DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

Image Protection Using Genetic Algorithm and Cipher Technique

Raad Abdul Ameer Qasim[1], Bashar Saadoon Mahdi[2]
[1,2] Computer Sciences Department, University of Technology, Baghdad, Iraq
[1]cs.19.31@grad.uotechnology.edu.iq, [2]110043@uotechnology.edu.iq

Abstract**—** *Image Protection is one of the most important issues that have created problems in technology challenges in the past and present years, whether they are stored or when sent to other parties. And how to develop the techniques adopted in encrypting it, devise new methods, or integrate the available technologies to provide high security in encrypting images or any important data and preserving them from loss or hacking. This paper presents a new method to generate a random keychain using genetic algorithm techniques to develop new generations and XOR technology to encrypt digital images. Where the results showed the high efficiency of the encryption method with its ease of use and the preservation of the original image data after decoding with high accuracy and speed in implementing the strategy used. The efficiency of these switches for use has been tested using the National Institute of Standards and Technology (NIST) and the statistical randomness test, and the tests were successfully passed.*

Index Terms— *Security, keys, Genetic Algorithm، XOR.*

I. INTRODUCTION

The quick growth of digital technology and Internet popularity has done work and living more convenient. Digital media, such as music, books, pictures, movies, etc., have considerably enhanced people's lives by their ease of access, convenient copying, rapid dissemination, and other benefits. However, as we can see, the communications parties' interests have been severely hurt by some of the hateful behaviours designed to intercept beneficial information with network transparency and sharing properties. Therefore, the technology for safe information exchange has to be developed urgently [1].
And due to progress in dispersed computer networks, storage devices and imaging equipment. When pictures are exchanged over public networks, they are subject to several security concerns, such as redundancies, unauthorized alterations, duplications, etc. In recent years, great effort has been paid to protect the picture efficiently. The security system is divided into two parts: concealing and cryptographic information methods. The concealing information technologies are further broken down into watermark and steganography [2].
More and more multimedia data and images are sent over the network and saved on cloud platforms thanks to the Internet's exponential expansion [3].

II. GENETIC ALGORITHM

Evolutionary algorithms such as the Genetic Algorithm (GA) have a long and illustrious history of success. Darwin's theory of survival as the fittest is mirrored by this algorithm's design. On the other hand, a list is provided with the most popular enhancements in the algorithm's primary component (selection, crossover, mutation) [4].
GA is a standard evolutionary optimization method that uses stochastic principles to discover the best solution to optimization problems [5].

Received 14/January/2022; Accepted 30/March/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

To determine which options are the best and which ones are the worst. An objective measurement, such as a statistical model or simulation, can be used as well as a subjective one, in which we prefer better solutions over the worst ones. When integrated with other methods and techniques, genetic algorithms can produce optimal results, increasing the computing time of retrieval systems and using genetic algorithms in various fields. Genetic Algorithms [6].

Genetic algorithms abstract the problem space as an individual population by iteratively producing generations and attempting to find the fittest person among them. Each member of the population provides a possible solution to the problem that needs to be solved. A fitness function quantifies each rule's ability to adapt to a given environment. The technique starts with a randomly created population of individuals as a starting point for the procedure [6].

As a result of genetic algorithms' adaptability have been used to manipulate fields in various industries as a result of genetic algorithms. For example, in cryptology, the Genetic Algorithm is being utilized to create new advanced encryption by combining the procedures of Crossover and Mutation. A cryptosystem is a collection of algorithms that use secret keys to encrypt and decrypt information or messages [7].

III. GENETIC ALGORITHM OPERATION

GAs start operations using a random string population that represents variables of design or decision. Therefore, to generate a new population of points, the population is managed by three major operators; selection, crossover, and mutation.

A. Selection

The selection operator of GA simulates the natural selection. In natural selection, the chance of survival is increased proportionally to fitness. Being selected causes their genes to be passed down to future generations. [1]. In selection, the goal is to find the best individuals to mate with so that the offspring produced are more fit than the previous population. The most common methods of selection are Roulette Wheel Selection *Fig 1*, Rank Selection, Tournament Selection, and Boltzmann Selection. [8].

