RESEARCH ARTICLE OPEN ACCESS

A Review on Recent Advancements of Image Steganography

Rahul Kumar M.Tech. Scholar
Computer Science & Engineering Rabindranath TagoreUniversity Raisen, Madhya Pradesh - India

Devendra Singh Rathore Asst. Professor
Computer Science & Engineering Rabindranath Tagore University Raisen, Madhya Pradesh - India

Mukesh Kumar Asst. Professor
Computer Science & Engineering Rabindranath Tagore University Raisen, Madhya Pradesh - India

ABSTRACT
As the name proposes, Image Steganography alludes to the most common way of concealing information inside an image record. The image chose for this design is known as the cover image and the image got after steganography is known as the stego image. An image is addressed as a N*M (in the event of greyscale images) or N*M*3 (if there should be an occurrence of shading images) network in memory, with every passage addressing the power worth of a pixel. In image steganography, a message is inserted into an image by adjusting the upsides of certain pixels, which are picked by an encryption calculation. The beneficiary of the image should know about a similar calculation to know which pixels the individual should choose to remove the message. The intension of this paper is to review various advancements which have been done in the field of image steganography.
Keywords: **-** Image Steganography, Advanced Encryption Standard, Least Significant Bit, K-LSB, Data Hiding, Region Detection Methods.

I. INTRODUCTION

The word Steganography has been achieved from two Greek words-'stegos' signifying 'to cover' and 'grayfia', signifying 'composing', subsequently meaning 'covered composition', or 'stowed away composition'. Steganography is a technique for concealing privileged information, by inserting it into a sound, video, image, or text record. It is one of the techniques utilized to shield mysterious or delicate information from pernicious assaults. Cryptography and steganography are the two strategies used to stow away or ensure privileged information. In any case, they vary in the regard that cryptography makes the information ambiguous, or conceals the importance of the information, while steganography conceals the presence of the information. In layman's terms, cryptography is like composing a letter in a mysterious language: individuals can understand it, however will not get what it implies. Nonetheless, the presence of a (most likely confidential) message would be clear to any individual who sees the letter, and assuming that somebody either knows or sorts out your mysterious language, then, at that point, your message can undoubtedly be perused [1]. Assuming a client to utilize steganography in a similar circumstance then it would conceal the letter inside a couple of socks that you would gift the planned beneficiary of the letter. To the people who don't be aware of the message, it

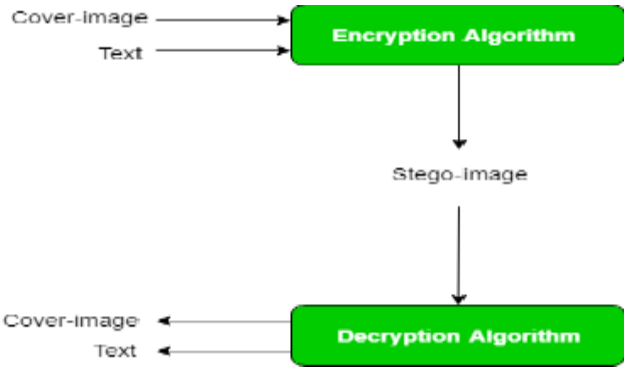

Fig. 1. Image Steganography [1]

Discovery of the message inside the cover image is finished by the course of steganalysis. This should be possible through examination with the cover image, histogram plotting, or commotion discovery. While endeavors are being put resources into growing new calculations with a more noteworthy level of invulnerability against such assaults, endeavors are likewise being dedicated towards working on existing calculations for steganalysis, to recognize the trading of privileged intel between fear based oppressors or criminal components. The most well-known type of steganography utilized today conceals records inside image documents on a PC. The secret record is encoded at

all huge pieces of the qualities encoding the shade of every pixel of the image. Changing the most un-critical pieces changes the presence of the image somewhat, and isn't noticeable to the unaided eye. Assuming that the change is distinguishable by any means, the shadings will simply look somewhat off as though the image was taken from a bad quality camera on in helpless light. A comparative interaction can be utilized to disguise information in strong records since the human ear is restricted in its capacity to separate unique, comparable frequencies (and in the scope of frequencies it can distinguish) [2].

