IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

Data Concealment Using Steganography Technique

Apurva Sankpal[1], Adarsh Singh[2], Sanket Takalkar[3], Shubham Varma[4], Prof. Ayesha Sayyed[5]

Department of Information Technology, Trinity College of Engineering and Research, Pune, Maharashtra, India.

Abstract**:** Visual secret sharing (VSS) systems hide hidden images in shares that are also published on clarity or decrypted and saved in digital form. The shares can seem as noise-like pixels or as meaningful images, but this will raise suspicion and increase the risk of interception during transmission. As a result, VSS schemes face a transmission danger problem for both the secret and the individuals involved in the VSS system. To solve this issue, we presented a new palette-grounded steganography technique that uses a texture with LSB, as well as a natural-image-grounded VSS scheme (NVSS scheme) that shares secret images via colored carrier media to hide the secret and the actors during the transmission phase. To conceal secret messages, we convert the texture conflation process into steganography. Rather than using a being cover image to conceal dispatches, our algorithm conceals the source texture image and embeds hidden dispatches during the printing process. Prints or hand-painted filmland in digital or published form can be used for the natural shares. We also propose possible methods for concealing the secret in order to reduce the transmission threat problem for the share. The experimental results show that the proposed approach is an excellent solution to the transmission threat problem for VSS schemes.

Keywords: visual secret sharing (VSS), steganography, natural-image-based VSS scheme (NVSS scheme), OR Code, Palette Based Steganography.

I. INTRODUCTION

The being image is used as the cover medium in almost all image steganographic methods. This has two disadvantages. Bedding a large secret communication will distort the image because the cover is fixed. As a result, a compromise between picture size and embedding capability should be made to improve the quality of the cover image. Visual Cryptography (VC) is a method of encrypting a secret image into n shares, with each side holding one or more. Anyone with fewer than n shares are prohibited from disclosing any information about the secret image. Mounding the n shares displays the secret image, which the mortal visual system may honor immediately. Colorful graphics, handwritten documents, photos, and other forms of images can be used as secret images. A visual secret sharing (VSS) technique entails participating in and distributing secret images. The primary purpose of VC was to safely share hidden images in computer-assisted environments; yet, prejudice against computational resources is still prevalent (e.g., smartphones). In most cases, no progress has been made in the field of motorized media, and steganography for motorized media has become a major source of concern. Steganography is a stand-alone technology for data concealment. It implants dispatches into a host medium with the goal of concealing secret dispatches in order to avoid a buttinsky's suspicion. A typical steganographic model involves uncommunicative correspondences between two groups whose presence is unknown to a potential bushwhacker and whose success is contingent on conveying the presence of this correspondence. Because the NVSS system employs various media as a carrier, it provides a variety of scripts for sharing hidden images. As an example, suppose a dealer chooses n-1 media as natural shares to share in a hidden image. To reduce transmission problems, the dealer can use an image that is difficult to mistake for the media's content (e.g., terrain, depiction prints, hand-painted cinema, and flysheets). To avoid being suspicious, the digital shares might be kept in a party's digital bias (e.g., digital cameras or cell phones). The printed media (such as flysheets or hand-painted films) can be distributed by postal or direct mail marketing services. The transmission channels are likewise diverse in this way, lowering transmission problems even further.

II. REVIEW OF LITERATURE

Paper 1: Evaluation of using Steganography Technique to Hide a Text in Grayscale Digital Images
Publication year: 2021
Author(s): Sultana O Alsharkasi, Mohammed M Elsheh , Farij O Ehtiba
Summary: The RSA encryption algorithm is used with steganography in the above-mentioned work. This method is based on looking for two-by-two similar bits between the sensitive data bits and picture pixel bit values. It hides the sensitive data bits at least scientific bits if the bits aren't identical (LSB fashion).

DOI: 10.17148/IJARCCE.2022.11595

Paper 2: A Novel RGB Image Steganography Using Simulated Annealing and LCG via LSB
Publication year: 2021
Author(s): Mohammed J. Bawaneh1, Emad Fawzi Al-Shalabi, Obaida M. Al-Hazaimeh
Summary: This paper proposes a new and more robust color image steganography framework that combines the Linear Congruential Generator (LCG), simulated annealing (SA), Cesar cryptography, and the LSB negotiation system into a single system to reduce steganography expostulation and deliver data securely to their destination.

