Expert Systems with Applications 41 (2014) 6123–6130

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm

Hamidreza Rashidy Kanan [*], Bahram Nazeri

Department of Electrical, Computer and IT Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

ARTICLE INFO

Keywords:
Steganography
Tunable image steganography
Spatial domain
Genetic algorithm

ABSTRACT

Steganography is knowledge and art of hiding secret data into information which is largely used in information security systems. Various methods have been proposed in the literature which most of them are not capable of both preventing visual degradation and providing a large embedding capacity. In this paper, we propose a tunable visual image quality and data lossless method in spatial domain based on a genetic algorithm (GA). The main idea of the proposed technique is modeling the steganography problem as a search and optimization problem. Experimental results, in comparison with other currently popular steganography techniques, demonstrate that the proposed algorithm not only achieves high embedding capacity but also enhances the PSNR of the stego image.

1. Introduction

Steganography is the science and art of hiding secret data in a host media (e.g. text, image, audio, video, etc.) (Cheddad et al., 2010). The purpose of a steganography algorithm is hiding a large amount of secret data into a meaningful host media such that the embedded secret data are concealed to prevent the attack of unauthorized persons. In steganography, there are three major goals including increasing hiding capacity, robustness to certain attacks and increasing security level (Cheddad et al., 2010). Image steganography (Morkel et al., 2005), where secret data is embedded within an image has been widely studied during the last decade due to the cost decreasing of image storage and communication and also the weaknesses of the human visual system (HVS). It should be mentioned that the cover or host image is referred as the original image without the embedded secret message, while the image that is obtained by *embedding secret* message into cover *image without* destroying the *cover image* is termed as stego image. The term payload is utilized to describe the size of the secret message that can be embedded in a specific image.

There are different steganography approaches including spatial domain (direct manipulation of image intensities) (Carvajal-Gamez, Gallegos-Funes, & Rosales-Silva, 2013; Chan & Cheng, 2004; Chen, Chang, & Le, 2010; Ioannidou, Halkidis, & Stephanides, 2012; Naor & Shamir, 1995; Sajedi & Jamzad, 2010; Shamir, 1979; Wu & Tsai, 2003; Yang, Cheng-Hsing et al., 2008), frequency domain (manipulates the image indirectly through various transforms like DFT, DCT, DWT, etc.) (Barni & Mauro, 1999; Chen, 2008; Chu et al., 2004; Jafari, Ziou, & Rashidi, 2013; Liu & Qiu, 2002; Noda, Niimi, & Kawaguchi, 2006) and the compression (substitution) domain (Chang, 2007; Chang, Nguyen, & Lin, 2011; Chang, Tai, & Lin, 2006; Chang, Wu, & Hu, 2007; Chung, Shen, & Chang, 2001; Yang, 2011). Each approach has different specifications. For instance, the spatial domain algorithms usually offer large hiding capacity for secret data and good visual quality for stego-images, but may not pass statistical steganalysis (Duric, Jacobs, & Jajodia, 2005; Luo et al., 2008; Nissar & Mir, 2010; Ziou & Jafari, 2012). On the other hand, the compression domain techniques perform better in statistical steganalysis, however may create less embedding capacity for secret data and lower visual quality for stego-images (Chang et al., 2006; Yang, 2011). The frequency domain methods are usually utilized in watermarking applications due to their good robustness against image distortion attacks.

Though numerous methods have been proposed for image steganography, limited studies have been done on metaheuristic-based image steganography and these papers could not present logical reasons for advantage of their methods. For example, (Fard et al., 2006) proposed secure jpeg steganography method based on a genetic algorithm (Goldberg, 1989). This method is based on OutGuess which is proved to be the least vulnerable steganographic system. Tseng et al. (2008) proposed a steganography method based on Optimal Pixel Adjustment Process (OPAP) and

[*] Corresponding author. Tel.: +98 9122454561.
E-mail addresses: h.rashidykanan@qiau.ac.ir (H.R. Kanan), b.nazeri@qiau.ac.ir (B. Nazeri).

http://dx.doi.org/10.1016/j.eswa.2014.04.022
0957-4174/© 2014 Elsevier Ltd. All rights reserved.

GA. This method alters secret bits for achieving more compatibility with host image. Steganography using session based stego-key and GA has been presented in Bhattacharya et al. (2008). This technique is similar to other methods that use encrypted secret data. In fact, this method encrypts secret data in two steps. First step is similar to other methods, but in second step encryption is optimized by GA. In Wang, Yang, and Niu (2010), a steganography method based on GA is presented which is secure against RS attacks. This method in first step embeds secret bits into host image just like simple LSB and in second step alters pixel values to make stego image RS parameters sit in secure area. Ghasemi and Shanbehzadeh (2010) proposed a steganography method based on GA which divides host image into sub blocks and find best pixel sequence in blocks for embedding.

In this paper, we try to find best place for embedding modified secret data in host image to achieve high level of security. The process of embedding is accomplished in two main steps, first to modify secret bits and second to embed it into host image. Different places in host image defined by order of scanning host pixels and starting point of scanning and best LSBs of each pixel. Other options of host bits are defined too. The genetic algorithm which was developed by Goldberg (1989) is utilized to find the best starting point, scanning order and other options such that the PSNR of the stego-image maximized. A feasibility and effectiveness investigation for the proposed method is conducted using some benchmark images. The system performance is compared with the performances of some previously popular existing approaches. Obtained results indicate that our proposed steganography algorithm is superior and reliable.

