The Image Steganography Utilizing LSB Substitution Technique Along with Neighbouring Pixel Value Distinguishing

Akshitha S [1], Ananya Desai S[2], Aishwarya MS [3], Sahana S U [4], Sridhar R[5]
[1,2,3,4]*Students, Department of Information Science and Engineering, Global Academy of Technology, Bangalore*
[5]*Assistant Professor, Department of Information Science and Engineering, Global Academy of Technology, Bangalore*

Abstract **- Data concealment has always been an important requirement in human history, whether on a global or personal level. The types and methods of data to be hidden are becoming increasingly diverse as digital technologies advance. Any data sent over transmission channels can be hidden. It's science of hidden confidential news inside a publicly visible news.**
Steganography is thought of as an additional layer of security, but it cannot be regarded as an alternative to or a replacement for cryptography. Secure communication can be protected via image steganography, which involves hiding hidden messages in the cover image. The main issue with steganography is concealing a lot of secret information without alerting the attacker. Steganography is a method of concealing confidential or delicate information within something that seems to be ordinary image. Steganography is the practise of disguising a picture such that it appears to be a regular image or other file. This study describes a brand-new colour picture message concealing algorithm. Bit-plane slicing and dual XOR operation work as the foundation of the created method. The proposed approach defines the maximum number of hidden bits in a set of pixels by considering the power of each visual plane to accept distortion and the gap in value between two adjacent pixels. Each plane is divided into a few different 3X3 components blocks. The concept of eight-neighbouring pixels is utilized in the ways to create octagonal sets of components in one block, so that the method can use every edge pixel in every conceivable direction. XOR coding technique is also utilized before the embedding process.

Index Terms **-secret picture; cover picture; pixel value differentiating; stegno picture; least significant bit.**

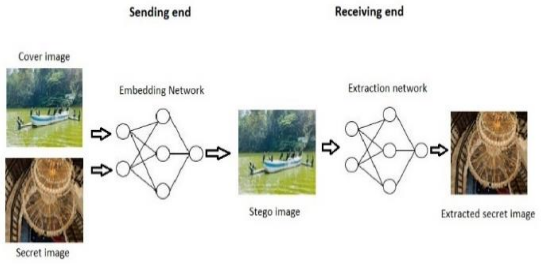
I.INTRODUCTION

Utilizing cutting-edge computer performance and Internet technology, the majority of significant information is now transmitted over the Internet. Because it is so simple to use and offers so many benefits, the internet makes information exchange convenient. Yet, in fact the Internet is an open platform, bad attackers may trick and manipulate crucial data.
By taking use of the limitations of the human eye when examining picture files, steganography exchanges data. Steganography is a method to clarify restricted details by including it in ordinary non-secret file or communication; the data is subsequently taken out at the intended location. Steganography can be utilizing in addition to encryption and also conceal or safeguard data. Steganography, or embedding a news in a cover item to hide it, has drawn a lot of interest from the general public.
Secret messages can now be conveyed by concealing them in a picture or text so that only the sender and the recipient can read or see them. Steganography is the process of both concealing and revealing data. As it conceals the secret message, the image that hides the data in steganography is known as the cover image. After the data has been hidden, the image is known as the stego-image. For encoding information on the cover photo, LSB insertion is a highly well-liked and often used technique in steganography. As stated to the LSB embedding approach, data can be concealed in the LSBs of the cover file so that it cannot be seen with the unaided eye. It is a solid space method.
When deciding how many secret bits to insert, the pixel-value distinguishing system compares the values of duplet adjacent picture element in a block. In Wu

and Tasi's point of view, there are two different forms of quantization range tables.

The slightly important branch(LSB), often known as the former or appropriate bit in a double integer, it is familiar steganographic method.

With this procedure, some of the LSBs in the cover image are exchanged out for the hidden message's confidential data part.



