IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 3, March 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

Secrete Communication System Using Multi Image Steganography for Military Application

Snehal Kokare[1], Nikita Mane[1], Mayuri Wagh[1], Prasad Kamthe[1], Dhanshri Alhat[1], Prof.Tushar Phadtare[2]

Student, Dept. of Computer Engineering, JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune, Maharashtra, India[2]

ABSTRACT: The study of undetectable communication is known as steganography. It usually has to do with the method of concealing the existence of the communicating data. It conceals informational details. It is the process of transferring data from one digital medium to another and then recovering the same information. The least significant bit (LSB) and the symmetric key between the sender and the receiver are used in this work to hide data in an image. We must select the bits that will result in the lowest resolution between the original image and the stego image. This paper goes into greater detail about the encryption and decryption methods.

KEYWORDS: LSB, PSNR, STEGANOGRAPHY, AND DYNAMIC SYMMETRIC KEY ARE SOME OF THE TERMS USED.

I. INTRODUCTION

Steganography is derived from the Greek terms Stego and Graphia, which mean "to cover" and "to write," respectively. The translation is "to cover writing" or "to hide data." The simplest method is to place the secret data bits in the LSB places of the original image. [1].

Image to image, Text to image, Image to text, Video to voice, and Voice to video are all examples of steganography.

Image to Image: Using the stego key[2], an image is embedded within another image in image steganography. Text to Image: In this case, the text is put into the image and the image is sent using the symmetric key. -From video to voice Hiding or embedding a message in a movie is similar to the art of concealing information because the sender is not only concealing but also preventing the message from being read by anybody other than the intended recipient. The art of hiding information includes hiding messages in videos. Video-based steganography techniques are similar to image-based steganography techniques. Information security is a critical example of security in today's society, and it is becoming increasingly vital to secure data from tampering. This steganography technique is used to ensure that the data is not tampered with. When the data is already on its way to be transmitted, protection should be required.

Dr. Amarendra K, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India, Department of Computer Science and Engineering Email:amarendra@kluniversity.in Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India. Venkata Naresh Mandhala, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India. Email:mvnaresh.mca@gmail.com B.Chetan Gupta, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India, Department of Computer Science and Engineering Email:chetangupta317@gmail.com G.Geetha Sudheshna, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India, Department of Computer Science and Engineering Email:geethasudheshna@gmail.com V.Venkata Anusha, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India; Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India; Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Email:anushavv2499@gmail.com

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

II. STEGANOGRAPHY VS CRYPTOGRAPHY

Cryptography is the process of converting plain text into cypher text using a symmetric key, and encryption is the result of this process. The fundamental drawback of cryptography is that the plaintext can be deciphered and the cypher text can be seen but not read[4]. Steganography is a technique for hiding plain text in digital material. Because the plaintext and cypher text are being concealed into another medium, the Trespasser will not be able to see them. The trespasser has no way of knowing if there is any sensitive information on the premises. The steganography technology is employed to improve the security of data transmitted across a computer network.

