IJIRCCE

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

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 7, July 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107007 |

# Data Security Hiding Technique Using Image Steganography with LSB

**Sunil Kumar, Ms. Sapna Rani**

PG Student, Dept. of Computer Science and Engineering, Swami Vivekananad Institute of Engineering and Technology Ramnagar, Banur, India

Assistant Professor, Dept. of Computer Science and Engineering, Swami Vivekanand Institute of Engineering and Technology Ramnagar, Banur, India

**ABSTRACT:** In today's digital era, ensuring data security and confidentiality has become crucial. This research paper presents a novel attitude for data security using image steganography with LSB (Least Significant Bit). Steganography is a technique that allows for the hidden transmission of information within seemingly innocent carriers, such as images. The LSB method, which involves replacing the least significant bit of each pixel in an image, offers an imperceptible means to embed sensitive data. This study explores the imperceptibility of LSB modifications, leveraging the human visual system's limited sensitivity to minor pixel alterations. The proposed technique focuses on seamlessly integrating the confidential data into the LSBs of the cover image, ensuring that the modifications are visually indistinguishable from the original image. To achieve data security, the secret message is divided into binary bits, and each bit is sequentially embedded into the LSBs of the cover image pixels. This embedding process preserves the image's visual quality while hiding the sensitive data effectively. The LSBs of the stego-image are extracted to extract the hidden data, and a decoding algorithm is applied to reconstruct the embedded bits, thereby recovering the original secret message.

The experimental outcome demonstrates the effectiveness of the proposed technique in securely hiding data within images with minimal impact on the visual quality. However, it is essential to consider additional encryption techniques in conjunction with steganography for enhanced data security.

**KEYWORDS:** Data security, steganography, LSB, image hiding, information hiding, data confidentiality

## I. INTRODUCTION

There are countless strategies through which instant messages are covered within Advanced pictures (RGB, Dark scale and BW). The best way is abusing useless parts of any documents or vague memory to put away mystery information which is likewise straightforwardly gotten. A small amount of data might be covered within the accessible parts of the header documents [1].

If the segment needs to be evident in standard conditions, there are a few instruments that, in the meantime, permit full access. However, there are numerous steganography holders, and the most prominent technique will be depicted in whatever remains of this paper. The fundamental standard of the framework dependent on the substitution is substituting spare parts of the picture with mystery information.

To comprehend this rule, it is essential to have information on the Stefano-graphical holder structure, and we give a concise portrayal of the RGB (Red-Green-Blue) frameworks. Within the RGB framework, each shading is spoken to by the general forces of every one of the three existing parts red, green & blue.

A solitary octet dictates every RGB segment; since the RGB framework contains three segments, this technique for introduction, we get the 24-bit to conspire, which underpins a 14,77,216 one-of-a-kind hue. A large portion of the present applications for handling and showing pictures portrayed backings 24-bit conspire, yet permits the use of an 8-bit plan to spare the picture measure.

Such a plan entirely utilizes 24-bit shading pixels and has a palette that determines the shade utilized in the picture. Pixels are coded with 8 bits. Where do the records show that Esteem wanted shading in the palette? Subsequently, this strategy confines the number of utilized hues in the picture at 256 for 8-bit. 8-bit design is run of the mill for GIF (Illustrations Exchange Arrangement) picture groups, commonly viewed as a lossless picture pressure.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107007 |

## II. LITERATURE REVIEW

**Varela (2005)** proposed a system to detect malignant masses in mammograms. The behavior of the iris filter was found at different scales. After the iris filter was applied, the suspicious region was segmented utilizing an adaptive threshold, and the suspected regions were characterized with features based on the iris filter output, grey level features and morphological features extracted from the image.

**Dacheng Tao (2006)** proposed a straightforward method of direct kernel BDA to solve the small sample size problem of the modified BDA in the kernel feature space. DKBDA removes the null space of the negative scatter concerning the positive centroid matrix. Then the eigenvectors of the positive within-class scatter matrix corresponding to the smallest Eigenvalues are extracted as the most discriminate directions in the kernel space. Incremental DKBDA is also developed to speed up the DKBDA.