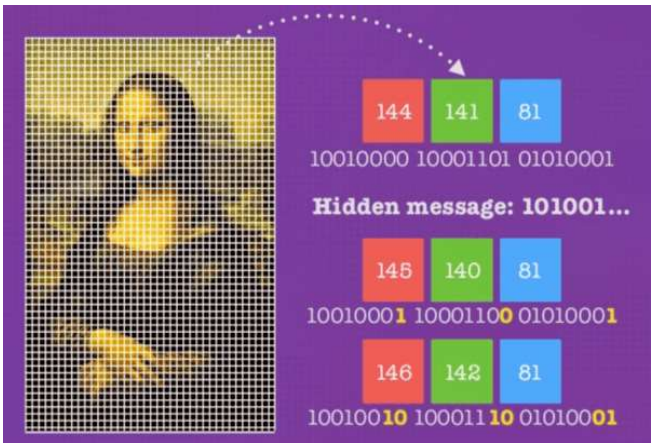

Fig. 2. Image Steganography Data Concealing [2]

II. RELATED WORKS

A. Related Works

Shivani et al. [3] et al. proposed a system which is based on zero distortion technique. Zero distortion technique is a clever methodology for performing steganography, in which computerized medium is utilized as a kind of perspective and privileged information is concealed in such a way so that there is no distortion in the cover medium. Zero distortion technique has been applied to dim just as on shading images. In shading images huge measure of information can be concealed when contrasted with dark images since shading image contains RGB groups. Benefits of utilizing images is that changes are practically intangible to human vision and drawback is stego image is ship off recipient's end so odds of assault are more. This technique is applied on text for example to conceal secret text inside cover text. Cryptography is joined with steganography to expand security. For encryption reason Indexed Based Chaotic Sequence has been utilized. Srilekha Mukherjee et al. [4] proposed a system which is based on mid position value technique. From there on, Mid Position Value (MPV) technique is executed to insert information bits from the mysterious image inside the mixed cover. Ultimately, converse Arnold change is applied on the above image. The outcomes in a descrambling activity, for example returning the ordinary direction. Hereafter the stego is produced. Every one of the test results examines the result of the full strategy. For this reason, a few quantitative and subjective benchmark examination relating to this methodology have been made. Every one of the outcomes shows that the impalpability, for example non perceptibility of restricted information is all around kept up with. Likewise the payload is high with immaterial distortion in the image quality. In the sender side, the cover image is first mixed by applying Arnold Transformation over it. A tumultuous portrayal of the cover is the resultant result.

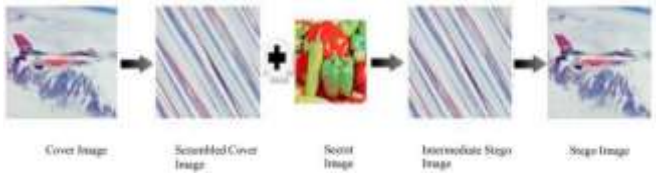

Fig. 3. Embedding Process of mid position value technique [4]