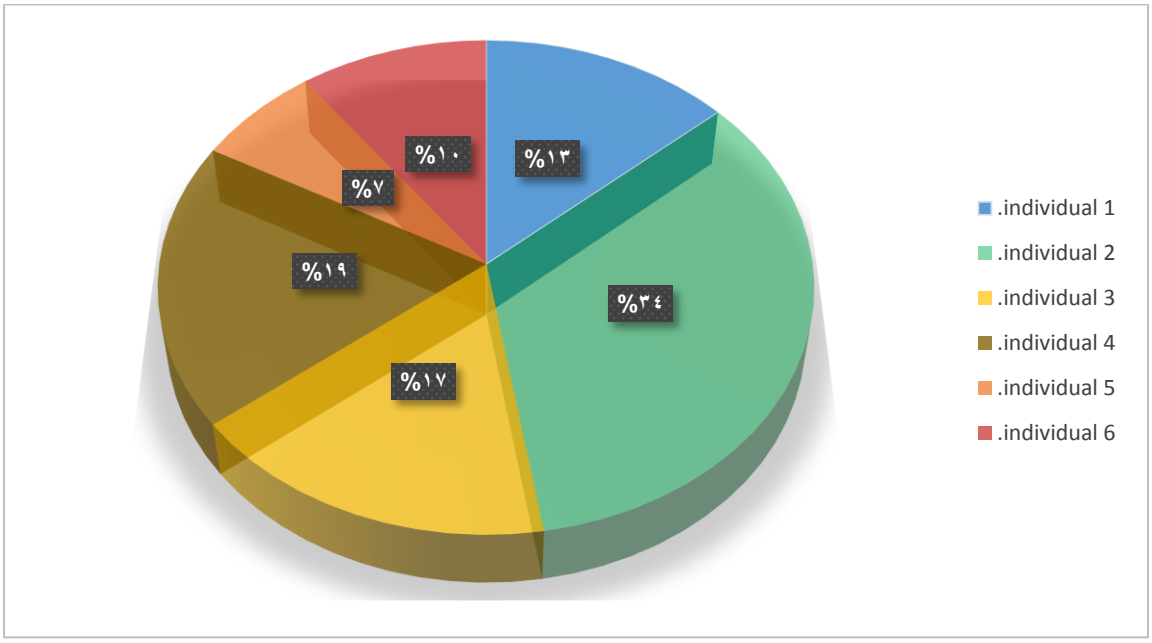

FIG. 1. ROULETTE WHEEL IN GA.

Received 14/January/2022; Accepted 30/March/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

B. Crossover

Two strings are combined using the crossover operator to produce an improved sequence of strings. After two individuals from one generation have been integrated, a recombination process creates new individuals in the next generation [9].

C. Mutation

In optimal local conditions to avoid trapping, mutation unexpectedly introduces new information to the genetic search process. After repeated use of reproduction and crossover operators, the population becomes homogeneous, introducing diversity. Individuals' chromosomes may differ from those of their parents as a result of mutation[9].

IV. XOR

The XOR is one of the simplest additive ciphers available to us today. Although, when it is used as a one-time pad cipher, in which the binary data is combined with a random key, it is theoretically impossible to crack. In addition to being one of the fastest ciphers, the XOR Cipher is also used in many encryption standards like AES. Wireless communications are encrypted using XOR Cipher, which is more efficient than many chaotic encryptions because the system for creating entropy isn't very efficient [10].

V. THE PROPOSED METHOD

Pixels are the basic building blocks of images. A pixel consists of a Red/Blue/Green (RGB) value for each color, ranging from 0 to 255. In this study, the image data is read through the pixel values, and there are 8 bits for each of the three primary colors in one pixel, and their sum is 24 bits. After reading the image and extracting its primary colors (RGB) and By using the XOR technique with three keys that are generated by the genetic algorithm and encoding them with the pixel values of the original image for encryption, *Fig 2*.

The first key is used directly with the image's red channel using XOR technique. In contrast, the second and third key uses the XOR twice the first time after it is generated from the genetic algorithm and combined with the first key, then it is used to encrypt with the green channel of the image. The third is used with the blue channel of the image to increase Complexity and camouflage in the encryption process. The three encoded image data are combined into a single image at the final step.