II. LITERATURE REVIEW

Since 440 BC, steganography has been a subject of discussion. In the past, it has changed from shaving the heads of subordinates to carving a secret message with invisible inks during World War II to more modern digital steganography.

In the compression domain, a lossless concealment method is required, Wu et al recommended a reversible picture steganographic approach based on anticipating coding to insert hidden details into compression codes during the lossless image constriction.

In order to provide space for data hiding, Zeng et al gave out a lossless data hiding scheme that was based on pixel dissimilar bar graph shifting. Between a instance of pixel and its nearest in a block that has already been assigned, pixel disputes are produced. Zhaoa et al. described a resolvable truth obfuscation method on spontaneous photographs by building a multilayer histogram based on discrepancies connecting adjacent pixel pairs. An adaptive correctable information technique established by the growth of dispute enlargement was used by Lee and Chen.

In the first security layer, adaptive filtering of a cover picture is used, along with compressions using the SPIHT technique and encryption using the AES algorithm.

One of the most straightforward and established techniques is data concealment via LSB. Data is concealed using this method in the pixels' least significant bits (LSB). Notwithstanding how significant it is, some visual alterations could damage the encoded data.

III. LITERATURE SUMMARY

1: Summary of Literature Survey

Sl No	Author Names	Year of Publication	Methodology	Pros	Cons
[1]	Ashraf A. M. Khalaf And Osama Fouad Abdel Wahab	2021	Encrypted by RSA (Rivert Shamir Alderman) cryptography to enhance security plaintext compressed bu Huffman coding algorithm	More effective visual quality and storage capacity and it has high security.	It is suitable only for audio-based steganography. A complete, colourful picture cannot be inserted into another, smaller picture.
[2]	Krishna Chaitanya Nunna and Ramakalavathi Marapareddy	2020	LSB and the AES algorithm are used for visual cryptography to embed data.	Two degrees of security, no interference from other parties, a high level of communication integrity, and message confidentiality.	To make the data safer, hide it in the noisy image when transmitting.
[3]	Abhishek Das	2021	Use of multiple prep and reveal networks in implementation for multiple audio signal steganography. Encoders, Decoders and Reveal networks are used.	Hiding duo confidential pictures over a one cover image.	It is suitable only for image-based steganography. Increasing the number of confidential pictures with bottom misplacement cannot be done
[4]	Nandhini Subramanian	2021	Precising module and Company Owned Company Operated (COCO) dataset is used	Each element of the cover image incorporates a piece of the hidden image, demonstrating the concealing ability's effectiveness.	The region where the secret image is concealed cannot be expanded without altering the cover images.
[5]	Supriyadi Rustad	2021	Inverted LSB substation method .	Increasing the imperceptibility.	Addition of parameters to determine patters and to do

					optimization using artificial intelligence methods.
[6]	Manashee Kalita	2019	Adjacent pixel value differencing and LSB substation technique	The stego image's robustness, embedding capability, and quality are all maintained.	It is also possible to provide an effective mechanism for choosing cover images.
[7]	mohammed aloraini	2022	Discrete cosine transformation coefficient	Jpeg steganography in which gaussian model for the cover coefficients and also the hidden message elements.	Improve the performance of the existing JPEG steganography algorithms.
[8]	kevin zhang	2019	Encoder that takes a cover image and a data tensor produces a steganography image. Decoder to recover the data.	A flexible new approach to image stegnography which supports different sized cover images and arbitrary binary data.	Video steganography is not implemented. Image quality is less.
[9]	jonathan lwowski	2019	Deep digital steganography purification, Autoencoder Architecture, GAN training, Image stegnography.		