Mohammed Abbas Fadhil et al. [5] proposed a system which is based on Mapping algorithm. In this work, a clever steganography framework was introduced. The principle ventures for applying this framework are clarified. We can finish up the fundamental properties and benefits of this framework through the accompanying focuses: When the framework fabricates the FT from the pixels of the stego-image, and afterward maps these frequencies to the request for frequencies (of the alphabetic English letters). This will add one more solid property to the protection of the secret message. This activity is like the utilization of various replacement tables sequestered from everything a similar message. Since the proposed framework isn't changing the first stego-document, this implies that the framework is satisfactory for concealing any message in any one more sorts of records like (.doc, .txt, .mp3, and so forth) Simply the stego-document should have sufficient additional byte toward its finish. Jia Lui et al. [6] proposed a system which is based on Generative Adversarial Networks. With the generative models, image steganography started to converge with the field of PC vision. Conventional PC vision analysts have likewise begun to concentrate on image steganography. A blend of the exploration fields widens the spaces of image steganography. In addition, the presentation of GANs into the examination thoughts of data concealing will likewise altogether affect the improvement of other data concealing advances, for example, computerized watermarking innovation. In this paper, creators survey image steganography with GAN. First and foremost, creators give the guideline and qualities of steganography. Randa Atta et al. [7] proposed a system which is based on neutrosophic set. This paper has proposed an image steganography strategy dependent on edge EMD and neutrosophic set. In the proposed plot, the cover image is separated into blocks which are arranged into edge and non-edge blocks dependent on the changed neutrosophic set edge finder (MNSED). Dissimilar to the current steganography

techniques dependent on EMD, the proposed strategy works with inserting the mysterious digits in two unique - ary notational frameworks into the edge and non-edge blocks. Additionally, it ensures assessing the specific edge areas subsequent to installing the mysterious message and thus keeps away from the weight of implanting of overhead edge data in the cover image. Test results showed the prevalence of the proposed strategy over best in class plans as far as both implanting limit and stego-image quality. Vikas Verma et al. [8] proposed a system which is based on Midpoint Circle Approach. As contrasted and the customary Least Significant Bit calculation, the information stowing away steganographic strategy introduced in this paper was viewed as of expanded intangibility to steg analysis assaults on the cover image. Along these lines, this strategy is most appropriate for the reasons for correspondence applications. The suggested method of transmission of stego images is through email connections or web postings. Sadly LSB addition is defenseless against slight image control, for example, editing and pressure. For instance, changing over a GIF or a BMP image, which remakes the first message precisely (lossless pressure), to a JPEG design, which doesn't (lossy pressure), and afterward changing over back, can obliterate the information in the LSBs. Omar Elharrouss et al. [9] proposed a system which is based on k-LBS technique. In this paper, an image steganography technique has been introduced for concealing an image into another. Utilizing the k-LSB-based technique the proposed strategy start by blending the cover image and the images to be covered up. To distinguish the area that contains the secret images, a district discovery activity has been introduced utilizing the neighborhood entropy channel. Then, at that point, subsequent to extricating the secret image, an image quality improvement technique has been applied to upgrade the image that can honey bee impacted during the stowing away processes.from the trial results, and utilizing the assessment measurements, the proposed strategy can conceal the images and concentrate it with the base expense in term of distortion and the lose of data.

Fig. 4. (a) original image (b) image to be hidden (c) stego image (d) entropy filter [9]

Daxa L. Vasoya et al. [10] proposed a system which is based on classification algorithm. This paper proposed a clever technique for image steganography dependent on DCT and information mining order techniques. Two 8 digit dim level image of size P X Q and M X N are utilized as cover image and mystery image individually. DCT is performed on both mystery image and cover image. ID3 calculation is utilized to observe the pixel value or number on where the mysterious image will be implanted. ID3 Algorithm produces the Decision tree to get the legitimate pixel because of which the implanting distortion will be less. Again two degree of safety is given in the framework one, preceding installing the discharge image on the cover image we apply the Arnold change, and second key is accommodated getting the information. Here key is the pixel number of cover image on which we will install the discharge image. Wa'el Ibrahim A. Almazaydeh et al. [11] proposed a system which is based on dynamic symmetric key. This paper shows two techniques for Steganography: the first is the notable technique which is known as Least Significant Bit, and the subsequent one is the new technique with LSB +KEY.The execution of the outcomes have been analyzed utilizing the PSNR values of individual calculations. It is noticed that the LSB +KEY calculation gives better result regarding the PSNR values This is one of the trial brings about this exploration work and the work is being worked on to work on the calculations for still better code intricacy and time intricacy .Also it is additionally expected to foster calculations for secret sharing of patient information in clinical images under telemedicine.