The rest of the paper is organized as follows: Section 2 presents the main idea of the proposed approach and its capabilities in details. The experimental results and discussion are presented in Section 3. Finally, the paper concludes in Section 4.

2. The proposed steganography method

For introducing the main idea, it is necessary to explain some preliminary definitions. In this section raster order will be explained then the proposed method will be presented in two phases.

2.1. Raster order

In LSB substitution method, host pixels are scanned row by row and trough first row to last one while in each row, pixels are scanned from left to right. This order of pixels is known as raster order. For example if image dimension is 5 × 5, raster order refers to Fig. 1.

2.2. The main idea of the proposed method

The main idea of the proposed scheme is modeling the steganography problem as a search and optimization problem. In other words, for a secret-host image pair, order of Fig. 2 maybe better than raster order or for another one, order of Fig. 3 maybe better. Accordingly, there are different orders and different places in host image for hiding secret image which lead to different PSNRs. The mentioned problem which is the direction of pixel scanning has 16 possible solutions. Therefore, if a mechanism is designed for testing all possible orders to find the best order for host and secret images, the result can be improved from simple LSB.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Fig. 1. Raster order.

25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

Fig. 2. Pixel scanning order 1.

21	16	11	6	1
22	17	12	7	2
23	18	13	8	3
24	19	14	9	4
25	20	15	10	5

Fig. 3. Pixel scanning order 2.

2.3. Development of the main idea

Another option which can be considered through the development of the main idea is the starting point. In other words, in raster order, if we choose another starting point instead of first column and first row for a secret-host image pair, we may be able to obtain better results. For example, Fig. 4 shows raster order with different starting points. For a secret-host image pair, different starting points results different PSNRs and there is no guarantee that the default starting point be the best.

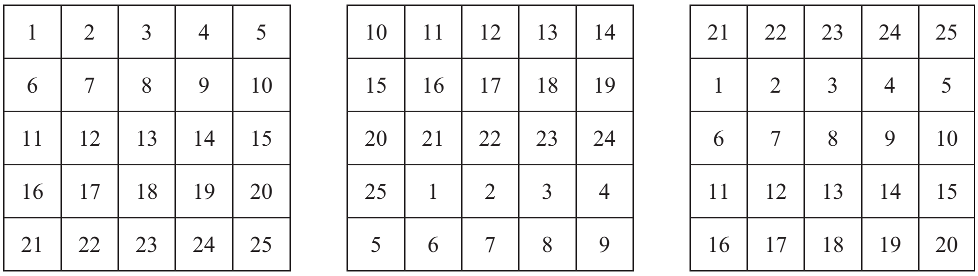
In this paper, steganography is modeled as a search problem in which the purpose is finding the best direction and the best starting point in host image for hiding secret data such that the PSNR of the stego-image maximized. In order to search this space, a genetic algorithm is utilized and the PSNR of the stego-image is considered as a fitness function. In the following the details of the proposed algorithm will be presented.

2.3.1. Chromosome representation

In the utilized genetic algorithm, the proposed chromosome contains 7 genes which are indicated in Table 1.

In the defined chromosome, since the direction of pixel scanning has 16 possible states, so we represented it as a gene with 4 bits length. Starting point is represented as two genes including *X*-offset and *Y*-offset with 8 bits length for each of them. Bit-Planes utilized for determining LSB planes in host pixels which are used for embedding secret data in host pixels. Possible values for Bit-Planes are shown in Table 2.

SB-Pole used to determine secret Bits-Pole, SB-Dire used to determine direction of secret bits and the last gene is BP-Dire



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	1	2	3	4
5	6	7	8	9

21	22	23	24	25
1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

Fig. 4. Raster order with different starting points.

Table 1
Chromosome representation.

Gene name	Value range	Length	Description
Direction	0–15	4 Bits	Direction of host image pixel scanning
X-offset	0–255	8 Bits	*X*-offset of starting point
Y-offset	0–255	8 Bits	*Y*-offset of starting point
Bit-Planes	0–15	4 Bits	Used LSBs for secret bit insertion
SB-Pole	0–1	1 Bit	Pole of secret bits
SB-Dire	0–1	1 Bit	Direction of secret bits
BP-Dire	0–1	1 Bit	Direction of bit planes

Table 2
Possible values for Bit-Planes gene.

Value	Description	Value	Description
0000	Use none of LSBs	1000	Use fourth LSB
0001	Use first LSB	1001	Use first and fourth LSBs
0010	Use second LSB	1010	Use second and fourth LSBs
0011	Use first and second LSBs	1011	Use first, second and fourth LSBs
0100	Use third LSB	1100	Use third and fourth LSBs
0101	Use first and third LSBs	1101	Use first, third and fourth LSBs
0110	Use second and third LSBs	1110	Use second, third and fourth LSBs
0111	Use first, second and third LSBs	1111	Use 4 LSBs

shows direction of LSB planes. Further information of last three genes is indicated in Table 3.

According to the existing genes in chromosome, we can separate genes in two distinctive groups. The first group contains the genes that denote the inserting place of secret bits in host image, and the second includes the genes that create some changes on secret data, to adapt more with the host image.

