International Journal of Computers and Applications

ISSN: 1206-212X (Print) 1925-7074 (Online) Journal homepage: https://www.tandfonline.com/loi/tjca20

An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function

Jannatul Ferdush, Greetashree Mondol, Amrita Pritom Prapti, Mahbuba Begum, Mohammad Nowsin Amin Sheikh & Syed Md. Galib

To cite this article: Jannatul Ferdush, Greetashree Mondol, Amrita Pritom Prapti, Mahbuba Begum, Mohammad Nowsin Amin Sheikh & Syed Md. Galib (2019): An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2019.1662170

To link to this article: https://doi.org/10.1080/1206212X.2019.1662170

Published online: 10 Sep 2019.

INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS
https://doi.org/10.1080/1206212X.2019.1662170

Taylor & Francis
Taylor & Francis Group

An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function

Jannatul Ferdush[a], Greetashree Mondol[a], Amrita Pritom Prapti[a], Mahbuba Begum[b], Mohammad Nowsin Amin Sheikh[a] and Syed Md. Galib[a]

[a]Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh; [b]Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh

ABSTRACT

Image encryption is a very common and attractive issue in digital image processing. Here, a combination of genetic algorithm and particle swarm optimization with a chaotic function model is proposed for image encryption. This paper uses the genetic algorithm for the enhanced encryption of pixel value and particle swarm optimization for improving the optimization process. The proposed method is divided into two parts. In the first stage, the plain RGB image is used for the initial population and then the genetic algorithm is applied to encrypt the image. In the next stage, the particle swarm optimization algorithm is applied for deciding the best-encrypted image. Next, the best image is re-encrypted until the best value is found. The double-point crossover is used for encryption. On the other hand, entropy is used as a fitness function for analyzing the fitness value. The obtained average entropy of the image is approximately 7.999, which is very close to the ideal value of entropy.

ARTICLE HISTORY
Received 20 February 2019
Accepted 26 August 2019

KEYWORDS
Image encryption; chaotic map; genetic algorithm; particle swarm optimization

1. Introduction

Nowadays, the Internet has become a very common tool to transfer data. Transferring data through the internet is very easy while it is risky also. This risk perhaps may worsen when there is no protection. In the case of protecting data, some encryption techniques are applied. Sometimes, images are stored and transferred as a means of data. In these cases, image processing techniques are used mostly to reduce image sizes. The images are also encrypted in order to protect them from unauthorized access and thereby store, communicate, and transfer data confidentially. Image encryption is applied in communication, multimedia systems, telemedicines, and so on [1]. The application of image encryption process is very imperative for the system of better security standards.

There can be symmetric or asymmetric techniques to encrypt data. However, for image encryption, asymmetric encryption techniques may become very complex due to public–private keys combination. Therefore, symmetric encryption techniques are more used to encrypt images. Symmetric encryption methods require random sequences of key and chaotic function is very popular to generate random sequences as finding a pattern is very hard in sequences generated by it [2]. Thus, encrypting an image with a chaotic function may result in a better-encrypted image. At 2017, chao-based image encryption is proposed which combined the idea of logistic and kent map [3]. At 2018, this image algorithm cryptanalysis is shown and also an improved algorithm is proposed [4]. At 2019, another chaotic map-based image encryption is proposed which is used in the idea of the double spiral scan to increase the strength of encryption [5].

While talking about image encryption, optimization is a factor as the encryption should be done in such a way that the entropy becomes higher and the encryption can be done faster. Moreover, there should be minimal correlation coefficient among adjacent pixels. Therefore, optimization techniques are being applied to network security applications [6] as well as to image encryption. Evolutionary algorithms (EAs) are also applied to image encryption techniques [7–10] where genetic algorithm (GA) and particle swarm optimization (PSO) algorithms are very popular. Abdullah et al. [11] proposed a novel method to encrypt images using chaotic function and to find out the best-encrypted image which had the highest entropy and the lowest correlation coefficient among adjacent pixels applying GA. Enayatifar et al. [10] proposed an improvement over their previous work [11] which encrypts an image using DNA masking, GA, and logistic map. Another combined DNA and GA-based algorithm is proposed by Saswat. This algorithm is simple, fast and also maintains high security [12].

PSO is another popular optimization technique where a solution is found through moving candidate solutions or particles around the search space [13]. The main difference between PSO and GA is that GA uses crossover and mutation to skip the local optima, while PSO uses the personal best position and global best position in the search space and uses the velocity to move towards the global best [14]. Sabarinath et al. [15] proposed a modified PSO algorithm to encrypt images. Ahmad et al. [16] also applied PSO in image encryption along with a chaotic map to achieve the optimal encrypted image with high de-correlation with adjacent pixels as well as good entropy level.

However, PSO and GA have not been applied in a hybrid way to solve the image encryption problem and therefore, we become interested to identify whether a hybrid approach can efficiently solve the problem. Here in this article, we propose a novel hybrid approach to encrypt an image using PSO and GA along with a chaotic map. An image is initially encrypted using chaotic function and then PSO and GA are applied to find the best-encrypted image. The best-encrypted

CONTACT Jannatul Ferdush jannatulkuet@gmail.com Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore 7408, Bangladesh

image is the image which has the highest entropy and the lowest correlation coefficient among adjacent pixels. We measure the efficiency of our proposed method by looking at the entropy level, correlation coefficient among adjacent pixels and finally, the time to complete the encryption process and compare the efficiency with other existing methods of Abdullah et al. [11] and Ahmad et al. [16].

