongly resists statistical attacks. Correlation coefficient ‘r’ between two images is computed using an Eq. (1) [6, 8, 15]. If the correlation coefficient equals one, that means the original image and its encryption is identical. If the correlation coefficient equals zero, that means the encrypted image is completely different from the original. If the correlation coefficient equals minus one that means the encrypted image is the negative of the original image [6].

$$r = \frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2} \sqrt{n(\sum y^2) - (\sum y)^2}} \tag{1}$$



**Fig. 6** Histogram of images shown in Fig. 3. **a** For original image. **b** Case 1 For the image with edges only. **c** Case 1 For the encrypted image with edges only. **d** Case 2 For the image without edge information. **e** Case 2 For the encrypted image without edges information. **f** Case 3 For the encrypted image after fusion operation

where

- 'r' Correlation value
- 'x' and 'y' Pixel values of the original and encrypted images
- 'n' Number of pairs of data
- $\sum x y$  Sum of the products of paired data
- $\sum x$  Sum of x data
- $\sum y$  Sum of y data
- $\sum x^2$  Sum of squared x data
- $\sum y^2$  Sum of squared y data

We computed correlation coefficient of input color image and encrypted image obtained from Case 3 and encryption method in Ref. [1]. Images of type uniform

**Table 1** Correlation coefficient for different types of images

Image type	Correlation coefficient for Case 3	Correlation coefficient for method [1]
Uniform colored	0.000378 to 0.002794	-0.0000378-0.001980
Random textured	-0.00148 to -0.0009	0.0018-0.00063
Complex background	0.000817 to -0.00283	0.000232-0.00287

color, random textured and complex background are considered. The correlation coefficients obtained are shown in Table 1. From these values, it can be concluded that the cipher images are completely different from the original images in both. This also proves that the cipher images are robust to statistical attack.

## 6 Comparative Study

The proposed approach is compared with method [1]. From the Table 1, it is evident that Case 3 and method [1] both are efficient. Method [1] is sufficient for images with uniform color. However, due to advances in multimedia technologies images with uniform colors are rare. Most of the images are textured or with complex background. So edge information will be more. When encrypted image from Case 1 or Case 2 is decrypted receiver can perceive the image, but could not get exact contents of the image. To get the exact original image, Case 3 is more suitable. It provides security at two levels. Further, more expensive compared to Case 1 and Case 2. The encrypted image in Case 1 or Case 2 acts as a key image. For decryption, encrypted image and key image both are needed in Case 3.

## 7 Conclusions

In this work, a hybrid approach is proposed which is a combination of image processing and encryption to enhance the security of image contents. To increase the level of security, both encrypted sub images obtained are fused together.

It is observed from the analysis that for the images having uniform color background direct encryption itself sufficient. The methods are tested on images with varieties of background and foreground. Statistical analysis is carried out through histogram and by evaluating correlation coefficient. Form Histogram it is evident that occurrence of each pixel is almost uniform in encrypted images. Correlation coefficient values shows that input images and corresponding encrypted images are completely different. Hence, the proposed encryption process is robust to statistical attack.

## References

1. Kumar J, Nirmala S: Encryption of images based on genetic algorithm. In: Third international conference on communications security and information assurance (CSIA), Delhi, India, *Advances in Intelligent and Soft Computing*, 2012, vol 167/2012, pp 783–791. doi:[10.1007/978-3-642-30111-7\\_75](https://doi.org/10.1007/978-3-642-30111-7_75)
2. Husainy M (2006) Image encryption using genetic algorithm. *Inf Technol J* 5(3):516–519
3. Abuhaiba ISI, Hassan MAS (2011) Image encryption using differential evolution approach in frequency domain. *Singal image process Int J (SIPIJ)* 2(1):51–69
4. Alghamdi AS, Ullah H, Khan MU, Ahmad I, Alnafajan K: Satellite image encryption for C4I System. *Int J Phys Sci* 6(17):4255–4263
5. Zhou Y, Panetta K, Aгаian S (2009) Image encryption based on edge information. In: *Multimedia on mobile devices 2009, Proceedings Of SPIE-IS&T Electronic Imaging*, SPIE, San Jose, CA, USA, vol. 7256
6. El-Wahed MA, Mesbah S, Shoukry A: Efficiency and security of some image encryption algorithms. In: *Proceedings of the world congress on engineering 2008*, vol 1, pp. 822–1706
7. Mitra A, Subba Rao YV, Prasanna SRM (2006) A new image encryption approach using combinational permutation techniques. *Int J Electr Comput Eng* 1(2):127–131
8. Bani Younes MA, Jantan A (2008) Image encryption using block-based transformation algorithm. *IAENG Int J Comput Sci* 35(1)
9. Isasi P, Hernandez JC (2004) Introduction to the applications of evolutionary computation in computer security and cryptography. *Comput Intell* 20(3):445–449
10. Picek S, Golub M (2011) On evolutionary computation methods in cryptography. In: *Proceedings of the information systems security, MIPRO 2011*, 23–27 May, pp. 1496–1501
11. Kumar A, Ghose MK (2009) Overview of information security using genetic algorithm and chaos. *Inf Secur J Glob Perspect* 18(6):306–315
12. Enayatifar R, Abdullah AH (2011) Image security via genetic algorithm. In: *2011 international conference on computer and software modeling, Singapore, IPCSIT*, vol. 14, pp. 198–202
13. YC Hou (2003) Visual cryptography for color images. *Pattern Recogn* 36:1619–1629
14. Lisa Gordon Photography, [http://www.lgordonphotography.com/2010\\_11\\_01\\_archive.html](http://www.lgordonphotography.com/2010_11_01_archive.html)
15. Maniyath SR, Supriya M: An uncompressed image encryption algorithm based on DNA sequences. *Comput Sci Inf Technol, CCSEA 2011, CS and IT 02*, pp 258–270