Paper 3: A New Method of Coding for Steganography Based on LSB Matching Revisited
Publication year: 2021
Author(s): Mansoor Fateh, Mohsen Rezvani, Yasser Iran
Summary: This study provides a refined version of the LSB matching redefinition technique that works for n> 2. -The suggested approach is divided into two phases: embedding and rooting communication. We turn the secret communication into a bit-sluice during the embedding phase. The bit-sluice is divided into a series of blocks, each with n bits. For hiding comparable n bits of the secret transmission, we use 2n 1 pixel. In the next stage, we select the operations required to elicit such communication. Finally, we apply the acquired procedures to the sections in order to conceal the hidden communication.

Paper 4: Image Steganography Using K-Means and DES Algorithm
Publication year: 2020
Author(s): Sampritha S. Shetty, K. Athmaranjan, Shambhavi, Shreya D. Rai, Soujanya R. Shetty
Summary: For picture segmentation, the K-means clustering technique is used. Segmentation entails a large amount of knowledge inside the pixel design, with each pixel having three factors: red, green, and blue. To provide correct leads in a short duration, a K-means clustering technique is used. The DES algorithm is used to hide the data using segmented images.

Paper 5: Improving Data Hiding Capacity in Code Based Steganography using Multiple Embedding
Publication year: 2020
Author(s): Katandawa Alex Kingsley, Ari Moesriami Barmawi
Summary: In order to boost the coverlet capacity, the paper suggested a steganography technique that enforced Reed Muller canons and modulus functions. Using mistake detection and correction, these fault-tolerant methods can recover secret dispatches from attacks. Despite this, the schemes have a limited embedding capacity (150) and a low PSNR (48dB). To overcome this difficulty, this work developed a multiple embedding method that intends to tore-embed secret bits on the same LSBs of the named pixels based on a secret key.

Paper 6: Securing LSB2 Message Steganography
Publication year: 2020
Author(s): Dr. Saleh A. Khawatreh, Dr. Jihad Nader, Dr. Mohammad S. Khrisat, Prof. Yousif Eltous, Prof. Ziad Alqadi
Summary: It is critical to protect the non-public secret and specific dispatches. We will demonstrate how to improve the security of the LSB2 data steganography system to encompass communication embedded in a digital colour image in this study. The caching procedure will include an encryption step, which will be based on dividing the held picture into blocks and reordering the blocks to obtain the translated image; the reordering sequence will then be saved as a PK to decipher the translated image. Steganography, encryption, blocking factor, reordering table, PK, MSE, PSNR are some of the terms used.

Paper 7: Data Hiding Techniques Using Steganography Algorithms
Publication year: 2020
Author(s): Ashi Tyagi, Rahul Veer Singh, Srishti Sharma
Summary: The review paper addresses each aspect in order to promote awareness. The main goal of this review paper is to gain a comprehensive understanding of current steganography styles and compare them to old cryptography styles, as well as to speculate on an approach that could learn from cryptography's mistakes and work on current styles in such a way that the field would grow.

Paper 8: Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography
Publication year: 2020
Author(s): Yuyuan Sun, Yuliang Lu, Jinrui Chen, Weiming Zhang, and Xuehu Yan
Summary: The study proposes a meaningful SISS based on Natural Steganography (MSISS-NS). To improve the visual quality of shadow photographs, this system combines SSS and steganography. The MSISS-NS cover pictures are RAW images, which comprise data reused from a digital camera or scanner's image detector. They're called that since they've

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

never been reused, published, or edited. As a result, RAW photos will save extensive information about the exposure time, white balance, ISO sensitivity, and other aspects of filming. In other words, RAW photos store all relevant information without loss or with minor loss.

III. PROPOSED SYSTEM

We sought to improve data security by ensuring secure data transmission via social media while keeping data hidden inside texture images. As a result, this system is suited for maintaining high-level security in the network for data transmission or image preservation. Palette stenography is employed in the proposed work to hide the secret message in the image as well as retrieve the secret message from the texture image. We also use cover image shares to design efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. Digital and printed media are both covered by the proposed algorithms. The various options for concealing the generated share are also explained. The suggested NVSS approach is user-friendly and manageable, and it decreases transmission risk while also improving the security of participants and shares.

ADVANTAGES OF THE PROPOSED SYSTEM:

1. The printed media (for example, hand-painted, filmland, or flysheets) can be distributed by postal or direct correspondence marketing services.
2. To lessen the risk of transmission, the dealer can use an image that isn't immediately recognised as the media's content (e.g., geography, portrayal photos, hand-painted, painted filmland, and flysheets).