2. Chaotic function, genetic algorithm, particle swarm optimization

As mentioned in the previous section that our proposed method uses the chaotic function to generate the initial encrypted images and then GA and PSO are applied to find the best-encrypted image, here in this section we briefly discuss the terminologies.

2.1. Chaotic function

Chaotic functions are like a noise signal that can reproduce the exact signal if we have the primary key and the chaotic function. These signals have some advantages such as they are sensitive in the primary condition. Thus, a minor change in the primary amount will make a significant change in the subsequent measure. Chaotic processes or functions are used to develop and study several secure image processing techniques, e.g. image encryption, digital image and signal processing, image compression, etc. Here, chaos-based algorithms are used to encrypt important components. It produces a cipher of the test image which has good properties such as confusion and diffusion [17]. Another advantage is that it has random behavior and hence, it is heavily explored in cryptography system [1].

Among all chaotic functions, logistic map is very popular and it is defined as

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

where r is a number between [0, 1]. There are three regions which are based on the range of parameter r. The signal will be fully chaotic if the value of r ranges between 3.57 and 4.

2.2. Genetic algorithm

Constrained and unconstrained optimization problems are solved using GA which is based on natural selection. Natural selection process is used to raise the effectiveness of group of possible solutions to meet an environmental optimum [18]. The foundation of this algorithm is laid on selection rules, crossover rules, and mutation rules. GA generates a population of points at each iteration by random number generators rather than generating single point at each iteration using deterministic computation. The flowchart of GA is shown in Figure 1(a). After crossover, mutation, only the selected population with best-fitness value go on the next stage. It can be applied to solve a variety of optimization problems including discontinuous, non-differential, stochastic, or highly nonlinear problems which are not well suited for standard optimization algorithms. Recently, EAs have received a large amount of attention from researchers and have been considered to be useful in many applications [10,11]. A wide application of GAs are robotics, automotive design, optimized telecommunications routing, engineering design, and computer-aided molecular design.

2.3. Particle swarm optimization

PSO is an example of the population-based optimization method. It is invigorated by communal behavior like of bird flocking and fish schooling. Implementation of PSO is easy and there are a few parameters to adjust. Initialization, velocity updating, position updating, memory updating, and termination checking are required [19]. A group of random particles is used for initialization and to update generations, the searches for optima are applied. Each fleck is updated by two 'best' values in every iteration. The best solution is the first one it has achieved so far and that is called the particle best value, PBest. Other 'best' esteem that is calculated by particle swarm optimizer is the best value and it is gained by any grit in the population. This supreme value is called a global best, gBest. If a particle is engaged as topological neighbors of the population, then the best value called 'local best .' The flowchart of PSO is shown in Figure 1(b). The PBest

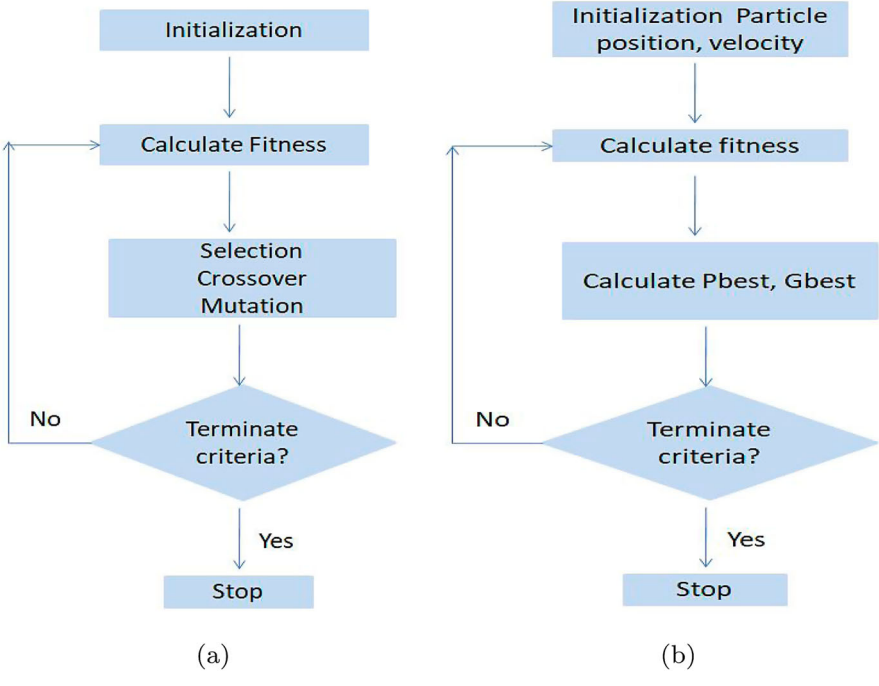


Figure 1. (a) Genetic algorithm and (b) particle swarm optimization.

and gBest are calculated depending on fitness value and here in this research we use entropy of image as the fitness function [19]. To determine the coefficient, the PSO method always reduces the time. Also a subsequent statistical analysis is not mandatory here [20,21]. Algorithms require normalization of the input vectors, to reach faster convergence. It has no genetic operators such as crossover and mutation, particle updates themselves using internal velocity and most importantly, they have memory.