**Orlando J Tobias (2017)** has suggested "an approach for histogram Thresholding according to the similarity between grey levels" because "methods for histogram thresholding based on the minimization of a threshold-dependent criterion function might not work well for images.
They had multimodal histograms". To overcome the local minima, authors have used a fuzzy measure to assess the similarity between grey levels.

**Anita Sahoo and Dr Manu Pratap Singh (2018). This** scheme has two phases, the pixels corrupted with impulse noise are detected using mathematical morphology tools in the first phase, and the degree of noisiness is labeled in the second phase by using the fuzzy membership function. A better restoration performance and the capability of preserving color and image details can be achieved using this scheme.

## III. RESEARCH METHODOLOGY

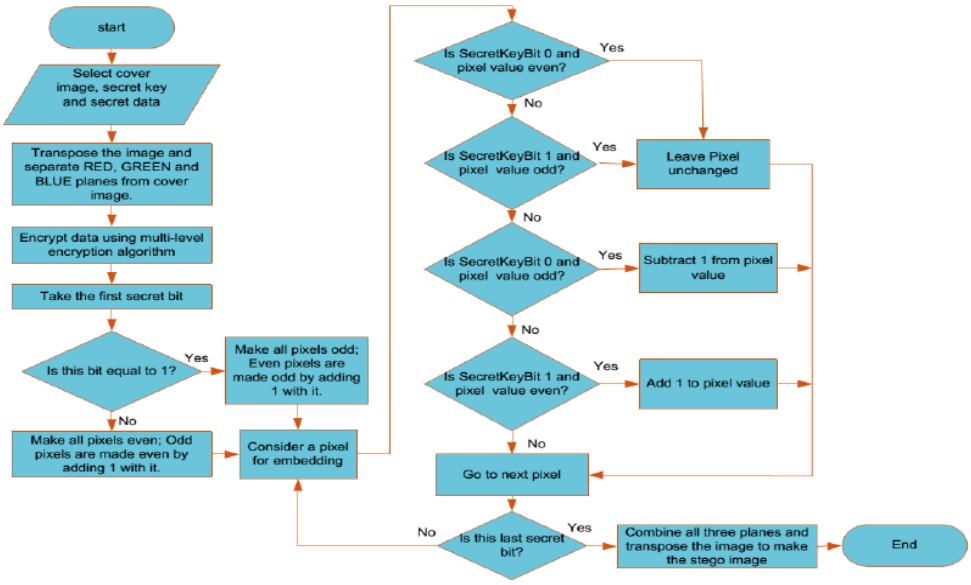
### Sequential Encoding

That is the type of encoding where data is hidden in an image based on some fixed pattern that needs to be described. The decoding process should include the same pattern to get the hidden message. The pattern is the sequence of color channels of each pixel chosen to hide the data of grey scale converted "hide to image." A channel of each pixel is selected to replace the grey value of that channel with the grey value of greyscale "hide to image." Furthermore, the grey value of the respective replaced channel will be stored for future decoding processes.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

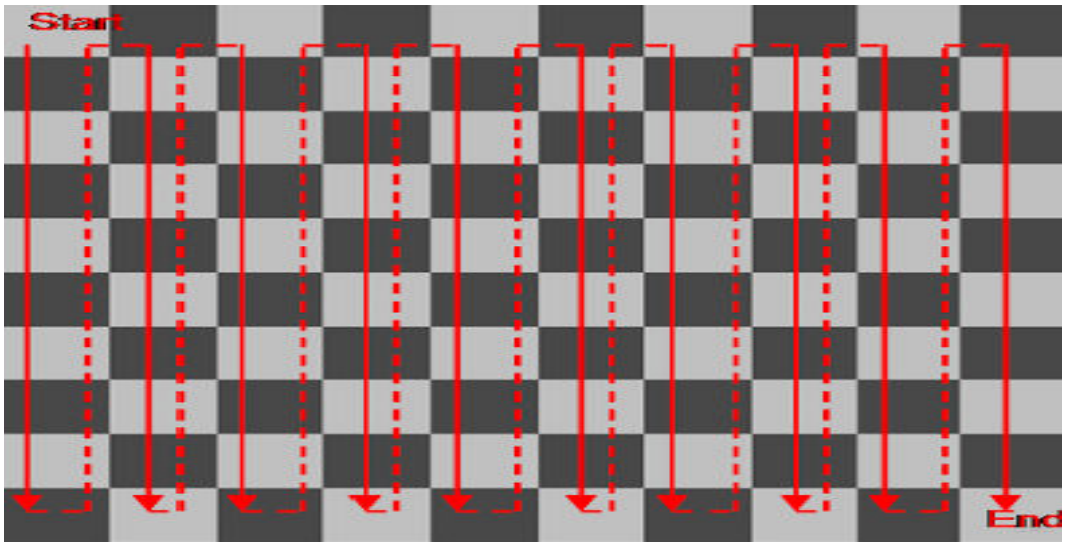
|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107007 |