Received 14/January/2022; Accepted 30/March/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

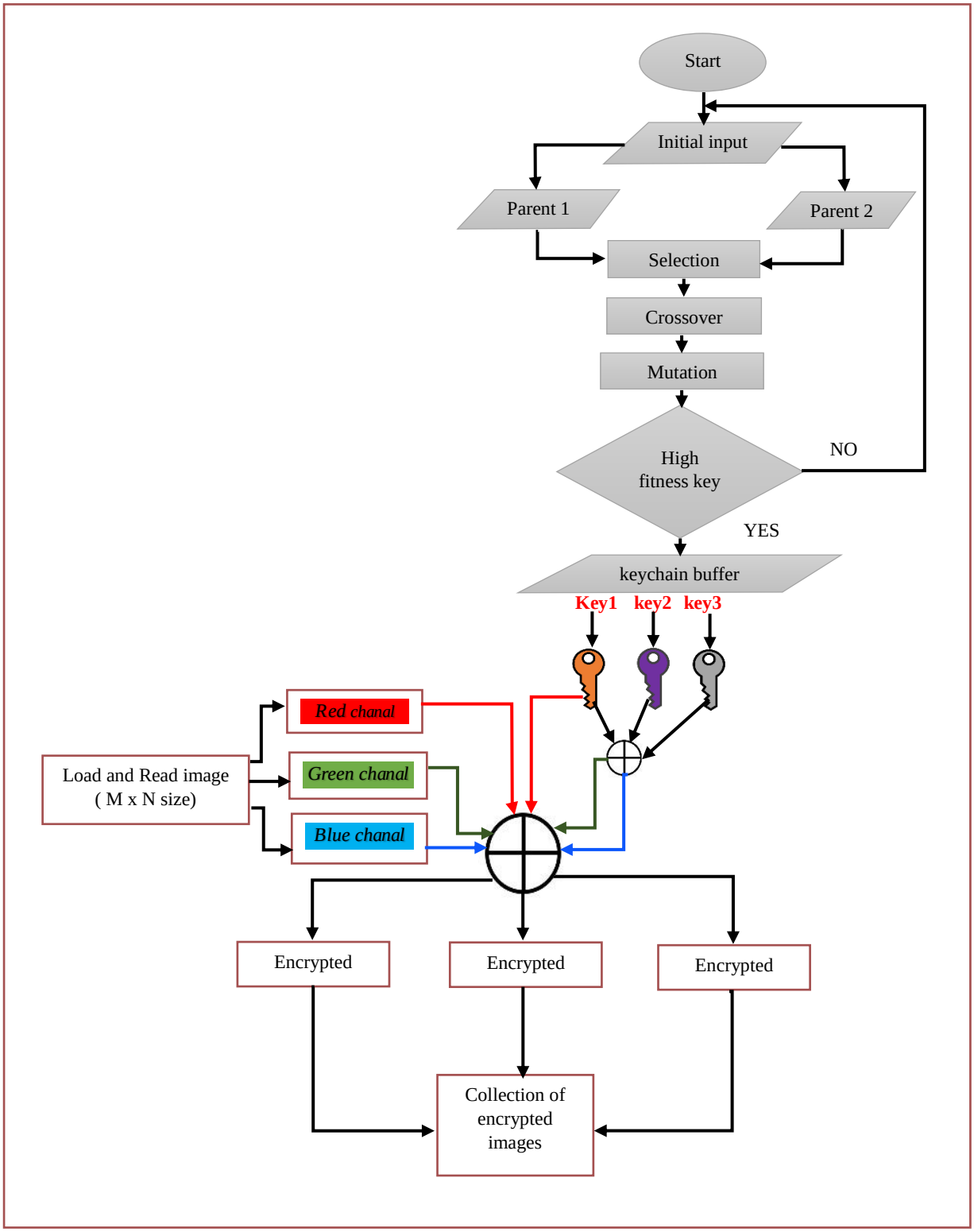

FIG. 2. PROPOSED METHOD.

Received 14/January/2022; Accepted 30/March/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

VI. RESULTS OF IMAGE ENCRYPTION

The results of image encryption is shown in *Fig. 3*.

