Chapter 13
Enhanced Image Steganography Technique Using Cryptography for Data Hiding

Jasvinder Kaur and Shivani Sharma

Abstract The fast improvement of the Web has expanded the simplicity of sharing data to individuals around the world. In any case, this headway additionally raises a trouble about information control when the data is transferred by the sender to the beneficiary. Along these lines, data security is a significant issue in information correspondence. Steganography and cryptography assume significant jobs in the field of data security. Steganography can be applied, however, a different computerized media, for example, video, pictures, and sound to cover data in such a manner that nobody else realizes that there is a secret data. Cryptography alludes to the specialty of changing over a plaintext (message) into an ambiguous organization. Both steganography and cryptography strategies are strong. The contents obtained after doing so is secret and its existence is also hidden. This method is tested and it is observed that it prevents steganalysis too as well as parameters like PSNR and MSE are also tested which gave good results.

13.1 Introduction

Over past decades, the use of Internet has helped in devising different mechanisms for transmitting data from sender to the recipient. It has opened the new entryway for the aggressor to assault on that data and effectively takes the data of the clients [1]. There is a lot of classified data like military's privileged insights, law requirement's insider facts, and so forth. Fear-based oppressors can likewise utilize information covering up just as cryptography strategies for making sure about their information. Cryptography is the study of utilizing science to encode and decode the information. Steganography is a workmanship and science of concealing the mystery information into another

J. Kaur (✉) · S. Sharma
Department of Computer Science and Engineering, PDM University, Bahadurgarh, Haryana, India
e-mail: jasvinder.kaur@pdm.ac.in

S. Sharma
e-mail: shivanibitto@gmail.com

R. Kountchev et al. (eds.), *New Approaches for Multidimensional Signal Processing*,
Smart Innovation, Systems and Technologies 216,
https://doi.org/10.1007/978-981-33-4676-5_13

media. This paper presents the combination of cryptography and steganography so as to ensure effective delivery of message to the recipients.

13.1.1 Steganography

Steganography is characterized as the "concealed composition" that assists with concealing the nearness of data. By doing this, it becomes very hard for gate crashers to retrieve the information as it is hard to track down the contrast between the images [2]. The sender is communicating something specific which has been implanted by a mystery key and a stego-picture is framed. This procedure is known as steganalysis, after this the picture is additionally handled and the collector will separate the picture with utilization of the key. Thus, the message will be effectively sent to the beneficiary. Steganography assists with concealing the record in the different structure, for example, in picture, sound, video, or text. Also, the target to do this is concealing the accessibility of information in the spread picture that is mixed up by people. Steganography involves essential three segments which are transporter, message, and key [3]. The bearer can be a picture, media player, or a TCP/IP parcel. Furthermore, a key is used to encode or unscramble a message and the secret phrase can be anything, a design, or a video. The thought driving steganography is that if an individual needs to send a message to other person, the correspondence between them is compelled by a switch or server. We can watch that one gathering needs to move a message to beneficiary, to do so it inserts message into a spread picture and gets a stego-picture. In a standard definition, this methodology of exemplifying message is not referred to and is kept as a secret between the two [4]. In any case, it is seen that the calculation being utilized is not a riddle yet the key is secret between the two, and it is otherwise called Kerchoff's rule. It is a method to make sure about the unstable information [5] (Fig. 13.1).

13.1.2 Cryptography

We can define cryptography as the process in which it encrypts the actual message and converts it into secret message [6]. This message can be retrieved by receiver by using either private key or public key. Also, the message can be encapsulated by using a mathematical equation or algorithm and converts it into a non-readable form which can be any mystery information. Cryptography helps to encapsulate the data in order to protect it from an attacker, whereas steganography helps to conceal the presence of that data from the attacker. So, the combination of these two techniques gives superior communication. The aim of this paper is to combine the technologies and have better experience. Some basic terms are as follows:

- Load: data that requires to be concealed.

