International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Improved LSB Based Image Steganography Using Linked Pixel Technique: A Linked-List Inspired Approach

Vibhash Dwivedi[1], Vaibhav Srivastava[2], Er. Aayush Pratap Singh[3]

[1, 2] UG student of Department of Computer Science & Engineering, Shri Ramswaroop Memorial College of Engineering and Management, Lucknow.

[3]Assistant Professor, Department of Computer Science & Engineering, Shri Ramswaroop Memorial College of Engineering and Management, Lucknow

Abstract - ***Image steganography is the art of hiding data into images. Secret data such as messages, audio, images can be hidden inside the cover image. This is mainly achieved by hiding the data into the LSB (Least Significant Bit) of the image pixels. To improve the security of steganography, this paper introduces LPS (Least Significant Bit Plane Steganography), a novel approach inspired by linked lists, which diverges from traditional LSB techniques. LPS utilizes the LSB of each channel to encode both data and pointers to subsequent pixels, creating a linked-list-like structure within the image.***

Keywords: *Steganography, LSB, Information hiding, Linked Pixel Steganography*

I. INTRODUCTION

STEGANOGRAPHY comes from the Greek Words: STEGANOS – "Covered", GRAPHIE – "Writing", which basically means to hide data and information into a plain sight. Steganography refers to the art and science of covert communication, where information is hidden within various carrier mediums to obscure its existence. Steganography is a way of concealing a file, message, image, audio, or video into another file of the same or different category in a way such that the hidden data cannot be easily recognized by anybody other than the sender and receiver. While cryptography deals with the security of the message, steganography deals with the method of hiding the data in a way that doesn't change the original file data at a very large cost but yet implements the secret data into it. Imperceptibility is an important feature in steganography also called transparency or anti-detection performance. The imperceptibility of steganography can be improved by enhancing the method of steganography or improving the matching relationship between secret information and carrier. Steganography complements the deficiency of concealment of the encryption. This paper provides an alternative to a well-known steganographic method.

LSB based steganography has been there for a while in which the secret data is encrypted in the LSB of a pixel in sequential order. The problem of sequential ordering of this secret data is that once the user is handed over a stego image he/she may be able to find the secret data if not encrypted with a well-known encryption algorithm. This paper tries to overcome the traditional way of implementing LSB based by adopting a more intricate approach inspired by linked lists, dispersing the hidden data across multiple pixels in a non-sequential manner. This complex arrangement enhances security and robustness by requiring traversal of the image following embedded pointers for decoding, making detection more challenging and resistant to steganalysis techniques.

II. LSB SUBSTITUTION TECHNIQUE

LSB substitution is one of the spatial domain techniques where each bit of the text or an image is substituted with the least significant bit of the original image. It is simple and easy to implement. This technique is popular because the human eye cannot easily distinguish the real image and stego image if the information change is done at least significant bit. This technique can also be extended to 2, 4 or up to 8 bits but this may cause distortion and noise in the image resulting in a lossy image. To understand better, let's consider an image as a 2D matrix of pixels. Each pixel contains some value depending upon the type and depth. Consider the most widely used modes - RGB (3x8-bit pixels true color). These values range from 0-255 (8-bit values). We can convert the message into decimal values and then into binary, by using ASCII values. Then we iterate over the pixel values one by one, after converting them to binary, we replace each least significant bit with that message bits in the sequence. To decode the message we again take the least significant bits of the pixels split them into groups of 8 and convert it back to ASCII character to get the hidden message.