3. Proposed method

The proposed method can be defined as follows: it is divided into two key parts, Part A and Part B. At the first part, total images are divided into eight parts. For encrypting these eight parts separately, eight keys are required. These keys are generated from the first five pixels from these images with the corresponding generation. Then every pixel is encrypted by the chaotic function. After finding two generations, it needs to apply GA for crossover among these populations. Instead of using a single crossover, here double crossover is applied because of the increasing confusion. After the double crossover among generations, we find two encrypted images. At the second part, the PSO algorithm is applied to find the best-encrypted images among these two images, which are selected by calculating the entropy (as fitness function) value. This total process is continued until the best-fitness result is achieved by maximum iteration number. The total procedure is shown pictorially in Figure 2.

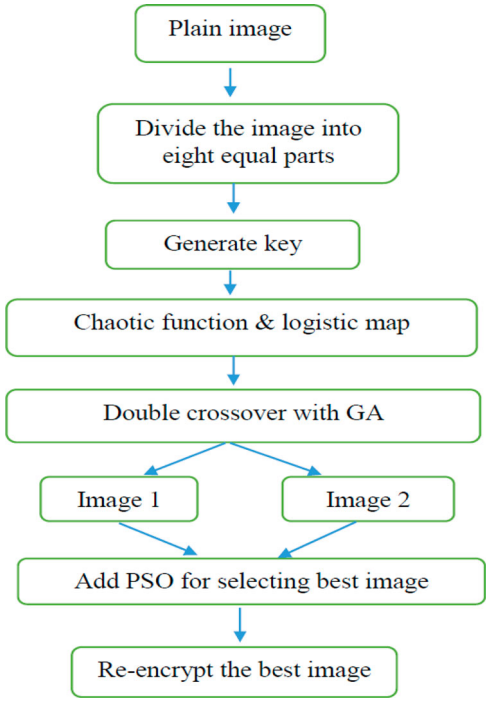


Figure 2. Flow chart of the proposed method.

3.1. Part A

In this part, we divide our work into part for better realization of the whole process. Firstly, we describe how the initial population is created using the chaotic function in the case of RGB image. Secondly, we narrate about genetic optimization to enrich our encryption process. The first part of the proposed method used the idea of [11]. They divided images into four equal parts, but we divide the image into eight equal parts to create more confusion. Another difference is that they apply their method for the gray image but we apply for the RGB image. We mostly use on the RGB image; nowadays, we mostly use the RGB image.

(1) *Creation of the initial population:* First the plain RGB image is indicated at eight equal parts shown in Figure 3(a). Then the chaotic function is applied to severally encrypt all of the pixels existing on these eight parts described below. To encrypt the pixel value, a five-encryption key is selected from each part of the image shown in Figure 3(b).Then using these encryption key and the chaotic logistic map function, the initial population is created. The offspring's numbers directed that which pixels are chosen as encryption keys. For example, the first five pixels from the first row are selected if the offspring is the first generation, for the second generation, the pixels are selected from the second row and so on. Since we have an RGB image, we repeat our same process for three times. One for red image and other two for green and blue. We show a general method for one channel like red image. For generating key, we use a chaotic logistic map. At first, five pixels from red image are selected by the following equation:

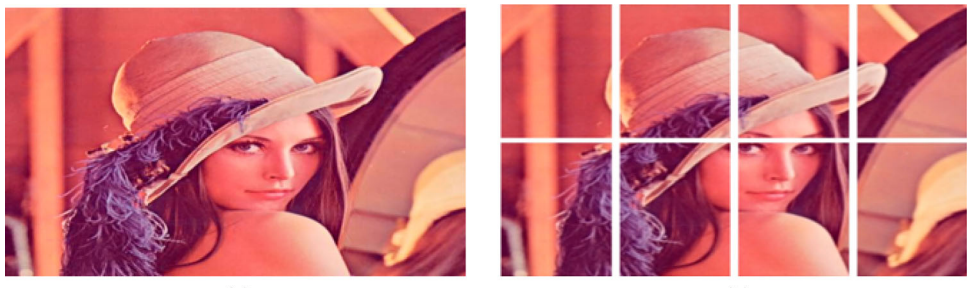
$$g_r = [g_1, g_2, g_3, g_4, g_5](Decimal) \tag{2}$$

Here, g_r is an eight-bit block for the red image of original RGB image. So, for corresponding green and blue images, we find g_g and g_b, respectively. These decimal values are converted into ASCII value.

$$A_r = [g_{1,1}, g_{1,2} \ldots . g_{2,1} \ldots . g_{5,7}, g_{5,8}](ASCII) \tag{3}$$

Thus string A_r with length 40 bits is derived. Finally, the elementary value of the chaotic function, logistic map can be obtained by using Equation (4):

$$R_{0m}(r) = \frac{g_{1,1} * 2^{39} + g_{1,2} * 2^{38} + .g_{5,7} * 2^2 + g_{5,8} * 2^0}{2^{40}} \tag{4}$$



(a) (b)

Figure 3. (a) Original image and (b) original image divided into eight equal parts.