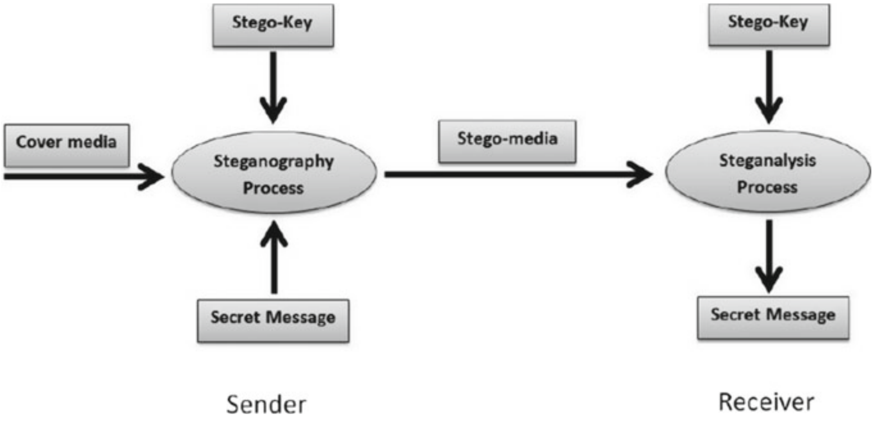


Fig. 13.1 Generalized steganographic technique

- Carrier file: medium in which the load has to be covered up.
- Stego-medium: place where the data has to be covered up [7].
- Redundant-bits: the data inside a record, which can be adjusted without harming the document.
- Steganalysis: The way toward identifying the hidden data which is put away inside a document [8] (Fig. 13.2).

This is the figure for cryptography:

So, now, the paper contains Sect. 2 which has the review and analysis briefly described that are about our proposed technique. Section 3 describes the presented technique which is followed by results and discussions in Sect. 4. The conclusion and future scope are present in Sect. 5.

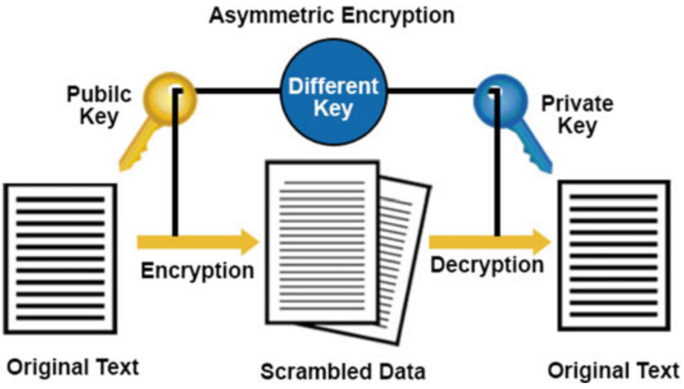


Fig. 13.2 Generalized cryptographic technique

13.2 Related Work

We have many algorithms present today for securing the data and sending it efficiently. But each of them has their own advantage and disadvantage. Let us have a look on some of them:

- Ammad Ul Islam, Faiza Khalid et al. suggested a picture steganographic strategy dependent on MSB. The procedure utilizes the distinction of two pixel's bits of the spread picture bit No. 5 and 6 of pixels are focused for installing. The contrast between bit 5 and 6 is set by the approaching mystery data bit.
- Ian McAteer, Ahmed Ibrahim et al. has recognized two essential applications consolidating biometrics and steganography, which are get to control and the transmission of touchy eHealth/biometric information. In any case, neither of these applications have made the effective change from the laboratory to this present reality setting. Proposed models for e-casting a ballot and e-shopping are remembered for this audit, yet neither of these or comparative frameworks have been executed so far.
- Ying Zou, Ge Zhang, Leian Liu show that the proposed technique dependent on multi-task has preferable execution over the immediate cross-breed preparing strategy.
- N Wu, P Shang, J Fan, Z Yang understood the steganography to secure data dependent on Markov model which was frequently utilized in regular language handling. For different reasons, past-related calculations had not completely used or dismissed the significant ideas, progress likelihood, in Markov chains.

So, the methods discussed above have one or other drawback which we can easily fix by applying a two-layer protection on the data, i.e., using both of the technologies together. Results of above method have low-quality stego-image and also easily detectable image. This present research work solves this problem and proposes a new scheme which gives good quality stego-image as well as increasing security of data while transmission.