2.3.1.1. Numerical examples of the proposed chromosome. In order to better understand the proposed chromosome, two numerical examples are organized in this section.

- First example.

Table 3
Possible values for SB-Pole, SB-Dire and BP-Dire genes.

Gene Name	Value	Description
SB-Pole	0	In this case, no changes is made to secret bits
	1	In this case, all secret bits are changed to be apposite
SB-Dire	0	In this case, no changes is made to secret bits
	1	In this case, secret bits are reversed from end to beginning
BP-Dire	0	In this case, bit-planes are used from MSB to LSB
	1	In this case, bit-planes are used from LSB to MSB

The first example of the proposed chromosome to be evaluated is a special case which is exactly the classic LSB method. It means LSB is a special case of the proposed method. The values of different genes in this chromosome are tabulated in Table 4.

In Table 4, *X*-offset and *Y*-offset are 0, it means starting point is first column in first row. On the other hand, value of Direction is zero which it means scanning the host image is in raster order, Bit-Planes show that only first and second LSB planes are used for inserting secret data and finally values of SB-Pole, SB-Dire and BP-Dire are zero which it means no changes are made to secret data before inserting in desired pixel bits.

- Second example.

The second example is a chromosome with the value 60,305,498 which is shown in Table 5.

According to values in Table 5, starting point is column 90 and row 48 and scanning order is Direction number 8. On the other hand, first and fourth LSB planes are used to hiding secret data. Secret data are inverted and reordered from end to beginning.

2.4. Data insertion and extraction

In this section, the proposed insertion and extraction methods will be explained.

Table 4
First example for chromosome.

Gene name	Binary value	Value
X-offset	00000000	0
Y-offset	00000000	0
Direction	0000	0
Bit-Planes	0011	3
SB-Pole	0	0
SB-Dire	0	0
BP-Dire	0	0
Chromosome	3145728	
Binary chromosome	000001100000000000000000000	

Table 5
Second example for chromosome.

Gene name	Binary value	Value
X-offset	01011010	90
Y-offset	00110000	48
Direction	1000	8
Bit-Planes	1001	9
SB-Pole	1	1
SB-Dire	1	1
BP-Dire	0	0
Chromosome	60305498	
Binary chromosome	011100110000011000001011010	

2.4.1. Inserting secret data

The flowchart of the proposed inserting secret data method is shown in Fig. 5. This flowchart is an illustrative of inserting secret data steps in host image and also modeling of stego image. In the first step, after preparing the host image, secret image and the corresponding chromosome, pixel bits are achieved using the genes of chromosome. Besides, the secret image is also converted to the secret bits sequences based on corresponding genes (i.e. SB-Dir and SB-Pole). Afterwards, number of pixel bits and secret bits are compared because each of the pixel bits can only reserve one secret bit. If the number of secret bits is more than pixel bits, it means the related chromosome has no ability to insert this image in the host image, otherwise, we can insert each of the secret bits in the corresponding pixel bit and get the stego image and then calculate the fitness (PSNR) value for the stego image.

2.4.2. Extracting secret data

The flowchart of the proposed secret data extraction is indicated in Fig. 6. For extracting secret data, we extract the used chromosome from the predefined pixel bits (here, the last line of stego image) and separate its genes. According to the genes of chromosome, we obtain the pixel bits series and then achieve the raw secret bits series by using that. Then, based on chromosome genes, we obtain the final series of secret bits and produce the secret image accordingly.

2.5. Advantages of the Proposed Algorithm

The advantages of the proposed algorithm are as follows:

- Many of the presented methods in different articles can find only one solution as a stego image, but in the proposed GA-based model, the last generation that contains many good or close to optimal solution, can show many stego images which user can select one of them. In other words, our proposed method is not restricted to one solution and its stego image quality is tunable.
- Metaheuristic algorithms can usually find a solution, even when they face with time restriction. That solution would not necessarily a good one, but this can be either an advantage for the proposed algorithm, or an idea for reducing runtime of the algorithm.
- Other important properties of the proposed method are its robustness to data lost (data lossless) and its high embedding capacity.
- Moreover, in the proposed model, the secret image is converted into bit series, so it can insert the secret data (information) in any format in the host image and it is not restricted to the image data. That is; we can insert sound or any other formats of digital information in host image.
- The last advantage of the proposed technique is its high safety and security.