Steganography Process

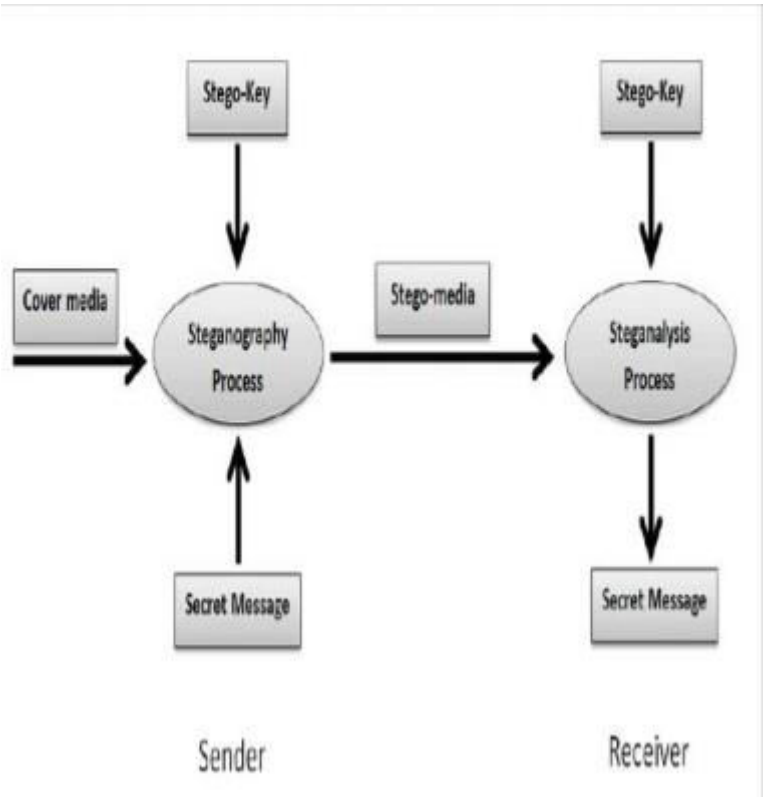


Fig. 1 Steganography Process

Secret Message: The information that must be entered into the digital medium. The key utilised in the Steganography process is known as the Stego-key. Cover Media: The medium used in the Steganography process, such as images, videos, and sounds. The approach used in this Steganography process is known as the Sender Algorithm. Stego-Media: The media created by incorporating the mystery message into a widely disseminated media using the Stego-key and encoding calculation. Receiver Algorithm: The method for extracting the mystery message from Stegomedia using the Stego-key algorithm.

III. LEAST SIGNIFICANT BIT (LSB)

The LSB is the most well-known steganography method. Steganography use the LSB of a picture's pixel data, which is also a popular approach nowadays. One section of the LSB is based on this investigation. It replaces one pixel in the first picture with one fragment of the double content piece. When using LSB methods to every byte of a 24 bit picture, three bits can be encoded into every pixel[3] when the record is longer than the message document and the picture is grayscale. For example, if we change the last bit of every color's byte with a bit from the message, we can employ graphics to hide things.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

IMAGE WITH 3 PIXEL

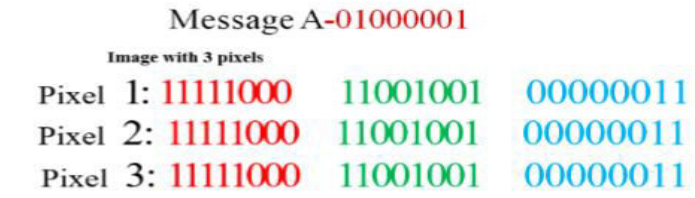


Fig. 2 Message A before encryption

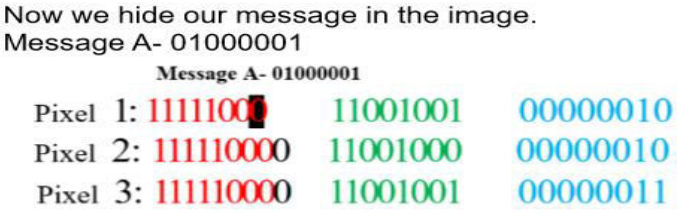


Fig. 3 Message A after encryption

3.1 ZIGZAG SCANNING:

For added security, we used the Zigzag scanning method, which is based on the Steganography technology. By turning the secret message into bits, image pixels are employed to disguise the secret message in this manner. The secret message bits are hidden via patterns in this Zigzag scanning. Only the sender and receiver will be aware of this pattern. The receiver can extract his secret message using this pattern.

3.2 PSNR:

PSNR stands for Peak Signal to Noise Ratio, which can be easily determined. It's a tool for comparing the quality of compressed photos and movies. The image resolution will be reduced if the PSNR is high. Our objective is to get a high Peak Signal to Noise Ratio so that our image resolution is unaffected. There will be little difference between the primary image and the converted stego image if the PSNR value is high enough.

IV. METHODOLOGY

We employed the technique of employing the symmetric key between the sender and receiver, as well as the Least Significant Bit, in this term paper. We'll also examine how encryption and decryption work in this section.

