International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 1, ISSN No. 2455-2143, Pages 338-342
Published Online May 2022 in IJEAST (http://www.ijeast.com)

SECURE TEXT IN IMAGE STEGANOGRAPHY USING PIXEL-BASED ALGORITHM

Muhammed Ashiq Abdul Khader, Saranya Kavileswarapu, Ritika Sarkar
School of Computer Science and Engineering
Vellore Institute of Technology, Chennai

Sannasi Ganapathy, PhD
Centre for Cyber-Physical Systems & School of Computer Science and Engineering
Vellore Institute of Technology, Chennai

***Abstract*—The art of encrypting a hidden message within a public message is known as steganography. Traditionally methods like LSB (least significant bit) modification, the five-modulus method and other algorithms have been utilized to encode a lower quality image into a higher resolution image via steganography. This research aims to implement a novel text in image steganography using pixel-based algorithms where the security of the text is enhanced by integrating encryption before embedding secret messages. We use the Chinese Remainder Algorithm (CRT) to cryptographically secure the secret message inside the image and the least significant bit algorithm to store the message inside the image. A novel method is propounded for the key generation of the CRT algorithm and the results have been studied and compared with the results of the methods in existing studies.**

***Keywords*— Cryptography, Steganography, LSB, CRT, Encryption.**

I. INTRODUCTION

The advent of technological advancements and the sheer amount of information have entailed the need of protecting the information being transmitted through various mediums, be it text or image. Information security systems aim to deploy network architectures that have a high level of security and ensure that the integrity of the information is also maintained. When the security of messages is considered, the method that would most often come to mind is cryptography, which converts the data into a form that cannot be comprehended by a sniffer. Steganography is another interesting way to protect the information, but here the presence of the message is itself hidden from the hacker. Hence this provides a more secure way of communication, whereas in cryptography the data is visible but in an unintelligible format, and if the key for the encoded message is decoded by the attacker the message can be read. The text message can be hidden either in another small or large text file or in an image. Usually, text in image steganography is more prevalent because of the large number of bits present in the image which can be used to hide the data inside. The other methods of hiding text are embedding the messages in audio signals which is significantly more complex than the other methods, in videos where large amounts of data can be concealed, and finally embedding the data inside network protocols like TCP and UDP packets by modifying their headers. Some well-known automated tools which aid in the above methods have been prepared as libraries that can be executed on the command line by downloading the library. Some popular libraries for the task are steg hide which works for text in images and audio, stegosuite to hide text in images, and OpenPuff which helps store the messages in images, audio, and videos as well as flash files.

The limitation of steganography is that if the algorithm for steganography embedding is known to the attacker, then it is very easy to retrieve the text from the other text or image. Therefore, another layer of security to protect the text inside the text or image is needed. This layer can encrypt the text using cryptography or any other suitable method with a key to decrypt the encrypted text.

In our paper, we aim to perform text in image steganography using pixel-based algorithms which hide the text in the image array by using statistical techniques to manipulate the arrays and store the text character by character. Then the additional security level is implemented where we use the Chinese Remainder Theorem algorithm in combination with a cryptographic technique to encrypt the text. Hence, we devise a novel method to improve the level of security of transmitted messages through a communication channel by utilizing both steganography as well as cryptography. We first present a survey of the existing works in this field, then highlight the proposed method in detail with the help of algorithms and pseudocodes, and finally, we come to the results where the accuracy and time complexity of our methods have been demonstrated.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 1, ISSN No. 2455-2143, Pages 338-342
Published Online May 2022 in IJEAST (http://www.ijeast.com)

II. LITERATURE SURVEY

Darbani Abbas et al [1] propose a method where text steganography is carried out using two less significant bits of pixels to disguise the image's encoded message. The steganography operation is applied to the image after its transformation from time into frequency space and exactly (or right away) after the discretization of modified data in the JPEG compression technique before encoding.

In [2], the authors propose a method by using a pixel-based algorithm for steganography. They have a cover picture file and a message in their algorithm. The pixel of the cover image will then be considered. They put each piece of hidden text there. This procedure will be repeated until the last sliver of secret text is found. The data is then concealed beneath the image after this stage. Then this image file is transmitted to the client, who will reverse the procedure to get the original text out of the image.