Figure 4. First five pixels of the first row of each selection.

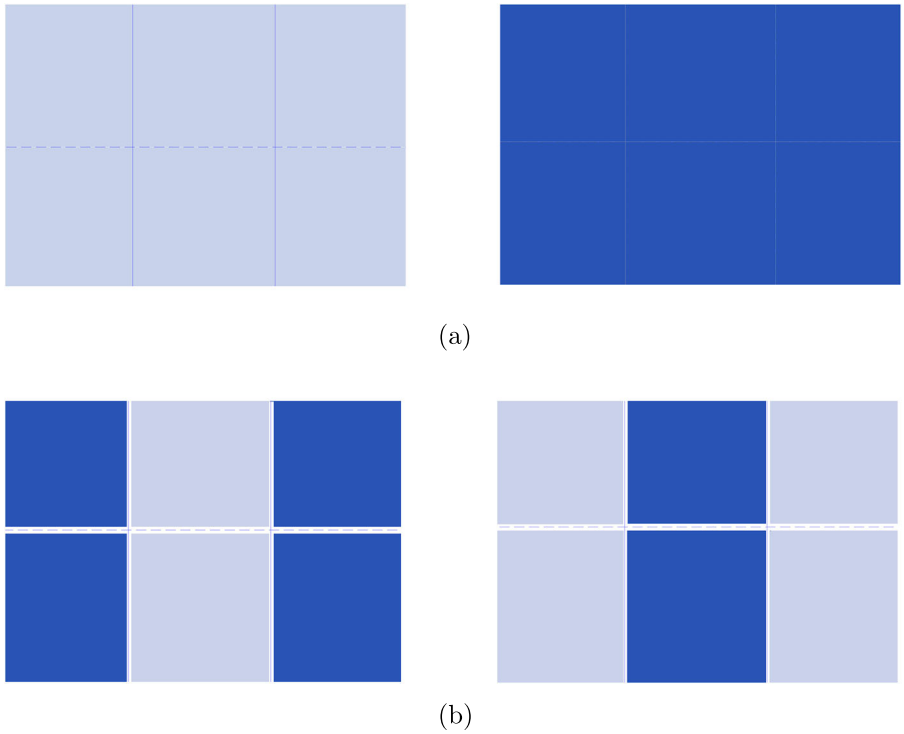


Figure 5. (a) Original image and (b) image after double crossover.

