Hybrid Image Steganography Algorithm Security Enhancements for High-Quality Image Transactions

Pritesh J. Bhor[1] Prof. Monika D. Rokade[2]
[1,2]Department of Computer Engineering
[1,2]Sharadchandra Pawar College of Engineering, India

Abstract— Steganography is a technique for concealing a secret (coded) message within a regular communication. The goal of steganography is to keep information hidden while both the sender and the receiver share it. Steganography and cryptography are inextricably linked; cryptography scatters the message so that it cannot be understood, but steganography conceals the message's existence. The seed values are used in such a way that the IMAGE QUALITY, as measured by PSNR, improves but the data within the image stays protected. The procedure is as follows: a pseudo-random number generator generates a sequence of random numbers using an arbitrary seed. The cover image is then divided into dynamic-size chunks. Using this sequence, a route is formed, and the secret data is placed in the LSB of the pixels along this path. In this study, we used Discrete Wavelet Transformation to develop the frequency domain approach and DNN to do classification to discover the LSBs in the input image. To improve security, it employs the ECC technique for encryption. Following that, the encryption method used in the imaging system classifies the secure information. To compare the existing algorithm and evaluate performance metrics such as peak signal to noise ratio, Structure Similarity Index Measure, and Decryption time factor in order to obtain this outcome.

Keywords: Steganography, Image Quality Parameter, Embedding Process, ECC Methods, and DNN Algorithm to Hide Information

I. INTRODUCTION

Steganography is a method of concealing a secret (coded) [1] message within a regular communication. [2] The objective of steganography is to keep information hidden while both the sender and the receiver share it. Steganography and cryptography are inextricably linked; cryptography dissipates the message so that it cannot be detected, but steganography conceals the existence of the message. Cryptography was created to protect the privacy of information, but steganography is an art form that conceals the existence of communication. [3] Steganography is an extension of cryptography that has been pushed to a higher degree such that no one can suspect the existence of a coded message. Steganography replaces undesired or unused bits in ordinary files with bits that contain an unseen message. A coded message could be a consistent file or data that has been encoded. Steganography differs from cryptography in that it conceals the presence of the communication, whereas cryptography conceals the subject matter of the message. Steganography is sometimes used in conjunction with encryption. The contents in an encrypted file may be hidden via steganography, so that the coded message cannot be read even in a decrypted file.

Text steganography is accomplished by altering text elements such as characters. It is the most difficult type due to the lack of needless information in the text file. The coding methods are used to create alternatives that are easily decoded. The inconsistency and difficulty in designing document marking systems is due to the reliable decoding and less obvious change. A text file provides its content and formatting using standard format description languages such as PostScript2 [10]. Image Steganography is a technique for hiding communications in images that is commonly used nowadays. A photograph with a hidden message can quickly circulate around the internet. Niels Provos, a German steganography expert, investigated the use of steganography in newsgroups by developing a scanning cluster that identifies the existence of secret messages in photographs posted on the internet. Steganography's practical application is still limited. Hiding a message in a picture without changing its visible properties, the cover source in "noisy" places can be changed with numerous colour choices to deflect attention [11]. In this suggested work, we develop the DWT algorithm for filtration and represent the upper and lower boundaries. Then, using the ECC method, we create the cryptography technique to securely hide the information. If we have secured the information, we may use the classification approach to classify the stego image.

We compare Decryption Time, PSNR (peak signal to noise ratio), and SSIM (Structural Similarity Index Measure) performance characteristics to earlier techniques.

II. LITERATURE REVIEW

Text and image steganography techniques are examples of steganography methods covered in this section. Several techniques are used in the proposed study, including Least Significant Bit (LSB), Discrete Wavelet Transformation (DWT), Elliptic Curve Cryptography (ECC), and Deep Neural Networks.