Muhammad et al [3] provide a new method for image steganography based on Least Significant Bits that uses the Hue-Saturation-Intensity (HSI) color scheme (LSB). The suggested approach converts an image from RGB to Hue-Saturation-Intensity (HSI) color space, then embeds secret data inside the Intensity Plane (I-Plane), and then converts it back to RGB color model. Subjective and objective analyses are used to evaluate the procedure. The proposed method is found to have higher Peak Signal-to-Noise Ratio (PSNR) values, good imperceptibility, and many security levels in experiments, demonstrating its superiority over several current methods. In [4], the goal of the study is to provide a realistic steganographic system for hiding text within grayscale photographs. Using the Five Modulus Method, the secret message is hidden inside the cover image. The key benefit of this unique technique is that it keeps the size of the cover image constant while increasing the size of the secret message.

Dumre et al [5] investigated image steganography utilizing the least significant bit (LSB) technique in conjunction with AES-128 encryption in this paper. They proposed that the order be reversed traversing the RGB planes while secretly encoding a message in the image. The traversal order was determined by image properties such as file format and resolution, preserving the image's steganography capacity. Kumar et al [6] present an image steganography approach based on the Least Significant Bit color model and the YCbCr color model (LSB). The approach suggested in this work converts a picture from RGB to the YCbCr color system, then hides secret data inside the YCbCr color space using the least significant bit, and then converts it back to RGB color space.

In [7], the suggested method encrypts data using a combination of cryptography and steganography, resulting in a higher level of security. A deep learning model recognizes text from photos and documents, which is then encrypted using an improved encryption algorithm and then buried in an image using image steganography.

Srilakshmi et al [8] introduced a new image steganography approach for text embedding in the geographical domain. In the proposed embedding, the message is dropped into the image using a randomly generated key, and text is extracted from the image using this key. As a result, this method is very safe against eavesdropping and highly complex to detect the text data in the image, as well as obtaining the text message from the message.

Ganapathy et al [9] present a new data storage strategy based on the Chinese Remainder Theorem (CRT) for securely storing user data in cloud databases. The suggested CRT-based secured storage strategy employs two encryption schemes that employ novel formulae for the first and second encryption, as well as a new formula for decrypting cloud data. In addition, a novel formula for accessing encrypted cloud data from a cloud database in a cloud server is added in the process of group key generation.

III. PROPOSED METHOD

The proposed model makes use of the pixel-based steganography algorithm proposed by Kazi et al [2] and reinforces the security of the embedded message by encrypting it before the embedding stage. The proposed model can be divided into Encoding and Retrieval Blocks. The encoding block receives the cover image and secret message, encrypts the secret message, and then embeds the encrypted message into the image. The retrieval block receives the embedded image, extracts the encrypted message, and then decrypts it.

The proposed method is using the size of the image as the key for encrypting the secret message. This removes the necessity of sharing the key while transferring the embedded image.

A. Encoding

The encoding block Fig. 1 contains the message encryption and message embedding modules. The message encryption module takes in the image and message as input and returns an encrypted message. This encrypted message along with the cover image is received by the message embedding module which returns an embedded image.

B. Message Encryption

The message encryption process is performed as follows:

1. The secret message and image size are taken as input

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 1, ISSN No. 2455-2143, Pages 338-342
Published Online May 2022 in IJEAST (http://www.ijeast.com)

2. The secret message is converted to a list of integers where the elements are the index of the character in the message from a predefined string of characters.
3. All the elements in the list are added with the magnitude of the size of the image

C. Message Embedding

The embedding process is performed as follows:

1. Input the secret message
2. Choose a cover picture file with a resolution of M x N pixels.

Create a series of pixels starting at 0,0 and increasing in length, and produce a number of iterations for each of these series of pixels.

3. Find the length of the secret message
4. Iterate for the length of the message

a. Using ASCII values, the character is transformed to an 8-bit binary representation.

b. Encode the first three sets of pixels. The secret message character is made up of eight bits. These eight bits are packed into three pixels, giving a total of nine bits of RGB values.

c. Change the pixel to even for 0 and odd for 1 as you go from left to right.

