Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

A new steganography technique based on genetic algorithm

Shahbaa Mohammed Abdulmaged [1,*] and Nadia Mohammed Abdulmaged [2]

[1] *Law Dep. College of Law and Political Science, Al-Iraqia University, Iraq.*
[2] *Computer Dep. College of Education for Pure Science, Ibn-Alhaitham, Baghdad University, Iraq.*

Global Journal of Engineering and Technology Advances, 2023, 16(02), 135–139

Publication history: Received on 18 June 2023; revised on 04 August 2023; accepted on 07 August 2023

Article DOI: https://doi.org/10.30574/gjeta.2023.16.2.0146

Abstract

As technology grows, it affect our daily lives becomes more penetrating. Our private information may be violated when communications media are used, to achieve information security this paper was based on a new technique of steganography using cryptography, color model and genetic algorithm. First, the secret text was encrypted with the advanced encryption standard (AES) algorithm. Second, the hiding was applied in two stages. First, the cover-image was converted in to the hue saturation intensity (HSI) color model and select one of the models, then divide it into a group of blocks and hiding the text in them by using least significant bit (LSB) method on specified bytes randomly, then using the genetic algorithm that calculates peak signal-to-noise-ratio (PSNR) for all blocks after the hiding process and thus obtain the best value for PSNR for the optimal block. Second, includes the final hiding of all blocks based on the results of the first stage of the best random distribution of bytes according to the results of the genetic algorithm.

The PSNR and mean square error (MSE) measures were adopted to prove the accuracy and efficiency of the results.

Keywords: Steganography; Cryptography; Color model; Genetic algorithm

1. Introduction

In the modern world, advances in digital communication have a major role to in our daily lives. Information security has a key role in securing information. Even if there are very robust and secure methodologies, they are still moving towards making these techniques safer and stronger in terms of performance measures. There is no doubt that data security is the spirit of data communication. In general, information security systems are divided into two main categories, one is encryption and the other is information hiding [1]. Both are responsible for securing information, but their techniques vary. Different researchers developed cryptography and steganography [2].

Steganography has many ways to embed the secret information by inserting it into another object. This way other people will ignore the fact that the object has hidden information [3].

The final goal of steganography and cryptography is the same, but their approaches are variant. Steganography does not change the form of data or message and retains the presence of its actual data, while in cryptography to keep the security of data is converted to an unreadable format. The weakness of encryption methods lies in the existence of the original data, even if the original data is encrypted. Information-hiding techniques are therefore additional security for encryption technologies. Combining them, it gives an additional level of security for the message through the data communication.

* Corresponding author: Shahbaa Mohammed Abdulmaged

Not only does the latest steganography techniques hide confidential information in images, but it also hide data in text [4, 5], codes [6], audio [7, 8], video [9] and DNA [10]. It also includes hiding information in different formats such as Hyper Text Mark-up Language (HTML) [1].

Information can be hidden in two ways. One is spatial domain steganography and the other is frequency domain steganography [11]. In spatial domain steganography the hidden information is embedded directly in the image pixels, for example, least significant bit based techniques [12]. In frequency domain steganography the image pixels are first converted to a frequency domain using a discrete fourier transformation [13] /discrete cosine transformation [14] /discrete wavelet transformation [12]. The information is then embedded in it. The genetic algorithm has been included along with steganography in the research work to add another level of security for more reliable application.

The organization of the paper is as follows: Section 2 includes AES. Section 3 comprises genetic algorithm. Section 4 presents the proposed technique (hiding and extracting). Results and discussion are shown in Section 5, and finally, Section 6 presents the conclusions.

2. AES

AES is based on Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The key size will specify the number of recursion of transition rounds.

The advantages of AES are lot. AES is unsusceptible to any attack but Brute Force attack. However, Brute Force attack is a difficult task even for a super computer. This is because the ciphering key size used by AES is of the order 128, 192 or 256 bits which outcomes in billions of alternations and combinations. High speed and low RAM needs were criteria of the AES chosen process. Thus, AES executes well on a large variety of hardware; from 8-bit smart cards to high execution computers. AES is also much faster than the classical algorithms; therefore, AES is adopted in our work.

3. General principle of the Genetic Algorithm

Genetic algorithm (GA) is a technique for optimization and search, which is based on the Darwinian principles of survival and reproduction [15].

The GA processes populations of chromosomes (individuals), which replace one population with another successively. The chromosome in the GA is often held in binary encoding. Each chromosome represents a candidate solution in the searching space. The GA usually needs a fitness function to assign a score (fitness) to each chromosome in current population [16].

The GA starts with initializing a population of individuals by guess. The individuals evolve through iterations, called generations. In each generation, each individual is evaluated against the fitness function. Genetic operators are used for individuals in the population to generate a next generation of individuals. The process is continued until some form of criterion is met (e.g., a given fitness is met) [16].