Sherin Sugathan (2016) [5] described an image steganography Algorithm based on LSB replacement for RGB colour images. Steganography is a popular method of concealing information that allows people to interact in private. The main advantage of image steganography is that secret encoded images do not draw the attention of the attacker. Image steganography methods are designed to preserve image quality while encoding a secret message. The orientation feature of data embedding is explored in order to provide a better embedding strategy for LSB. The suggested technique demonstrates an improvement in image quality using MSE and PSNR. Huayong Ge et al., (2011) [6] evaluated steganalysis and steganography-based digital images by highlighting commonly used cover media.

An idea and principle of steganalysis and steganography are illustrated. Steganalysis is advancing quickly as a result of the rapid evolution of steganography. The clash between steganography and steganalysis has become a fundamental issue in information security.

There are two types of generalized embedding methods: transform domain and spatial domain. The present state of steganalysis is summarized, and the performance of image steganography is discussed. They also discussed the obstacles they faced and the most recent trends. Ramadhan J. Mstafa et al., (2014) [7] introduced a secure video steganography technique based on the linear block code idea. High-speed internet and technological advancements encourage attackers to hack into more information. Several steganography techniques for data concealment have recently been presented. Steganography is a method of hiding hidden information in a host medium such as text, music, image, or video. Unauthorized users, on the other hand, employ steganography analysis software packages to obtain important embedded secret information in carrier files. Inadequate security, resulting in inefficiency Steganalytical detectors picked up on numerous steganography algorithms. To conceal data and a binary graphic logo as a hidden message, nine uncompressed video sequences were used. A secret message was encoded using Hamming code (7, 4) before embedding to make it very secure. The encoded message as a result of employing the XOR functions on random generated values. Furthermore, the suggested algorithm has a high embedding efficiency, as demonstrated by the obtained results. Tomas Denemark et al., (2014) [8] proposed an alternate form of the Spatial Rich Model (SRM) that makes use of a selection channel.

The meaningful probability to cover elements changed during message embedding must improve steganalysis, according to signal detection theory. Three cutting-edge content-adaptive steganography methods were described. To have inaccurate knowledge of embedding probabilities, which can greatly improve detection accuracy when compared to feature sets that don't take the selection channel into account. There were various embedding schemes that might be used. The most notable portion is composed in spatial space, where the compensation stack bits are covered up into the LSBs of unique picture to drive the stage picture stage-picture. Discrete wavelet and cosine transformation methods, on the other hand, are built in the frequency domain, in which the stage picture is transformed from the spatial domain to the frequency domain.

Avnet kauri et al., 2014 [7] developed a strategy to increase audio steganography security while simultaneously improving quality through two-phase steganography.

III. Stenographical issues (text-to-image)

Steganography is a strategy for disguising content from one configuration to another or inside the same game design. In the case of a photograph, a great deal of effort has been done in a similar complexity. It can go through a large number of publications and then focus on auditing previous approaches and algorithms.

The strategies have been shown to be a progressive advance in the field of information stowing. As time passes, the multifaceted character that shrouds the knowledge develops. They furthermore need to retain the base picture (refers to the image in which we are concealing the information), so that if the image is cleaved, the programmer won't be able to accept that some information has been incorporated into the base image by looking at the image [9].

A slew of previous algorithms, such as DWT and DCT, have been proposed to accomplish the same goal. This contributes to our concern explanation. Our worry explanation involves the use of seed values such that the IMAGE QUALITY, which is assessed in terms of PSNR, increases while the information remains safe within the image [12].

IV. Applied algorithms

Among the techniques proposed are:

A. LSB (Least Significant Bit)

Inserting LSBs is a key method for embedding data in a cover file. There are two sorts of digital images used as cover files: 8-bit images and 24-bit photos. In 8-bit graphics, 1 bit of data can be hidden, while 24 bit images can contain 3 bits of data. Steno-image is an image that contains a code message obtained by using the LSB algorithm. The LSB method, as the name suggests, trades the least significant bit of a pixel for coded data. Because the LSB is swapped, the cover picture has no effect, and hence the intermediate user has no idea about the coded message in the image. Although there is a little difference in the degree of intensity between the original and changed pixels, it is not visible.