*Flowchart of Data Hiding*

Let the pattern be RGBBGRRGBBGR. Alternatively, we are using the RGB pattern and reversing it in the next attempt. So here, in this pattern, we can say that the RED channel of the first pixel will be used to hide the grey value of the greyscale image (the grey value of the hide-to-image will replace the red channel grey value of the first pixel). Similarly, the GREEN channel of the second pixel and the BLUE channel of the third pixel will be used as before, and the pattern will follow according to above mentioned. Sequential encoding stores every message using this pattern, is encoded from the Top Left pixel, and is coded from Top to Bottom, Left to Right.




*Sequential Encoding*

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107007 |

## IV. RESULTS AND DISCUSSION

1. **Presentation of Results:** Present the results obtained from the experiments to evaluate the proposed technique. They may include quantitative measurements such as embedding capacity, perceptual quality, and robustness against attacks. Graphs, tables, or visual representations can effectively convey the findings.
2. **Comparison with Objectives:** Compare the obtained results with the initially defined research objectives. Assess whether the proposed technique achieves the desired goals, such as enhanced data hiding capacity, improved imperceptibility, or resistance against common attacks.
3. **Evaluation of Performance:** Analyze the performance of the proposed technique in terms of its effectiveness in concealing data securely within the LSBs of the image pixels. Discuss the achieved embedding capacity and whether it meets the requirements of practical applications. Evaluate the carrier images' perceptual quality and assess the confidential data's visual imperceptibility.
4. **Robustness Analysis:** Evaluate the robustness of the technique against various attacks, such as compression, filtering, or cropping. Assess how well the hidden data survives these operations and remains recoverable. Discuss the limitations, if any, observed during the robustness analysis.
5. **Comparative Analysis:** Compare the performance of the proposed technique with existing LSB-based steganography methods and other state-of-the-art techniques. Assess the proposed approach's advantages, limitations, and uniqueness in terms of its capacity, imperceptibility, and robustness. Highlight any significant improvements or advancements achieved.
6. **Discussion of Findings:** Interpret the obtained results and discuss their implications within the context of the research objectives and the broader field of data security and steganography. Address any unexpected or interesting observations and provide explanations or hypotheses for these findings.

## V. CONCLUSION

Stegano-graphy is an exceedingly amazing system that enable individuals to ensure and shroud correspondence. Using cryptography, will give you extra security. Stegano-graphical innovation is exceptionally easy to utilize and to a great degree, hard to recognize. As of late, steganography is the subject of numerous talks identified with its maltreatment, particularly in psychological oppressor exercises.

In previous years, steganography has been the subject of numerous discourses identified with its maltreatment, particularly in fear-based oppressor exercises. So numerous legitimate experts are developing worry about the utilization of steganography to share unlawful material by means of media records on sites. Steganalysis and a lot more youthful control of steganography. Today there are distinctive segno techniques by which we effectively recognize and avoid such criminal exercises.
Then again, there are numerous points of interest in utilizing steganography in a lawful setting, for example, advanced watermarking to decide responsibility for or more secure techniques for putting away critical and secret data..

