International Journal of Safety and Security Engineering
Vol. 12, No. 5, October, 2022, pp. 639-643
Journal homepage: http://iieta.org/journals/ijsse

GUI Implementation of Modified and Secure Image Steganography Using Least Significant Bit Substitution

Surya Prakash Yalla*, Archana Uriti, Abhisek Sethy

Department of Information Technology, GMR Institute of Technology, Srikakulam 532127, India

Corresponding Author Email: suryaprakash.y@gmrit.edu.in

https://doi.org/10.18280/ijsse.120513

Received: 6 August 2022
Accepted: 10 October 2022

Keywords:
steganography, least significant bit, discrete wavelet transformation, advanced encryption standard

ABSTRACT

Due to swift improvement of information innovation in recent times, providing security to data has become major concern and threat to Information Privacy has become inevitable. Data Hiding technology is an efficient way to solve the problems of data leakage and loss of information. Data hiding called steganography is a security method to provide security to secret data which is transferred from sender to receiver from harmful attacks. Steganography is an interaction of concealing a mysterious message inside a cover object which is not secret. There are many cover media like images, audio, video, text files etc. There are many ways to approach steganography like spatial domain, transformation domain, masking and filtering. This technique is helpful because the human eye is quite insensitive to the minute changes that help the embedded data stay safe and secure. The main motive of steganography is to get high stego image quality, low computational complexity, more embedding capability, visually unnoticeable, invisibility, and improved security. A capable steganographic technique must be resistant to any steganalysis approach the secret data is prone to. In this proposed system, implement the GUI implementation image steganography in spatial domain using Least Significant Bit (LSB) where the modified high capacity cover image undergoes the Discrete Wavelet Transformation (DWT) and propose an Advanced Encryption Standard (AES) secret key stego system such that the data is secure. The distortion between the two images in identified with the help of MSE and Histogram analysis.

1. INTRODUCTION

Data is very important to any person or an organization. The interchange of data between two possible parties should be processed in secured way to avoid any data tampering. The significance of data hiding method arises from the fact that there is no dependability on the medium through which the data is transferred. Aim of data hiding is to insert secret data into cover with purpose of recognition, copyright shielding, and notation. The motive of steganography [1] is to conceal and deceive. It is covered communication and it uses any medium like audio, video, text to hide messages. it is originally not a form of cryptography because it doesn't involve mixing up of data with a key [2]. Cryptography encrypts the data but if any intruder centralizes to achieve the key, he may identify the secret message [3]. So, the concept of steganography came into existence. The main limitations involved in this process are message go through the data line-by-line to identify definite patterns and build observations [4]. Visualization of data is not only important for data scientists and data analysts but also for the people who are there in finance, data size, need of immutability of embedded data during deformations [5] like third party removal or moderation [6].

1.1 Image definition

An image is a pixel combination of the basic colors red, blue and green. The binary conversion of the color code is represented using byte array. A cover image is chosen and it is the image that we are embedding our secret data into and we convert each pixel of the cover image into bits (8 each) where the last bit of each image is substituted with their corresponding bits of secret information. So this will not totally change image that we are transferring.

Suppose we take 8-bit gray scale image with bits

10101011	00101011	11101010	11011010
11011010	10011010	00101100	00011101

The secret information to hide: - 10110100.

If we insert these 8 bits into the LSB of the 8 bits above, we get the following sequence of bits.

10101011	00101010	11101011	10100001
11011010	10011011	00101100	00011100

Only a few bits are required to insert the secret message successfully, so only the last bits are changed. These modified bits have a negligible effect on the cover image.

The remaining paper is organized in such a way that, Section II gives the information of related work, and Section III shows the proposed work. The results are discussed in Section IV. The paper finally comes to an end in Section V.

2. RELATED WORK

Arora et al. [1] discussed about the overview of the LSB

technique of steganography. The important parameters taken into consideration in this paper are PSNR ratio, MSE, data hiding capacity.

Arora et al. [2] analyzed and reviewed different steganographic techniques for suppression of the information in an image. It provides us a comparative analysis of different image steganographic techniques like spatial domain, transformation domain, masking and filtering on various features like high capacity, perpetual transparency, robustness, temper resistance and computational complexity.

Emad et al. [3] proposed a Steganographic algorithm that conceal secret bit stream of the secret data into LSBs of the approximation coefficients which are obtained from Integer Wavelet Transform (IWT) of gray scale pictures and each segment of color pictures to obtain stego-pictures. This paper concentrates on high payload capacity with more security and higher invisibility.