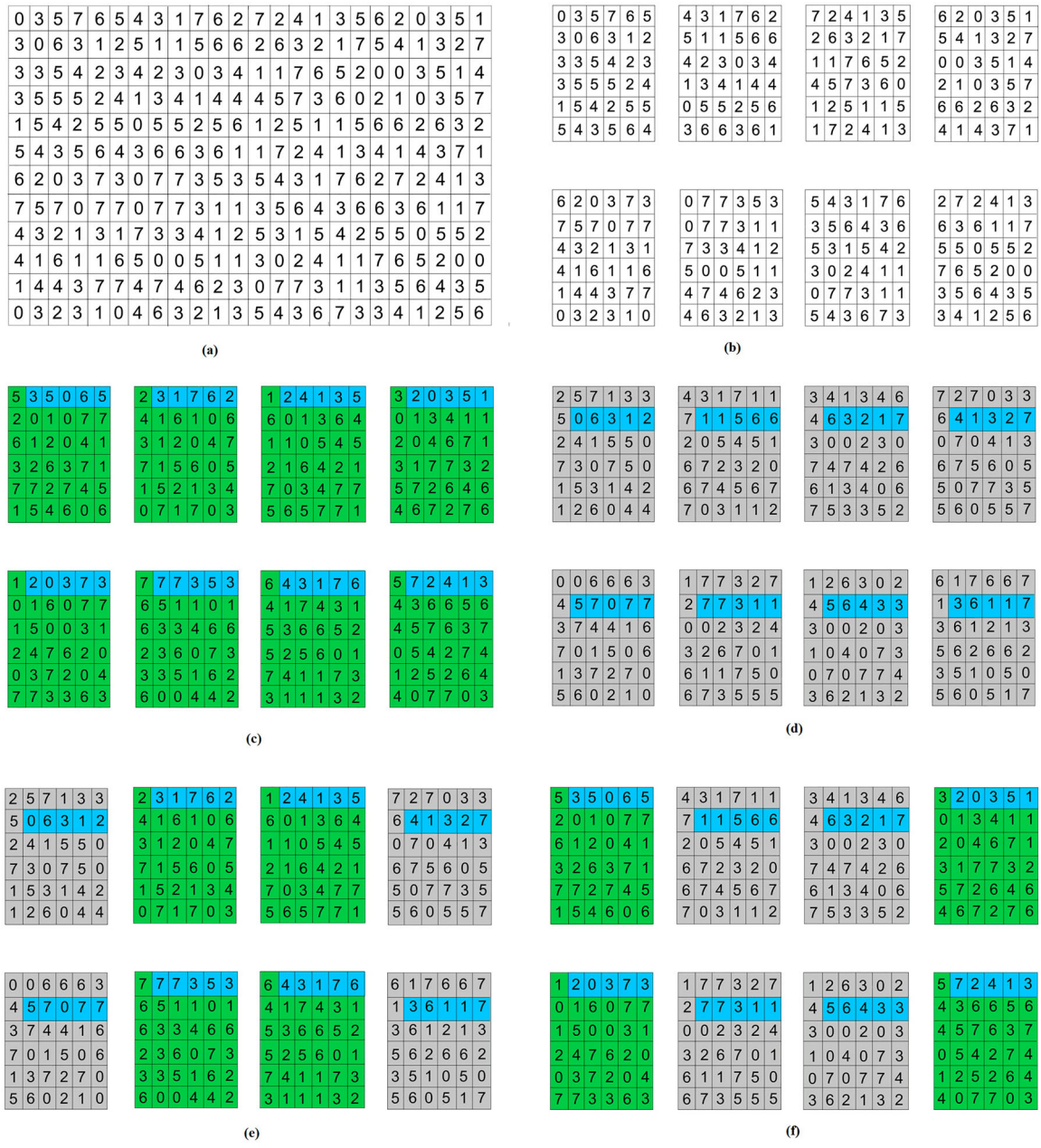


Figure 6. (a) Original image, (b) original image into eight equal parts, (c) first generation, (d) second generation, (e) third generation after double point crossover, (f) forth generation after double point crossover.

Here $m = 1, 2, 3, \ldots, 8$ where m implies the index number of the part of the image. By Equation (4) the elementary value of chaotic function logistic map is obtained, whose range is 0–1 that is further normalized. The above process is repeated for every eight parts and eight different initial values are calculated. To encrypt the remained pixel values, the initial values of each individual part and Equation (5) are used.

$$NewValue = round(R_{ik} \oplus 255) * OldValue \tag{5}$$

Here *OldValue* represent the actual pixel value of the image, symbol represents the operation and *NewValue* represents the encrypted value of the pixel. From the above, four equations of all of the pixel values of each part of the image will be encrypted only the encryption key will be the same as the previous value. The above five steps are repeated to fabricate the rest of the population. These steps are shown in Figure 4.

But, in the case of second generation, the first five pixels are taken from the second row and so forth and thus the initial value was obtained. So, the above process is repeated for also green and blue images.

(2) *Genetic optimization* To enrich the encryption process GA is applied. In GA after initial population, a crossover method has come. In previous paper [11] used single-point crossover but to increase more confusion and randomize, we use the idea of the double crossover. For fitness function, the value of entropy of the image is used. But, in [11] used correlation coefficient as fitness function. The new generation is produced every time depending on the value of the entropy and the previous populations are evaluated using this entropy value. The maximum value represents the best encryption and the minimum value represents the low-level encryption. The double crossover-system is shown

in Figure 5. To visualize this mechanism, the whole process is shown for an image in Figure 6.

3.2. Part B

After the process of PART A, the PART B is applied. In this part, we apply another optimization algorithm known as PSO. PSO iteratively updates its PBest and gBest value. After PART A, we get two images for each channel: red, green and blue. Then, combining red, green and blue, we get two images of two generations. Then it needs to know which encrypted member is best. Entropy value is calculated for every generated image. Then PBest and gBest is calculated. After at each iteration, these values are updated because in each single stage (PART A), this algorithm is applied and the best-encrypted one is selected which is used for re-encryption and this process is continued until we get the best-entropy value. This PSO based idea is taken from [16].

The whole algorithm of the proposed method is shown in Algorithm 1.

4. Results and discussions

In this section, we analyze the experimental results based on some factors. Then we have provided a general discussion on why the proposed technique is best. The efficiency of the proposed method is investigated by these points:

(1) Analysis of fitness function
(2) Histogram analysis
(3) Correlation analysis
(4) Analysis of run time

Table 1. Entropy values of various encrypted images.

Name of the image	Ref. [11]	Ref. [10]	Ref. [16]	Proposed
Lena	7.9978	7.9997	7.9720	7.9998
Pepper	7.9951	7.9995	7.9797	7.9999
Baboon	7.9952	7.9992	NA	7.9998

4.1. Analysis of fitness function

Fitness function is another most momentous and most commanding element for attaining the desired result. In our proposed method, we use the entropy value as a fitness function and optimizing the encrypted image based on it. Entropy is one of the significant properties in randomization. The ideal value of image entropy is 8. In image processing, entropy might be employed to classify texture, a certain texture might have a certain entropy as certain patterns repeat themselves in certain ways. Equation (6) is for calculating entropy. It is called Shannon entropy [22]

$$A = \sum_{n=0}^{2^N-1} P(S_i) \log\left(\frac{1}{P(S_i)}\right) \tag{6}$$

The value of entropy of our image is 7.9998, which is close to the ideal value 8. Table 1 shows entropy of different images for our proposed method with other methods also.