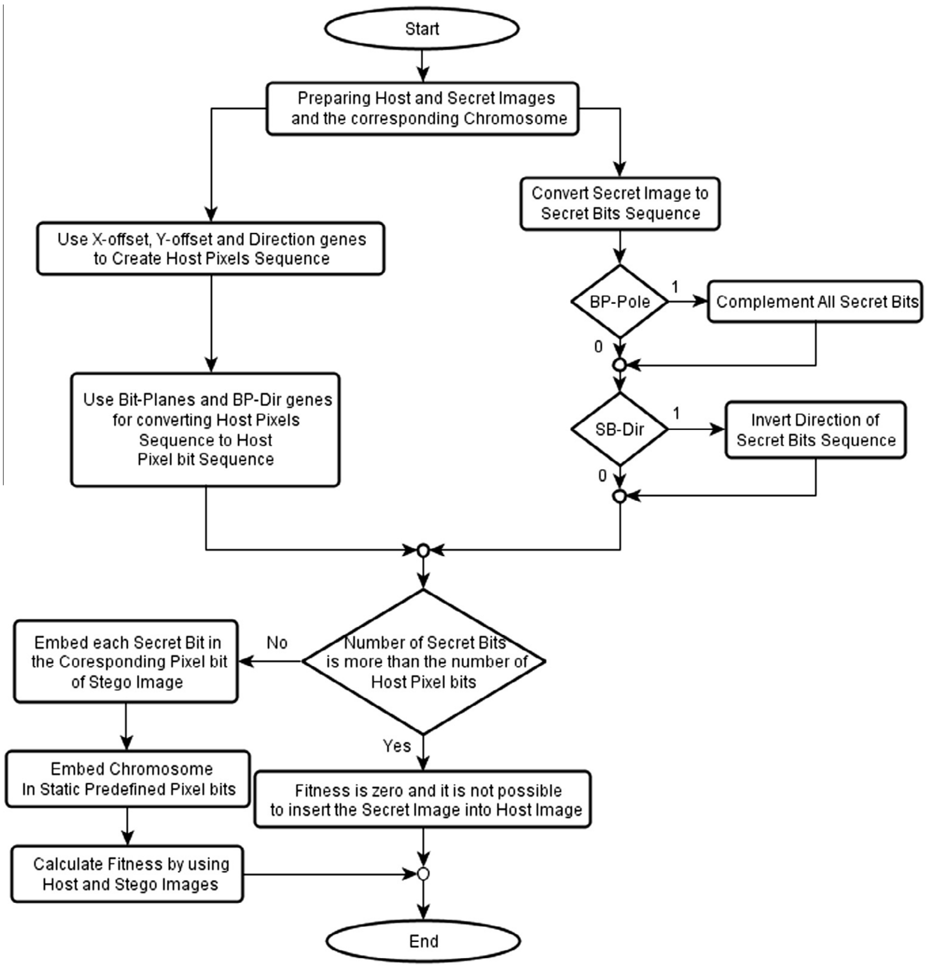

Start
Preparing Host and Secret Images and the corresponding Chromosome
Use X-offset, Y-offset and Direction genes to Create Host Pixels Sequence
Use Bit-Planes and BP-Dir genes for converting Host Pixels Sequence to Host Pixel bit Sequence
Convert Secret Image to Secret Bits Sequence
BP-Pole
1
Complement All Secret Bits
0
SB-Dir
1
Invert Direction of Secret Bits Sequence
0
Number of Secret Bits is more than the number of Host Pixel bits
No
Embed each Secret Bit in the Coresponding Pixel bit of Stego Image
Embed Chromosome In Static Predefined Pixel bits
Calculate Fitness by using Host and Stego Images
Yes
Fitness is zero and it is not possible to insert the Secret Image into Host Image
End

Fig. 5. Flowchart of the proposed secret bits embedding.

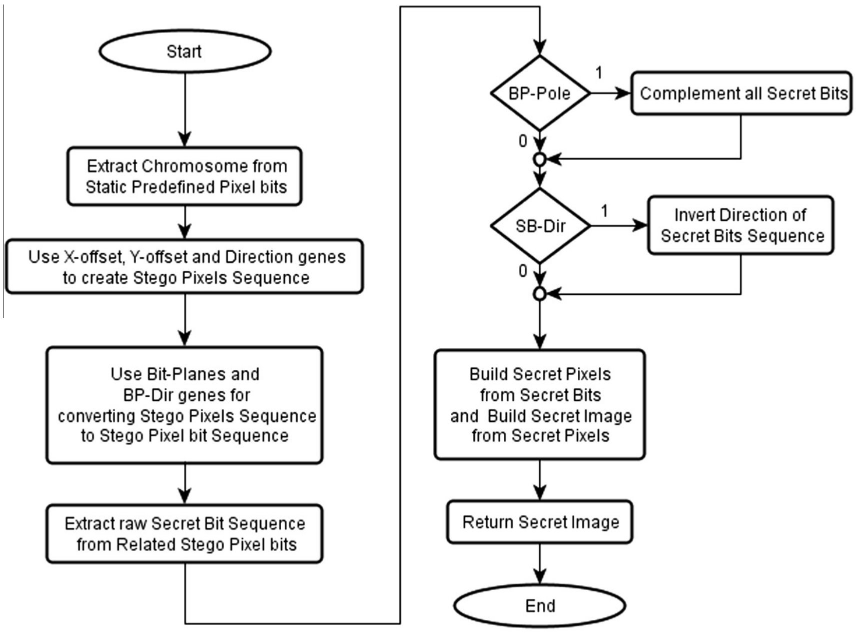

Start
Extract Chromosome from Static Predefined Pixel bits
Use X-offset, Y-offset and Direction genes to create Stego Pixels Sequence
Use Bit-Planes and BP-Dir genes for converting Stego Pixels Sequence to Stego Pixel bit Sequence
Extract raw Secret Bit Sequence from Related Stego Pixel bits
BP-Pole
1
Complement all Secret Bits
0
SB-Dir
1
Invert Direction of Secret Bits Sequence
0
Build Secret Pixels from Secret Bits and Build Secret Image from Secret Pixels
Return Secret Image
End

Fig. 6. Flowchart of the proposed secret data extraction.