Ahmed A. and Ahmed A. [4] proposed two layers of encryption and hiding stages. First, the image is encrypted by using a Secret key (extracted from MSB) and by using binary data double XOR operations, and then encrypted stream of bits is inserted into cover image using LSB technique.

AI-Ataby and AI-Naima [5] proposed an improved high capacity image Steganography method that mainly depends on the transformation of wavelet with tolerable degree of undetectability and deformation in cover image and a high degree of overall security.

Danny Adiyan et al. [6] combined steganography with vignere cipher. This paper also compares the size of an image file to the size of the information that can be inserted. The paper also completely analyses the Least Significant Bit substitution of steganography.

Singh [7] surveyed and gave an overview of different steganographic techniques, major types and classifications. This paper discussed about various steganographic quality measures, terminologies and types. Steganography techniques like Discrete Fourier Transform, Discrete Cosine Transform, Discrete Wavelet Transform, Least Significant Bit, Pixel Value Differencing, Edge Based data Embedding method, Random Pixel embedding method.

Agath et al. [8] gave an overview on the steganography and cryptography. It presents an honest comparative analysis between different selected encryption algorithms on the basis of parameters such as key size, block size, rate of encryption, impact of security of algorithm and memory usage. The comprehensive analysis shows the AES and HEX algorithms gives us high level of security and are strong in nature, hence providing confidentiality.

3. PROPOSED WORK

This section gives the implementation details of our work. In this proposed work, implementation work is shown in different phases. The first phase describes the transformation process of the image, i.e., converting the image from RGB to gray scale and then applying DWT [9] on the image. The second phase deals with the encoding process, resulting a stego image using LSB substitution method. In the third phase, we encrypt and decrypt the stego image using AES algorithm for secure transmission of the image storing secret data [10]. Finally, we perform the decoding operation [11] at the receiver side to extract the secret data.

Phase I: Gray scale and DWT

Firstly, convert the cover image into gray scale image by doing such image pixel intensity decreases to 0-127. Then resize image into 256*256. Then transform the image using the 2D- Discrete Wavelet Transformation [12] as it is a lossless compression and gives high resolution images when compared to other transformation techniques. As DWT is an enhanced version of Fourier transformation and it uses a low pass and high pass filter to decompose the images into horizontal, vertical and diagonally. So, in Figure 1 the steps involved in 2D-DWT is depicted.

Here in the Figure 1, the wavelet transformation of image is defined and can be theoretically as below:

LL — Passing through two simultaneous LPFs — gives an approximation

LH — Passing through LPH and then HPF — Horizontal features (HPF along rows)

HL — Passing through HPF and then LPF — Vertical features (HPF along col.)

HH — Passing through two simultaneous HPFs — Diagonal features (HPF distributed equally along both rows and col.)

It can be depicted with the below equation:

$$X_{a,b} = \int_{-\infty}^{\infty} x(t)\varphi_{a,b}\ (t)dt$$

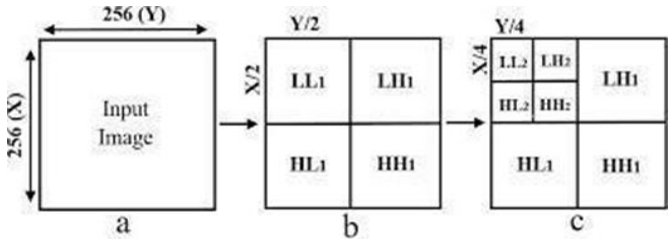

Figure 1. Two dimensional wavelet transformation of image

Phase II: Encoding process

1. Transform the text message to its binary form.
2. Set up the yield picture as insert picture.
3. Go through each and every pixel of the picture and do as follows:
   - Transform pixel rate to binary format.
   - Obtain the upcoming message bit to be inserted.
   - Generate variable which is named as temp.
   - If message bit and LSB value of the pixel are alike, assign temp to 0 else temp to 1.
   - This adjustment of temp variable is implemented by proceeding XOR message bit and LSB of pixel.
   - Change pixel of resultant image to sum of input image pixel value and temp.
4. Continue assigning the resultant image until all bits in the message are inserted.