The simplest form of genetic algorithm uses three kinds of operators to control chromatography, they are as follows:

- Selection: In the population select chromosomes for reproduction. The fitter the chromosome is, most likely it has been chosen. That is, fitter individuals have greater than average chance of promoting the information they contain within the next generation [16].
- Crossover: Choose pairs of individuals promoted by the selection operator, randomly choose a single point within the binary strings and swap all the information to the right of this point between the two individuals [16].
- Mutation: is used to randomly change (flip) the value of single bits within individual strings [16]. It can be performed in a way that randomly select one individual from the population then change some of its bits arbitrarily.

4. The proposed technique

The proposed technique is a new text in image steganography that gathered three effective methods, which are HSI color model, LSB and GA to obtain a best image quality and security.

4.1. Hiding algorithm

In this algorithm, the encrypted secret text was hidden in the cover image using the LSB method after identifying the hiding map for the optimal block (stego-key) specified by GA. The interface of the Matlab genetic algorithm was used to perform the work of the genetic algorithm after selecting the selection process type is stochastic uniform selection, crossover type is scattered crossover, Mutation type is adaptive feasible, the following are the steps of the hiding algorithm

- Read the cover-image.
- Read the secret text.
- Convert the secret text in to ASCII code and then in to binary code.
- Compute the length of the binary secret text.
- Encrypt the secret text using AES algorithm.
- Decompose the cover-image in to the HSI color model.
- Select one of color model.
- Divide color model in to 4 blocks.
- Divide each block in to other 4 blocks.
- Generate random numbers to specify bytes hiding.
- Hide the encrypted secret text in the randomly assigned bytes in step 8 within the blocks in the color model using the least significant bit method.
- Determine the parameters used in the genetic algorithm as follow:
  - An initial population of chromosomes (individuals), where the creation of the initial generation is a starting point in solving the problem, and the process of building the initial generation was done randomly, the number of generation chromosomes in this problem has been selected as the number of blocks, and the length of the chromosome is equal to the length of the binary secret text.
  - Composing resulted color model with the rest of color model to get the stego-image.
  - The fitness function of the genetic algorithm using the equation PSNR [17]:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(m,n)]^2}{M * N} \quad \ldots\ldots(1)$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \quad \ldots\ldots..(2)$$

    Where M, N are the total number of pixels in the image and L is the maximum dynamic range.
  - Selection process type is stochastic uniform selection.
  - Crossover type is scattered crossover.
  - Mutation type is adaptive feasible.
  - Modify the initial population and generate a new population by repeating the steps (b-f) until the stop condition become true (the maximum number of generations that are generated to reach the optimal solution).
- Adopting the result of the genetic algorithm represented by the highest value (PSNR) for the optimal block and according to random distribution of the bytes specified in it (stego-key), all blocks except the last block will be used in hiding process.
- Hide the length of the binary secret text and the stego-key in the last block using LSB, since the length of the secret text will be hidden in the first bit of each byte, the stego-key will be hidden in the second bit of each byte.
- View the stego-image.

4.2. Extracting algorithm

The extracting algorithm will be implemented as follows:

- Read the stego-image.
- Decompose the stego-image in to the HSI color model.
- Select the same color model (as in hiding algorithm).
- Divide color model in to 4 blocks.
- Divide each block in to other 4 blocks.
- Extract the length of the secret text from the last block.
- Extract the stego-key (Sequence of random bytes) from the last block.
- Extract the encrypted secret text from the image blocks depending on the stego-key.

- Decrypt the extracted secret text using AES algorithm.
- View the extracted secret text.

5. Results and Discussion

Two color cover-images are used. Fig (1) shows the images used in the experiments. The evaluation parameter PSNR is used to verify the image quality between cover-image and stego-image in experiments that varied depending on the variation of many factors effects the performance of the proposed technique such as the size of the cover-image and the length of the secret text. The stego-images are shown in fig (2) as a result of the proposed technique.

Figure (1) a) Peppers cover-image

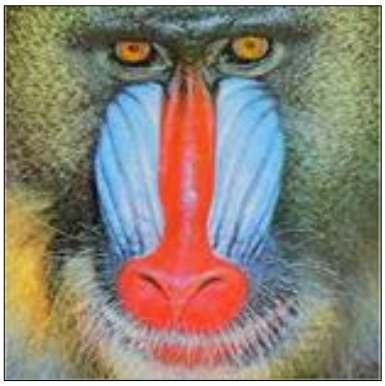

Figure (1) b) Baboon cover-image

Figure (2) a) Peppers stego-image

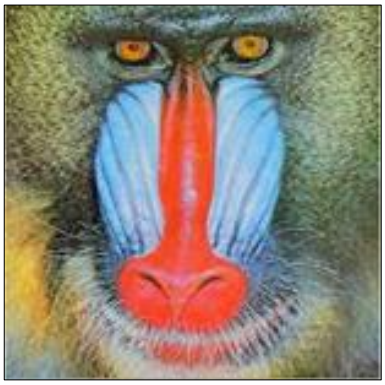

Figure (2) b) Baboon stego-image

Table (1) shows the result of the proposed technique for the images above:

Table 1 PSNR values of the results

Image name	**Peppers**	**Baboon**
Image size	256 x 256	256 x 256
Message (no. of char.)	50	150
Highest PSNR of stego-image	82.8769	79.6312
No. of the optimal block	12	14

6. Conclusion

- The results proved the strength and efficiency of the proposed technique.
- It was found that encryption of the secret text using the AES algorithm results in increased robustness of the proposed technique.