4.1 Steganography using LSB and Symmetric Key:

To reject anything else, we must convert the picture pixels to Binary characteristics using Zigzag Scanning with size=R*S*8, where R is the number of lines in the picture, S is the number of sections, and 8 is the amount of bits for each pixel. Finally, where the LSB position is 0 and the bit preceding the LSB is 1, retrieve the last two bits of every pixel. Convert the riddle message (which you need to hide) into coordinated qualities of size 1*N, where N is the number of bits in the mystery message, when using this procedure. When it comes to switching over the picture pixels and secret message, we'll just encourage the mystery message to be two fold bits with the two bits of the LSB. This procedure has three steps[5]. 1. If the confidential message bit is equal to the LSB's 0th position, the key value is "0." 2. If the confidential message bit equals position 1 of the LSB in this operation, the key value will be "1." 3. If the confidential message bit does not equal both position 1 and position 0 of the LSB during this procedure, the key value will be "0."

We'll only encourage the mystery message to be two fold bits with the two bits of the LSB when it comes to switching over the picture pixels and secret message. There are three steps in this procedure[5]. 1. The key value is "0" if the confidential message bit is equal to the LSB's 0th position. 2. In this procedure, the key value will be "1" if the

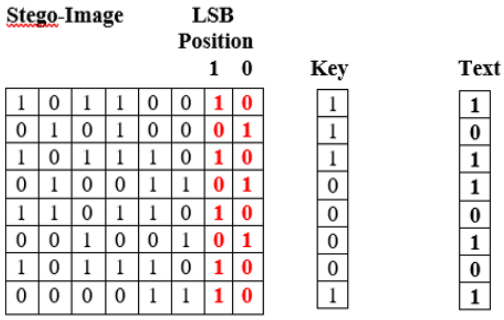
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

confidential message bit equals position 1 of the LSB. 3. During this method, if the confidential message bit does not equal both position 1 and position 0 of the LSB, the key value will be "0."

4.2 Encoding



1	0	1	1	0	0	**1**	**0**
0	1	0	1	0	0	**0**	**1**
1	0	1	1	1	0	**1**	**0**
0	1	0	0	1	1	**0**	**1**
1	1	0	1	1	0	**1**	**0**
0	0	1	0	0	1	**0**	**1**
1	0	1	1	1	0	**1**	**0**
0	0	0	0	1	1	**1**	**0**

Key	Text
1	**1**
1	**0**
1	**1**
0	**1**
0	**0**
0	**1**
0	**0**
1	**1**

Fig 4 : *Encoding Process*

4.3 Experimental Results:

A MATLAB software created by the creators for computational checks using appropriate models such as characters with data in a picture. GUI was created to rebuild the enjoyment with certain sensible models. In this application, a dull scale Petra photo (for example) of type jpeg has been utilised with a proportional size of (10241024 pixels). Going forward with advances is how the framework is addressed:

-Zigzag Scanning will be used to convert the grayscale image into binary values. - The degree of data (secret message) that can be embedded in the image is computed using the LSB technique: 1048549 bits (1024 x 1024) – 27 - Using the new wa'el calculation system, the degree of data (secret message) that can be placed in this image is computed: ((10241024) – 27)/2 = 524261 bits - Take, for example, the opening to this article, which was chosen to be the location of a secret message. The bits of the introduction are checked using the following formula: - 2136 characters x 7 bits = 14952 bits. - Select the Steganography technique (LSB). PSNR[6] was used to compare the findings of both approaches.

V. ENCODING

The improvements will demonstrate how to encode the (LSB+SPACING) computation using a Matlab Graphic User Interface (GUI) reproduction programme:

∟To select the Mysore-Palace photo from the drive, press the push catch (open picture).

∟To select the mysterious message from the local drive that is saved as a.txt record, press the push catch (open content).

∟The confidential message that we need to execute on this process is depicted in the figure, and the content of the confidential message will also appear in the programme window's content. –

∟Select the Steganography strategy (LSB+SPACING) from the Steganography technique drop-down menu. An exchange window will appear at the end of the Steganography method, requesting that the client save the key in the shower storage.

∟Figure 8 shows the key that was created using the (LSB+SPACING) approach with the information from the confidential letter and the Mysore-Palace photo. The stego media will then appear in the stego image.

