International Journal of Mathematics, Statistics, and Computer Science
Vol. 3
ISSN: 2704-1077 eISSN 2704-1069, DOI: 10.59543/ijmscs.v3i.11135

Hybrid Steganography for Enhanced Information Security

Nadia Mohammed Abdulmaged
Department of Computer Sciences, College of Education for Pure Sciences (Ibn AL-Haitham), University of Baghdad, Baghdad, 0053, Iraq
narimanfn@gmail.com

Received 21.10.2024, Revised 29.05.2025, Accepted 20.06.2025

ABSTRACT: The constant integration of technology in society has made it easy for personal information privacy to be violated. In response to this challenge, this paper develops a steganographic technique using cryptography, colour models, and Genetic Algorithm (GA). The proposed method starts with the Advanced Encryption Standard (AES) encryption of the secret text. After that, the encrypted data is embedded in an input image through a two-fold hiding technique. Initially, the input-image is altered into the Hue Saturation Intensity (HIS) colour model, and a particular model is chosen for the next process. Then the image is segmented into blocks, and the secret text is then hidden employing the Least Significant Bit (LSB) technique on some randomly chosen bytes. To improve the hiding efficiency of the hiding process, a genetic algorithm (GA) is used to find the peak signal-to-noise ratio of the blocks. A particular block that achieves the maximum PSNR value is chosen as the block that is suitable for embedding. In the second stage, all blocks are hidden according to the result of a GA, while the byte distribution is as optimal as possible. The performance of the proposed method is determined using functions like PSNR and Mean Squared Error (MSE). The results indicate that the method is fast and effective at keeping the secret information reliable while also maintaining the output- image quality.

Keywords: steganography, cryptography, colour model, genetic algorithm, data security.

1. INTRODUCTION

Modern communication technology has become an integral part of our society, where everyone is influenced by its use. Data protection is essential to prevent unauthorized access to our information. Despite advanced security methods being implemented today, new research has been directed towards fine-tuning of these methods in regular use to achieve better efficiency and security. Security without doubt is one of the most important facts of data communication. Data security systems are generally categorized into 2 primary approaches: encryption and information hiding [1]. Although both cryptography and steganography are processes of storage and communication undertaken to protect messages, they are done differently. The growth of cryptography as well as steganography was undertaken by a number of researchers [2].

Steganography involves the insertion of a hidden message in such a way that people will not notice what is hidden between them [3].

The ultimate objective of steganography and cryptography is identical: to protect information. However, they use different approaches in their strategies. Steganography techniques of securing data through embedding it in other data without changing the actual outlook of it, preserving the original message’s existence. On the other hand, cryptography alters data into a form that cannot be read easily in order to enhance its security. From this, it can be deduced that the weakness of the encryption procedures results from the unchangeable presence of the original information even when ciphered. Therefore, steganography techniques are used as the second factor of protection for encryption technologies. The use of these methods provides an additional safeguard for text during transmission of data.

Steganography can embed data in all types of media, text [4], [5], images, codes [6], sound [7], [8], animated images [9], and DNA [10]. It can also hide data in formats like hypertext markup language [1].

Data could be concealed either in the space or the frequency domain [11]. Spatial domain of steganography involves embedding of the data in the actual pixels of the image, mostly through manipulation of the LSBs [12]. In frequency domain data hiding, the pixels of an image are altered into the frequency domain by employing the discrete Fourier transform [13], the discrete cosine transform [14], or the discrete wavelet transform [12]. It is then saturated with the information. Another level of security for the application was added in this study through the integration of the two approaches, steganography and GA.

Therefore, the overall goal of this study is to propose an optimal steganographic method for achieving secure information hiding in digital images. The presented work exploits the use of cryptography, colour models and GA as means to improve data protection and avoid access by unauthorized people.

This paper is divided into six subtopics. In section 2, the AES is described, section 3 focuses on the GA, and section 4 the proposed methodology. Further analysis of the study findings is presented in section 5, while section 6 contains the conclusion of the paper.

2. AES

AES is a block cipher derived from the Rijndael algorithm, which operates only with a 128-bit block with key lengths of 128, 192, or 256 bits. The length of the key then determines the number of rounds in the encryption process.