- It turned out that decomposing the image into the HSI color model would increase the confidentiality of the proposed technique.
- It has been shown that the use of the technique of dividing the image into blocks increases the security level of the proposed technique and the difficulty of detecting hidden information.
- The optimal value of PSNR was obtained by using the genetic algorithm.
- The use of stochastic uniform selection in selection process and scattered crossover in crossover and adaptive feasible in mutation in genetic algorithm leads to the best results.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Majeed, M.A.; Sulaiman, R.; Shukur, Z.; Hasan, M.K. A Review on Text Steganography Techniques. Mathematics 2021, 9, 2829.

[2] V, G., G, I. A review on image steganographic techniques based on optimization algorithms for secret communication. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-15568-7.

[3] Jan, A., Parah, S.A., Hussan, M. et al. Double layer security using crypto-stego techniques: a comprehensive review. Health Technol. 12, 9–31 (2022). https://doi.org/10.1007/s12553-021-00602-1.

[4] Wagh, Dr. Mrs. S. K., Upadhyay, Mr. G., Bakan, Ms. U., Shinde, Ms. N., & Nimbalkar, Ms. S. (2020). Cryptography and Steganography Techniques in Video. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 9, Issue 2, pp. 1044–1048). Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP. https://doi.org/10.35940/ijrte.b4055.079220.

[5] S.S. Baawi, M.R. Mokhtar, R. Sulaiman, A comparative study on the advancement of text steganography techniques in digital media, ARPN J. Eng. Appl. Sci. 13, 5, (2018), pp.1854–1863.

[6] Ayantu Guye Berisa, Information Assurance and Security Handout, Woliso, Oromia, Ethiopia June, 2020. http://ndl.ethernet.edu.et/bitstream/123456789/90354/1/Information%20Assurance%20and%20Security%20all%20in%20One%20Handout.pdf

[7] Ahmed A. Alsabhany et al, The Progressive Multilevel Embedding Method for Audio Steganography, 2020 J. Phys.: Conf. Ser. 1551 012011DOI 10.1088/1742-6596/1551/1/012011.

[8] Wasif Ali Shah, Danish Shehzad et al, Audio Steganography Based on LSB MSB difference and FMC, International Journal of Computer Science and Information Security (IJCSIS),Vol. 15, No. 6, June 2017.

[9] S. Limkar, A. Nemade, A. Badgujar, R. Kate, Improved Data Hiding Technique Based on Audio and Video Steganography, Smart Comput. Informatics, Springer, (2018), pp.581–588. https://doi.org/10.1007/978-981-10-5547-8_60.

[10] Khalifa, A., A Secure Steganographic Channel Using DNA Sequence Data and a Bio-Inspired XOR Cipher. Information 2021, 12, 253. https://doi.org/10.3390/info12060253.

[11] Fayyad-Kazan, et al. JPEG Steganography: Hiding in Plain Sight. Int J Forens Sci 2021, 6(1): 000223. https://doi.org/10.23880/ijfsc-16000223

[12] Vajiheh Sabeti, Masomeh Sobhani, Seyed Mohammad Hossein Hasheminejad, An adaptive image steganography method based on integer wavelet transform using genetic algorithm, Computers and Electrical Engineering, Volume 99, 2022, https://doi.org/10.1016/j.compeleceng.2022.107809.

[13] Ritu Sindhu, Pragati Singh, Information Hiding using Steganography, International Journal of Engineering and Advanced Technology (IJEAT), Volume-9 Issue-4, April, 2020, DOI: 10.35940/ijeat.D8760.049420

[14] Zeena N. Al-Kateeb et al, Encryption and Steganography a secret data using circle shapes in colored images, 2020 J. Phys.: Conf. Ser. 1591 012019

[15] AlKhafaji, Baydaa jaffer et al. Segmenting video frame images using genetic algorithms. Periodicals of Engineering and Natural Sciences (PEN) 8 (2020): 1106-1114.

[16] Alam, Tanweer & Qamar, Shamimul & Dixit, Amit & Benaida, Mohamed, Genetic Algorithm: Reviews, Implementations, and Applications, (2020), DOI: 10.36227/techrxiv.12657173.

[17] Thung, Kimhan & Raveendran, Paramesran, A survey of image quality measures, (2010), p (1–4), DOI: 10.1109/TECHPOS.2009.5412098.