[10]	shrilekha mukherjee	2018	The idea of middle position and its associated values are used in the mid position value technique.	promotes the carrier image's strong embedding capacity.	Longer private data bits can be added to the work to fit inside the carrier pants.
[11]	NIR Yassin	2021	Least significant bit, Discrete Fourier transformation, Discrete wavelet transformation	Good performance for high embedding rates.	Using different transformation domains.
[12]	Alaknanda Patil	2021	Least significant bit encoding, bit plane inversion algorithm, stegnography with secret password	Higher security through secret key stegnography.	Apply stegnography techniques to conceal audio in video.
[13]	Nouran Mohamed Selim	2021	Generic algorithm, peak signal to noise ratio, least significant bit algorithm.	Higher values of PSNR, selecting best frames and pixel to embed small visual distortion.	Using stegnography to embed videos rather than just images.
[14]	Noor Alhuda F	2021	Leas at significant bit algorithm, pixel value differential, Huffman coding, random map function.	Enhanced security and payload values to easy determination of components. Good PSNR value achieved.	Pixel allocation with high complexities, pixel allocation with bits standing.
[15]	Shumeet Baluja	2020	Using auto-encoding networks and cryptography concealment methods, compress images.	The host image and container image both shared a striking similarity, and it was simple to identify the rebuilt images at the hidden images.	For better security double layer security can be introduced.

IV.METHODOLOGY

With the help of one cover image, we want to accomplish multi-image steganography and conceal three or more images. The hidden photos must be retrievable with the least amount of loss possible. The cover image that is encoded must resemble the original cover image.

The proposed technique for adaptive colour image steganography. It makes use of the principle of differentiating pixel values that are close to each other. The method embeds variable secret bits in accordance with each layer's tolerance capacity. As stated to a study (The Das and Mandal 2012), the influence of the green, red and blue layers on the creation of the colour is 59%, 30% and 11% respectively. And based on their ability to endure distortion, this equation determines the maximum sum of bits that may be accommodated in each plane. The concealed photo is combined with the cover image using the LSB approach.

V.CONCLUSION

In conclusion, image steganography is a well-liked method for concealing secret information in digital photographs. By using a block structure of 3 x 3 pixels, the provides use every corner pixel across every direction. The proposed methods are divided into three phases: (1) XOR data encoding; (2) embedding of the encoded bits utilising PVD and LSB substitution; and (3) extraction. Initial, the PVD topic was utilized to fixed on the additional focus value hidden in the pair

of pixels. The length of the letter was furthermore integrated into the stego image so that it could be effortlessly recover with the encoded confidential bits. To manage the number of bits to be encrypted, the disparity linking adjacent pixels and the volume of every colour in the human body vision platform to permit perversion were examined. The theory's degree of privacy is increased by the XOR encoding, the arbitrarily choice the picture element and the planes. The hidden details were extracted by way of the stego image during the removal stage.

The decision of the encrypting ultimately relies on the specific cloud applications and the acceptable degree of safety. LSB modification and image intensity variation strategies may be utilized to send user data securely and promptly with the suitable design and regulatory precautions.

REFERENCE

[1] Ahani, S., and S. Ghaemmaghami. 2015. Colour image steganography method based on sparse representation. IET Image Processing 9 (6):496–505. doi:10.1049/iet-ipr.2014.0351.

[2] Cancelli, G., and M. Barni. 2009. Mpsteg-color: Data hiding through redundant basis decomposition. IEEE Transactions on Information Forensics and Security 4 (3):346–58. doi:10.1109/TIFS.2009.2024028.

[3] Dande, S. C., S. S. Agrawal, and S. R. Hirekhan. 2016. Implementation of colour image steganography using LSB and edge detection technique: A lab view approach. In Proceeding of 2016 International Conference on Communication and Signal Processing (ICCSP), IEEE, 1466–1470.

[4] Fridrich, J., M. Goljan, and R. Du. 2001. Reliable detection of LSB steganography in color and grayscale images. Multimedia and Security 3657:27–30.

[5] Garcia-Hernandez, J. J., C. Feregrino-Uribe, R. Cumplido, and C. Reta. 2011. On the implementation of a hardware architecture for an audio data hiding system. Journal of Signal Processing Systems 64 (3):457–68. doi:10.1007/s11265-010-0503-8.

