iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41921

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Adversarial Embedding Using Steganography Technique

Apurva Sankpal[1], Adarsh Singh[2], Sanket Takalkar[3], Shubham Varma[4], Prof. Ayesha Sayyed[5]
[1, 2, 3, ,4,] *Department of Information Technology, Trinity College of Engineering and Research, Pune, Maharashtra, India*

Abstract: ***Conventional visual secret sharing (VSS) schemes hide secret images in shares that are moreover published on clarity or are decoded and stored in a digital form. The shares can appear as noise-suchlike pixels or as meaningful images, but it'll arouse dubitation and increase interception threat during transmission of the shares. Hence, VSS schemes suffer from a transmission threat problem for the secret itself and for the actors who are involved in the VSS scheme. To address this problem, we proposed a new fashion for the palette-grounded steganography using a texture with LSB and also a natural-image-grounded VSS scheme (NVSS scheme) that shares secret images via colorful carrier media to cover the secret and the actors during the transmission phase. We contrive the texture conflation process into steganography to hide secret dispatches. In comparison to using a being cover image to hide dispatches, our algorithm hides the source texture image and embeds secret dispatches through the process of print. The natural shares can be prints or hand-painted filmland in digital form or published form. We also propose possible ways to hide the secret to reduce the transmission threat problem for the share. Experimental results indicate that the proposed approach is an excellent result for working the transmission threat problem for the VSS schemes.***
Keywords: visual secret sharing (VSS), steganography, natural-image-based VSS scheme (NVSS scheme), OR Code, Palette Based Steganography.

I. INTRODUCTION

In utmost of the image steganographic styles, uses the being image as their cover medium. This leads to two downsides. Since the cover is fixed, bedding a large secret communication will distort the image. Therefore, a concession should be made between the size of the image and the embedding capacity to ameliorate the quality of the cover image. Visual Cryptography (VC) is a fashion that encrypts a secret image into n shares, with each party holding one or further shares. Anyone who holds smaller than n shares can not reveal any information about the secret image. Mounding the n shares reveals the secret image and it can be honoured directly by the mortal visual system. Secret images can be colourful types of images, handwritten documents, photos, and others. Participating and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original provocation of VC is to securely partake secret images in computer-aided surroundings; still, bias with computational powers is ubiquitous (e.g., smartphones). In utmost times no advances have been made in the range of motorized media, and much further concern has developed concerning steganography for motorized media. Steganography is a solitary system for data hiding strategies. It implants dispatches into a host medium keeping in mind the end to cover secret dispatches so as not to excite mistrustfulness by a buttinsky. A normal steganographic fashion incorporates uncommunicative correspondences between two gatherings whose presence is unclear to a conceivable bushwhacker and whose achievement is grounded on relating this correspondence's presence. The NVSS scheme uses different media as a carrier; hence, it has multiple possible scripts for sharing secret images. For illustration, assume a dealer selects n-1 media as natural shares for sharing in a secret image. To reduce the transmission trouble, the dealer can choose an image that is not easily suspected as the content of the media (e.g., terrain, depiction prints, hand-painted cinema, and flysheets). The digital shares can be stored in a party's digital bias (e.g., digital cameras or smartphones) to reduce the trouble of being suspected. The published media (e.g., flysheets or hand-painted cinema) can be transferred via postal or direct correspondence marketing services. In such a way, the transmission channels are also different, further reducing the transmission trouble.

II. REVIEW OF LITERATURE

1) 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 mentioned paper makes use of combining the RSA encryption algorithm with steganography fashion. This approach is grounded on searching for identical bits -two by two bits-between the sensitive data bits and image pixel bits values. In case the bits are non-identical, it hides the sensitive data bits at hitch least scientific bits (LSB fashion).

2) 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 presents a new and robust frame for color image steganography that combines Linear Congruential Generator (LCG), simulated annealing (SA), Cesar cryptography, and LSB negotiation system in one system to reduce the expostulation of Steganalysis and deliver data securely to their destination.

3) 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 paper proposes a bettered interpretation of the LSB matching redefined approach, which works for n> 2. -e proposed scheme contains two phases, including embedding and rooting the communication. In the embedding phase, we first convert the secret communication into a bit- sluice. The bit- sluice is divided into a set of blocks including n bits in each block. We choose 2n − 1 pixel for hiding similar n bits of the secret communication. We choose the operations demanded to induce such a communication in the coming step. Eventually, we perform the attained operations over the portions to hide the secret communication.

4) 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: K-means clustering algorithm is employed for image segmentation. Segmentation involves a huge set of knowledge within the style of pixels, where each pixel further has three factors viz. red, green, and blue. K- means clustering fashion is employed to induce accurate leads to a small period. Segmented images are used for hiding the data using the DES algorithm.

5) 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: The paper has proposed a steganography scheme that enforced Reed Muller canons and modulus function in an attempt to increase em coverlet capacity. These fault-tolerant schemes can recover secret dispatches from attacks using error discovery and correction. Still, being schemes have low embedding capacity (150) and low PSNR value (48dB). This paper proposed a multiple embedding system that aims to tore-embed secrets bits on the same LSBs of the named pixels grounded on a secret key to overcoming this problem.