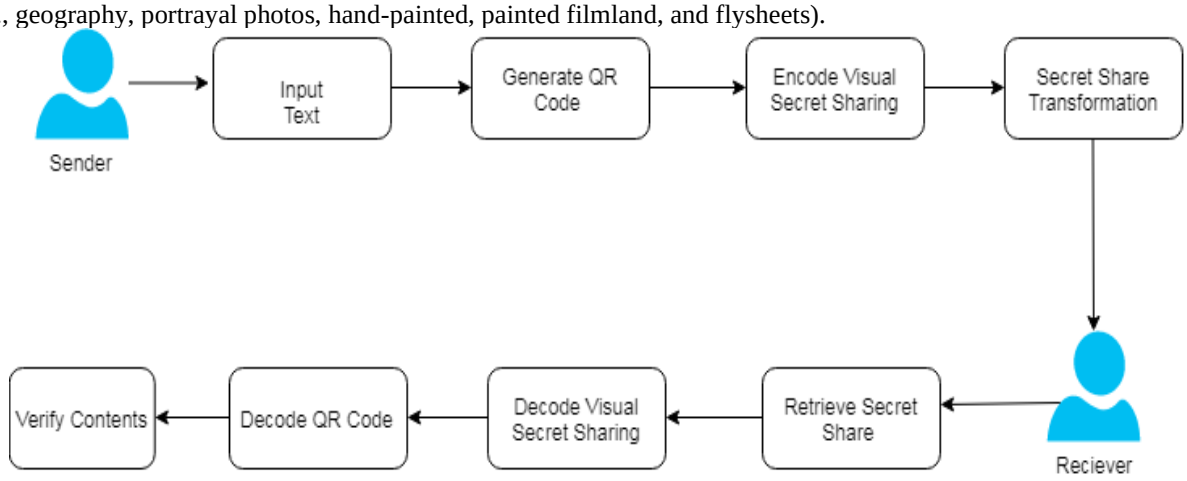

Fig. 1 System Architecture

III. ALGORITHM

Image Stenography:

Least Significant Bit (LSB):

In this paper, the least significant bit (LSB) algorithm employed in the negotiating system is spatial sphere steganography; the principle is to substitute information in the image's least bit with non-public information. The grayscale value of each pixel in 256 grayscale cover pictures can be used to represent an 8-bit double, with a specific bit of all pixels constituting a certain bit plane, such as the least significant bit of all pixels constituting the least significant bit plane.

The more advanced the bit plane, the lower the argentine value contribution, and the smallest bit plane is equivalent to random noise. Steganography is the art of concealing the fact that communication is taking place by encasing data in other data. There are a variety of carrier train forms available, but digital photos are the most common due to their prevalence on the Internet. There are numerous steganographic methods for hiding hidden information in photographs, some of which are more difficult than others and all of which have distinct strengths and weaknesses. Different operations have different steganography fashion conditions. For example, some activities may require complete secret information invisibility, while others require a larger secret communication to be made hidden.

Message Embedding and Extraction Steps:

i) Embedding phase:

The embedding process is as follows:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

Step 1: Extract all the pixels in the given image and store them in the array called Pixel-array.
Step 2: Extract all the characters in the given text file and store them in the array called Character array.
Step 3: Extract all the characters from the Stego key and store them in the array called Key- array.
Step 4: Choose the first pixel and pick characters from the Key array and place it in the first component of the pixel. If there are more characters in the Key array, place the rest in the first component of the next pixels.
Step 5: Place some terminating symbols to indicate the end of the key. '0' has been used as a terminating symbol in this algorithm.
Step 6: Place characters of Character- Array in each first component (blue channel) of the next pixels by replacing them.
Step 7: Repeat step 6 till all the characters have been embedded.
Step 8: Again, place some terminating symbols to indicate the end of the data.
Step 9: The obtained image will hide all the characters that are input.

ii) Extraction phase:
Step 1: Read the stego image.
Step 2: Extract the pixels of the stego image
Step 3: Declare a message byte; here the size of the message is 8 bits.
Step 4: Read a pixel from the array starting from address=0.
Step 5: Extract the LSB and replace i th bit in the message byte where i =1 to 8 Address=address=1. When i =8, a byte is extracted.
Step 6: Repeat the same for extracting the next byte.

Palette-Grounded Stenography: The image is palette-based. For 24-bit color images, stenography is similar to the widely used LSB format (or 8- bit grayscale images). It embeds the message into the LSB of indicators pointing to the palette colors after the palette colors are sorted by brightness. Communication recovery is as simple as selecting the identical pixels and adding all of the indicators' LSBs to the sorted palette. The benefits of wearing a spatial sphere are as follows:

1. The original image has a decreased chance of declination.
2. An image can store additional information.
3. Mathematical Complexity is Low.