4.2. Histogram analysis

An image histogram is one kind of histogram that feints as a graphical delegation of the color distribution in the case of a digital image. For each total value, the number of pixels is plotted. The entire tonal distribution can be judged by glancing at

Algorithm 1 GA-PSO image encryption

Input : Original RGB Image, I
Output: Encrypted RGB Image, I_e

Divide I into eight equal parts for each channel namely $[I_r(1), I_r(2), ..., I_r(8)]$, $[I_g(1), I_g(2), ..., I_g(8)]$ *and* $[I_b(1), I_b(2), ..., I_b(8)]$.
Initialize PBest and gBest.
for $g \leftarrow 1$ *to max − generation* **do**
  for $c \leftarrow r$ *to* b **do**
    for $i \leftarrow 1$ *to* 8 **do**
      Select first five pixel $g_{ic}(1) = [g_1, g_2, g_3, g_4, g_4]$ *from* 1*st row* $g_{ic}(2) = [g_1, g_2, g_3, g_4, g_4]$ *from* 2*nd row*
      Convert $g_{ic1}(b) = binary(ASCII(g_{ic1}))$
      Convert $g_{ic2}(b) = binary(ASCII(g_{ic2}))$
      Calculate R_1, R_2 *according to* $g_{ic1}(b)$,$g_{ic2}(b)$ *by equation*(4)
    for $i \leftarrow 1$ *to* 8 **do**
      for $j \leftarrow 1$ *to* w **do**
        for $k \leftarrow 1$ *to* h **do**
          Calculate $I'_{c1}i(j,k) = round(R_{i1} \oplus 255) * I_{c1}i(j,k)$
          Calculate $I'_{c2}i(j,k) = round(R_{2i} \oplus 255) * I_{c2}i(j,k)$
    for $i \leftarrow 1$ *to* 8 **do**
      Swap $I'_{ic1}1$ *with* $I'_{ic2}1$
      Swap $I'_{ic1}4$ *with* $I'_{ic2}4$
      Swap $I'_{ic1}5$ *with* $I'_{ic2}5$
      Swap $I'_{ic1}8$ *with* $I'_{ic2}8$
    for $i \leftarrow 1$ *to* 8 **do**
      $f_1 = fitness(I_{ic1})$
      $f_1 = fitness(I_{ic2})$
      I_{ic} *is image with gBest*
  $I_{ie} = [I_i r; I_i g; I_i b]$

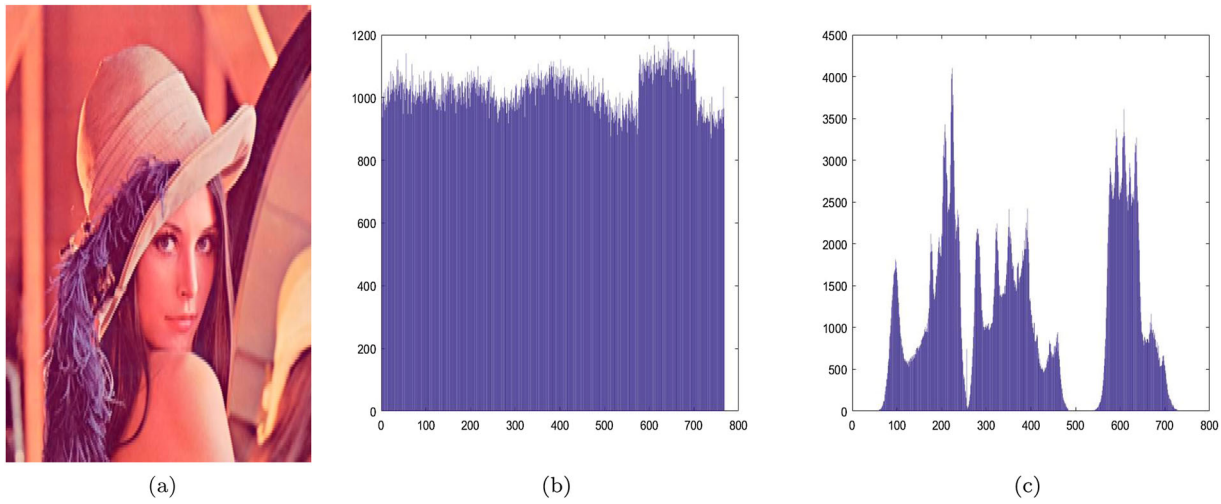


Figure 7. (a) Original image, (b) histogram of encrypted image, and (c) histogram of original image.