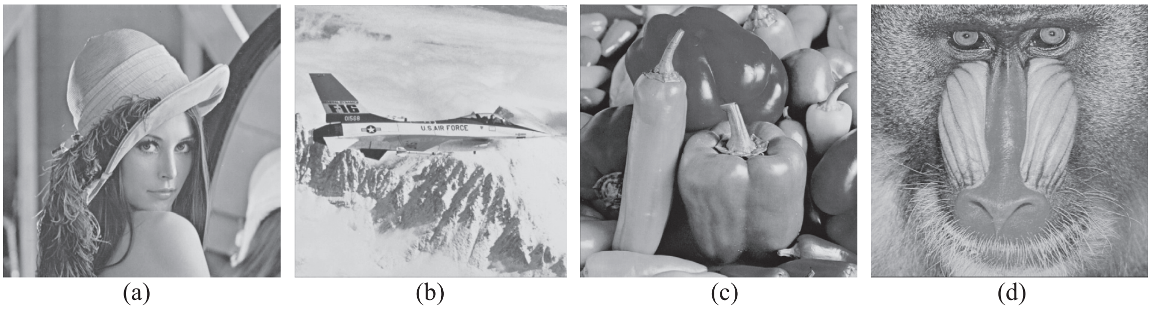


Fig. 7. The host and secret images used in the experiment. (a): The host image, (b)–(d): The secret images.

3. Experimental results

This section presents the performance of the proposed approach against other existing algorithms. To evaluate the effectiveness of the proposed steganography method, the stego image quality is considered from two viewpoints. First, we utilized the peak-signal-to-noise ratio (PSNR) metric between the stego image and the host image which is defined as follows. Second, we compare the quality of the stego image to that of the host image as seen by the human visual system (HVS).

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

where, MSE is the mean-square error between the host and the stego images. For a host image whose dimensions are W and H, MSE is defined as:

$$\mathrm{MSE} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (X_{i,j} - Y_{i,j})^2 \tag{2}$$

where, $X_{i,j}$ and $Y_{i,j}$ denote the pixel values of the host and the stego images, respectively.

To conduct our experiments, we used “Lena” with sizes of 256×256 as a host image and “Jet”, “Pepper” and “Baboon” as

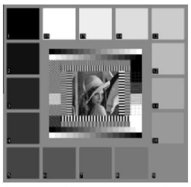
Table 6
Experimental results of the proposed method for different secret images.

Capacity		PSNR (%)		
%	bpp (bits per pixel)	Jet	Pepper	Baboon
6.25	0.50	54.30	54.28	54.25
10.0	0.80	52.20	52.19	52.16
20.1	1.61	46.52	46.53	46.60
24.6	1.96	45.66	45.61	45.61
29.9	2.39	41.73	41.71	41.68
40.0	3.20	35.70	35.81	36.51
49.4	3.95	34.67	34.93	35.42

Table 7
GA parameters used in the Experiments.

Parameter	Value
Population size	300
Crossover rate	0.7
Mutation rate	0.04
Replacement rate	0.8

Table 8
Comparative performance of the proposed method and the different steganography algorithms.

Secret image (256 × 256)	PSNR (%)					
	Stego image (512 × 512)	Lin and Tsai's method (Lin & Tsai, 2004)	Yang et al.'s method (Yang, 2007)	Chang et al.'s method (Chang et al., 2008)	Wu et al.'s method (Wu et al., 2011)	The proposed method
	Lena	39.20	41.60	40.37	43.54	45.12
	Jet	39.25	41.66	40.73	43.53	45.18
	Pepper	39.17	41.56	39.30	43.56	45.13
	Sailboat	39.16	41.51	38.86	43.55	45.10
	Baboon	39.18	41.55	39.94	43.54	45.12
(General test pattern)	Average	39.19	41.58	39.84	43.54	45.13

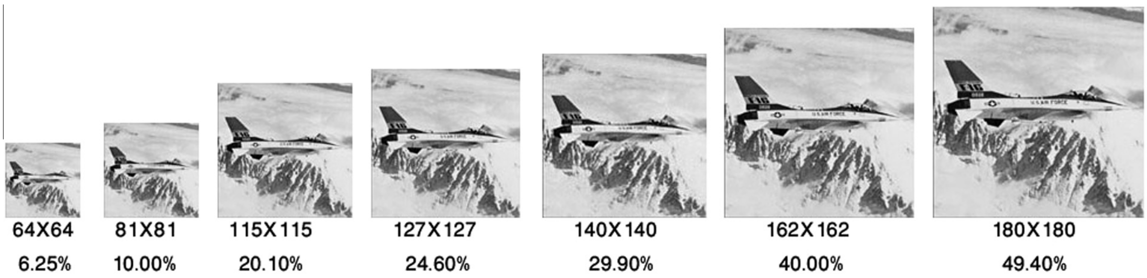


Fig. 8. Jet secret image in different sizes.