NVSS Encryption/Decryption Algorithm
The critical generation phase and the encryption phase are the two important phases of the proposed new NVSS method. The Key has uprooted a number of noteworthy nature imagery. These natural images can be 24bit/pixel color images that are named arbitrarily from any public Internet website or photos in the system. To extract the key from these photos, some pre-processing is required.
The natural image must first be binarized so that the individual pixel values, which might be either black or white, can be reused. The 24-bit pictures are transformed to an 8-bit grayscale or double image.

IV. RESULTS AND DISCUSSION

Experiments can be run on a PC with the following specifications: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB RAM, Windows, MySQL backend database, and Jdk 1.9. The application is a web application that runs on the Tomcat server and is used to design code in Eclipse.
QR code security using texture patterns is achieved by using an X-OR based Visual Cryptography Scheme to share secrets with the receiver. The QR code example is shown in the diagram. There are two steps in the experiment: encryption and decryption.

Sender:
Enter the message, the number of parts to create, and enter the number of parts required to reconstruct the secret and specific user participants.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

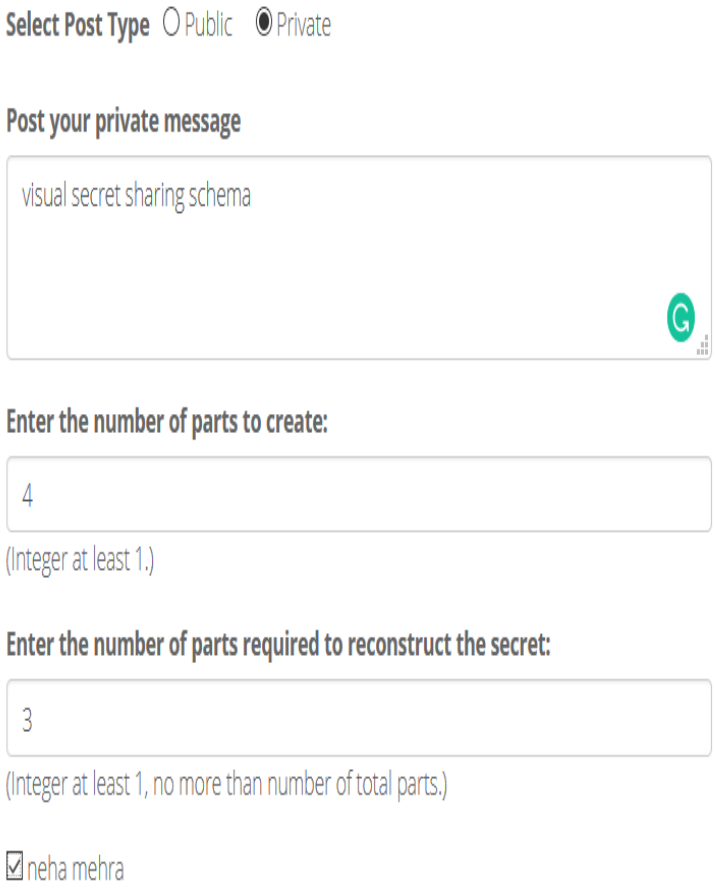

Fig.2 Message – visual secret sharing schema

Generate the number of Parts using an advanced partitioning technique i.e. k-means clustering.

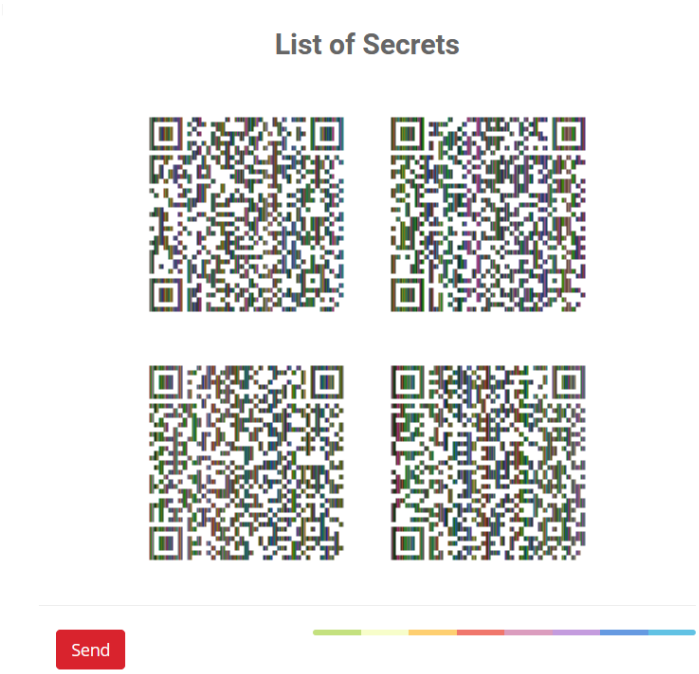

Fig. 3 Generation of parts

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

Receiver:

View Message:

Fig. 4 Message Viewed

Select required parts:

Fig. 5 Number of parts

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.11595

Decode Message:

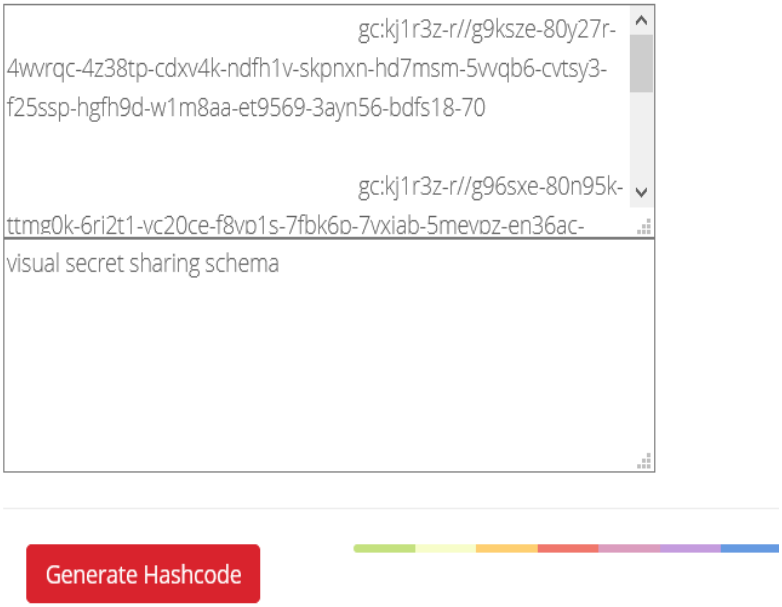

Fig. 6 Message Decryption

V. CONCLUSION

GUI format is used to load the communication and image. In our system, the print process is used to hide the secret communication in the image and to prize the hidden communication from the texture image. We employed palette-grounded print with the LSB fashion in this proposed work. The receiver will treasure the hidden communication. Palette print is used in the proposed way to hide data inside images using the LSB manner, which inputs the texture picture pattern for hiding textbooks. The proposed NVSS system can significantly limit transmission risk while also providing the highest level of stoner generosity for sharing and secret photos.

VI. REFERENCES

[1] Sultana O Alsharkasi, Mohammed M Elsheh, Farij O Ehtiba "Evaluation of using Steganography Technique to Hide a Text in Grayscale Digital Images", Journal of Academic Research (Applied Sciences), VOL.19, July 2021.

[2] Mohammed J. Bawaneh1, Emad Fawzi Al-Shalabi, Obaida M. Al-Hazaimeh, "A Novel RGB Image Steganography Using Simulated Annealing and LCG via LSB", IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.1, January 2021

[3] Mansoor Fateh, Mohsen Rezvani, and Yasser Iran, "A New Method of Coding for Steganography Based on LSB Matching Revisited". Hindawi Security and Communication Networks Volume 2021.

Sampritha S. Shetty, K. Athmaranjan, Shambhavi, Shreya D. Rai, Soujanya R. Shetty, "Image Steganography Using K-Means and DES Algorithm" IJRESM International Journal of Research in Engineering, Science and Management Volume-3, Issue-6, June-2020.

[5] Katandawa Alex Kingsley, Ari Moesriami Barmawi, "Improving Data Hiding Capacity in Code Based Steganography using Multiple Embedding", Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous International, March 2020.

[6] Dr. Saleh A. Khawatreh, Dr. Jihad Nader, Dr. Mohammad S. Khrisat, Prof. Yousif Eltous, Prof. Ziad Alqadi, "Securing LSB2 Message Steganography", IJCSMC International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 6, June 2020.

[7] Ashi Tyagi, Rahul Veer Singh, Srishti Sharma, "Data Hiding Techniques Using Steganography Algorithms", ResearchGate, Feb,2020.