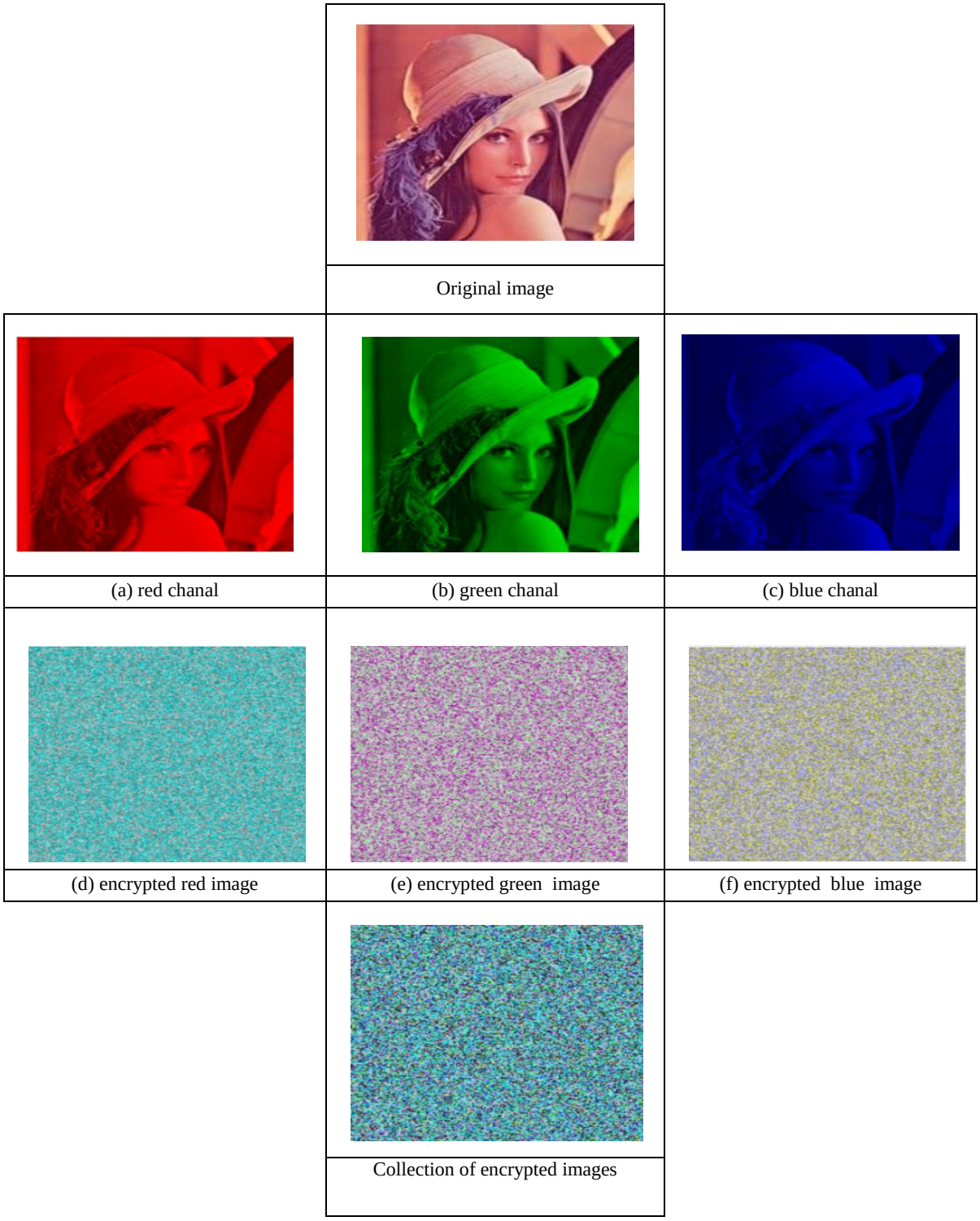

FIG. 3. THE RESULT OF ENCRYPTION.

Received 14/January/2022; Accepted 30/March/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

VII. RELATED WORK

In 2019 (Ruiz et al.) Proposed Three sets of benchmark problems from the seemliness were utilized to solve the open vehicle routing problem; the acquired results demonstrated the algorithm's strong performance because the best-known answers for 16 of the 30 cases were improved. [11].

In 2018 (Aboughalia and Alkishriwo) presented A block permutation and XOR operation-based picture encryption technique by dividing the picture is into blocks, which are then shuffled together. And to achieve the encrypted concept, the pixels of the blocks are XORed with the chaotic keystream according to simulation findings and performance analyses, were concluding the given technique can successfully resist various known assaults, ensuring safety performance and secure picture encryption [12].
In 2020 (Kaur et al.) proposed to tun the 5D chaotic map (TFCM) by breaking the image into subbands via Dual Tree-Complex Wavelet (DTCWT) transformation and diffusing subbands with the secret key obtained from the optimized 5D chaotic map, applying reverse DTCWT to get the image into an internal, non-dominate sorting genetic algorithm and locally chaotic photo-encryption technique [13].