AES is considered very secure; no known attacks other than Brute Force exist. Nonetheless, Brute Force attacks are not tactfully achieved due to the large key size; therefore, it has billions of possibilities. AES was also chosen because of its speed and low memory utilization, which is good for any sort of hardware. Further, AES is faster than most of the earlier encryption algorithms, and therefore it is suitable for several applications.

3. GENERAL PRINCIPLE OF GENETIC ALGORITHM

Similar to the theory of evolution presented by Charles Darwin, GA follows the survival of the optimization and fittest to determine solutions.

The GA operates by modifying, during each cycle, a set of possible solutions, also called chromosomes (population of individuals). Such chromosomes are normally described by means of a binary code. Each chromosome is a solution that determines how well (fitness) the chromosome being tested solves the problem. The GA gradually replaces a current population of chromosomes with a new population that is likely to be better. GA starts with an initial population or set of possible solutions, all created at random. This is followed by a process known as evolution, where the solutions are advanced and are made better all the time. In each generation, these solutions are evaluated in order to assess how well each of the solutions meets the problem. The genetic operators of crossover and mutation are used to produce new solutions. Such negotiations go on until a satisfying solution is elicited [15].

Most basic GA operates three control chromatography operators. These operators are:

Selection: When it comes to a population’s heredity, the only and best-fitting chromosomes are normally transmitted to another population. Fitter individual have a higher probability of transmitting their genetic information.

Crossover: Choose a couple of individuals from the population. Choose one of their binary strings at random, and select a position within that string. Change this position to carry the bits to the right of this position in the middle of two individuals.

Mutation: It works in a very random manner by flipping the bits within strings, which can affect traits of an individual.

4. THE PROPOSED METHOD

The proposed text in the image data hiding method combines three effective techniques: the HSI colour model, LSB, and a genetic algorithm. This approach is used to ensure that image quality and security are ideal in the process.

4.1. HIDING ALGORITHM

The GA found out the best block, which is the output-key in the input image. Use this block and the LSB technique, and the secret text was encrypted and concealed. The GA’s interface in MATLAB entails a stochastic uniform selection, scattered crossover, and adaptive feasible mutation. The following outlines the hiding algorithm’s steps:

1. Read an input-image.
2. Input the secret message.
3. Take the secret message and change it into an ASCII code, then change that code to binary.
4. Calculate the binary length of the secret message.
5. Make the secret message more secure by encrypting it using AES.
6. Use colour segmentation to convert the input image into the HSI colour model.
7. In the colour space, it is always possible to choose one of the channels (H, S, or I).
8. The desired/ chosen colour channel should be divided into four blocks.
9. Divide each block into 4 equal smaller blocks.
10. Random number generators will be used to decide which of the bytes in the blocks will be used for the purpose of hiding.
11. Conceal the encrypted secret message in the selected random bytes using the LSB method.

12. Determine the parameters for the GA as follows:
    a) Initial population: from a first population of individuals, also known as chromosomes, to be an equal number to the blocks. All the chromosomes have a length, which is equal to the binary secret text. These chromosomes should be generated at random.
    b) Output- image creation: authentically blend the above derived colour pattern with the rest of the colour pattern and generate an output-image.
    c) Fitness function: take the PSNR [16] and incorporate the same as a fitness function for the GA.

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

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \qquad (2)$$

We will use the variables M and N to symbolize the combined total of pixels in the image, while L would represent the ultimate dynamic scope of the image.

    d) A stochastic uniform selection method is employed.
    e) There is crossover occasionally.
    f) Adaptive feasible mutation is applied.
    g) As the initial population is generated, make successive modifications on and from it to produce more populations through (b-f), while going, until a stopping condition of the maximum number of generations is reached.

13. Choose the PSNR highest block that is selected as the optimal choice. From the given notion that the bytes in this block are randomly distributed, here called (output-key), all blocks up to another block before the last one will be employed in the hiding process.
14. LSB substitution to conceal the size of the binary secret message and output-key in the least block. The size of the secret message is kept in the 1st bit of each byte and the output -key is kept in the 2nd bit of the respective byte.
15. Output the output - image that has been generated.

For a better understanding of the proposed algorithm, see the flowchart shown in Figure 1, which gives the main steps of the above algorithm.