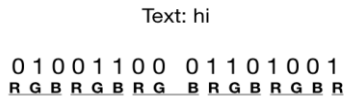

Fig. 1. Encryption of string ”hi” in pixels

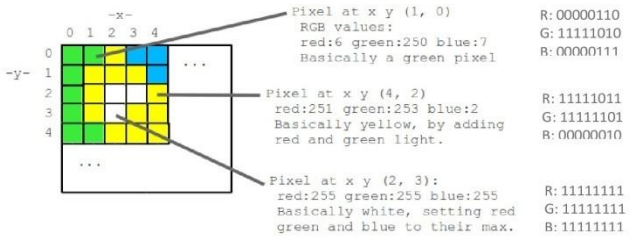

Fig. 2. RGB (3x8-bit pixel) mode

III. PROPOSED WORK

LPS diverges from traditional LSB steganography by adopting a more intricate approach inspired by linked lists. Instead of sequentially embedding data, LPS utilizes the LSB of each channel to encode both data and pointers to subsequent pixels with additional data fragments. This creates a linked-list-like structure within the image, dispersing hidden data across multiple pixels in a non-sequential manner. Just like linked lists, every “block” contains data parts and a pointer to the next pixel holding the rest of the data. Each pixel of an image is composed of at least three channels (R, G, B). LPS uses the LSB of each channel for different usage.

Since LPS uses LSB, several pixels are needed to store the binary representation of the coordinate of the next pixel. That’s why LPS uses blocks of consecutive pixels. The block size is calculated from the image size in pixel, it’s the number of bits needed to store the highest value (height or width). Data is then split into chunks of the same size and padding is added at the end if needed. Block positions are randomly selected.

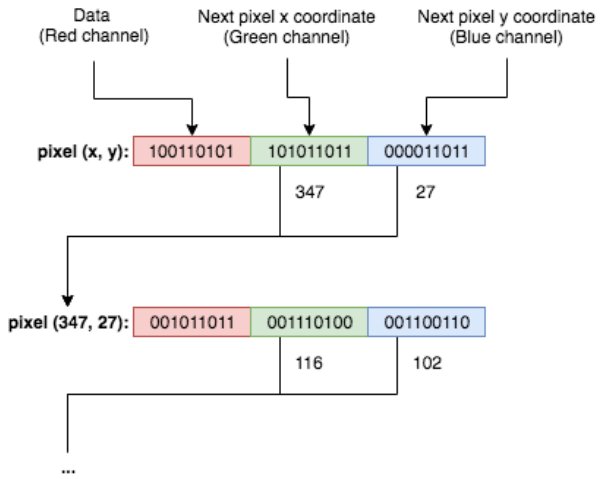

Fig. 3. Linked Pixel Steganography

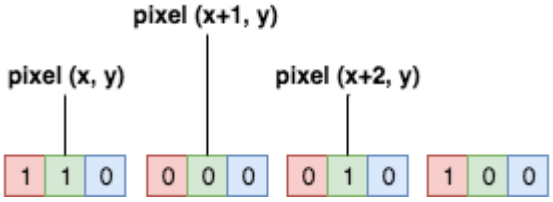

Fig. 4. LPS Blocks

To recover data correctly, one needs to know the coordinates of the starting pixel and calculate the block size. From then, every next pixel can be recovered by reading blocks, until the coordinates of the next pixel are (0, 0). Like in linked lists, the last element has a NULL pointer, which in this case is represented with coordinate values of 0.

IV. ENCODING AND DECODING

The encoding algorithm takes as input the data to be hidden (e.g., a secret message), the cover image in which the data will be embedded, and optionally, starting coordinates for the embedding process. The algorithm first partitions the input data into blocks or chunks. For each block of data: It determines the appropriate starting pixel for embedding (either based on user input or through a random selection process). It embeds the data and encodes pointers to subsequent pixels with additional data fragments using the LSB of each color channel in the pixel. The algorithm traverses the image, following the embedded pointers, and continues embedding data in a non-sequential manner until all data blocks are encoded. The output of the encoding algorithm is the stego image, which contains the hidden data embedded in a linked-list-like structure across multiple pixels.