[8] Yuyuan Sun, Yuliang Lu, Jinrui Chen, Weiming Zhang, and Xuehu Yan, "Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography". Mathematics, 30 August 2020.

[9] Yaseen Hikmat Ismaiel, Sahlah Abed Ali. Crescenzo, "Enhanced Steganography Using Visual Cryptography", ResearchGate, September 2019.

DOI: 10.17148/IJARCCE.2022.11595

[10] A. K. Sahu and G. Swain, "Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis" International Journal of Electronic Security and Digital Forensics Vol. 11, No. 4, Feb 2019.
[11] S. Singh, "Adaptive PVD and LSB based high capacity data hiding scheme," Multimedia Tools and Applications, vol. 79, pp. 18815–18837, 2020.
[12] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," Multimedia Tools and Applications, vol. 78, no. 8, pp. 9971–9989, 2019.
[13] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," Multimedia Tools and Applications, vol. 79, pp. 7951–7985, 2020.
[14] G. Kaur, S. Singh, R. Rani, and R. Kumar, "A comprehensive study of reversible data hiding (RDH) schemes based on pixel value ordering (PVO)," Archives of Computational Methods in Engineering, pp. 1–52, 2020.
[15] D. Kaur, H. K. Verma, and R. K. Singh, "Image Steganography: Hiding Secrets in Random LSB Pixels," in Soft Computing: Theories and Applications, ed: Springer, 2020, pp. 331 -341
[16] G. Kaur, S. Singh, and R. Rani, "A high capacity reversible data hiding technique based on pixel value ordering using interlock partitioning," in Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 727–732, Noida, India, 2020.
[17] A. Y. Hindi, M. O. Dwairi, and Z. A. AlQadi, "A Novel Technique for Data Steganography," Engineering, Technology & Applied Science Research, vol. 9, pp. 4942 - 4945, 2019.
[18] N. Akhtar, V. Ahamad and H. Javed, "A compressed LSB steganography method, 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT),2017.
[19] R. Kumar, S. Chand, and S. Singh, "An optimal high capacity reversible data hiding scheme using move image size to front coding for LZW codes," Multimedia Tools and Applications, vol. 78, no. 16, pp. 22977–23001, 2019.
[20] R.H. adekar, N.M. jadhav, N.D. Pergad, "Digital image sharing by diverse image media using nvss technique", IJARIIE-ISSN (O)-2395-4396, Vol-2 Issue-1, 2016.
[21] Miss A.A.Naphade, Dr. R.N.khobaragade, and Dr.V.M.Thakare, "Improved nvss scheme for diverse image media". International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.
[22] Priyanka R. Pawar, Manjusha S. Borse, "Transmission risk reduction in image sharing scheme with diverse image media". International Conference on "Recent Research Development in Science, Engineering, and Management",2016.
[23] Mohmmad J. Bawaneh, Atef A. Obeidat. "A Secure Robust Gray Scale Image Steganography Using Image Segmentation", Journal of Information Security(JIS),7,1,152-164,2016.
[24] Bawaneh, Mohammed J. , "An Adaptive Virtual Gray Scale Image Steganography Using Simulated Annealing." International Journal of Computer Science and Information Security 14.9 (2016): 612 (2016).
[25] M. H. Mohamed and L. M. Mohamed, "High capacity image steganography technique based on LSB substitution method," Applied Mathematics & Information Sciences, vol. 10, no. 1, pp. 259–266, 2016.
[26] J. N. Abdel-Jalil, "Performance analysis of color image encryption\decryption techniques", International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016.
[27] P. Rai, S. Gurung, and M. K. Ghose, "Analysis of image steganography techniques: a survey," International Journal of Computer Applications, vol. 114, no. 1, pp. 11–17, 2015.
[28] Diljeet Singh, "An approach to steganography using the local binary pattern on CIELAB based k-means clustering," Computing Communication & Networking Technologies (ICCCNT), 2015 Third International Conference on, pp. 1-11, 26-28 July 2015.
[29] G.Rajathi, G.Sangeetha, D.Tamizharasi, S.Praveen Kumar, "Secret sharing schemes by diverse image media". International Journal of Innovative Research in Computer and Communication Engineering an ISO 3297: 2007 Certified Organization Vol.3, Special Issue 1, February 2015.
[30] Shridevi Shetty, "A secure image steganography based on RSA algorithm and hash- LSB technique," Information and Communication Technologies (WICT), 2015 World Congress on, pp. 755-758, Oct. 30-2012, Nov. 2, 2015.