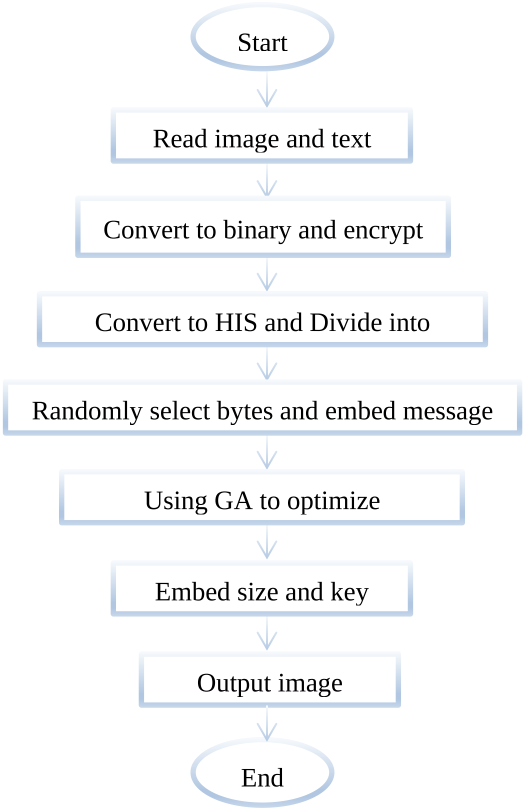
Start
Read image and text
Convert to binary and encrypt
Convert to HIS and Divide into
Randomly select bytes and embed message
Using GA to optimize
Embed size and key
Output image
End

Figure (1): Flowchart of hiding algorithm.

4.2. EXTRACTING ALGORITHM

The extraction process involves these steps:

1. Load the output- image.
2. Convert the output-image into HSI colour model.
3. The colour space selected for hiding should be used for finding hidden data also.
4. To take the final colour space, divide it into four blocks.
5. Divide each block into four parts.
6. Read the last block of the message and get its secret text length.
7. Take out the output-key (random byte sequence) from the least block.
8. Decode the ciphered secret message through the image blocks using the output-key.
9. Use AES to decrypt the secret text.
10. Extract the secret message and show it.

5. DISCUSSION

In order to quantify the quality of the proposed method, two coloured host images, Lena and Plane, were used as shown in Figure 2. To evaluate the quality of the output-images produced by the method, PSNR was used as the measurement index since it calculates image distortion.

To assess how other conditions could affect the efficiency of the method, the experiments were performed under different circumstances. These factors included the size of the input-image and the length of the secret message. In both cases, the size of the input-image and the length of the secret message had affected the results obtained from the steganography operation. Fig. 3 displays the output-images that are generated using the proposed method.

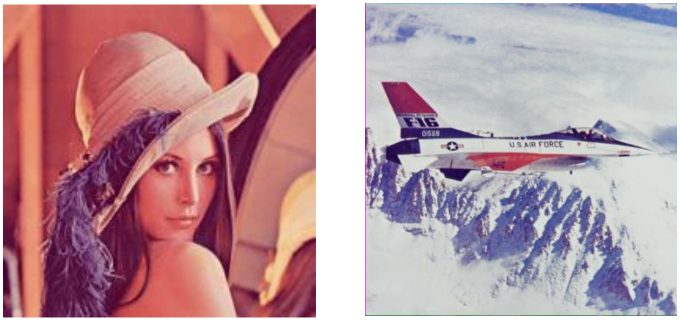

Fig (2) a) Lena input-image b) Plane input-image

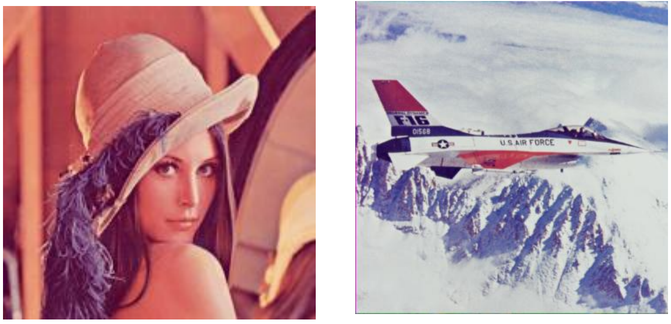

Fig (3) a) Lena output-image b) Plane output-image

In Table (1), the average PSNR obtained by both the input-images in different experiment settings is mentioned. The results show the feasibility and practicality of the proposed method in application to image retrieval without significant loss in image quality and with secret information embedding. The localization of the ideal block for embedding was found out with the help of GA, and the numbers of the blocks together with it are shown in Table 1.