13.3 Proposed Methodology

The presented work is categorized into two steps, firstly data is encrypted and converted into cipher then secondly conceal the information using LSB technique given by the algorithm. The message is hidden into two layers such as first layer conceals it using cryptography and second conceals the message using the new algorithm. This new method is combined with existing technology to build up the security and have smooth communication. Firstly, we encode the data then the message is hidden using algorithm. Simply LSB was not efficient as it was easy to discover so we used combined layer of steganography and cryptography which automatically increased the security and efficiency of data [9]. Even after detecting, the steganography attacker needs to decode the new algorithm which is quite difficult to access.

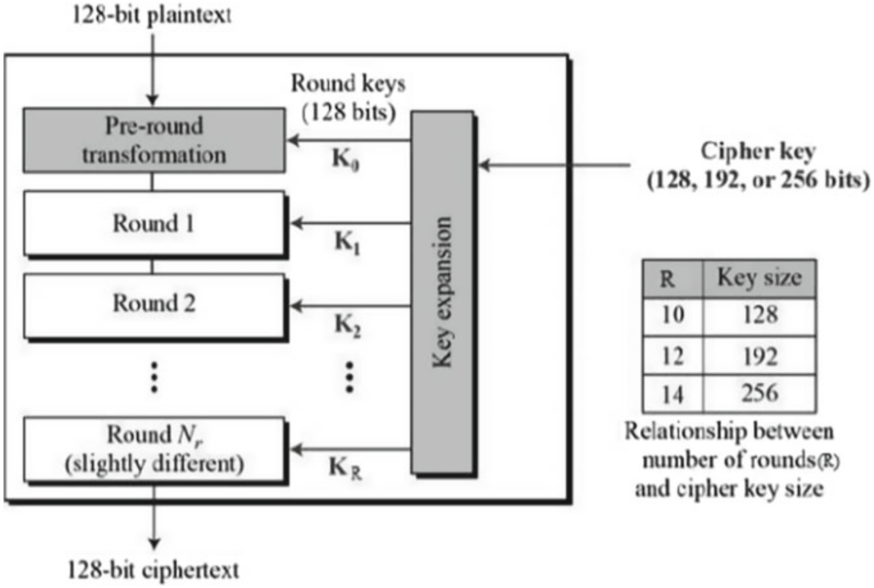
13.3.1 AES Algorithm

Here, we show the design of our technique, which can use any encryption algorithm. The encryption method which we used here to scramble the information is AES algorithm. The steps are as follows:

i. In this technique, we use bytes instead of bits. There are 128 bits of plaintext taken as 16 bytes.
ii. These bytes are masterminded in 4 lines and 4 segments to fill in as a grid.
iii. The no. of rounds is changeable and relies upon the measurement of our key.
iv. There are 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256 keys.
v. Most of them has distinctive key that is assessed by unique AES key.

Now, we have the diagram showing the functionality of this algorithm. There are two steps in this algorithm which are substitution and permutation. The 128-bit plaintext goes to pre-round transformation which goes on from 1, 2, … *N* and gives us 128-bit cipher text [10] (Fig. 13.3).

Now, we begin with the embedding algorithm.



R	Key size
10	128
12	192
14	256

Fig. 13.3 AES algorithm

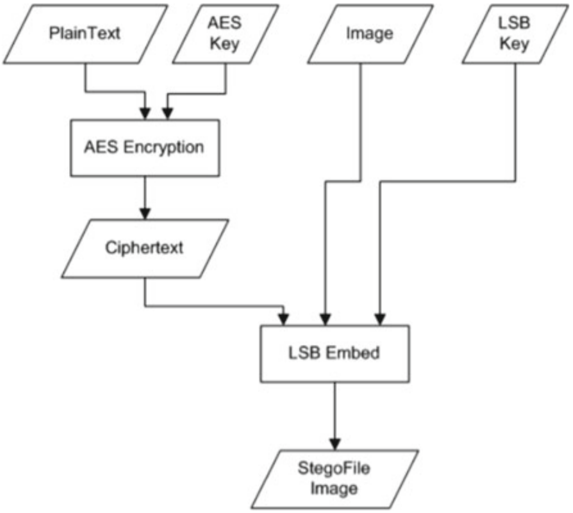


Fig. 13.4 Embedding process

13.3.2 Encryption Module

Encoding image file to give output as a text.