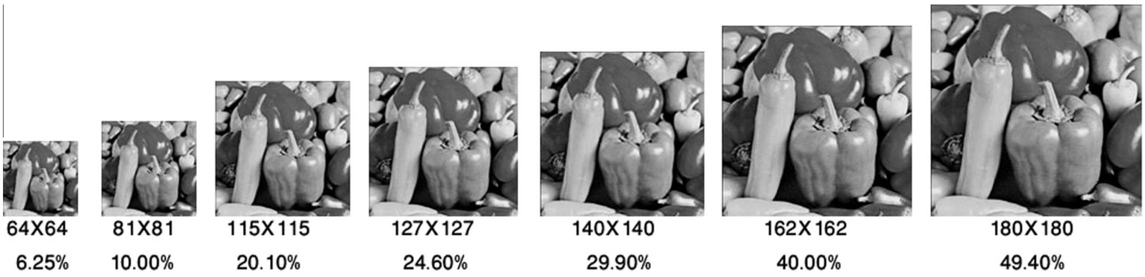


Fig. 9. Pepper secret image in different sizes.

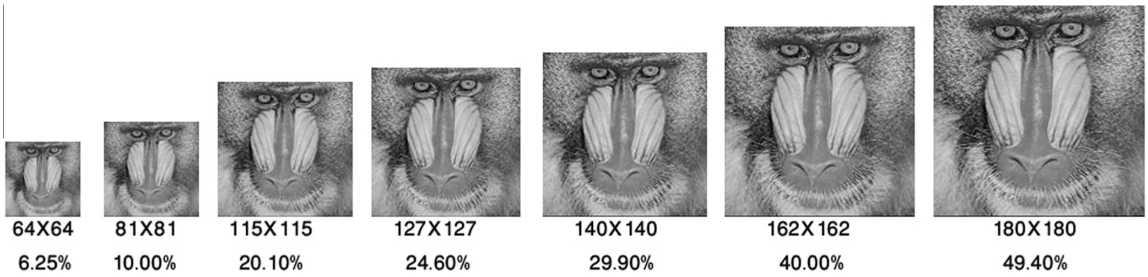


Fig. 10. Baboon secret image in different sizes.

secret images which are displayed in Fig. 7. The dimensions of the secret images as shown in Figs. 8–10, have been changed in different experiments and the results of different storage capacities are tabulated in Table 6. It should be noted that, we perform this experiment 10 times for each secret image and we report the average value of all PSNRs as the result of the proposed method in Table 6.

In the proposed method, we considered Tournament as a selection mechanism and as stated before, PSNR of the stego-image as a fitness function for the genetic algorithm. The genetic algorithm stops when the user-specified maximum number of generations is reached or the chance of achieving significant changes in the next generation is excessively low. It should be mentioned that, the maximum number of generations is set to 200 in this paper. Further GA parameters are summarized in Table 7.

It can be observed from Table 6 that the obtained results of the proposed approach are satisfactory from the aspect of PSNR and capacity. Table 6 also indicates that, even when the capacity of embedded secret image is increased, the PSNR value of the stego image is almost acceptable.

In order to investigate the performance of the proposed algorithm over other methods, we compared the visual quality (i.e. PSNR) of the stego images among the proposed method and the following popular steganography schemes.

- Secret image sharing with steganography and authentication (Lin & Tsai, 2004; Yang et al., 2007).

In these papers, authors proposed secret image sharing schemes incorporating steganography and authentication based on Shamir's polynomials. The methods divide a secret image into some shadows which are then embedded in cover images in order to generate stego images transmitted to authorized recipients securely. To attain better authentication capability, Chang, Hsieh, and Lin (2008) proposed an improved method based on Chinese remainder theorem (CRT) which not only improves the authentication capability but also enhances the visual quality of the stego images.