The following example shows how to hide the letter A within three pixels, or eight bytes, of a 24-bit image. [13]

Pixels: (00100111 11101011 11001010)
(00100111 11011000 10101001)
(11001000 00110111 11011001)
A: 010100111
Result: (00100110 11101011 11001010)
(00100111 11011000 10101000)
(11001001 00110111 11011001)

The key advantage of the LSB technique is that it is simple to implement and reduces the possibility of damaging the quality of the original image. Because data is weak and susceptible to picture shuffling, it can be easily extracted or corrupted by simple attacks.

B. Discrete Wavelet Transform

Discrete Wavelets Transforms (DWT) is a mathematical tool for hierarchically dissecting an image by dissolving a signal into a series of fundamental functions known as wavelets. DWT is a multi-resolution analysis (MRA) that analyses a signal at several frequencies and produces distinct results. Wavelets are defined as functions that are obtained over a set interval and have a mean value of zero. The modification is a must-have method for signal analysis and image processing, particularly for multi-resolution confirmation. A signal is broken up into a number of constituents in the frequency range. 1-D DWT divides the cover picture into two major elements known as approximate and detailed components, whereas 2-D DWT is used to section a cover image into four sub components: one is an approximate component, denoted by LL, and the remaining three are detailed parts denoted by (LH, HL, and HH).

A wavelet is a tiny signal that fluctuates and decomposes in time. The DWT (Discrete Wavelet

Transform) is a modern and computationally powerful approach. Wavelet analysis has the advantages of Fourier Transformation in that it does local and multi-resolution analysis and reveals elements such as discontinuities, breakdown spots, and so on more effectively than Fourier Transformation. Multi Resolution Analysis (MRA) is the process of analyzing signals with different frequencies and resolutions. This procedure changes the object to wavelet domain, and then uses the coefficients to do an inverse wavelet transform to characterize the stage object's original format. [15]

C. Curve Cryptography

ECC (Elliptical curve cryptography) is an elliptic curve-based public key encryption method. Theory applied to generate quick, smaller, and more effective results keys used in cryptography ECC creates keys using rather than elliptic curve equation properties regular methods of generation, such as the product of prime numbers in abundance ECC is a well-known technique up to this point, equipped with the knowledge to investigate spectacular results in complete exponential interval. The technology used in the existence of the majority of public key encryption techniques, such as RSA and Daffier-Hellman. Several sources state that ECC researchers can produce a level of security with a 164-bit key, while other systems require a to achieve a 1,024-bit key. ECC contribute to the upkeep of equivalent security with reduced computing Power and battery usage ECC was created by Certicom, a mobile e-business security provider, and currently licenced by Hifn, the creator of IC and network security commodity RSA is evolving. own version of ECC. Several manufacturers, including Pitney Bowes, 3COM, Motorola, Cylink, Siemens, and Verifone, have evaluated ECC support in their devices.

The functions and features of elliptic curves have been studied in mathematics for 150 years, and their application in cryptography was originally proposed in 1985, independently by Neal Koblitz of the University of Washington and Victor Miller of IBM. An elliptic curve is not an oval (ellipse), but rather a looping line that intersects two axes. ECC is based on the qualities of a specific equation formed by a mathematical group and taken from locations where the line meets the axes. The point on the curve is multiplied by a number to create another point on the curve. Even knowing the originating point and the outcome, determining which number was utilised is difficult.

Equations based on elliptic curves offer a crucial trait for cryptography: they are simple to perform but exceedingly complex to reverse. [17]

D. Deep Neural Network

Deep-learning networks are more prominent than ordinary single-hidden-layer neural networks in terms of depth, which is defined as the number of node layers between data passes in a multi-level pattern recognition approach. DNN was initially designed as an ML (machine learning) solution to dealing with complicated input-output mapping. DNN works effectively by collecting complicated links between English words and air pressure records, as well as innumerable pixels and textual representation.

