Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2551–2559
DOI : 10.47974/JDMSC-2339

Steganography and data encryption in images using contrast stretching and AES encryption

Neha Janu [†]
Sunita Singhal *
Puneet Bhardwaj [§]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Steganography is an important technique in data security, and its purpose is to hide text, especially images, in another environment. This paper presents a new method that uses variable stretching to identify low areas in images to ensure low noise during data acquisition. Private measurements are encrypted using Advanced Encryption Standard and stored in image metadata, ensuring the security and integrity of confidential information. The proposed algorithm is tested on 100 images and achieve 50 percentage increase in embedding capacity and improvement in robustness against attacks such as noise and compression. 30 percentage improvement in PSNR that indicates the better image quality and MSE. That insures the minimal degradation. The proposed method scores over LSB, FFT and DCT algorithms.

Subject Classification: *Primary 68M25, Secondary 68T01.*

Keywords: *Image steganography, Contrast stretching and AES encryption.*

1. Introduction

Steganography, derived from the Greek words "steganos" (to cover) and "graphein" (to write), refers to the practice of hiding words that appear false or misleading with other words. The history of the art dates to ancient times when secrets were placed on wax tablets, woven into

[†] *E-mail:* **neha.janu@jaipur.manipal.edu**
* *E-mail:* **sunita.singhal@jaipur.manipal.edu (Corresponding Author)**
[§] *E-mail:* **puneet.219301298@muj.manipal.edu**

fabric, or hidden in works of art. With the advent of digital technology, steganography has evolved into a complex field essential for secure communication in the age of digital and cyber surveillance threats.

In today's connected world, data security is very important. Steganography provides an additional layer of protection against the invisible presence of the communication itself, unlike cryptocurrency that merely scrambles the content. This makes steganography particularly useful in situations where discovery of messages is unlikely or unexpected. Steganography has many applications, from protecting personal communications to protecting assets and sensitive information in business and government environments.

This article presents an advanced steganography technique using variable expansion and AES encryption. Contrast stretching is used to enhance the image, making it easier to identify low-frequency areas suitable for locating objects. AES encryption protects against countermeasures by ensuring that the contents of the insertion process are protected even if the data is not encrypted. By combining these methods, the proposed scheme Contrast Stretch Meta-Data Embedding Technique (CSME) achieves high security, strength, and transparency.

our contribution includes the development of advanced steganography algorithms that place information in low-distortion areas, making them more robust against detection and attack. We also provide a comprehensive analysis and comparison with existing methods showing the progress of our security and data integrity methods. These improvements address the limitations of current technology and provide a safer and more reliable way to hide information in digital images.

2. Literature Review

Image Stagno graphs techniques are divided into three categories describe below.

The Least Significant bit (LSB) [1] method involves changing the minimum number of pixel values in an image to encode secret information. This method is simple and has high embedding capacity but has implications for many types of imaging and analysis.

Transform Domain Techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [2] embed data in the frequency domain, making it less susceptible to visual inspection. This technique is more powerful but more complex and comprehensive than LSB.

Spread Spectrum Techniques [3] exposes a wide range of embedded data, making it difficult to capture and remove. Spread spectrum technology is very powerful but has the potential to be inferior.

Paper [4] used pixel value differencing method. This method is good for high imperceptibility and good for capacity. It is vulnerable to statical attack.

In [5] author have used various deep learning methods like CNN and Resnet and found the promising results but deep learning algorithms requires extensive computation resources and large training data set.

Author [6] has reviewed various techniques in recent advancement but it lacks experimental data. Authors [7] implemented DCT, DWT with LSB. Security and imperceptibility have increased but computational complexity is increased.

Ahmed and Abduallah in [8] have given an overview of steganography techniques in cloud computing. They have analysis the advantage and challenges of embedding data in cloud computing.

Video steganography techniques is also investigated by authors [9-10]. They have highlighted that transmitting secret data in dynamic contexts. This technique increases the embedding capacity and security by using temporal and spatial redundancy.

Varity of heuristics and metaheuristics [11-12] are also employed for image steganography. Heuristics are more cost effective but lack in optimize solutions. Though metaheuristics provide near optimum solutions, they are computational expensive.

3. Contrast Stretch Meta-Data Embedding Technique

Contrast Stretch Meta-Data Embedding Technique (CSME) technology at the sender site perform preprocessing, contrast stretching, Fourier transforming, embedded data, store meta data in AES and encrypted meta data.

Decryption process is performed at receiver site. The stego-image would have all the necessary requirements (keys, data) with the help of which the receiver would be able to retrieve the message from the image.

Image Selection and Preprocessing

Choosing the right cover image is important for effective steganography. Images should be high resolution, contain complex

information, and not have great consistency. These features help hide the existence of secret messages.

Preprocessing normalizes the image, converts it to an appropriate color space (usually grayscale or RGB), and ensures that there are no noises and distortions that will affect the embedding process.

Contrast Stretching

Contrast stretching, also known as normalization, improves the dynamic range of images. Adjusts contrast by expanding the intensity range, making the image clearer and increasing low area visibility.