Phase III: Encrypting and decrypting stego image

For each round of AES, plain image and a secret key is taken. The secret key chosen is the same for encryption and decryption process, thus simplifying the pattern. For the two ciphers and inverse cipher [13], AES implements the round function which consists of four different types of byte oriented

transformations [14]: substitute bytes, shift rows, mixed columns, add round key. Advanced Encryption Standard integrates operations like XOR, Octet substitution with an S-box, row and column rotations and a MixColumn for a round shown in Figure 2. The main advantage, a regular computer can take reasonable amount of time to implement. As it can be implemented in both hardware [15] and software, it makes algorithm most robust. Disadvantages are, A simple algebraic structure used in AES round operation. Later every block is encrypted in same way [16].

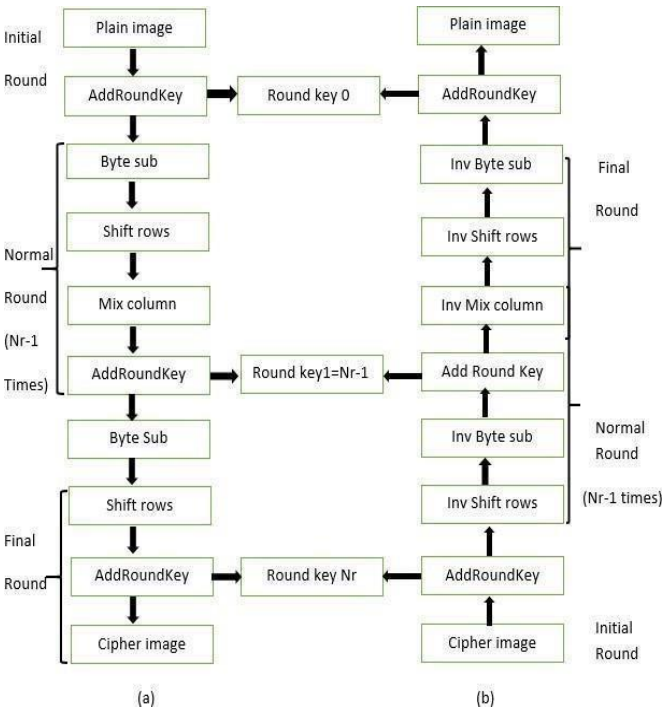

Figure 2. AES image encryption and decryption

Phase IV: Decoding process

1. Compute the total number of pixels the text is reserved.
2. Every character is expressed in 8 bits each.
3. The number of pixels = characters * bits.
4. Now, traverse through the image and one pixel from time to time.
5. Store the LSB of every pixel in the array.
6. Later the extraction process of LSBs of the needed pixels, take every 8 bits from the array and transform it into a corresponding character.
7. The text in stego image will get extracted.

Algorithm

Sender side:

Step 1: Input – Cover image (shown in Figure 3).

Step 2: Gray scale version of cover image (shown in Figure 4).

Step 3: DWT of gray scale cover image.

Step 4: Encode secret data into the transformed image using LSB substitution (shown in Figure 5).

Step 5: Encrypt the stego image obtained in step 4 using AES algorithm (shown in Figure 6).

Receiver side:

Step 6: Decrypt the stego image.

Step 7: Decode stego image, extract secret data.

4. RESULTS

By observing, there is not much difference among the transformed cover image and the stego image which is the main advantage of LSB Substitution [17] as it pertains the data quality and helps in seemingly insensitive to the eyes of the third party [18]. The minute differences are found by plotting histogram, which is shown in Figure 7, and calculating the mean squared error [19] between the two images.

Figure 3. Cover image taken as input

Figure 4. Grayscale image

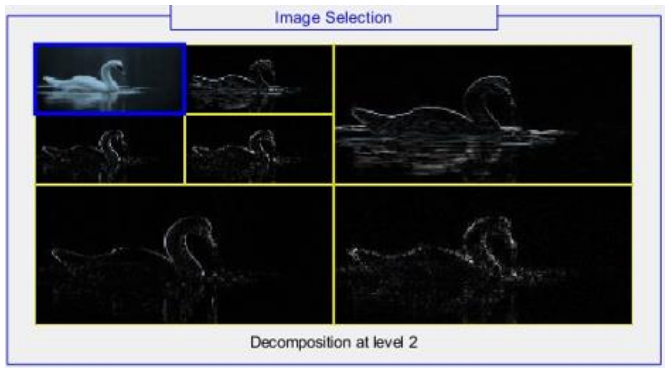

Figure 5. Transformed image

Figure 6. Stego image

The above AES implementation is done in MATLAB. Here stego image is taken as input to the AES and encryption is performed and again decrypted constructing the original stego image back without any distortion shown in Figure 8 & Figure 9. This helps the data be protected from any unauthorized

access [20]. AES algorithm having extremely large key space can withstand many attacks like brute force, cipher [21] and plaintext attacks [22].