Fig. 5. Preprocessing [11]

Hayat Al-Dmour et al. [12] proposed a system which is based on Edge Detection and Hamming Code. In this paper, a proficient clinical image steganography technique is proposed for concealing patient secret data. The proposed technique can be utilized as an effective enhancement to cryptography strategies. It consolidates edge recognition to recognize and implant in high differentiation spaces of the image, and thus, draw in less consideration from interlopers. The distortion presented by the implanting of the mysterious message information is limited by utilizing a Hamming code and an expense function that controls the quantity of pieces to install in each square dependent on its edge strength. The ROI pixels are not used in the inserting strategy, so the

symptomatic area isn't compromised. The trial results exhibit that the proposed technique offer both high payload and great nature of stego images. Shalaw Mshir et al. [13] proposed a system which is based on ASCII embedding technique. This technique has the accompanying qualities: The first image and the Stego image seem to beindistinguishable. The natural eye can't see the distinction on account of the great PSNR result. The technique endeavors to find a mysterious message in the higher layers of the pre-owned image and changes the last layer of the comparing block. This will build the level of heartiness of the Stego investigation techniques. Bit mistake = 0 for generally trial results; the installed secret message is recuperated effectively with no blunders. The Stego framework addresses BLIND and PURE steganography, which implies the getting party doesn't need the first image or any mysterious key sent with the image. High limit: The test results show that the limit of this framework is high. Elshazly Emad et al. [14] proposed a system which is based on least significant bit and integer wavelet transform. This paper proposes a protected image steganography algo rithm for inserting a mysterious text in computerized images by us ing the IWT technique dependent on the LSB calculation. Four distinct instances of IWT-LSB are proposed, which are IWT LSB-1, IWT-LSB-2, IWT-LSB-3 and IWT-LSB-4.

The proposed half and half IWT-LSB calculations are performed us ing the MATLAB programming. The proposed calculations are applied on both grayscale and shading images. On account of grayscale images, the IWT is taken, the mysterious text is concealed nook in the LSBs of every pixel of the estimate coeffi cients of the image, and afterward the converse IWT is taken. On account of shading images, the IWT is taken for each chan nel, the mark of the transmitter and the length of the mysterious text are concealed in the estimate coefficient of the red part of the shading image, the mysterious text itself is concealed in the guess coefficient of both green and blue parts, and the backwards IWT is taken.

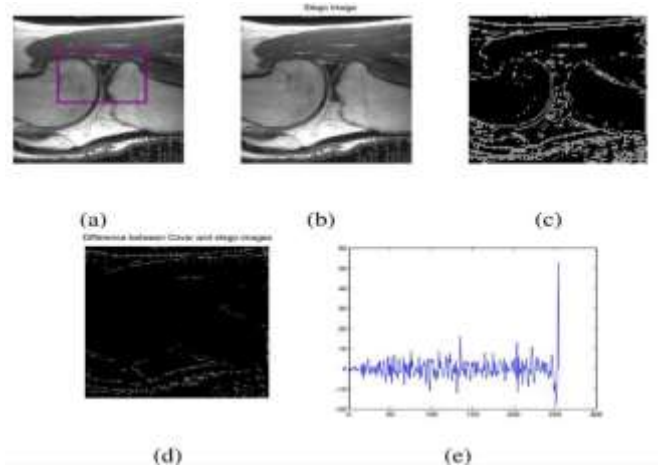

Fig. 6. (a) Cover Image, (b) Stego Image, (c) Edge Detected image, (d) Difference between (a) and (b) & (e) Difference between the cover and stego histograms [14]