The algorithm is as follows:

Begin

i. Take input as any audio, video, image, or text. Here, we are taking an image.
ii. Select the image where you want to insert another image. And run the program using AES algorithm.
iii. Do the encryption process using AES which will create a cipher text.
iv. Now take the cover image and key and perform embedding using the algorithm.
v. Lastly, we obtain result as our stego-image.

Stop (Fig. 13.4).

13.3.3 Extraction Module

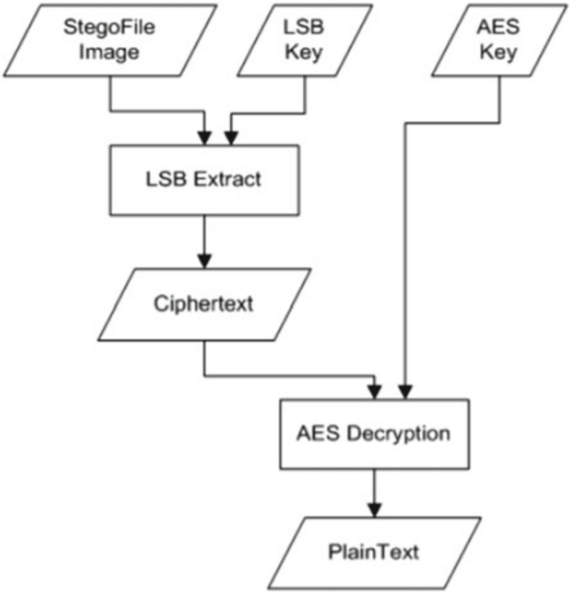
Extracting image file to give output as plaintext.

The algorithm is as follows:

Begin

i. Initially we put the stego bmp file and LSB key to do the decoding part.
ii. After doing so, we obtain the cipher text.
iii. Lastly, we use the AES key to do the extraction part. This process goes until we obtain plaintext.

Fig. 13.5 Extracting process



Stop (Fig. 13.5).

13.4 Results and Discussion

The proposed calculation was actualized utilizing MATLAB. This area presents the trial results and shows the estimations of PSNR and MSE determined for stego and carrier picture utilizing formulas are given beneath.

13.4.1 PSNR

PSNR is the peak signal to noise ratio which helps in getting to the nature of stego-picture as for the first picture. It ascertains the subtlety of the stego-picture. It helps to compare two pictures and helps to determine the closeness between them [11]. The more is the PSNR of the image the more it will be accurate. The formula for PSNR is depicted beneath (Fig. 13.6).

$$\mathrm{PSNR} = 10\,\log_{10}\left[\frac{I^2}{\mathrm{MSE}}\right] \tag{1}$$

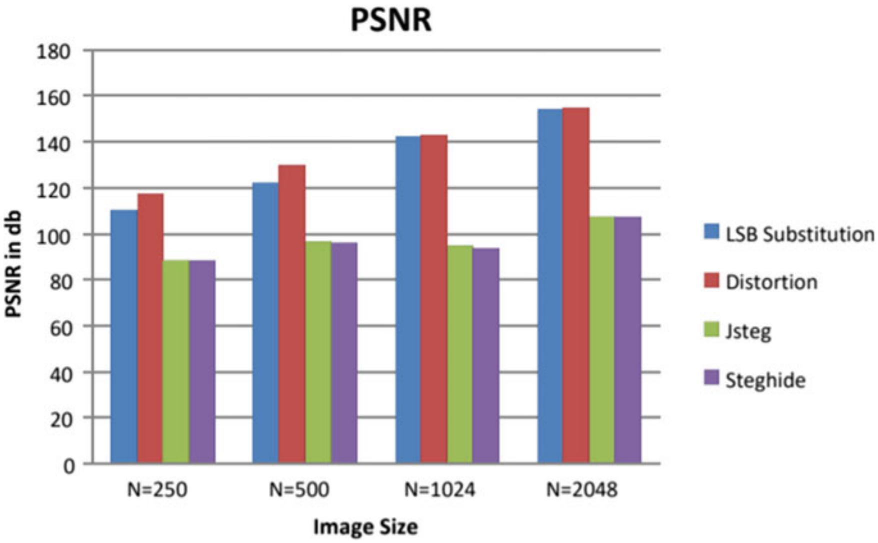


Fig. 13.6 PSNR values of few techniques

13.4.2 MSE

MSE is defined as mean square error that helps in ascertaining the error in the first picture and stego-picture. The contrast among the estimations of unique and stego-picture are multiplied and afterward their normal is determined. It is utilized essentially if there should arise an occurrence of huge mistakes since it gives generally high weight to these blunders. In this way, RMSE is extremely requesting when huge blunders are unfortunate in the image. The little is the estimation of RMSE, the more will be the nature of framework. Formula to compute MSE is as follows:

$$\text{MSE} = \frac{1}{(R * C)^2} \sum_{i=1}^{N} * \sum_{j=1}^{M} \left(X_{ij} - Y_{ij}\right)^2 \tag{2}$$

where:

I = max estimation of the pixel. The maximum incentive for gray scale picture is 255.

R and C are the no. of lines and segment in the spread picture (Fig. 13.7).

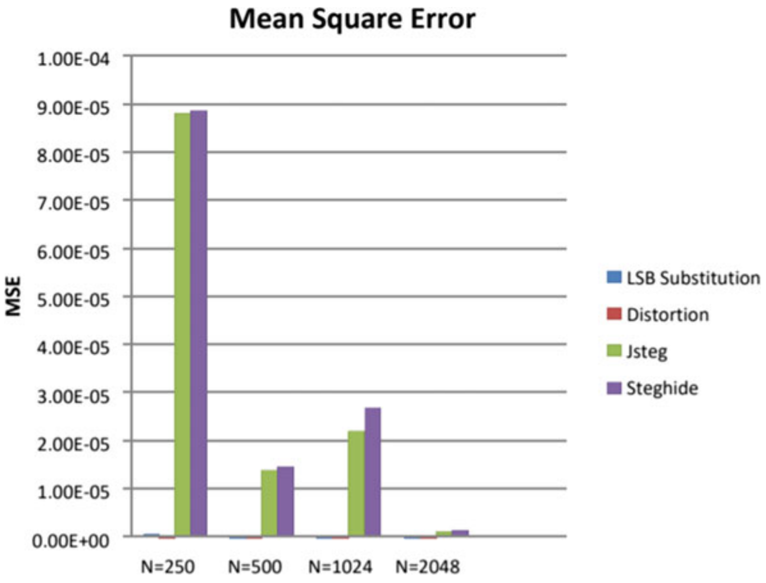


Fig. 13.7 MSE of few techniques

13.4.3 Embedding Capacity

It is the size of the mystery information that can be embedded in spread picture without crumbling the honesty of the spread picture. It very well may be spoken to in bytes. It relies on the qualities of spread picture and the inserting calculation utilized for steganography (Fig. 13.8).

Now in Fig. 13.9, we are showing the comparison graph of few techniques discussed here, in which the output of proposed method is much better than others.

13.5 Conclusion

Here, we intended combined approach for image steganography which overcome the limitation of existing methods. This approach used them as a combination of layers and is implemented in MATLAB. The results obtained provide us a better security and privacy of data and enhance communication. This also overcome the problem of steganalysis. This method improved the quality of stego-image as well as gave a good PSNR and MSE values. This method creates multiple barriers in front of the attacker so it is impossible for intruder to extract the data.