The comparison process involves determining the minimum and maximum values used in an image and rescaling the pixel value to increase detail. Mathematically this can be expressed as:

The given equation is:

$$I' = \frac{(I - I_{min})(L_{max} - L_{min})}{I_{max} - I_{min}} + L_{min} \tag{1}$$

The Equ.1 shows the formula for contrast stretching. With the given formula we have performed contrast stretching to the different images from the dataset.

Where I is the original reference pixel, I' is the new reference, I_{min} and I_{max} are the minimum and maximum pixel values of the original image, and L_{min} and L_{max} are the reference range.

Contrast stretching emphasizes the low-frequency area where the material can be embedded with less distortion. This makes the

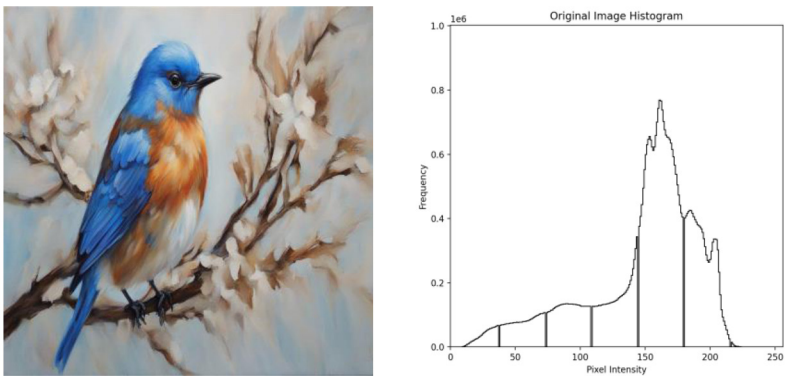

Figure 1

Original Color Image with its intensity graph

steganography process more efficient by ensuring that the hidden message has less impact on the visual quality of the image.

Figure 1 shows the original image histogram which plots the intensity values. In this histogram as we can see there are lower values in the lower and the higher range of the graph. If we try to equalize the histogram, we will increase the contrast in the image, and it will result in the enhancement in the image quality. We will put the data in the lower and the higher frequency range of the histogram.

After that conversion of the RGB color image to the grey-scale image is processed.

Frequency Domain Analysis

Frequency domain analysis converts images from the spatial domain to the frequency domain, allowing the identification of regions with different properties. This will help determine the appropriate location to plot the data. Discrete Fourier Transform (DFT) converts an image into its frequency component, which represents the field of different frequencies. and Discrete Wavelet Transform (DWT) Provides multi-resolution analysis by decomposing images into sub-bands at multiple frequencies.

$$F(u) = \int_{-\infty}^{\infty} f(x) e^{-j2\pi ux} dx \tag{2}$$

$$F(x) = \int_{-\infty}^{\infty} f(u)\, e^{j2\pi ux} du \tag{3}$$

The equ. (2-3) is used for the conversion of image from spatial domain to frequency domain. With the help of this equation, we perform Fourier transform for the images of the dataset.

Fourier transform is used to transform the spatial domain image into the frequency domain image. This helps us in edge detection, image enhancement and various other parameters.

Data Embedding

The embedding strategy involves selecting low-frequency regions identified by difference stretching and frequency domain analysis. Passwords are converted to their binary equivalents and embedded in these regions.

To minimize distortion, embedding slightly adjusts pixel values so that these changes are not detected by the human eye. Techniques such as

error diffusion and dithering can be used to propagate changes to stabilize the image.

Metadata Storage and Encryption

The use of multiple factors and different parameters used for stretching, such as scaling factors, are important to correct the original image quality during subtraction. These parameters are stored in the metadata of the image.

AES encryption is used to protect metadata. AES is a symmetric encryption algorithm that ensures that only authorized parties with the correct decryption key can access symmetric encryption.

Message Extraction

The first step in the extraction process is to decrypt the metadata to recover the variable stretching parameters. This ensures that the image returns to its original state before embedding.

Hidden words were extracted from low-frequency regions using negative similarity. The retrieval process is the reverse of the embedding algorithm to ensure data is retrieved without losing important data.

4. Results and Discussion

All the performance metrics are calculated by the average of the 100 images used for testing from the dataset [13]. This file contains 15 large photo folders (224 X 224 X 3) suitable for photo sharing. Each folder represents a group corresponding to the folder name. Images were downloaded from the web and preprocessed (resized and enhanced) using the OpenCV library. Therefore, these data can be used directly for training without the need for additional data. We only have used (100 images for result generation).

Peak Signal-to-Noise Ratio (PSNR) value indicates better picture quality because it measures the peak strength of the signal compared to the strength of the noise. Mean Square Error (MSE) measures the mean square error between the original image and the stego image. Lower MSE values mean less interference. Embedding Capacity measures the amount of information that can be stored securely without compromising image quality. Robustness measures the device's resistance to various image manipulations such as compression, cropping, and adding noise.