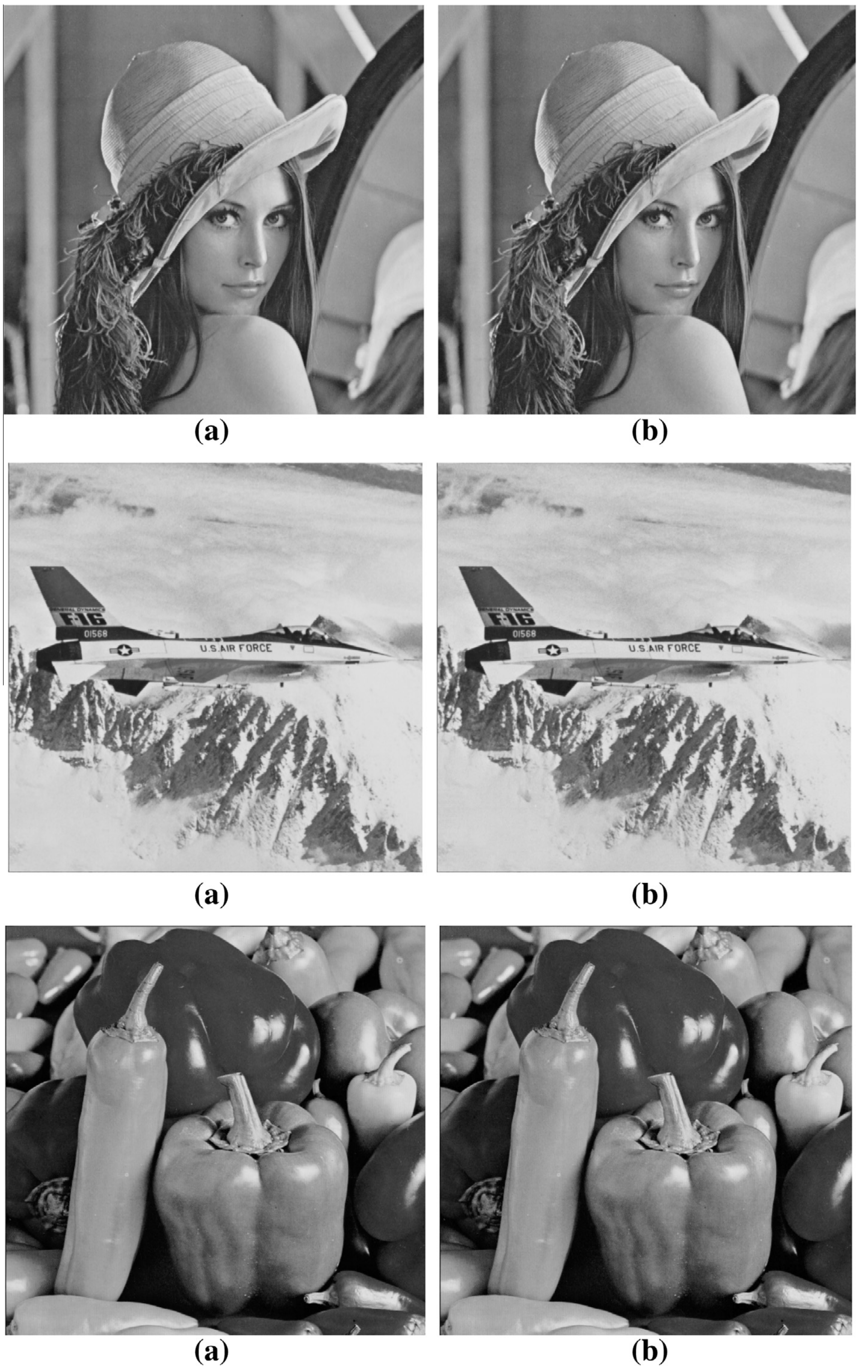


Fig. 11. Enlarged original cover images and stego-images generated by the proposed method using "general test pattern" with the sizes of 256 × 256 as a secret image. (a): cover images, (b): stego-images.

- Image sharing with steganography and adaptive authentication scheme (Wu, Kao, & Hwang, 2011).

This manuscript, proposed an improvement for the flaw in Yang et al.'s method (Yang, 2007) and Chang et al.'s scheme (Chang et al., 2008). To enhance the image quality of the stego image, the optimal LSBs method proposed by Chan & Cheng (2004) has been adopted in this paper.

In order to make a direct comparison of the proposed method against the above algorithms (Chang et al., 2008; Lin & Tsai, 2004; Wu et al., 2011; Yang, 2007), the same experiment strategy as utilized in Lin and Tsai (2004), Yang (2007), Chang et al. (2008) and Wu et al. (2011) was employed, in which the secret image is "General test pattern" with the sizes of 256 × 256, as shown in Table 8 and Four 512 × 512 pixels images including "Lena", "Jet", "Pepper" and "Baboon" as shown in Fig. 7, are utilized as the cover images. The PSNRs of the proposed approach and the above algorithms (Chang et al., 2008; Lin & Tsai, 2004; Wu et al., 2011; Yang, 2007) are tabulated in Table 8.

Table 8 indicates that the proposed algorithm is superior to all the compared methods.

To evaluate the visual quality of stego images that are generated by the proposed algorithm, we enlarged original cover images and stego-images, as shown in left column and right column of Fig. 11. It can be seen that the distortion between original cover images and stego-images is visually almost imperceptible from visual perception as indicated in Fig. 11.

4. Conclusions

In this paper, a novel high quality and data lossless spatial domain image steganography approach is proposed based on a genetic algorithm. In the presented algorithm, steganography is modeled as a search problem. The utilizing a genetic algorithm avoids the exhausting searching and allows us to find the best place in host image for embedding modified secret data. Thus, the proposed method can achieve high embedding capacity and also enhances the stego image quality (i.e. the PSNR value). The process of embedding is accomplished in two main steps, first to modify secret bits and second to embed it into host image.

The algorithm has been evaluated and compared with some previously popular existing approaches from the viewpoint of secret hiding effectiveness and stego-image quality. It is a very encouraging finding that the proposed approach performs consistently superior to the compared benchmark approaches. Experimental results have also demonstrated that, even when the capacity of embedded secret image is increased, the stego image is visually indistinguishable from its corresponding host image.

We conclude that our proposed algorithm can generate a high quality stego image satisfied the favorable demand of the embedding capacity by users. Our scheme is simple, and feasible for adaptive steganographic applications.

Even though our algorithm already obtains good results, some further improvements are conceivable. Our future work will focus on improving the efficiency of the proposed method specially by utilizing another efficient metaheuristic optimization algorithm.

References

Barni, M. et al. (1999). DWT-based technique for spatio-frequency masking of digital signatures. *Electronic Imaging'99. International Society for Optics and Photonics*.

Bhattacharya, T., Bhowmik, S., & Chaudhuri, S. (2008). A steganographic approach by using session based stego-key, genetic algorithm and variable bit replacement technique. In *International conference on computer and electrical engineering, 2008. ICCEE 2008*. IEEE.