∟ Using the PSNR catch, the client may determine the PSNR value between the first and stego images. After that, the client can save the stego image on the plate by pressing the push catch (Save Stego Image).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

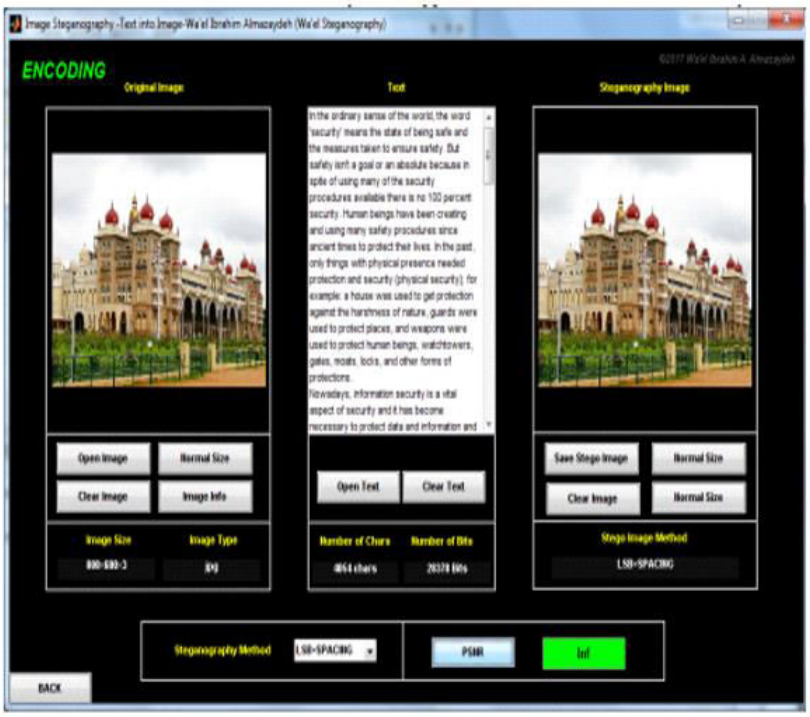


Fig. 5 Encoding Process

Key:

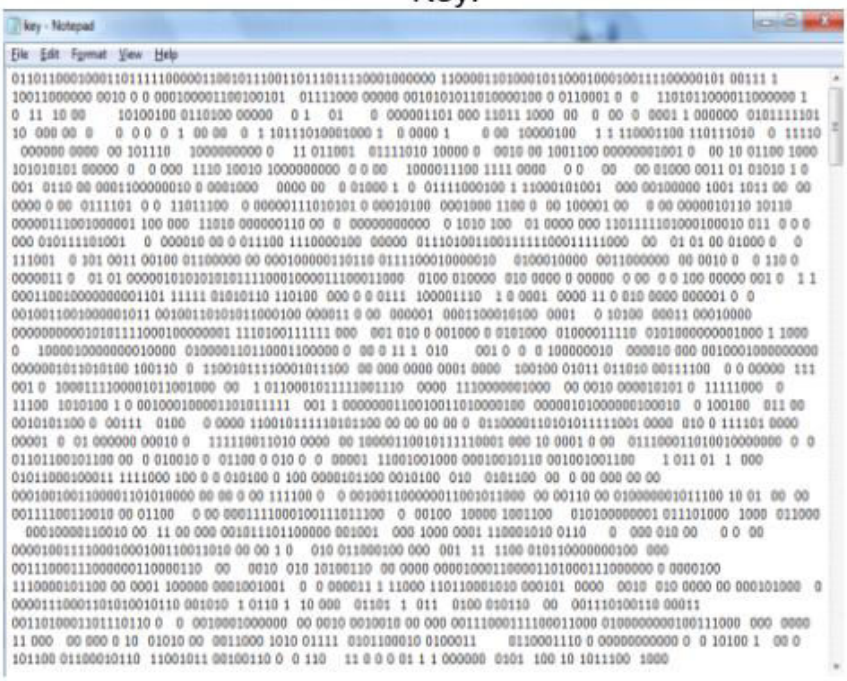


Fig. 6 Key Value for the encryption process

VI. DECODING

This approach will be used by the recipient, and it will expel the confidential message from the stego picture using the sender and receiver's shared key. As technology advances, we will demonstrate the decoding process using the Matlab software shown in the figure:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

∟To select a stego image from the collecting shower, use the button (Open Stego Image).
∟When you smash the push, you'll get (Show). The unwinding mechanism will begin removing the secret message from the stego image.
∟ A trade window will popup, requesting that the customer select the key from the accumulating circle.
∟The consumer will select the key from the plate, which will be stored as a substance report.
∟ The erased confidential message will thereafter display in the application window's substance region.
∟ Finally, the customer can save the puzzling message that appears in substance on the programme window by pressing the button (Save Text) to save it as a substance archive in the plate amassing.