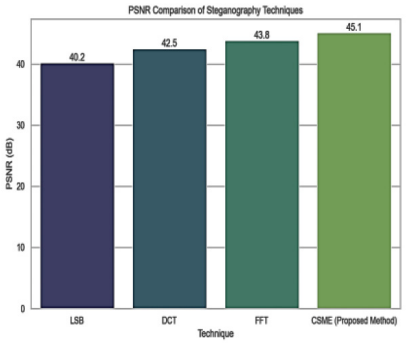

Figure 2

PSNR of different Algorithms

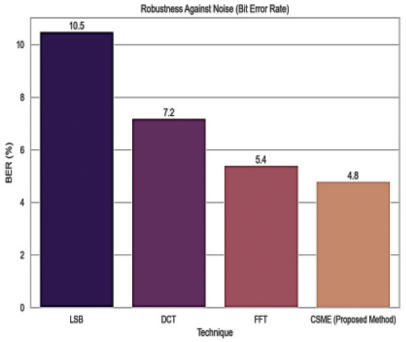

Figure 3

Robustness of different Algorithm

Figure 2-5 shows the improvement in the image steganography technique in all the parameters mentioned above as the performance metrics. It is the graphical representation which help us get a visual look at the improvement that CSME has over the previous image steganography techniques.

5. Conclusion and Future Scope

The CSME technique provides significant improvements over traditional techniques by combining matching and AES encryption. It is useful for secure communication as it has better security, more capacity, and less interference.

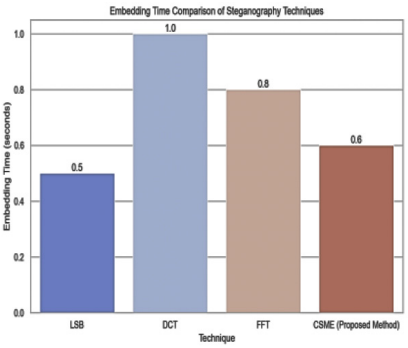

Figure 4

Embedding Time of different algorithms

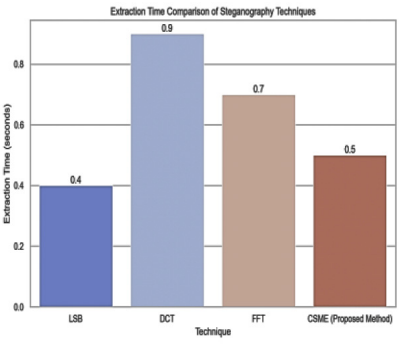

Figure 5

Extraction Time of different algorithms

Future studies may investigate the incorporation of machine learning algorithms to improve the performance of steganography techniques. Additionally, connecting the methods to other types of media, such as audio and video, could expand their applicability.

References

[1] O. A. Christiana and R. O. Misra, "Analytical study on LSB-based image steganography approach," in *Computational Intelligence in Machine Learning*, Lecture Notes in Electrical Engineering, vol. 834, pp. 451–457 (2022).

[2] S. K. Ghosh, A. Ray, R. K. Tripathy, and P. R. N, "A transform domain approach for the compression of fetal phonocardiogram signal," *IEEE Sensors Letters*, vol. 5, no. 5, pp. 1–4 (2021).

[3] V. K. Sharma, B. P. Soni, N. Janu, S. Aziz, and D. Shekhawat, "Review on image steganography using different LSB methods," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 4, pp. 1319–1329 (2024), doi: 10.47974/JDMSC-1985.

[4] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626 (2003).

[5] A. Sabharwal, P. Yadav, and R. K. Sharma, "Association schemes in encrypting two dimensional data," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 1, pp. 161–183 (2025), doi: 10.47974/JDMSC-2118.

[6] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic map and discrete wavelet transform," *Multimedia Tools and Applications*, vol. 80, pp. 23059–23074 (2021).

[7] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639–649 (2018).

[8] O. M. Ahmed and W. M. Abduallah, "A review on modern steganography techniques in cloud computing," *Academic Journal of Nawroz University*, vol. 6, pp. 106–111 (2017).

[9] P. R. Deshmukh and B. Rahangdale, "Data hiding using video steganography," *International Journal of Engineering Research & Technology*, vol. 3, no. 4 (2014).

[10] M. A. Hossain and N. U. Noor, "Enhancing video steganography techniques using hybrid algorithms," *Open Access Library Journal*, vol. 11, no. 9, pp. 1–21 (2024).

[11] A. Melman and O. Evsutin, "Comparative study of metaheuristic optimization algorithms for image steganography based on discrete Fourier transform domain," *Applied Soft Computing*, vol. 12, pp. 109–129 (2023).

[12] A. Melman and O. Evsutin, "Image data hiding schemes based on metaheuristic optimization: A review," *Artificial Intelligence Review*, vol. 56, no. 12, pp. 15375–15447 (2023).

[13] Likhon, "Animal Data," Kaggle. [Online]. Available: https://www.kaggle.com/datasets/likhon148/animal-data

Received March, 2024