Table (1): Results of PSNR.

Name of image	Lina	Plane
Size of image	512 x 512	512 x 512
Message (number of characters)	25	75
Maximum PSNR of output-image	83.8567	77.6114
Number of the optimal block	10	12

6. CONCLUSION

The proposed method is intended to be more efficient than conventional methods if implemented. AES encryption of the secret text added much more strength to the concept, making it more reliable. To perform the image transformation to the HIS colour model, several benefits arose, such as improving the secrecy of the proposed method. Image partitioning using the block-based techniques took the security level to another level, additionally camouflaging the hidden data in the proposed method. GA optimization provided the optimal value of PSNR as compared with the other methods. The best result was obtained when stochastic uniform selection, scattered crossover, and adaptive feasible mutation were incorporated into the GA.

Funding: This research received no external funding.
Conflict of interest: The authors declare no conflicts of interest.

REFERENCES

[1] Knöchel, M., & Karius, S. (2024). Text Steganography Methods and their Influence in Malware: A Comprehensive Overview and Evaluation. Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security.

[2] Ahmad Bamanga, M., Kamalu Babando, A., & Ahmed Shehu, M. (2024). Recent Advances in Steganography. IntechOpen. doi: 10.5772/intechopen.1004521.

[3] H. Abood, M., & W. Abdulmajeed, S. (2022). High Security Image Cryptographic Algorithm Using Chaotic Encryption Algorithm with Hash-LSB Steganography. Al-Iraqia Journal for Scientific Engineering Research, 1(2), 65–74. https://doi.org/10.58564/IJSER.1.2.2022.53.

[4] Mohammed Abdulmaged, S., Mohammed Abdulmaged, N., & Abdulbaqi Salman, S. (2024). New Steganography Technique by Integrating Genetic Algorithm and Data Hiding. Journal of Al-Qadisiyah for Computer Science and Mathematics, 16(2), Comp. 112–117. https://doi.org/10.29304/jqcsm.2024.16.21547.

[5] S. M. Abdulmaged, N. M. Abdulmaged, "A new steganography technique based on genetic algorithm", Global Journal of Engineering and Technology Advances, Vol. 16, Issue 2, pp. 135–139, 2023. DOI: https://doi.org/10.30574/gjeta.2023.16.2.0146.

[6] Fikadu Wayesa, "Information Assurance and Security Handout", Wachemo University Faculty of Engineering and Technology School of Computing and Informatics Department of Information Technology, Hosanna, SNNP, Ethiopia, 2022.

[7] Muhammad Harith Noor Azam, Farida Ridzuan, et al. "A Method of Cover Audio Selection for Embedding Based on Various Criteria", ITM Web Conf. 63 01001 (2024). DOI: 10.1051/itmconf/20246301001.

[8] Vaibhavi P. Naik, Dr. Aisha C. F. Fernandes, " Audio Steganography, IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.196-201, May-June-2022. Available at doi: https://doi.org/10.32628/CSEIT5228368.

[9] Arpan Bhattacharya, Ananya Seth, Dheeraj Malhotra, and Neha Verma. 2023. Cloud Steganography: An Intelligent Approach to Improve Data Security in the Cloud Environment. In Proceedings of the 4th International Conference on Information Management &amp; Machine Intelligence (ICIMMI '22). Association for Computing Machinery, New York, NY, USA, Article 65, 1–5. https://doi.org/10.1145/3590837.3590902.

[10] Na, D. DNA steganography: hiding undetectable secret messages within the single nucleotide polymorphisms of a genome and detecting mutation-induced errors. Microb Cell Fact 19, 128 (2020). https://doi.org/10.1186/s12934-020-01387-0.

[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] Pranab K. Muhuri, Zubair Ashraf, Swati Goel, A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization, Applied Soft Computing, Volume 92, 2020, 106257, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2020.106257.

[13] Lwin, Thandar and Su Wai Phyo. "Information Hiding System using Text and Image Steganography." (2014).

[14] Abadin AZ, Sulaiman R, Hasan MK. Randomization Strategies in Image Steganography Techniques: A Review. Computers, Materials & Continua, 2024, 80(2): 3139-3171. https://doi.org/10.32604/cmc.2024.050834

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

[16] Sara, U., Akter, M., & Uddin, M. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. Journal of Computer and Communications.