5. Replace the new set of pixels with the pixels from the original cover picture.

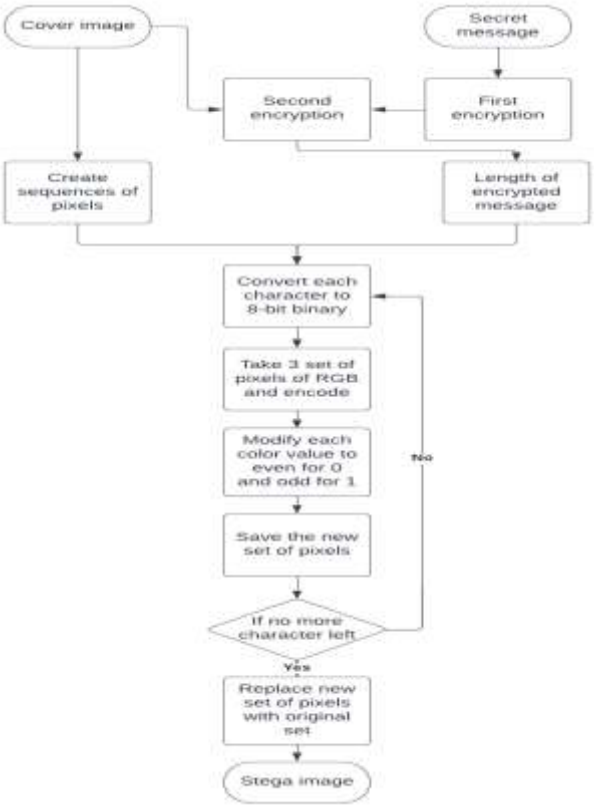

Figure 1: Encoder

D. Retrieval

The retrieval block Fig. 2 contains the message extraction and message decryption modules. The message extraction modules take the embedded image as input and return the encrypted message. This along with the cover image is taken as input by the decryption module and returns the original message after decryption.

E. Message Extraction

The message extraction process is performed as follows:

1. Select embedded image
2. Iterate over the pixels of the image

a. Choose the first set of 3 pixels

b. By left-shifting the pixels, you may extract the data byte from the set.

c. Save the bytes to an array and move to the next set

3. Return the final array of bytes

F. Message Decryption

The message decryption process is performed as follows:

1. The list of bytes of the encrypted message is received
2. Q = size(image)/256 is calculated
3. All elements of the list are added with the value of Q*265
4. The magnitude of the size of the image is abstracted from all the elements in the list
5. The characters are extracted from the string using the element from the list as the index.

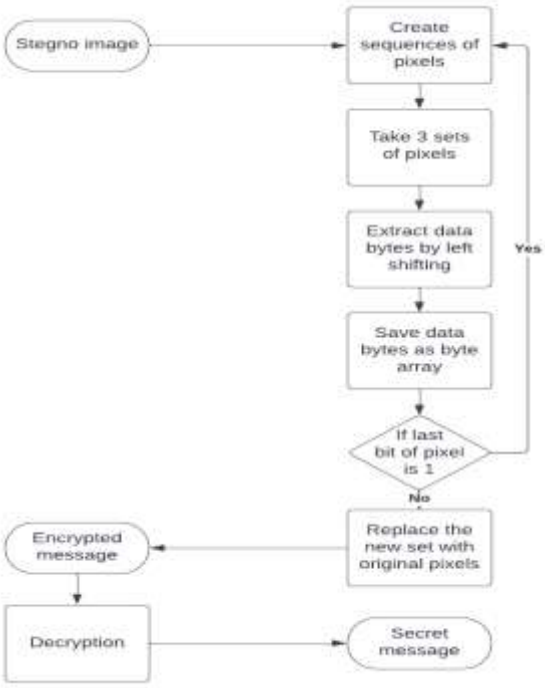

Figure 2: Decoder

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 1, ISSN No. 2455-2143, Pages 338-342
Published Online May 2022 in IJEAST (http://www.ijeast.com)

Fig. 3 and Fig. 4 shows the cover image before and after embedding the secret message respectively.

Figure 3: Cover image

Figure 4: Stegno image

IV. RESULT AND DISCUSSION

A. Parameters of evaluation

The parameters used for evaluating the original image and the encoded image are accuracy, precision, recall, and F1-score.

Accuracy

Accuracy = (TP + TN)/ (TP + TN + FP + FN)

The number of correctly classified data instances divided by the total number of data instances is known as accuracy.

Precision

Precision is the amount of information provided by a number in terms of its digits; it indicates how near two or more measurements are to each other. It is unaffected by accuracy.

Precision=TP/(TP + FP)

Recall

The fraction of relevant instances that were retrieved is known as recall (also known as sensitivity).

Recall = TP/ (TP + FN)

F1-Score

The harmonic mean of precision and recall is used to get the F1 score.

F1=(2*precision*recall)/(precision + recall)

Encryption and Decryption

Encryption and decryption time - The time taken for encrypting secret message and then decrypting it.