6) 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: Securing the nonpublic secret and particular dispatches is a vital task. In this paper, we will show how to increase the security of the LSB2 system of data steganography to cover the communication bedded in a digital color image. An encryption phase will be added to the caching process, this encryption will be grounded on dividing the holding image into blocks and reordering the blocks to get the translated image, the reordering sequence then will be kept as a PK to decipher the translated image.
Keywords Steganography, encryption, blocking factor, reordering table, PK, MSE, PSNR.

7) Paper 7: Data Hiding Techniques Using Steganography Algorithms
Publication year: 2020
Author(s): Ashi Tyagi, Rahul Veer Singh, Srishti Sharma
Summary: The given review paper touches on each point primarily to create mindfulness. The main idea of this review paper is to compactly understand the present styles used in steganography and compare them with the old cryptography styles and also to wonder for an approach that could learn from the miscalculations of cryptography and work on the present styles in such a manner that would lead towards the growth of the field.

8) 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: In the paper, a meaningful SISS grounded on Natural Steganography (MSISS-NS) is proposed. This scheme combines SSS and steganography to ameliorate the visual quality of shadow images. The cover images of MSISS-NS are RAW images, which contain data reused from an image detector of a digital camera or scanner. They're so named because they've not been reused, Published, or used for editing. Thus, RAW images will record detailed data, similar to the exposure time, white balance, ISO perceptivity, and others about taking filmland. In other words, all applicable information is stored in RAW images without loss or with slight loss.

III. PROPOSED SYSTEM

We are working to facilitate data security in getting secure transmission of data over social media which maintains the data hiding inside texture images. Hence this system is suitable for maintaining high-level security for data transmission or image preservation in the network. In the proposed work, palette stenography is used to hide the secret message in the image and also extract the secret message from the texture image. Also, we develop efficient encryption/decryption algorithms for the (*n, n*) -NVSS scheme using cover image shares. The proposed algorithms apply to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme has a high level of user-friendliness and manageability and reduces transmission risk and enhances the security of participants and shares.

A. Advantages of the Proposed System

1) The published media (eg hand-painted, filmland, or flysheets) can be transferred via postal or direct correspondence marketing services.
2) To reduce the transmission threat, the dealer can choose an image that isn't fluently suspected as the content of the media (e.g., geography, portrayal photos, hand-painted, painted filmland, and flysheets).

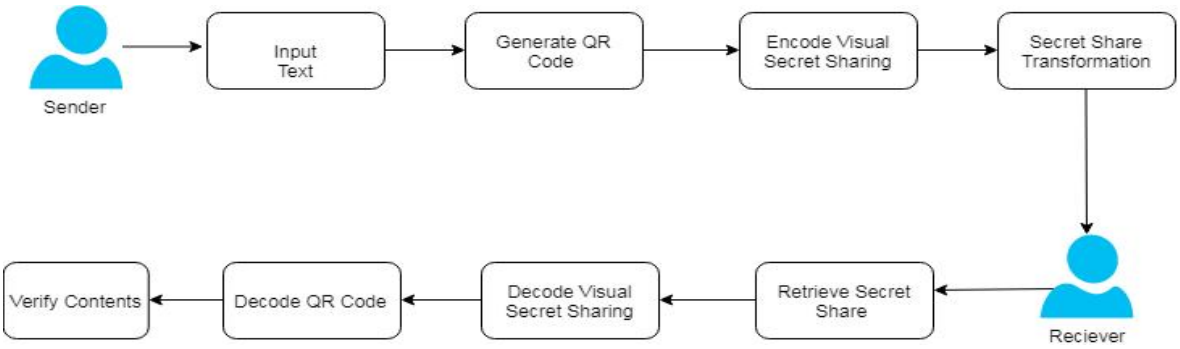


Fig. 1 System Architecture

III. ALGORITHM

A. Image Stenography

1) Least Significant Bit (LSB): The least significant bit (LSB) algorithm used in this paper is spatial sphere steganography in the negotiation system; the principle is to replace information in the least bit of the image with nonpublic information. For 256 grayscale cover images, the grayscale value of each pixel can be used to represent an 8- bit double, taken out a certain bit of all pixels constitute a certain bit airplane, for illustration, the least significant bit of all the pixels constituting the least significant bit airplane.

The advanced the bit airplane, the lesser the donation of the argentine value, and the smallest bit airplane is analogous to arbitrary noise. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Numerous different carrier train formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic ways some are more complex than others and all of them have separate strong and weak points. Different operations have different conditions of the steganography fashion used. For illustration, some operations may bear absolute invisibility of the secret information, while others bear a larger secret communication to be hidden.

Palette-Grounded Stenography The palette-grounded image Stenography is analogous to the generally used LSB system for 24- bit color images (or 8- bit grayscale images). After the palette colors are sorted by luminance, it embeds the communication into the LSB of indicators pointing to the palette colors. Communication recovery is simply achieved by opting for the same pixels and collecting the LSBs of all indicators to the ordered palette. General advantages of spatial sphere fashion are

1) There's a lower chance for declination of the original image.
2) Further information can be stored in an image.
3) Low Mathematical Complexity.