Abbas Darbani et al. [15] proposed a system which is based on JPEG embedding technique. In this paper, a steganography technique in JPEG images is proposed. Since a piece of information might be lost after the discretization (or quantization) of recurrence values in the JPEG pressure methodology, in the proposed strategy, the implanted message is added to the image after the discretization stage. The strategy uses two contiguous pixels in the steganography interaction. For this reason, two less huge pieces of every pixel are considered for the inserting. The installing system is performed by a substitution table. In view of the pieces values in the inserted message, the pixel pieces might be changed (expanded or diminished). To assess the exhibition, two measures, PSNR and greatest limit of steganography have been determined. The outcomes involve that our technique can maintain more measure of mystery information while the nature of the stego image is practically like the first. Reza tavoli et al. [18] proposed a system which is based on LSB. This paper at first examines the various methodologies of steganography in an image . It has shown that the space pixel gives more limit than the recurrence area. Likewise, the sort of an image is viable in accomplishing the ideal outcome in steganography.In correlation with the present proposed techniques in recurrence space; our calculation has the capacity of putting away a bigger measure of data. Pressure prior to concealing advance is more suitable in imperceptibility of the steganography. Besides it expands the image limit with respect to information incorporation. Blending the utilization of a fitting cover with the use of a specific sweep of an image, and also adding a stage of encryption with each, takes into consideration various separate periods of data security. By consolidating the referenced stages with LSB approach, an advantageous level of steganography was yielded. Subsequently these means decline the chances of finding the secret information.

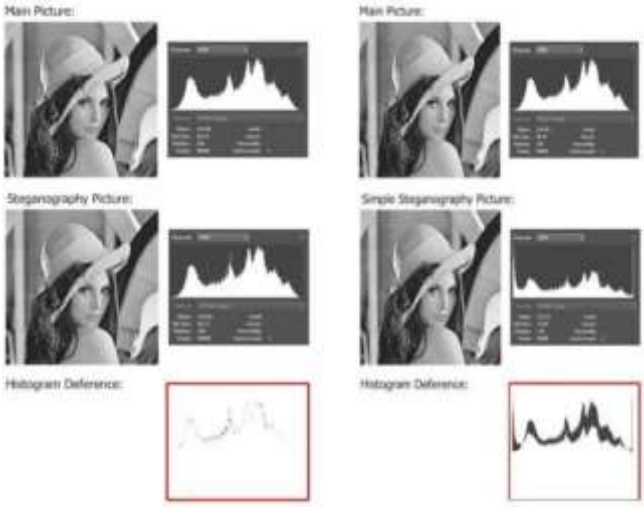

Fig. 7. Histogram Comparison [18]

Sumeet Kaur et al. [19] proposed a system which is based

on hybrid hiding model. In this examination, image steganography framework has been proposed and executed for concealing a classified image in a host image. The wellness job of African bison is utilized to observe the mid area of the cover image after that the privileged information is concealed in the cover image in the mid area. Additionally, the removed stego image is as old as unique mystery image. Here, the encryption and unscrambling process is worked utilizing the IHED approach.