In 2015 (Wu et al.) Proposes a new color picture encoding schema based on deoxyribonucleic acid (DNA) sequence operations and numerous one-dimensional (1D) chaotically enhanced systems with outstanding four-step performance. First, three enhanced 1D chaotic systems use the secret keys and basic picture to produce the key streams. Second, the DNA and XOR operations on the DNA matrices to obtain the scratched DNA matrices have been conducted. Thirdly, the scratched DNA matrices have been split into blocks and randomly mixed with those blocks. The DNA XOR and DNA matrices acquired from the previous phase and the key streams were finally executed. The experimental findings and security analysis demonstrated a satisfactory encryption effect and a high level of security of the suggested encryption system. In addition, it offers high stability for typical image processing and geometric assaults [14].

In 2016(Arul Thileeban S), Used XOR to pixel-by-pixel encryption of binary data into pictures, not to be readily abused or cracked by an application. The analysis also demonstrated that the pictures are correctly encrypted with the suggested model [10].

VIII. CONCLUSIONS

This proposed paper show how the genetic algorithm can generate secret random keys and use xor in the image encryption process. It showed good results in testing the difference in images and comparing them before and after encryption. Therefore, this method of encryption can be relied upon. This technology can be developed in the future and used in video and audio encoding operations.

REFERENCES

[1] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, 2018, doi: 10.1016/j.sigpro.2018.06.008.
[2] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Arch. Comput. Methods Eng.*, vol. 27, no. 1, pp. 15–43, 2020, doi: 10.1007/s11831-018-9298-8.
[3] S. Beugnon, P. Puteaux, and W. Puech, "PRIVACY PROTECTION FOR SOCIAL MEDIA BASED ON A HIERARCHICAL SECRET IMAGE SHARING SCHEME S ´ ebastien Beugnon Pauline Puteaux STRATEGIES , Rungis , France," *2019 IEEE Int. Conf. Image Process.*, pp. 679–683, 2019.
[4] S. Mirjalili, J. Song Dong, A. S. Sadiq, and H. Faris, *Genetic algorithm: Theory, literature review, and application in image reconstruction*, vol. 811. Springer International Publishing, 2020.
[5] A. Askarzadeh, "A Memory-Based Genetic Algorithm for Optimization of Power Generation in a Microgrid," *IEEE Trans. Sustain. Energy*, vol. 9, no. 3, pp. 1081–1089, 2018, doi: 10.1109/TSTE.2017.2765483.
[6] I. Editor, J. Parag Meht, D. M. Rat hod, L. Haldurai, T. Madhubala, and R. Rajalakshmi, "A Study on Genetic Algorithm and its Applications Related papers Effect of Genet ic Algorit hm on Art ificial Neural Net work for Int rusion Det ect

Received 14/January/2022; Accepted 30/March/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.13

ion Syst em IJCSE Edit or A review: accuracy opt imizat ion in clust ering ensembles using genet ic algori," 2016, [Online]. Available: www.ijcseonline.org.

[7] M. Tabassum, "a Genetic Algorithm Analysis Towards Optimization Solutions," *Int. J. Digit. Inf. Wirel. Commun.*, vol. 4, no. 1, pp. 124–142, 2014, doi: 10.17781/p001091.

[8] M. O. Okwu and L. K. Tartibu, "Genetic Algorithm," *Stud. Comput. Intell.*, vol. 927, pp. 125–132, 2021, doi: 10.1007/978-3-030-61111-8_13.

[9] N. Saini, "Review of Selection Methods in Genetic Algorithms," *Int. J. Eng. Comput. Sci.*, vol. 6, no. 12, pp. 23261–23263, 2017, doi: 10.18535/ijecs/v6i12.04.

[10] S. Arul Thileeban, "Encryption of images using XOR Cipher," *2016 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2016*, pp. 1–3, 2017, doi: 10.1109/ICCIC.2016.7919607.

[11] E. Ruiz, V. Soto-Mendoza, A. E. Ruiz Barbosa, and R. Reyes, "Solving the open vehicle routing problem with capacity and distance constraints with a biased random key genetic algorithm," *Comput. Ind. Eng.*, vol. 133, pp. 207–219, 2019, doi: 10.1016/j.cie.2019.05.002.

[12] R. Aboughalia and O. Alkishriwo, "Color Image Encryption Based on Chaotic Block Permutation and XOR Operation," no. march, pp. 3–7, 2018.

[13] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5 D chaotic map," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 333–350, 2020, doi: 10.1016/j.future.2020.02.029.

[14] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput. J.*, vol. 37, pp. 24–39, 2015, doi: 10.1016/j.asoc.2015.08.008.

Received 14/January/2022; Accepted 30/March/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*