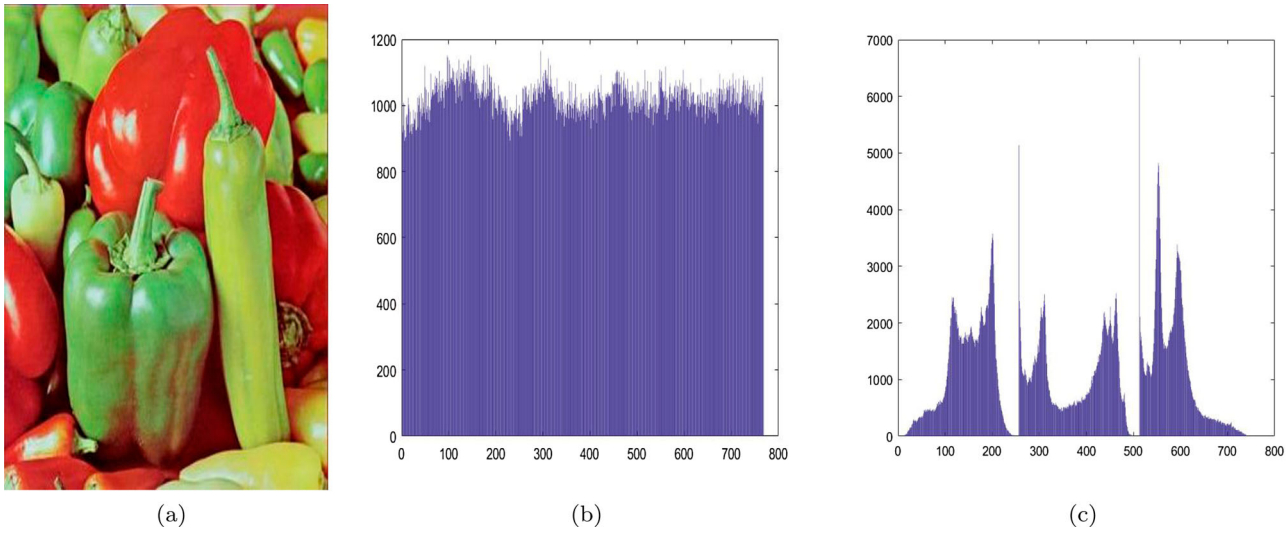


Figure 8. (a) Original image, (b) histogram of encrypted image, and (c) histogram of original image.

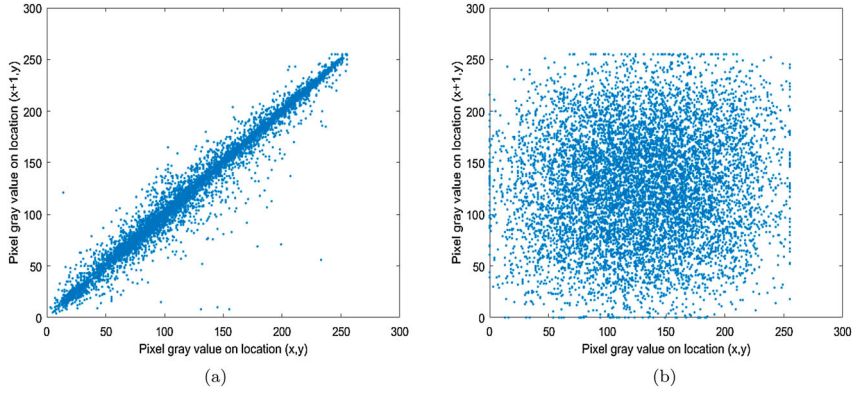


Figure 9. Correlation coefficient in horizontal direction: (a) original image and (b) encrypted image.

the histogram. This image histogram refers to the RGB-level frequency. It is one of the most monumental statistical fervidly of an image. The image histogram is shown above and after encryption, the proposed method shows the efficient result. After encryption, using the proposed method, the histogram is shown in Figures 7 and 8.

4.3. Correlation analysis

Correlation coefficients are used to calculate the relationship between two things. In the image, a pixel has a relationship its adjoint pixel. That means adjacent pixels values are close to each other for the meaningful image. However, after encryption, a meaningful image is turned into a meaningless image by decreasing relationship. So,

by calculating one pixel, it is difficult to calculate its adjoining pixel. Figure 9 shows the relation of correlation coefficient between original and encrypted image with the horizontal direction. It is shown that Figure 9(a) every pixel is close to one another but in Figure 9(b) pixels are decentralized, randomly distributed. It proves a lower correlation among encrypted image which is one of the goals for image encrypting. This analysis can be also done on the vertical, diagonal direction.

4.4. Analysis of run time

We use a double crossover instead of a single crossover. Double crossover means more confusion. But it does not only increase confusion but also reduces run time. It takes about 40.23 s to encrypt (5 times) when we take the Lena image with a single crossover. But it takes about 39.14 s to encrypt (5 times) the same image with double crossover and the reason for this is that the initializing number of an element is much than single-point crossover. Thus, it is effective to encrypt image by double-point crossover.

5. Conclusions

In this paper, we proposed a novel approach based on the combination of GA and PSO with the chaotic function. Here, we firstly use the chaotic function for the initial population then implement the GA for encrypting the image and finally applied the PSO to optimize the best-encrypted image. In the case of entropy, our method is better than other methods. We hope that our proposed method will fulfill most of the categories for online image security. In future, other optimization technique such as Ant Colony Optimization, Bee Colony Optimization, and so on can be applied on image encryption and found which optimization technique is better on image encryption. Also, an interesting task can be finding information from encrypted images which turned on privacy preserving Image computation.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Jannatul Ferdush is lecturer at department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh. She completed her B.Sc. and M.Sc. from Khulna University of Engineering and Technology, Khulna, Bangladesh. Her main research focuses on cloud outsourcing and image encryption.