B. NVSS Encryption/Decryption Algorithm

The proposed new NVSS scheme has two major phases the crucial generation phase and the encryption phase.

The Key has uprooted from 'n' natural meaningful images. These natural images can be 24bit/ pixel color images that are aimlessly named from any websites on the public Internet or photos stored in the system. To prize the key from these images, it has to first suffer some pre-processing.

The natural image has to be binarized first so that we can reuse the individual pixel values which can be either a black or white pixels. The 24- bit images are converted into an 8- bit double image or grayscale image.

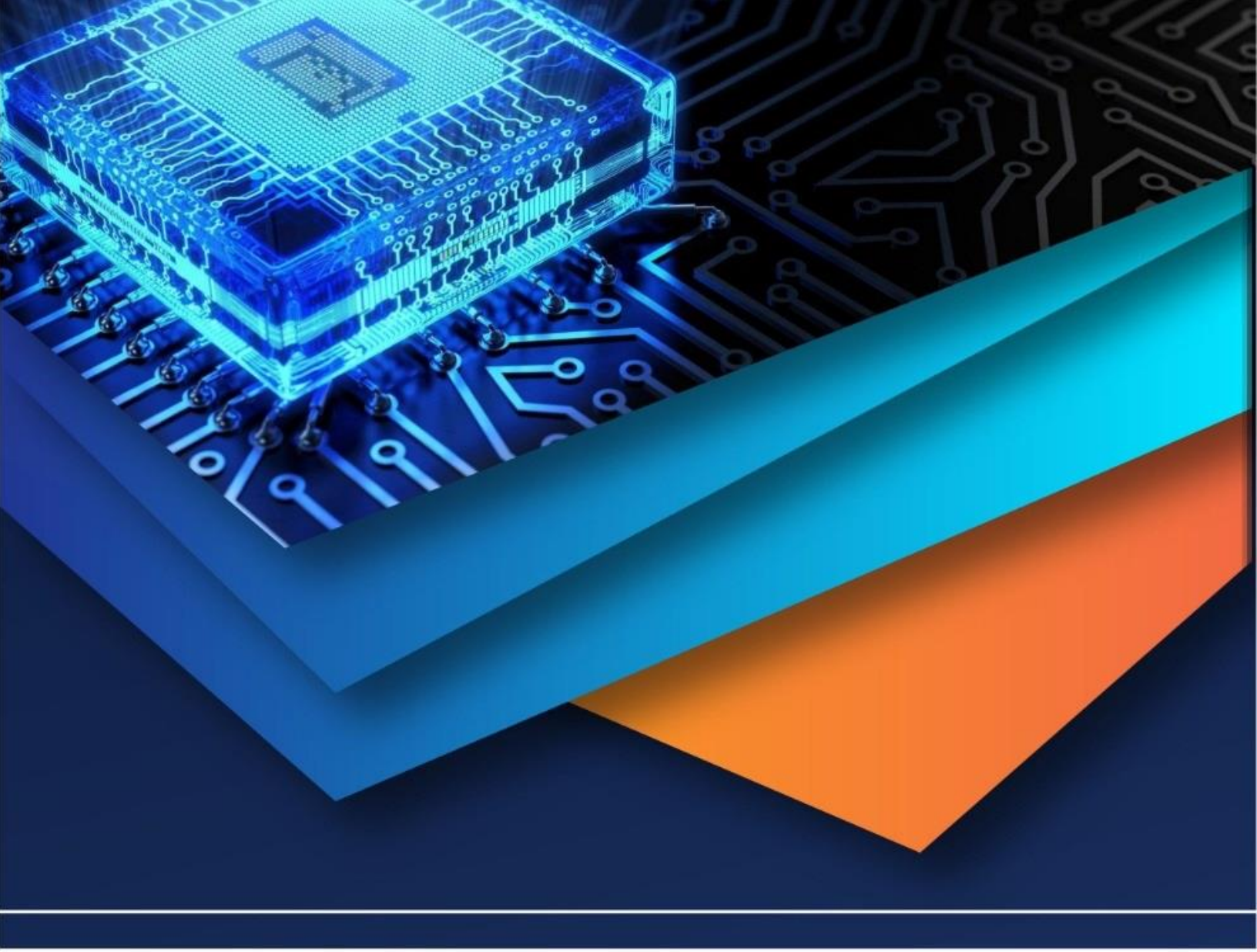
IV. CONCLUSION

The communication and image are loaded using GUI format. The print process is used to hide the secret communication in the image and also prize the secret communication from the texture image in our system. In this proposed work we used palette-grounded print with the LSB fashion. The secret communication will prize by the receiver. The proposed methodology uses palette print to hide data inside the image using the LSB fashion, which inputs the texture image pattern for hiding textbooks. The proposed NVSS scheme can effectively reduce transmission threat and give the loftiest position of stoner benevolence for shares and secret images.

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.
[4] 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.
[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] Diljjeet 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY