Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 05 Issue 01
2023

Research Article
https://doi.org/10.56979/501/2023

Security Enhancement of Light Weight Data Transmission by Using Combination of Image Steganography and Cryptography

Muhammad Shahzad[1*], M Fuzail[1], M Kamran Abid[1], Naeem Aslam[1]
[1]NFC Institute of Engineering and Technology Multan, Pakistan.
[*]Corresponding Author: Muhammad Shahzad. Email: myselfmshahzad@gmail.com.

Received: March 27, 2023 **Accepted:** May 30, 2023 **Published:** June 05, 2023.

Abstract: Today, everyone around the world demands privacy in terms of secure communication. For this purpose, the most used techniques are cryptography and steganography. Cryptography is used to encrypt text-type data of information into cipher text by using some encryption algorithm. Steganography is the process of hiding data in a digital image which is the original medium called cover medium used as the career of information. This research proposed a technique to hide the secret data in the LSB of the cover image pixel. First, we encrypt the data being concealed using the AES algorithm. Then we applied a mathematical model on encrypted data and embed it in the cover object using the three least significant bits in reverse order. Concealed information is extracted in reverse steps of the proposed technique. Experimental results show that for lite weight data, the human eye cannot observe the existence of the hidden data in the Stego image.

Keywords: Steganography, Cryptography, Cover Media, Stego Media, Secret data.

1. Introduction

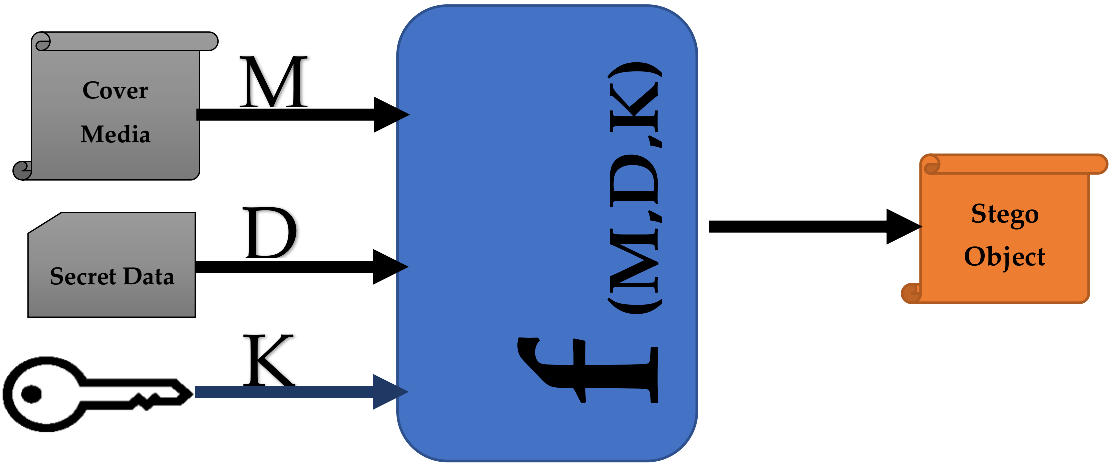
Images and various sorts of data have been shared continuously since the internet was invented. Information security is crucial for communication including information technology. To protect the privacy of communications, many cryptographic approaches have been developed. But keeping a message's contents secret is not enough; it is also important to keep the message's existence hidden. Steganography [1], [2] which conceals a message within an item like a picture, audio file, or video, enables unseen communication. Due to their attractiveness and safety, images are currently the most used type of online transmission. In image steganography, information is added to an image to create a tagged image that may be readily shared with others. The person who can decipher the image's hidden meaning is the only recipient.

In today's world of technology, everyone demands privacy and security of data being transmitted using the internet. Many stenographic and cryptographic algorithms are practiced to secure the given information from an intruder. But nothing is fully secured, there might be a loophole that needs to be improved.

This research proposed a technique to hide the secret data in the LSB of the cover image pixel. First, we encrypt the data being concealed using the AES algorithm. Then we will take the 1's complement of secret data and then embed it in the cover object in the three least significant bits in reverse order. Our proposed technique improves the security of hidden data as compared to existing ones.

2. Basic Steganography Model

Components of a basic model of steganography are cover media: M, Secret data: D, and a stego key: K takes as input and a function f (M, D ,K) which gives stego object as output. The basic model is shown in the figure.1



Figuer 1. Basic Steganography Model

3. Related Work

The most common method for image steganography is LSB substitution in which cover media LSB bits are replaced with secret data bits that cause minimum distortion in the carrier image. In [3] Hash base LSB technique was presented which uses a combination of cryptographic and steganographic techniques and results in the secure utilization of these techniques. The hash value is used in cover image file base luminosity histogram, visual analysis, file size, hamming distance, and also by pixel comparison. Copyrights protection is one of the applications of the proposed hash LSB method.

Yıldıray Y, proposed in [4] a technique based on the LSB method and apply to store the information of students in the carrier image. The secure information is first compressed using the LZW compression algorithm and then hidden in the image.

In 2014, K. Thangadurai performs an analysis of image-based steganography techniques and conclude that the LSB method is simple to embed the secret information into the carrier object[5]. The LSB method can be used with GIFF as well as PNG files. GIFF is better than PNG to store maximum data.

In 2020, Omar Elharrouss proposed a technique that hides an image into another image[6]. The proposed technique was based on the k-LSB substitution method in which the k number of the least significant bits is used to store the image. Decoding is performed by region detection technique for finding the blocks of carrier image that contain the hidden image.

In 2018, Mark Rennel presented a technique based on the LSB approach and used the YCbCr color family in the embedding phase[7]. To make the proposed method more strengthen another cover selection approach was discovered in this article. To measure the detection probability of cover media, two factors are used in process of cover selection. One of those two factors is kurtosis and the other is the skewness of cover media. High correlation coefficient kurtosis and skewness of cover image yield the selection of the best suitable cover image which further can be used for the embedding process.

In [8], Ki-Hyun Jung combines the PVD and LSB on image bit planes. Bit regions are first divided and both techniques are used simultaneously on a single-bit plane. Experimental results declare that the proposed technique has a control on embedding capacity and no visual distortions can be found by the human eye.

In [9], different LSB-based and discrete wavelet transform steganography schemes are compared concerning capacity and efficiency while hiding multiple images into a single carrier image. The proposed technique was about embedding multiple images into a single carrier object. The performance of the proposed technique for both algorithms was measured concerning carrier image capacity, data imperceptibility, and security.

In [10], the proposed method of steganography is applied on carrier image edges humans can't focus on these areas, and therefore more imperceptibility can be achieved. The second main thing is the security of secret data which also was considered in the proposed method and the one-time-pad (OTP) is used to keep the message secure. Better imperceptibility value is achieved during the experiment. Histogram of both the carrier image and stego image are compared which shows minimum distortion in the carrier image.

In [11], a Systematic Literature Review is performed on 20 research articles published during 2016-2022. It is found that among those articles, 17 articles are presented related to image steganography techniques, and 3 leading tools are presented. They found 4 main parameters to measure image steganography quality which are size, imperceptibility, MSE (Mean Squared Error), and PSNR (Peak-signal-noise-ratio)

In [12], a combined approach of cryptography and steganography is presented to prevent tempering in medical images that are transmitted on the public network. Confidential medical images are embedded into another image which is the carrier image. Hashing technique is used to secure the data and encrypted secret medical image data is embedded using DWT (Discrete wavelet transform) into the carrier image. Experimental results have proven the enhanced security of medical images.

In [13] the same embedding scenario is used and applies the edge detection technique to the same component that served as the index for embedding (i.e., lower the edge detector's threshold value until the right number of edge positions are obtained). Read the LSBs of the other component that was utilised for embedding using the edge position as an index. Concatenate the LSBs in to obtain the secret message. In essence, there are two main methods for maintaining the privacy of data. One such tactic is encryption, in which the data is transformed into an unintelligible format to make it challenging for an outsider to interpret [14].

In the case of digital photos, the adjustment is only made to the least important sections of the original image in order to lessen the impact of the original image's degradation. The perceptibility of the original image is not significantly altered since the secret message is only inserted at the least important bits. A directional embedding method for the stego picture that maximises image quality. In order to reduce bit changes in the cover picture when a secret data is inserted, the suggested approach conducts a selection of an appropriate direction for secret byte embedding [15].

In [16] first the Cover images and secret images are processed. With the exception of the requirement that the secret picture dimension should be a multiple of 8, as in the next phases we will be dividing the image into an 8X8 block, the provided cover image is downsized to a 256X256 grayscale image and binary secret image is set to variable size

4. Proposed Methodology

The proposed method contains two modules one to secure the secret information and the other used to hide it in the carrier image. During the first phase, secret data is encrypted first using the AES algorithm than a mathematical model is applied to form a more complex structure of secret information. Results obtained by applying a mathematical model are embedded using three LSB of the red, green, and blue channels of the color image. A total of nine bits of secret data can be stored in a unit pixel of the color image.

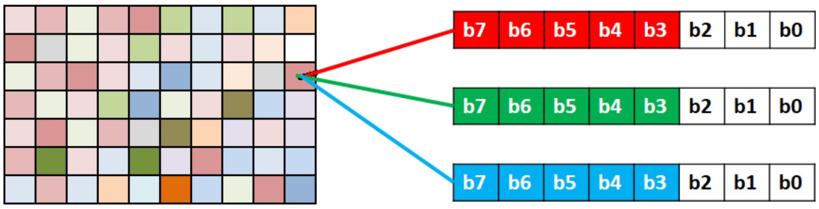


Figure 2. Layout of Cover Media

In an RGB color image, every pixel has three layers that are red, green, and blue having an 8-bit format. Three bits of secret data can be concealed in each layer and a total of 9 bits of confidential data can be stored in a single pixel of RGB image.

4.1 Embedding

While embedding confidential information into cover media, the three least significant bits of each layer of RGB pixels are replaced with secret information. The storage capacity of the cover image can be calculated using the formula HC= (height*width*9*3)/8.

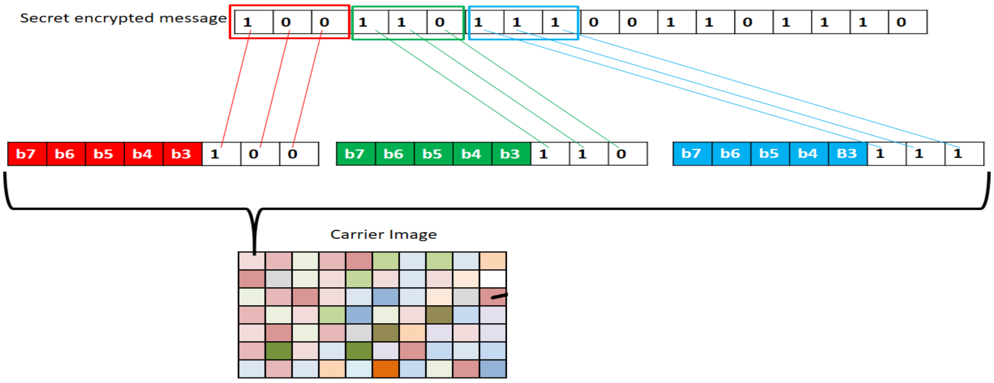


Figure 3. Embedding process

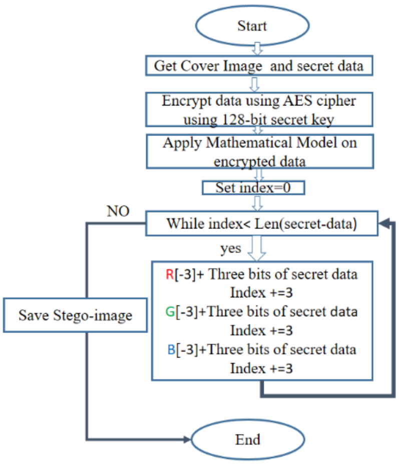

Start
Get Cover Image and secret data
Encrypt data using AES cipher using 128-bit secret key
Apply Mathematical Model on encrypted data
Set index=0
While index< Len(secret-data)
NO
yes
R[-3]+ Three bits of secret data
Index +=3
G[-3]+Three bits of secret data
Index +=3
B[-3]+Three bits of secret data
Index +=3
Save Stego-image
End

Figure 4. Embedding Algorithm

4.2 Extraction

In the opposite procedure from data embedding, data extraction is performed at the destination. When the decoder receives a stego picture as input, it will output an array of secret data bits in reverse order. The original message may be obtained by passing it through a suggested mathematical model.

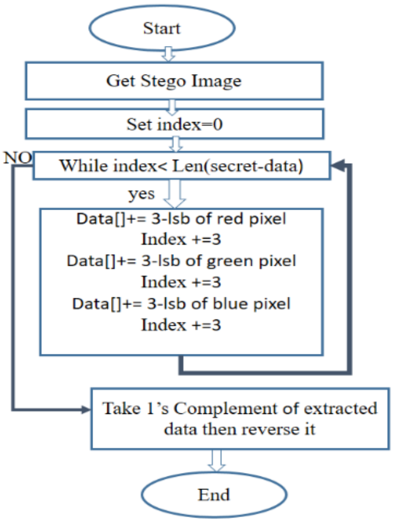

Start
Get Stego Image
Set index=0
NO
While index< Len(secret-data)
yes
Data[]+= 3-lsb of red pixel
Index +=3
Data[]+= 3-lsb of green pixel
Index +=3
Data[]+= 3-lsb of blue pixel
Index +=3
Take 1's Complement of extracted data then reverse it
End

Figure 5. Data Extraction Algorithm

Data is first removed at the receiver side of a stego object, then it is inverted and finally passes through the suggested mathematical model. The same key that was employed to encrypt the secret data is utilized to do the decryption once more using the AES technique.

5. Experimental Results & Discussion

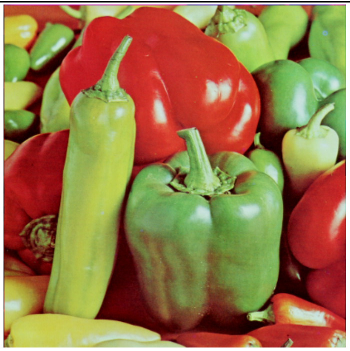
The proposed method is put into practice in the Jupyter Notebook 6.3.0 and Python 3.7 environments. In this project, cover media—color images—are utilized to hold confidential information. The approach that has been implemented employs LSB substitution to conceal the data in carrier media pixels. A 256-bit secret key is used to encrypt the data using the AES technique before the encrypted data is embedded into the three lSB bits of each layer R, G, and B of a color picture pixel. Take the encrypted data's 1's complement first, then embed it in reverse order into the cover picture pixel before adding the secret data. The same process is carried out in reverse on the destination side. Evaluation metrics used to measure the quality of stego objects are MSE, RMSE, PSNR, and UQI. "NFCIET MULTAN" is the coded information that we hid inside carrier pictures. In this experiment, the first 13 photos in the dataset "misc" contain the same hidden message, "NFCIET Multan." The first three bits of the secret data array are contained in the Red channel's 3-LSB bits, the next three in the Green channel's 3-LSB bits, and the final three bits are in the Blue channel of the RGB color picture pixel. One color picture pixel has a total of nine embedded pixels.

Humans cannot visually distinguish between the original and the Stego picture of little data that has to be hidden in an image. In our experiment, a little text reading "NFCIET Multan" that cannot be seen by the human eye is concealed in the stego picture. Table 1 provides a visual comparison of the first 13 photos (Original vs. Stego).

Table 1. Visual Comparison of Original vs. Stego Images

Size	Original Image	Stego Image
256x256		
256x256		
256x256		
256x256		
256x256		
256x256		
256x256		

256x256		
512x512		
512x512		
512x512		
512x512		

512x512		

5.1 Stego Image Quality Analysis

Stego picture quality is evaluated using the Python "sewar" module. This library has incorporated several metrics. Two photos are used in the calculation of Mean Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Universal Quality Image Index (UQI) (original, Stego Image). Table 4.2 provides a comparison of quality measures.

Table.2 Comparison of MSE, RMSE, PSNR, UQI

Size	Description	MSE	RMSE	PSNR	UQI
256x256	Female (NTSC test image)	0.002685	0.049901	72.9632	0.999999908
256x256	Couple (NTSC test image)	0.002910	0.049652	72.9667	0.999999296
256x256	Female (from Bell Labs?)	0.004169	0.066254	72.7241	0.999999989
256x256	Female	0.003413	0.058419	72.7896	0.999999937
256x256	House	0.003971	0.061223	71.23530	0.999999983
256x256	Tree	0.003259	0.056401	72.13590	0.999999992
256x256	Jelly beans	0.003415	0.060285	73.07213	0.9999999879
256x256	Jelly beans	0.002795	0.052691	72.9151	0.9999999878
512x512	Splash	0.000980	0.030289	77.9235	0.999995461
512x512	Mandrill (a.k.a.Baboon)	0.000731	0.028161	78.5132	0.99999992
512x512	Airplane (F-16)	0.000929	0.030530	79.0361	0.9999999101
512x512	Sailboat on lake	0.001132	0.029122	78.0971	0.999999912
512x512	Peppers	0.000971	0.031725	78.0343	0.9999999897

The MSE, RMSE, PSNR, and UQI values of several visual representations of identical-sized pictures may be seen in the above table. Different measurement values show how the aesthetic appeal of a picture influences its Stego image quality.