## VI. FUTURE WORK

The future work of the data security hiding technique using image steganography with LSB can include several areas of research and development to enhance its effectiveness further and address potential limitations. Some potential future work areas are as follows:

1. **Robustness against steganalysis techniques:** As steganalysis techniques advance, improving the robustness of the LSB steganography technique against detection becomes crucial. Future work can focus on developing countermeasures and strategies to withstand various steganalysis algorithms, ensuring that the confidential data remains undetectable.
2. **Capacity and efficiency improvements:** The capacity to hide data within the LSB of image pixels is limited by the number of available LSBs. Future work can explore techniques to increase the data capacity without significantly impacting the image quality. Additionally, efforts can be made to improve embedding and extracting data efficiency, reducing the computational overhead.
3. **Security enhancements**: While the LSB technique provides a certain level of data security, further improvements can be made to enhance its cryptographic strength. Future work can explore the integration of advanced encryption algorithms or cryptographic techniques to ensure more robust protection of confidential data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107007 |

**4. Multi-dimensional steganography:** The LSB technique currently focuses on embedding data within a single image. Future work can investigate multi-dimensional steganography techniques, where data is hidden across multiple images or other multimedia formats, providing increased security and capacity for data hiding.

**5. Adaptive embedding techniques:** The LSB technique typically uses a fixed pattern or order to embed data into image pixels. Future work can explore adaptive embedding techniques that dynamically adjust the embedding pattern based on image characteristics or other factors, further enhancing the imperceptibility and security of confidential data.

**6. Steganography in emerging technologies:** As new technologies, that is, virtual reality, augmented reality, and 3D imaging, gain prominence, future work can investigate the application of LSB steganography in these domains. Exploring how to hide data within these immersive and complex visual environments effectively can open up new avenues for data security.

**7. Real-world implementation and evaluation:** Future work should focus on the practical implementation and evaluation of the LSB steganography technique in real-world scenarios. That includes testing its performance on various image formats, considering different network conditions, and assessing its robustness against attacks.

By addressing these areas of future work, the data security hiding technique using image steganography with LSB can continue to evolve, offering improved security, capacity, and efficiency in concealing sensitive information within digital images.

## REFERENCES

[1] Ahmed, A. M., & Day, D. D. (2004). Applications of the naturalness preserving transform to image watermarking and data hiding. *Digital Signal Processing, 14*(6), 531-549. doi: 10.1016/j.dsp.2004.08.002

[2] Alturki, F., & Mersereau, R. (2001, Apr 2001). *A novel approach for increasing security and data embedding capacity in images for data hiding applications.* Paper presented at the Information Technology: Coding and Computing, 2001. Proceedings. International Conference on.

[3] Amat, P., Puech, W., Druon, S., & Pedeboy, J. P. (2010). Lossless 3D stegano-graphy based on MST and connectivity modification. *Signal Processing: Image Communication, 25*(6), 400-412. doi: 10.1016/j.image.2010.05.002

[4] Awwad, W. F., Mansour, R. F., & Mohammed, A. A. (2012). A robust method to detect hidden data from digital images. [Report]. *Journal of Information Security, 3*(2), 91+.

[5] Babu, K. S., Raja, K. B., Kiran, K. K., Manjula Devi, T. H., Venugopal, K. R., & Patnaik, L. M. (2008, 19-21 Nov. 2008). *Authentication of secret information in image Stegano-graphy.* Paper presented at the TENCON 2008 - 2008 IEEE Region 10 Conference.

[6] Chandra, M., & Pandey, S. (2010, 1-3 Aug. 2010). *A DWT domain visible watermarking techniques for digital images.* Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On.

[7] Chang, C.-C., Chen, W.-J., & Le, T. H. N. (2010). High payload stegano-graphy mechanism using hybrid edge detector. [Report]. *Expert Systems with Applications, 37*(4), 3292+.

[8] Chen, W.-Y. (2007). Color image stegano-graphy scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. *Applied Mathematics and Computation, 185*(1), 432-448. doi: 10.1016/j.amc.2006.07.041

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

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