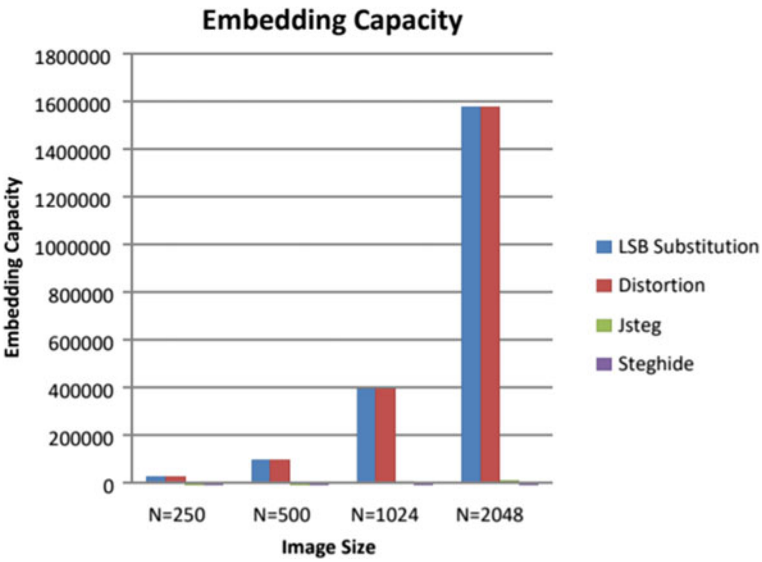


Fig. 13.8 Embedding capacity of few techniques

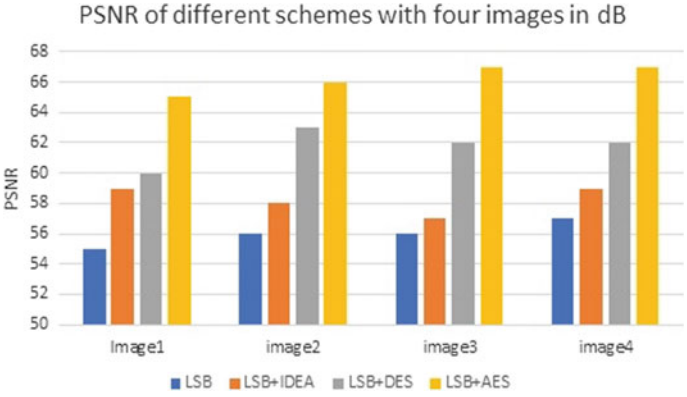


Fig. 13.9 Comparison graph of PSNR values

Acknowledgements This work is part of bilateral Indian-Bulgarian cooperation research project between Technical University of Sofia, Bulgaria and Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonipat, India under the title “Contemporary Approaches for Processing and Analysis of Multidimensional Signals in Telecommunications,” financed by the Department of Science and Technology (DST), India and the Ministry of Educations and Science, Bulgaria.

References

1. Islam, A., Khalid, F., Shah, M., Khan, Z., Mahmood, T., Khan, A., Ali, U., Naeem, M.: An improved image steganography technique based on MSB using bit differencing. In: The Sixth International Conference on Innovative Computing Technology, pp. 265–269. IEEE, Dublin (2016)
2. McAteer, I., Ibrahim, A., Zheng, G., Yang, W., Valli, C.: Integration of biometrics and steganography: a comprehensive review. Technologies **7**, 34 (2019)
3. Zou, Y., Zhang, G., Liu, L.: Research on image steganography analysis based on deep learning. J. Vis. Commun. Image Represent. **60**, 266–275 (2019)
4. Muhajjar, A.R., Badr, F.A.: Secure data communications using cryptography and IPv6 steganography. Int. J. Eng. Technol. **7**(4.19), 624–628 (2018)
5. Wu, N., Fan, P., Yang, Z., Ma, W., Liu, H.: Research on coverless text steganography based on single bit rules. J. Phys. Conf. Series 1237 (2019)
6. Ali, U.A., Sohrawordi, M., Uddin, M.: A robust and secured image steganography using LSB and random bit substitution. Am. J. Eng. Res. **8**(2), 39–44 (2019)
7. Thabit, R.: Improved steganography techniques for different types of secret data. Int. J. Adv. Syst. Sci. Appl. **6**, 38–51 (2019)
8. Verma, M., Saini, H.: Analysis of various techniques for audio steganography in data security. Int. J. Sci. Res. Netw. Secur. Commun. **7**(2), 1–5 (2019)
9. Kalamkar, P., Gaikwad, M., Gore, S., Sonule, D., Bodhe, V.: A review on implementation visual cryptography and steganography. Int. J. Sci. Res. Sci. Technol. **6**(2), 420–428 (2019)
10. Sharma, A., Poriye, M., Kumar, V.: A secure steganography technique using MSB. Int. J. Emerg. Res. Manag. Technol. 6(6) (2017)
11. Miramirkhani, F., Narmanlioglu, O., Uysal, M., Panayirci, E.: A mobile channel model for VLC and application to adaptive system design. IEEE Commun. Lett. **21**(5), 1035–1038 (2017)