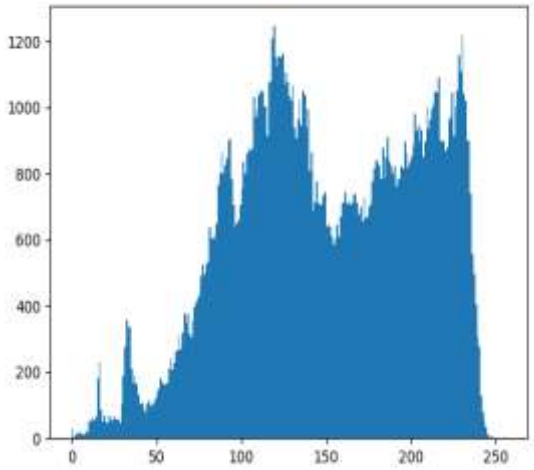

Figure 5: Histogram of cover image before embedding

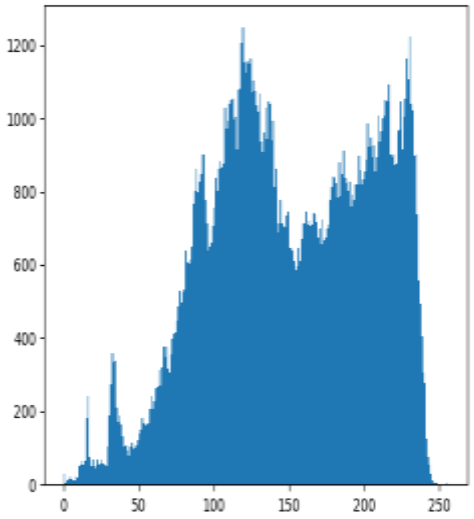

Figure 6: Histogram of cover image after embedding

Table 1: Image quality comparison

Parameter	Proposed method	Kazi et al
Accuracy	99.5387	99.9959
Precision	99.0218	99.9959
Recall	98.9292	99.9959

F1-score	98.9688	99.9959

Table 2: Encryption and Decryption time analysis

Algorithms	**Encryption time (ms)**	**Decryption time (ms)**
AES	0.5500	0.5402
RSA	0.4132	0.4015
DES	0.5823	0.5742
Proposed methods	0.3750	0.1428

B. **Obtained Results**

From Table I, it is observed that the image quality parameter's values of the proposed method is less than that of the reference Kazi et al [2]. This is due to the fact that the proposed method encrypts the secret message by replacing the characters with other characters that are often outside the ASCII domain. The added security compensates for the reduced image quality.

Table II, shows the computation time for encrypting and decrypting the secret message. the proposed method proved to be faster than the existing standard algorithms for encryption of 1024 bit secret message. Using cover image as the key differentiates the proposed method from the rest.

Fig. 5 and Fig. 6 shows the histogram of the cover image before and after embedding the secret message. It is visible clearly that the both histograms are indistinguishable by naked eye.

V. CONCLUSION

The main aim of an encryption system is to prevent unauthorized access to data. Traditionally keys were a requisite for encryption systems employing cryptography to secure their data. However, security flaws like the possibility of obtaining the key through illegal or unethical means and breaking the encryption call for smarter methods. Keyless encryptions can be implemented in a variety of ways, and are harder to guess or possess like a key. It advances the level of encryption and optimizes it by reducing the overheads incurred during key generation and handling in the traditional methods. The results of our proposed method for creating a secure text in an image algorithm look promising. Though there is a tradeoff between accuracy and security, it is easily customizable based on the area of application. The classification report has been generated by comparing the recovered image after decryption with the original image. The histograms of the cover image before and after embedding the encrypted text have been visualized and show practically no visible difference, validating the robustness of the proposed method.

VI. REFERENCE

[1]. Darbani, Abbas, Mohammad M. AlyanNezhadi, and Majid Forghani. "A new steganography method for embedding message in JPEG images." 2019 5th conference on knowledge based engineering and innovation (KBEI). IEEE, 2019.

[2]. Kazi, Jawwad A. R., et al. "A novel approach to Steganography using pixel-based algorithm in image hiding." 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2020.

[3]. Muhammad, Khan, et al. "A novel image steganographic approach for hiding text in color images using HSI color model." arXiv preprint arXiv:1503.00388 (2015).

[4]. Jassim, Firas A. "A novel steganography algorithm for hiding text in image using five modulus method." arXiv preprint arXiv:1307.0642 (2013).

[5]. Dumre, Rutvik, and Aashka Dave. "Exploring LSB Steganography Possibilities in RGB Images." 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021.

[6]. Kumar, Deepak. "Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach." 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 1 (2019): 1-5.

[7]. Sathiaraj, SJ Fiona G., et al. "Secure Transfer of Image-Acquired Text Using a Combination of Cryptography and Steganography." 2019 1st International Conference on Advances in Information Technology (ICAIT). IEEE, 2019.

[8]. Srilakshmi, P., et al. "Text embedding using image steganography in spatial domain." International Journal of Engineering & Technology 7.3.6 (2018): 1-4.

[9]. Ganapathy, Sannasi. "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications." Computer Networks 151 (2019): 181-190.