VII. RESULTS

The values of PSNR for LSB and LSB+KEY methods

The Number of copies of introduction	Number of characters	Number of bits	Steganography Method	
			LSB PSNR	LSB+KEY PSNR
1	4073	28511	66.8017	69.8102
3	12219	85533	62.0194	65.0455
6	24438	171066	59.0098	62.0196
9	36657	256599	57.2485	60.2694
12	48876	342132	55.9999	59.027
15	61095	427665	55.0369	58.0561

Fig. 8 Results

VIII. CONCLUSION

This paper presents two Steganography structures: The first is the striking reasonableness, also known as Least Significant Bit (LSB), and the second is the most recent LSB+KEY system. The executions of the outcomes have been checked up for PSNR estimations with separate checks. It can be seen that the [7] calculation of LSB+KEY yields superior demands in terms of PSNR. This is one of the explored results in this work, and the work is still in progress to improve the computations for even better code irregularity and time complexity. It is also projected to generate estimates in awe-inspiring exchange of patient data in healing images under telemedicine.

REFERENCES

[1] J. Fridrich and M. Goljan, SPIE Symposium on Electronic Imaging, San Jose, CA, 2003, "Digital picture steganography utilising stochastic modulation.
[2] T. Morkel, J. H. P. Elloff, and M.S. Olivier, "An Overview of Image Steganography."
[3] Provos, N., and Honeyman, P., 2003, IEEE Security and Privacy Journal, "Hide and Seek: An Introduction to Steganography."
[4] Johnson, N.F., and Jajodia, S., Computer Journal, February 1998, Exploring Steganography: Seeing the Unseen. Detecting Steganographic Content on the Internet,
[5]N. Provos and P. Honeyman, Proc. 2002 Network and Distributed System Security Symp., Internet Soc., 2002.
[6] D. McCullagh, "Secret Messages in.Wavs," Wired News, February 2001, www.wired.com/news/politics/0,1283,41861,00.html.
[7] M C Trivedi Sharma, S., and Yadav, V. K. (2016). A overview of picture steganography approaches in the spatial domain. In: ICTCS 16: Second International Conference on Information and Communication Technology for Competitive Strategies. Article 84 of the ACM.
[8] D. A. Wu and W. H. Tsai, 2003. Using pixel-value differencing as a steganographic method for photographs. 24(9–10):1613–1626 Pattern Recognit. Lett.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 3, March 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1003034 |

[9] Hwang M S, Wu H-C, Wu N I, Tsai C S, Wu N I, Wu N I, Wu N I, Wu N I, Wu N I, Wu N I, Wu N I, Pixel-value differencing and LSB replacement methods are used to create an image steganographic scheme. 611–615 in IEE Proceedings: Vision, Image, and Signal Processing.

[10] Anand J V and Dharaneetharan G D 2011 A new technique to steganography that combines many LSB algorithms and uses the randomization principle to improve security. 474–476 in Proceedings of the 2011 International Conference on Communication and Computing

[11] M. Jain and S. K. Lenka, 2016. A look into LSB and LSB array for digital image steganography. 11(3):1820–1824 in International Journal of Applied Engineering Research

[12] Edge adaptive picture steganography based on LSB matching revisited, Luo W, Huang F, and Huang J, 2010. 5(2): 201–214 in IEEE Trans. Inf. Forensics Secur.

[13] Pattern Recognit. Lett., vol. 25, pp. 331–339, 2004. X. Zhang and S. Wang, Vulnerability of pixel-value differencingsteganography to histogram analysis and modification for enhancedsecurity.

[14]Pattern Recognition, vol. 37, pp. 469-474, 2004. [14] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, pp. 469-474, 2004.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details