[6] Hussain, M., A. Wahid Abdul Wahab, N. Javed, and K.-H. Jung. 2016. Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Technical Review 35 (1): 53–63. DOI: org/10.1080/02564602.2016.1244496.

[7] Johnson, N. F., and S. Jajodia. 1998. Exploring steganography: Seeing the unseen. Computer Magazine 2 (2):26–34. doi:10.1109/MC.1998.4655281.

[8] Jung, K.-H., and K.-Y. Yoo. 2014. Three-directional data hiding method for digital images. Cryptologic 38 (2):178–91. doi:10.1080/01611194.2014.885817.

[9] Kalita, M., and T. Tuithung. 2016. A novel steganographic method using 8-neighboring PVD (8NPVD) and LSB substitution. In Proceedings of International Conference on Systems, Signals and Image Processing. Vol. 1, IWSSIP, IEEE, 15.

[10] Khodaei, M., and K. Faez. 2012. New adaptive steganographic method using least-significant bit substitution and pixel-value differencing. IET Image Processing 6 (6):677–86. doi: 10.1049/iet-ipr.2011.0059.

[11] Kumar, V., G. G. Singh, A. Bansal, and S. K. Muttoo. 2014. Data hiding method based on inter-block difference in eight queens' solutions and LSB substitution. International Journal of Information Security and Privacy (IJISP) 8 (2):55–68.

[12] Kutter, M., and F. A. P. Petitcolas. 1999. A fair benchmark for image watermarking systems. Electronic Imaging 3657:25–7. Lee, C.-F., and H.-L. Chen. 2010. A novel data hiding scheme based on modulus function. Journal of Systems and Software 83 (5):832–43. doi:10.1016/j.jss.2009.12.018.

[13] Luo, W., F. Huang, and J. Huang. 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensics and Security 5 (2):201–14.

[14] Mandal, J. K., and D. Das. 2012. Color image steganography based on pixel value differencing in spatial domain. International Journal of Information Sciences and Techniques 2 (4):83–93.

[15] Mielikainen, J. 2006. LSB matching revisited. IEEE Signal Processing Letters 13 (5):285–7. doi:10.1109/LSP.2006.870357.

[16] Pradhan, A., K. R. Sekhar, and G. Swain. 2016. Digital image steganography based on seven-way pixel value differencing. Indian Journal of Science and Technology 9 (37):1–11. doi: 10.17485/ijst/2016/v9i37/88557.

[17] Pradhan, A., A. K. Sahu, G. Swain, and K. R. Sekhar. 2016. Performance evaluation parameters of image steganography techniques. IEEE international conference on research advances in integrated navigation systems, Bangalore, 1–8. doi:10.1109/ RAINS.2016.7764399.

[18] J. Balle, D. Minnen, S. Singh, S. J. Hwang, and N. Johnston, "Variational image compression with a scale hyperprior," arXiv: 1802.01436, 2018.
[19] O. Rippel and L. Bourdev, "Real-time adaptive image compression," in Proc. Int. Conf. Mach. Learn., 2017, pp. 2922–2930.
[20] L. Theis, W. Shi, A. Cunningham, and F. Huszar, "Lossy image compression with compressive autoencoders," in Proc. Int. Conf. Learn. Representations, 2017.
[21] J. Balle, V. Laparra, and E. P. Simoncelli, "End-to-end optimized image compression," in Proc. Int. Conf. Learn. Representations, Apr. 2017. [Online]. Available: https://arxiv.org/abs/1611.01704
[22] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P. Manzagol, "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion," J. Mach. Learn. Res., vol. 11, no. Dec, pp. 3371–3408, 2010.
[23] D. Kingma and J. Ba, "Adam: A method for stochastic optimization," in Proc. 3rd Int. Conf. Learn. Representations, 201
[24] Faheem Ahmed H, Rizwan U. Embedding multiple images in an image using bit plane slicing. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(1).