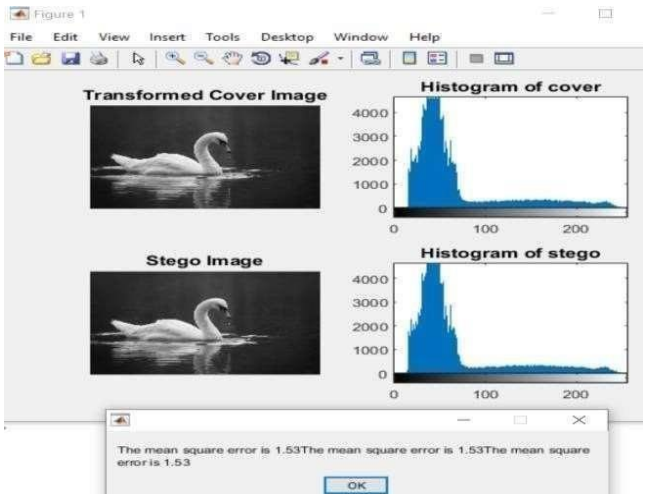

Figure 7. Histogram analysis and MSE of the 2 images

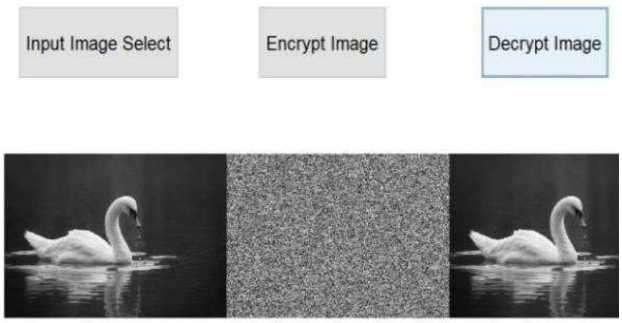

Figure 8. AES encryption and decryption of stego

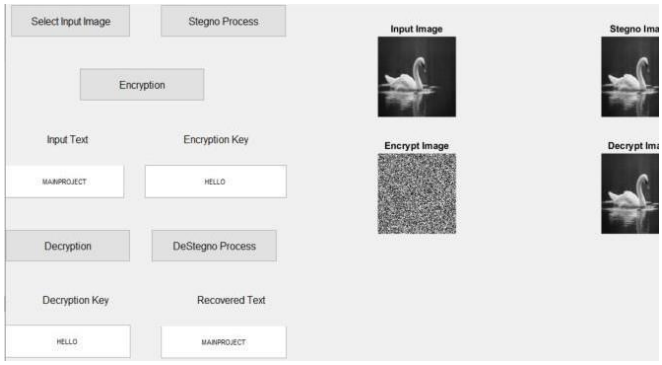

Figure 9. Overall GUI implementation & decoding process

5. CONCLUSION AND FUTURE SCOPE

In this proposed work, a secure steganographic algorithm is developed that facilitates the transmission of the image with data embedded inside it safely and the data is procured by the recipient without any deviations. This technique offers double security as the stego image is encrypted first and then sent to the receiver. The secret key is shared only among the sender and the receiver. Here mainly focused on the security parameter and in future one can enhance the technique for the parameter specifications mentioned earlier and understand the level of accuracy and facilitation. While learning about how steganography works in an improved manner over cryptography as it does not encapsulate the secret data but only changes its form. In this, mention the benefits a combination of cryptography and steganography technique. Apart from this, here focus on fidelity of an image, i.e., to check the quality of the image after steganography and learn more number of other algorithms and analyze their efficiencies.an equation. Set the equation flush left, without indenting it.