Greetashree Mondol completed her B.Sc in Computer Science and Engineering from Jashore University of Science and Technology, Jashore-7408, Bangladesh.

Amrita Pritom Prapti completed her B.Sc in Computer Science and Engineering from Jashore University of Science and Technology, Jashore, Bangladesh.

Mahbuba Begum is working as an assistant professor at the department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. She received her B.Sc. and M.Sc. degree in Computer Science and Engineering from Jahangirnagar University, Bangladesh. Her research interests include cryptography, image processing, pattern recognition, face recognition, and trademarks recognition.

Mohammad Nowsin Amin Sheikh is working as an assistant professor at the department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh. He completed his B.Sc. and M.Sc. from Jashore University of Science and Technology, Jashore, Bangladesh. His main research focuses on networking, IoT, cloud computing, security issues, association rule mining.

Syed Md. Galib is working as an associate professor at the department of Computer Science and Engineering in Jashore University of Science and Technology, Jashore, Bangladesh. He received his B.Sc. from Khulna University, Khulna, Bangladesh. After he completed his M.Sc. from Dalarna University, Sweden, he received his PhD from Swinburne University of Technology, Australia. His research interest includes cryptography, image processing, computer vision, robotics.

References

[1] Dhanalaxmi B, Tadisetty S. Multimedia cryptography – A review. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017; Chennai. p. 764–766.
[2] Access date: 2019 Feb 19. Available from: https://en.wikipedia.org/wiki/Chaos_theory
[3] Wanga W, Si M, Panga Y, et al. *An encryption algorithm based on combined chaos in body area networks*. Comput Electr Eng. 2017;65:282–291.
[4] Ahmad M, Solami EA, Wang XY, et al. *Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos*. Symmetry. 2018;10:266.
[5] Tang Z, Yang Y, Xu S, et al. *Image encryption with double spiral scans and chaotic maps*. Hindawi J Sec Commun Netw. 2019;2019:Article Id: 8694678, 15 pages.
[6] Swapna BS, Sivanandam N. *A survey on cryptography using optimization algorithms in WSNs*. Int J Inform Technol. 2015;8:216–221.
[7] Raj R, Singh PK, Singh RS. *Multi-image encryption using genetic computation*. CSI Trans ICT. 2016;4(2–4):95–101.
[8] Souici I, Seridi H, Akdag H. *Images encryption by the use of evolutionary algorithms*. Analog Integr Circuits Signal Process. 2011;69(1):49–58.
[9] Zhu GL, Wang WP, Zhang XQ. *Image encryption algorithm based on genetic algorithm*. Mater Sci Inform Technol II. 2012;532:1512–1516.
[10] Enayatifar R, Abdullah AH, Isnin IF. *Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence*. Optics Lasers Eng. 2014;56:83–93.
[11] Abdullah AH, Enayatifar R, Lee M. *A hybrid genetic algorithm and chaotic function model for image encryption*. Int J Electron Commun. 2012;66:806–816.
[12] Bhattacharjee G, Pujari SK, Bhoi S. *A hybridized model for image encryption through genetic algorithm and DNA sequence*. Proc Comput Sci. 2017;125:165–171.
[13] Kennedy J, Eberhart R. Particle swarm optimization. International Conference on Neural Networks; Perth, WA, Australia; 1995. p. 1942–1948.
[14] Mitchell M. An introduction to genetic algorithms. Cambridge (MA): MIT Press; 1998.
[15] Sabarinath R, Jegadeesan S, Venkatalakshmi K. *Image encryption using modified particle swarm optimization*. Int J Res Comput Commun Technol. 2014;3:241–246.
[16] Ahmad M, Alam MZ, Umayya Z, et al. *An image encryption approach using particle swarm optimization and chaotic map*. Int J Inform Technol. 2018;10:247–255.
[17] Maadeed SA, Ali AA, Abdalla T. *A new chaos-based image-encryption and compression algorithm*. J Electr Comput Eng. 2012;2012:1–11.
[18] Tong X, Cui M. *Image encryption with compound chaotic sequence cipher shifting dynamically*. Image Vision Comput. 2008;26:843–850.
[19] Jones KO. Comparison of genetic algorithm and particle swarm optimization. International Conference on Computer Systems and Technologies, Varna, Bulgaria; 2005.
[20] Villarroel RD, García DF, Dávila MA, et al. *Particle swarm optimization vs genetic algorithm, application and comparison to determine the moisture diffusion coefficients of pressboard transformer insulation*. IEEE Trans Dielectr Electr Insul. 2015 Dec;22(6):3574–3581.
[21] Rajendra R, Pratihar DK. *Particle swarm optimization algorithm vs genetic algorithm to develop integrated scheme for obtaining optimal mechanical structure and adaptive controller of a robot*. Intell Control Autom. 2011 Nov;2:430.
[22] Shannon CE. *Communication theory of secrecy systems*. Bell Syst Techn J. 1949;28:656–715.