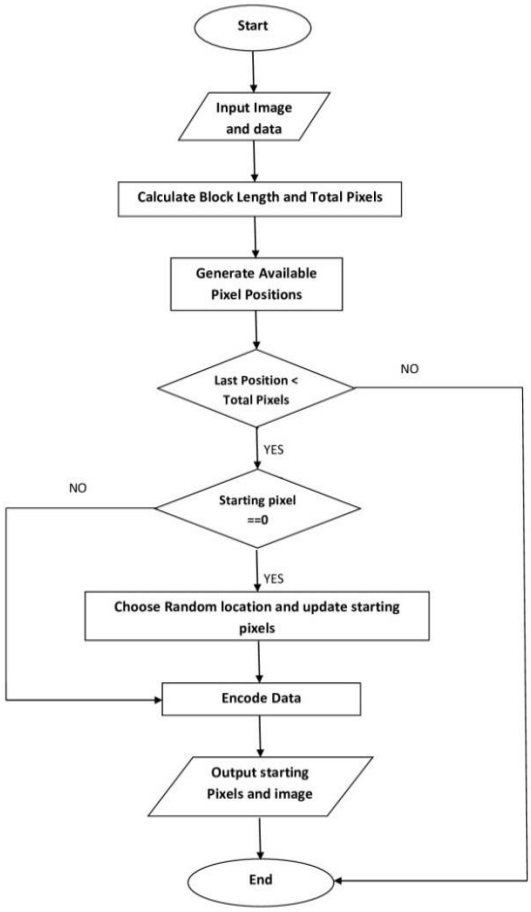

Fig. 5. Encoding Process

The decoding algorithm takes as input the stego image containing the hidden data and optionally, starting coordinates for the decoding process. The algorithm begins by traversing the stego image, starting from the specified or default coordinates. It extracts data and follows the embedded pointers encoded in the LSB of each color channel to retrieve subsequent data fragments. The algorithm continues traversing the image until all data fragments are decoded, following the linked-list-like structure established during encoding. The output of the decoding algorithm is the extracted hidden data, which may correspond to a secret message or other concealed information.

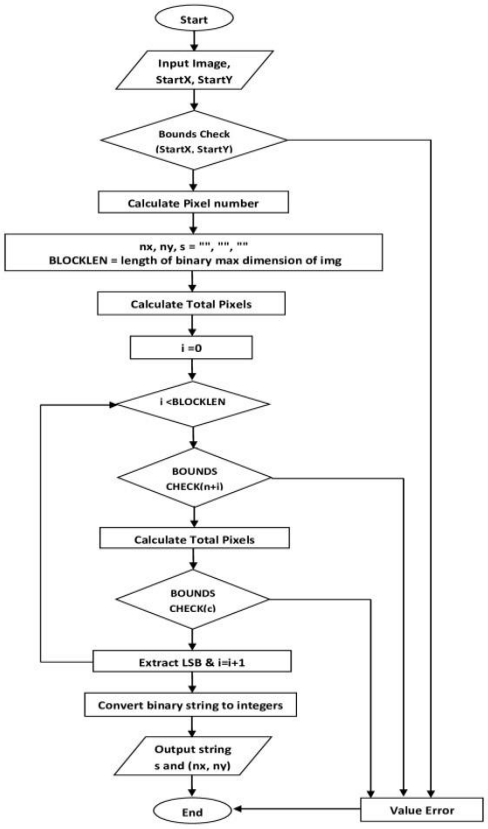

Fig. 6. Decoding Process

V. V. RESULT AND ANALYSIS

LPS on regular PNG image with Alpha channel:
Message hidden:
"*Microsoft se plie à l'écriture inclusive à sa façon. La dernière mise à jour de son logiciel de traitement de texte Word, réservée aux abonnés Office, comprend dans ses paramètres de grammaire et de style une option de «langage inclusif». Une telle fonctionnalité «cible le langage genré à même d'exclure, de rejeter ou de stéréotyper», est-il indiqué sur le site de l'entreprise. Pour rappel, l'écriture inclusive consiste à inclure le féminin, entrecoupé de points, dans les noms, comme dans «mes ami·e·s» ou «les candidat·e·s à la présidentielle, pour le rendre «visible» et prôner des règles grammaticales plus neutres. L'expression est le fruit d'une réflexion amorcée il y a une vingtaine d'années, autour de l'idée de neutralité dans l'écriture. Longtemps cantonnée aux mouvements féministes, cette graphie s'impose désormais dans le débat public. Le logiciel Word, lui, ne propose pas l'utilisation du point milieu. Il remplacera, par exemple, le terme «les experts» par «les experts et les expertes»*"

Fig. 7. Original Image

Fig. 8. Stego Image

Like with LSB steganography, there is no visual difference.