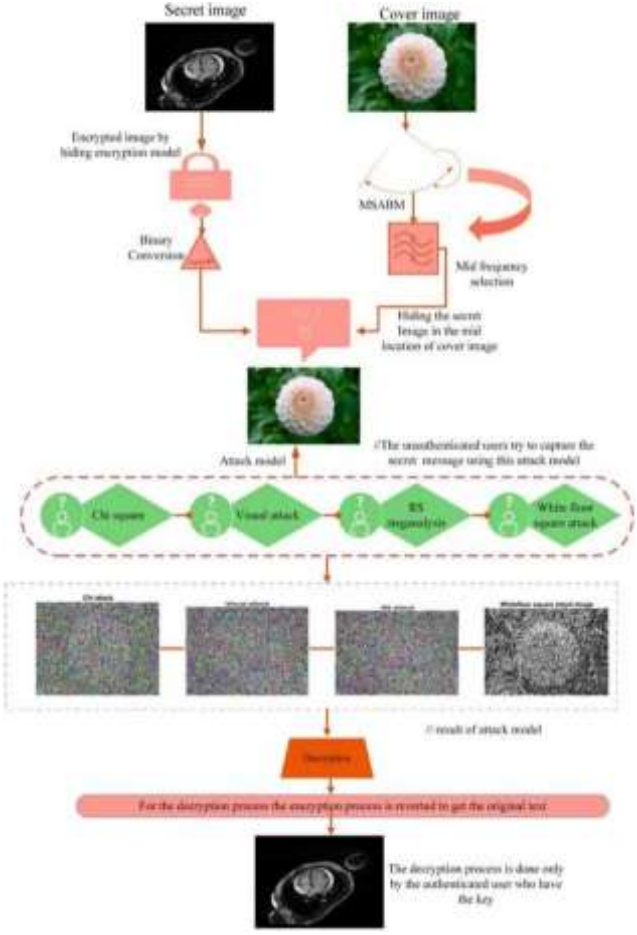

Fig. 8. Process Model [19]

Wei Lu et al. [20] proposed a system which is based on histogram of structure element. In this paper, author proposed a new measurable model dependent on the histogram of SEs to address double images. We examined PMMTM exhaustively, talked about the connection between the histogram of SEs and the co-event grid of SEs (sub SEs) exhaustively, and presumed that the previous can supplant the last option in the errand of double image steganalysis. There are a few motivations to utilize the proposed model, including the aversion of invariant boundaries and the rearrangements of the issue. In view of the proposed model, they examined the issue of planning appropriate SE for the errand of steganalysis from the parts of the size of the SE and the balance among the SE designs, and tentatively attempted a few unique SEs for the induction. Vipul Sharma et al. [21] proposed a system which is based on LSB. This paper proposed a new steganographic calculation for concealing text documents in images. Here we have likewise utilized a fundamental pressure calculation with greatest pressure proportion of 8 pieces/pixel. We have fostered a framework in java dependent on the proposed calculation. Here we have tried not many images with various sizes of text records to be covered up and reasoned that the subsequent stego images don't have any recognizable changes. Additionally we tracked down that for .bmp images this calculation works effectively. Thus this new steganographic approach is vigorous and extremely productive for concealing text records in images

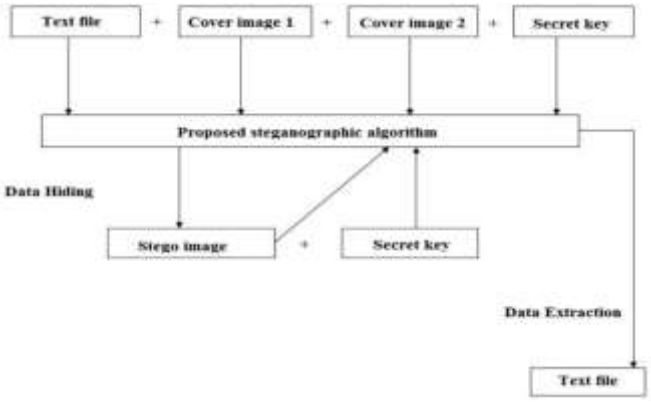

Fig. 9. Block Diagram Model [21]

Deepak kumar et al. [21] presents an image steganography strategy utilizing YCbCr shading model dependent on Least Significant Bit (LSB). In this paper proposed technique convert the image from RGB to YCbCr shading space then privileged information is concealed inside YCbCr shading space utilizing least significant bit and subsequent to concealing the information, convert it back to RGB shading space. Various methods of cryptography are looked at utilizing Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). YCbCr Color Model is bit differ from RGB color model where luma component along with blue and red difference components are present. The color intensity range is similar as RGB which is 0 to 255. Extracting hidden message from YCbCr based image is bit possible as compare to the RGB image because the luminance is quietly more visible in YCbCr instead of that RGB is bit complex for prediction because of natural colors. RGB images are not predictable and hardly find the altered region. Instead of changing the color model of the image; it is better to improve the security of the encryption as well as data hiding approach. For ideal system PSNR value should between 50 to 55 which maintains the quality of the image and also maintain the prediction rate for attackers because it does not much affect the image and it seems to be an original image.