Carvajal-Gamez, B. E., Gallegos-Funes, F. J., & Rosales-Silva, A. J. (2013). Color local complexity estimation based steganographic (CLCES) method. *Expert Systems with Applications, 40*(4), 1132–1142.

Chan, C.-K., & Cheng, L.-M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*(3), 469–474.

Chang, C.-C. et al. (2007). Reversible hiding in DCT-based compressed images. *Information Sciences, 177*(13), 2768–2786.

Chang, C.-C., Hsieh, Y.-P., & Lin, C.-H. (2008). Sharing secrets in stego images with authentication. *Pattern Recognition, 41*(10), 3130–3137.

Chang, C.-C., Nguyen, T. S., & Lin, C.-C. (2011). A reversible data hiding scheme for VQ indices using locally adaptive coding. *Journal of Visual Communication and Image Representation, 22*(7), 664–672.

Chang, C.-C., Tai, W.-L., & Lin, C.-C. (2006). A reversible data hiding scheme based on side match vector quantization. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(10), 1301–1308.

Chang, C.-C., Wu, W.-C., & Hu, Y.-C. (2007). Lossless recovery of a VQ index table with embedded secret data. *Journal of Visual Communication and Image Representation, 18*(3), 207–216.

Cheddad, A. et al. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727–752.

Chen, W.-Y. (2008). Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Applied Mathematics and Computation, 196*(1), 40–54.

Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with Applications, 37*(4), 3292–3301.

Chu, R., & et al. (2004). A DCT-based image steganographic method resisting statistical attacks. *IEEE international conference on acoustics, speech, and signal processing, 2004. Proceedings. (ICASSP'04)* (Vol. 5). IEEE.

Chung, K.-L., Shen, C.-H., & Chang, L.-C. (2001). A novel SVD- and VQ-based image hiding scheme. *Pattern Recognition Letters, 22*(9), 1051–1058.

Duric, Z., Jacobs, M., & Jajodia, S. (2005). Information hiding: Steganography and steganalysis. *Handbook of Statistics, 24*, 171–187.

Fard, A. M., Mohammad, R., Akbarzadeh, T., & Farshad Varasteh, A. (2006). A new genetic algorithm approach for secure JPEG steganography. In *IEEE international conference on engineering of intelligent systems, 2006*. IEEE.

Ghasemi, E., & Shanbehzadeh, J. (2010). An imperceptible steganographic method based on Genetic Algorithm. In *5th International symposium on telecommunications (IST), 2010*. IEEE.

Goldberg, D. E. (1989). *Genetic algorithms in search, optimization, and machine learning* (vol. 412). Reading Menlo Park: Addison-Wesley.

Ioannidou, A., Halkidis, S. T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. *Expert Systems with Applications, 39*(14), 11517–11524.

Jafari, R., Ziou, D., & Rashidi, M. M. (2013). Increasing image compression rate using steganography. *Expert Systems with Applications, 40*(17), 6918–6927.

Lin, C.-C., & Tsai, W.-H. (2004). Secret image sharing with steganography and authentication. *Journal of Systems and Software, 73*(3), 405–414.

Liu, T., & Qiu, Z. -D. (2002). A DWT-based color image steganography scheme. In *6th International conference on signal processing, 2002* (Vol. 2). IEEE.

Luo, X.-Y. et al. (2008). A review on blind detection for image steganography. *Signal Processing, 88*(9), 2138–2157.

Morkel, T., Eloff, J.H.P., & Olivier, Martin S. (2005). An overview of image steganography. ISSA.

Naor, M., & Shamir, A. (1995). Visual cryptography. *Advances in cryptology—EUROCRYPT'94*. Berlin Heidelberg: Springer.

Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. *Digital Signal Processing, 20*(6), 1758–1770.

Noda, H., Niimi, M., & Kawaguchi, E. (2006). High-performance JPEG steganography using quantization index modulation in DCT domain. *Pattern Recognition Letters, 27*(5), 455–461.

Sajedi, H., & Jamzad, M. (2010). BSS: Boosted steganography scheme with cover image preprocessing. *Expert Systems with Applications, 37*(12), 7703–7710.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612–613.

Tseng, L. -Y., & et al. (2008). Image hiding with an improved genetic algorithm and an optimal pixel adjustment process. In *Eighth international conference on intelligent systems design and applications, 2008. ISDA'08* (Vol. 3). IEEE.

Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm. *Journal of Information Hiding and Multimedia Signal Processing, 1*(1), 28–35.

Wu, C.-C., Kao, S.-J., & Hwang, M.-S. (2011). A high quality image sharing with steganography and adaptive authentication scheme. *Journal of Systems and Software, 84*(12), 2196–2207.

Wu, D.-C., & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*(9), 1613–1626.

Yang, C.-N. et al. (2007). Improvements of image sharing with steganography and authentication. *Journal of Systems and Software, 80*(7), 1070–1076.

Yang, C.-H. et al. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security, 3*(3), 488–497.

Yang, C.-H. et al. (2011). Reversible steganography based on side match and hit pattern for VQ-compressed images. *Information Sciences, 181*(11), 2218–2230.

Ziou, D., & Jafari, R. (2012). Efficient steganalysis of images: Learning is good for anticipation. *Pattern Analysis and Applications*, 1–11.