LSB Analysis:

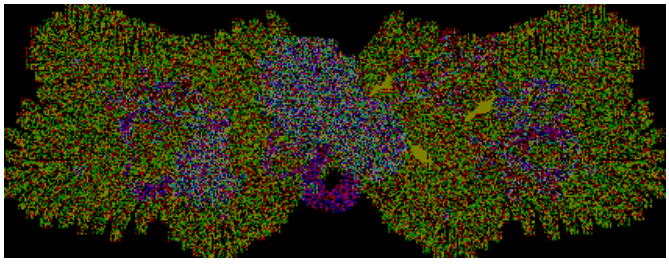

Fig. 9. LSB Analysis of original image

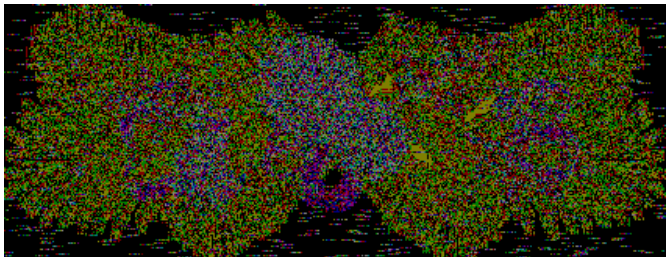

Fig. 10. LSB Analysis of Stego image

We can clearly see stripes in homogenous areas, revealing the presence of hidden data. But in the center of the image it is very difficult to tell if something is hiding in the LSB. Unlike the classical LSB steganography technique, the randomness of the location where data is hidden makes steganalysis more difficult if the image is chosen correctly

Table 1: Comparison between LSB and LPS

Feature	LSB	LPS
Embedding	Sequential	Linked-List Inspired
Efficiency	Less	More
Detection	Easier	Challenging
Robustness	Less	More
Security	Limited	Enhanced
Alternation Imapct	Significant	Partial

VI. CONCLUSION

In this paper, a new LSB steganography method is proposed which overcomes the security limitation of the existing LSB steganographic technique. LPS represents a significant advancement in the field of image steganography, introducing a novel approach inspired by the organizational principles of linked lists. By leveraging the LSB of each color channel to encode both data and pointers, LPS fundamentally transforms the embedding process, dispersing hidden information across multiple pixels in a non-sequential manner. This departure from traditional LSB methods results in a more complex and interconnected embedding scheme, reminiscent of the structure found in linked lists. As a consequence, LPS offers enhanced security and robustness in concealing sensitive information within digital images.

The adoption of LPS introduces several key advantages over traditional LSB steganography techniques. By dispersing data across multiple pixels and encoding pointers to subsequent data fragments, LPS significantly enhances resistance against detection and extraction. This distributed approach makes it increasingly challenging for adversaries to detect and decipher hidden information, thereby bolstering the security of covert communication channels. Furthermore, the utilization of the LSB of each color channel for both data and pointer encoding ensures a more efficient use of available embedding capacity, allowing for greater amounts of information to be concealed within images without sacrificing security.

Because LPS uses only 1 channel to store the actual data, it takes at least three times more storage space than classical LSB.