III. CONCLUSION & FUTURE SCOPE

The paper surveyed various models related to the image steganography. There are so many researches have been done in this field. Most of the systems are based on single layer model for hiding the data in an image. Certain researches are based on zero distortion technique and histogram structural models. But these system are lacking somewhere like PSNR value and MSE. An image should be not very much affected by the system and the PSNR value should lies between 30 to 50 for idea system. It should not higher than the original image. A dual layer security can enhance the system in future that should pertain effective PSNR and MSE values.

REFERENCES

[1] https://www.geeksforgeeks.org/image-steganography-in- cryptography/

[2] https://www.commonlounge.com/discussion/4bc16dbc2c7145ff87ad0 f0d5401a242

[3] Shivani, Shivani & Kumar, Virendra & Batham, Saumya. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. Procedia Computer Science. 57. 10.1016/j.procs.2015.07.457.

[4] Mukherjee, Srilekha & Roy, Subhajit & Sanyal, Prof(Dr.) Goutam. (2018). Image Steganography Using Mid Position Value Technique. Procedia Computer Science. 132. 461-468. 10.1016/j.procs.2018.05.160.

[5] Al-Husainy, Mohammed. (2010). A Novel Steganography- Cryptography System. Lecture Notes in Engineering and Computer Science. 2186.

[6] J. Liu et al., "Recent Advances of Image Steganography With Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 60575-60597, 2020, doi: 10.1109/ACCESS.2020.2983175.

[7] Singh, Balvinder & Kataria, Sahil & Kumar, Tarun & Shekhawat, Narpat. (2014). A Steganography Algorithm for Hiding Secret Message inside Image using Random Key. International Journal of Engineering Research and. V3 10.17577/IJERTV3IS120844.

[8] Atta, Randa & Ghanbari, Mohammed & Elnahry, Ibrahim. (2021). Advanced image steganography based on exploiting modification direction and neutrosophic set. Multimedia Tools and Applications. 80 10.1007/s11042-021-10784-5.

[9] Verma, Vikas & Poonam, & Chawla, Rishma. (2014). An enhanced Least Significant Bit steganography method using midpoint circle approach. 105-108. 10.1109/ICCSP.2014.6949808.

[10] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566.

[11] D. L. Vasoya, V. M. Vekariya and P. P. Kotak, "Novel approach for image steganography using classification algorithm," 2018 2nd

[12] International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1079-1082, doi: 10.1109/ICISC.2018.8398970.

[13] W. I. A. Almazaydeh and H. S. Sheshadri, "Image Steganography Using a Dynamic Symmetric Key," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 1507-1513, doi: 10.1109/ICOEI.2018.8553778.

[14] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image steganography based on edge detection and hamming code," 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI), 2015, pp. 1486-1489, doi: 10.1109/ISBI.2015.7164158.

[15] S. Mshir and A. Varol, "A New Model for Creating Layer Planes Using Steganography for Text Hiding," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757498.

[16] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018, doi: 10.21629/JSEE.2018.03.21.

[17] A. Darbani, M. M. AlyanNezhadi and M. Forghani, "A New Steganography Method for Embedding Message in JPEG Images," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), 2019, pp. 617-621, doi: 10.1109/KBEI.2019.8735054.

[18] Tavoli, Reza & bakhshi, Maryam & Salehian, Fatemeh. (2016). A New Method for Text Hiding in the Image by Using LSB. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070416.

[19] Kaur, Sumeet, Savina Bansal and Rakesh Kumar Bansal. “Image steganography for securing secret data using hybrid hiding model.” Multim. Tools Appl. 80 (2021): 7749-7769.

[20] W. Lu, R. Li, L. Zeng, J. Chen, J. Huang and Y. -Q. Shi, "Binary Image Steganalysis Based on Histogram of Structuring Elements," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 9, pp. 3081-3094, Sept. 2020, doi:

10.1109/TCSVT.2019.2936028.

[21] Sharma, Vipul & Kumar, Sunny. (2013). A New Approach to Hide Text in Images Using Steganography. International Journal of Advanced Research in Computer Science. 3. 701-708.

[22] D. kumar, "Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019, pp. 1-5, doi: 10.1109/ICICT46931.2019.8977644.