6. Conclusion

Everyone in the world today needs privacy for safe communication. In this study, a brand-new method for blending data into images is suggested. Using Python's AES method, which encrypts messages with a 256-bit secret key, private data is first encrypted. Following encryption, 1's complement of the secret cipher text is extracted, which again modifies the structure of the secret message. Additionally, the reverse function receives the complement's result and returns the opposite of the hidden text. The form of the results produced by the reverse function is an array of bits. The first three bits of the array are now encoded in the Red channel's 3-LSB, the Green channel's 3-LSB, and the Blue channel of the RGB color picture pixel. One color picture pixel has a total of nine embedded pixels. The 3-LSB bits of each channel (R, G, and B) of the color pictures are extracted at the destination until no more data can be recovered. Complement and reverse the extracted data after that, and then the output is decrypted using the same secret key that was supplied to the AES method.Two images are used in the calculation of Mean Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Universal Quality Image Index (UQI) (original, Stego Image). Table 4.2 shows that various visual representations of identical-sized pictures have varying MSE, RMSE, PSNR, and UQI values. Different measurement values show how the aesthetic appeal of a picture influences its Stego image quality.From a security standpoint, the distinction between the source and Stego picture for little data that is to be disguised in an image cannot be visually observed by humans. The complement and reversal of private encrypted data can also be used to change the encrypted secret text. The following suggestions for future work are made in light of this study that the RGBA (32-bit) multichannel pictures, which are an expanded form of RGB color images, may be used with the proposed approach.

References

1. A. K. Sahu and G. Swain, "Dual stego-imaging based reversible data hiding using improved LSB matching," Int. J. Intell. Eng. Syst., vol. 12, no. 5, pp. 63–73, 2019, doi: 10.22266/ijies2019.1031.07.
2. G. Swain, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution," Arab. J. Sci. Eng., vol. 44, no. 4, pp. 2995–3004, 2019, doi: 10.1007/s13369-018-3372-2.
3. S. D. Muyco and A. A. Hernandez, "A modified hash based least significant bits algorithm for steganography," ACM Int. Conf. Proceeding Ser., pp. 215–220, 2019, doi: 10.1145/3335484.3335514.
4. Y. Yigit and M. Karabatak, "A stenography application for hiding student information into an image," 7th Int. Symp. Digit. Forensics Secur. ISDFS 2019, pp. 9–12, 2019, doi: 10.1109/ISDFS.2019.8757516.
5. K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," 2014 Int. Conf. Comput. Commun. Informatics Ushering Technol. Tomorrow, Today, ICCCI 2014, pp. 3–6, 2014, doi: 10.1109/ICCCI.2014.6921751.
6. O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 131–135, 2020, doi: 10.1109/ICIoT48696.2020.9089566.
7. M. R. D. Molato and B. D. Gerardo, "Cover image selection technique for secured LSB-based image steganography," ACM Int. Conf. Proceeding Ser., 2018, doi: 10.1145/3302425.3302456.
8. K. H. Jung, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," J. Real-Time Image Process., vol. 14, no. 1, pp. 127–136, 2018, doi: 10.1007/s11554-017-0719-y.
9. A. Gutub and F. Al-Shaarani, "Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons," Arab. J. Sci. Eng., vol. 45, no. 4, pp. 2631–2644, 2020, doi: 10.1007/s13369-020-04413-w.
10. D. Deenadayalan, A. Kangaiammal, and B. K. Poornima, Integrated Intelligent Computing, Communication and Security, vol. 771. Springer Singapore, 2019.
11. M. A. Aslam et al., "Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review," Proc. 2022 2nd Int. Conf. Comput. Inf. Technol. ICCIT 2022, pp. 32–38, 2022, doi: 10.1109/ICCIT52419.2022.9711628.
12. I. Conference, C. Technologies, T. Student, E. C. E. Lbsitw, and P. Trivandrum, "Medical Integrity Verification System," 2017.
13. R. D. Rashid, "Edge Based Image Steganography : Problems and Solution," 2019 Int. Conf. Commun. Signal Process. their Appl., pp. 1–5, 2019.
14. R. A. Subong, "LSB Rotation and Inversion Scoring Approach to Image Steganography," 2018 15th Int. Jt. Conf. Comput. Sci. Softw. Eng., pp. 1–4, 2018, doi: 10.1109/JCSSE.2018.8457333.
15. S. Sugathan, "An Improved LSB Embedding Technique for Image Steganography," no. 4, pp. 609–612, 2016.
16. K. Patel and L. Ragha, "Binary image Steganography in wavelet domain," 2015 Int. Conf. Ind. Instrum. Control. ICIC 2015, no. Icic, pp. 1635–1640, 2015, doi: 10.1109/IIC.2015.7151012.