REFERENCES

[1] Arora, A., Singh, M.P., Thakral, P., Jarwal, N. (2016). Image steganography using enhanced LSB substitution technique. In 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, pp. 386-389. https://doi.org/10.1109/PDGC.2016.7913225

[2] Arora, H., Bansal, C., Dagar, S. (2018). Comparative study of image steganography techniques. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, pp. 982-985. https://doi.org/10.1109/ICACCCN.2018.8748451

[3] Elshazly, E., Abdelwahab, S., Abouzaid, R., Zahran, O., Elaraby, S., Elkordy, M. (2018). A secure image steganography algorithm based on least significant bit and integer wavelet transform. Journal of Systems Engineering and Electronics, 29(3): 639-649. https://doi.org/10.21629/JSEE.2018.03.21

[4] Ahmed, A., Ahmed, A. (2020). A Secure Image Steganography using LSB and Double XOR Operations. International Journal of Computer Science and Network Security, 20(5): 139-144.

[5] Al-Ataby, A., Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transform. Changes, 4: 6.

[6] Danny Adiyan, Z., Purboyo, T.W., Nugrahaeni, R.A. (2018). Implementation of secure steganography on jpeg image using LSB method. International Journal of Applied Engineering Research, 13(1): 442-448.

[7] Singh, N. (2017). A survey paper on Steganography. International Refreed Journal of Engineering and Science (IRJES), 6(5).

[8] Agath, A., Sidpara, C., Upadhyay, D. (2018). Critical analysis of cryptography and steganography. IJSRSET, 4(2): 2395-1990.

[9] Chintada, K.R., Yalla, S.P., Uriti, A. (2021). A deep belief network based land cover classification. In 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), Kuala Lumpur, Malaysia, pp. 1-5. https://doi.org/10.1109/i-PACT52855.2021.9696524

[10] Sethy, A., Patra, P.K., Nayak, S.R. (2022). A hybrid system for handwritten character recognition with high robustness. Traitement du Signal, 39(2): 567-576. https://doi.org/10.18280/ts.390218

[11] Uriti, A., Yalla, S.P., Chintada, K.R. (2021). An approach of understanding customer behavior with an emphasis on rides. In 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), Kuala Lumpur, Malaysia, pp. 1-5. https://doi.org/10.1109/i-PACT52855.2021.9696837

[12] Archana, U. (2020). An approach to analyze YouTube data using Hadoop. International Journal of Advanced

Science and Technology, 29(6): 4910-4918.
[13] Archana, U., Sridhar, U. (2017). A novel quantization approach for approximate nearest neighbor search to minimize the quantization error. IJIRSET, 2017.
[14] Yalla, S.P., Uriti, A., Sethy, A., Chintada, K.R. (2022). Wheel chair movement through eyeball recognition using raspberry Pi. Specialusis Ugdymas, 1(43): 8583-8591.
[15] Yalla, S.P. (2020). IoT based location survelliance using QuadrappedRobot. IJAST, 29(4): 4825.
[16] Sethy, A., Raut, A.K., Nayak, S.R. (2022). Face recognition based automated recognition system. In 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 543-547. https://doi.org/10.1109/Confluence52989.2022.9734135
[17] Sethy, A., Patra, P.K., Nayak, S.R. (2022). A deep convolutional neural network-based approach for handwritten recognition system. In Computational Intelligence in Pattern Recognition, pp. 607-617. https://doi.org/10.1007/978-981-16-2543-5_52
[18] Sethy, A., Patra, P.K., Nayak, R.K., Sahoo, D. (2019). Transform based approach for handwritten character and numeral recognition: a comprehensive approach. In International Conference on Artificial Intelligence in Manufacturing & Renewable Energy (ICAIMRE).
[19] Sethy, A., Patra, P.K. (2018). Optical character recognition of Odia handwritten scripts and numerals: A survey on web based utility application. Journal of Web Engineering, 17(6): 3629-3653.
[20] Daniya, T., Vigneshwari, S. (2019). A review on machine learning techniques for rice plant disease detection in agricultural research. System, 28(13): 49-62.
[21] Sethy, A., Patra, P.K., Nayak, S.R., Poonia, R.C. (2022). Offline handwritten character and numeral recognition: A kernel-based approach. International Journal of Social Ecology and Sustainable Development (IJSESD), 13(1): 1-21. https://doi.org/10.4018/IJSESD.295087
[22] Yousif, N.A., Mahdi, G.S., Hashim, A.T. (2022). Medical image encryption based on frequency domain and chaotic map. International Journal of Safety and Security Engineering, 12(4): 467-473. https://doi.org/10.18280/ijsse.120407