VII. FUTURE DIRECTION

In future directions, this paper could delve into several avenues to advance LPS (Linked Pixel Steganography) and its applications further. Firstly, exploring enhanced security measures, such as integrating encryption techniques, could significantly bolster the security of hidden data, rendering it more resilient against unauthorized access and detection. Secondly, research could focus on evaluating the robustness of LPS against advanced steganalysis techniques, including statistical analysis and machine learning-based detection methods, to ensure its effectiveness in real-world scenarios. Additionally, developing adaptive embedding strategies that dynamically adjust the embedding process based on image characteristics and security requirements could optimize the trade-off between embedding capacity and detection resistance. Furthermore, investigating the applicability of LPS in multimedia content beyond images, such as audio and video

files, could expand its utility in diverse domains. Lastly, real-world implementations of LPS in practical settings, such as secure messaging applications or digital watermarking systems, would provide valuable insights into its performance, usability, and potential limitations, paving the way for its widespread adoption in various applications requiring secure communication and data concealment.

VIII. REFERENCES

[1] M. Pavani1, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467.

[2] D. C. Wu and W. H. Tsai., "A steganographic method for images by pixelvalue differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, p. 16131626, June 2003.

[3] S. Kurane, H. Harke, and S. Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH," Natl. Conf. "Internet Things Towar. a Smart Futur. "Recent Trends Electron. Commun., 2016

[4] M. H. and M. Hussain, "A Survey of Image Steganography Techniques," Int. J. Adv. Sci. Technol., vol. 54, pp. 113–124, 2013.

[5] N. Hamid and R. B. Ahmad, "Image Steganography Techniques: An Overview," no. 6, pp. 168–187, 2012.

[6] J. Kour and D. Verma, "Steganography Techniques –A Review Paper," Int. J. Emerg. Res. Manag. &Technology, vol.9359, no. 35, pp. 2278– 9359, 2014.

[7] A. MILLER, "LEAST SIGNIFICANT BIT EMBEDDINGS: IMPLEMENTATION AND DETECTION," 2012. [Online]. Available: http://www.aaronmiller.in/thesis/.

[8] E. C. Vidyasagar M. Potdar, "Grey Level Modification Steganography for Secret Communication," 2004. [Online].Available:https://www.researchgate.net/publication/4137627_Grey_level_modification_steganography_for_secret_communication.

[9] H.-W. T. and H.-S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," 2013. [Online].Available:http://www.hindawi.com/journals/jam/2013/189706/.

[10] C. A. Petr Klapetek, David Nečas, "Wavelet Transform," 2016. [Online]. Available: http://gwyddion.net/documentation/user-guide-en/wavelettransform.html.

[11] Information Hiding using Audio Steganography – A Survey, Jayaram P, Ranganatha HR, Anupama H S

[12] https://medium.com/@achyuta.katta/audio-steganography-using-phase-encoding-d13f100380f2#:~:text=in%20our%20implementation.-,Phase%20Coding%20Technique,data%20portion%20of%20the%20audio.&text=The%20data%20part%20is%20segmented,is%20applied%20on%20each%20chunk

[13] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9105752/

[14] https://www.hindawi.com/journals/scn/2023/6295486/fig1/

[15] Naharuddin, A.; Wibawa, A.D.; Sumpeno, S. A high capacity and imperceptible text steganography using binary digit mapping on ASCII characters. In Proceedings of the 2018 International Seminar on Intelligent Technology and Its Applications (ISITIA), Bali, Indonesia, 30–31 August 2018; pp. 287–292.

[16] Li, Y.; Zhang, J.; Yang, Z.; Zhang, R. Topic-aware neural linguistic steganography based on knowledge graphs. *ACM/IMS Trans. Data Sci.* **2021**, *2*, 1–13.

[17] Wu, N.; Yang, Z.; Yang, Y.; Li, L.; Shang, P.; Ma, W.; Liu, Z. STBS-Stega: Coverless text steganography based on state transition-binary sequence. *Int. J. Distrib. Sens. Netw.* **2020**,

[18] Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32-44.

[19] Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscaleimages. Proceedings of the 5th International Workshop on Information Hiding, 340-354.

[20] Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems. Proceedings of Information Hiding, 61-76.

[21] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336.