Conventional machine learning relies on shallow nets, which are made up of an input layer, an output layer, and a hidden layer. "Deep" learning is defined as having more than three layers. Deep is a technical phrase that refers to more than one buried layer. Layer of nodes taught by a different set of features based on the output of the preceding layer in deep-learning networks.

Because of their accumulated information from the preceding layer, nodes identify more complex characteristics as the neural net is elevated. It is correct.

Unlike traditional machine-learning algorithms, deep-learning networks enable autonomous feature extraction without the need for human intervention. Feature extraction is a time-consuming procedure that takes data scientists years to complete. Deep learning is a technique for avoiding expert-assigned milestones. It increases the power of tiny data science teams, which cannot be quantified due to their nature. While training data, the node layer automatically learns features by continually attempting to restore input from which samples are chosen, with the goal of reducing the gap between the probability distribution of the data entered and the network's estimates [18].

The network learns to recognise correlations between important characteristics and ideal outcomes drawn connections between feature signals and shows it as either complete reconstruction or tagged data. With access to input, a deep-learning network trained on unstructured data may be built. It's a recipe for amazing performance; the more data learned on the internet, the greater the accuracy. Deep learning's capacity to learn from massive amounts of unlabeled data is clearly superior than previous methods. [18] DNN produces an output layer, which is a classifier that assigns a specific output that is predictive in nature.

V. SUGGESTIVE MODEL

The following phases must be completed:

1) Insert a picture into the system.
2) To train and evaluate the DNN for LSB detection. Figure 3 shows a proposed flow chart.
3) Use the DWT transformation in conjunction with the filtration procedure to extract distinct viewpoints from the picture. It was used to extract the real byte positions from the image so that bits could be initialised for the following stage, which was to simulate with artificial intelligence and identify the least significant bits.
4) Encrypt the input data for added protection. It protects the embedded bits and decrypts them during the decoding process.
5) Create a simulation of the bits and input data that will be included in the picture.
6) To produce this result, performance metrics such as peak signal-to-noise ratio, mean square, and time factor must be evaluated.

VI. CONCLUSION AND FUTURE SCOPE

A standard least significant bit replacement methodology, filteration method to eliminate the noise factor in the image, encryption method utilised for information security, and classify that might improve the quality of the stego image are all discussed in this study article. The results show that when

the secure message is embedded at higher Least significant bit or Upper bound places, the innovative technique performs well. Some strategies for improving the image quality of stego images include embedding secure information or messages only in components of low significance. The proposed work can be linked to those strategies as well, but it will improve the outcome in an optimization with embedding capacity. The issue's information-like nature makes it ideal for design in a comparable phase. The direction bit's placement might also be changed, and the position could even serve as a component of a key for extracting the protected message or information. The methodology could be used in conjunction with encryption methods and classification to increase security. It completes the work by not modifying the image quality after embedding the confidential notion in the linked image. Steganography is the art of using techniques to conceal sensitive information. In the image, our proposed method is for any type of colour component image by continuous effort of filtration method and attribute memory feature of auto-deep neural network, recently in next method implementation to get maximum quality stegoimage with no-difference in canvas and stego image.

REFERENCES

[1] Shipra Bharti, Sunny Behal, Vishal Sharma" Security Enhancements for High Quality Image Transaction with Hybrid Image Steganography Algorithm" International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3
[2] Monika D.Rokade, Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic." IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
[3] Monika D.Rokade, Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE
[4] Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. International Journal of Advanced Science and Technology, 29(9s), 2324 - 2331.
[5] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
[6] Sunil S.Khatal, Dr.Yogesh kumar Sharma, "Data Hiding in Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume: 4, Issue: 5
[7] Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. International Journal of Advanced Science and Technology, 29(9s), 2340 - 2346.
[8] Sugathan, Sherin. "An improved LSB embedding technique for image steganography." In Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on, pp. 609-612. IEEE, 2016.
[9] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A highly secure video steganography using Hamming code (7, 4)." In Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, pp. 1-6. IEEE, 2014.

