An Exploratory Survey on Data Protection Using Data Steganography

Balaram Baliarsingh[#1], Ajay Kumar Barapatre[*2]

[#]*Research Scholar & Department of ECE &RKDF University Bhopal*

[*]*Asst. Prof & Head Department of ECE &RKDF University Bhopal*
Gandhi Nagar Bhopal (MP) India

[1]baliarsingh@gmail.com

[2] barapatre.ajay@yahoo.co.in

Abstract— *The unique knowledge concealing techniques in image encryption and decryption are discussed in this survey paper. It is often important to not only translate data into an unreadable format, but also to conceal its presence. Steganography is used for this purpose. Information protection requires steganography. Steganography's main aim is to mask the existence of the actual correspondence. The genuine data can be shrouded in other data using steganography, making it impossible for a burglar to spot it. Data can be hidden in transporters such as images, audio files, text files, and video files in steganography. The various image steganography techniques are discussed in this paper. This paper offers an overview of image steganography, including its different methods, benefits and drawbacks, and applications.*

Keywords — steganography, spatial domain techniques, transform domain technique, cover image and stego-image.

Introduction

I. INTRODUCTION

Different traditional methodologies such as Cryptography, Steganography, and Data Hiding can be used in the field of image processing for information security. Steganography refers to the study of numerical methodology and related aspects of information security such as information confidentiality, data integrity, and data validation. In today's world, the use of computers and the internet, as well as the transmission of sensitive information through them, is growing by the day. As a result, information security is becoming increasingly important. Encryption is one method for ensuring the protection of such data. Information is encrypted in such a way that it cannot be accessed be find by burglar. However, during encryption, the message is corrupted, leaving the burglar unaware of the existence of sensitive information. Steganography is another way to keep the confidential information secure. Steganography is a form of data encryption. Steganography is a means of concealing details in apparently harmless media. The terms steganography and staeganos (covered) come from the Greek words staeganos and graptos (writing). "Covered or obscured writing" is the definition. Reversible data hiding is a strategy in which data is embedded in the host end and the hidden data, as well as the host end, is retrieved at a lossless level at the receiving end.

A. **Reversible data hiding**

Reversible information stowing away can be described as a method of concealing information in a host media that may be used to spread an image. After the information has been separated, a reversible information disguise is a calculation that can recover the genuine picture loss with less effort. Wrap symbol, additional documents, encryption join, and statistics thrashing response are all part of the transmitter elevation of such systems. The concrete icon will be encrypted, the documents will be obscured, and then the icon will be sent. As a result, the recipient must decrypt the icon and extract the data. Because of the reversibility, not only the inserted mystery details and actual image, but also the encoded spread picture must be extricated with less misfortune on the collector's end.

II. BACK GROUND

Processes for hiding image data are an important part of any secret data communication. When secret data is hidden in an image, the image quality suffers. As a result, techniques that ask for improving the interpretability or recognition of images for human viewers while also providing more feedback for automated image processing techniques are being developed. This paper focuses on various image-based data steganography techniques.

Steganography –

Image steganography have some terminologies are as follows:-

Cover-Image: Inventive icon which is use for hide information.

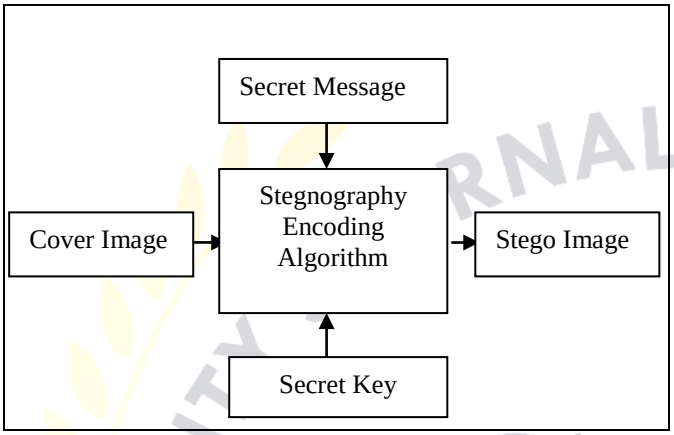
Message: Concrete information which is use to conceal into cover image. Message could be a pure book or some other picture.

Stego-Image: Subsequent to implanting message into spread picture is known as stego-picture.

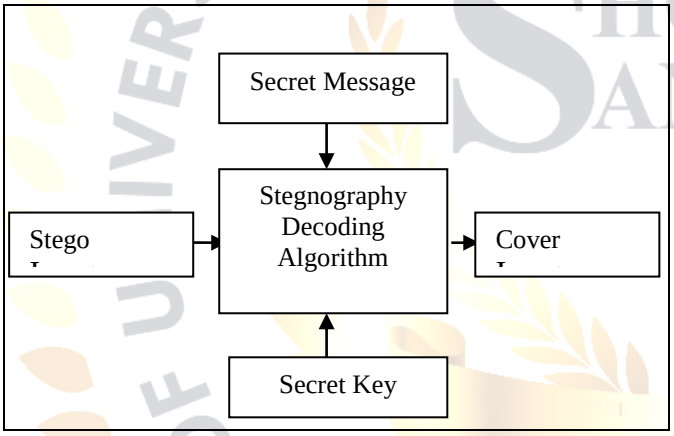
Stego-Key: A key is use for embedding or extracting the message from cover-images and stego-images.

In general, image steganography is a technique for concealing a hidden message in a cover image and creating a stego-image. This Stego-image is sent to the second party by some established middling, and the third revelry is oblivious to the stego-secret image's message. The receiver end can easily extract a stego-image hide message after receiving it using stego-key or without stego-key (depending on the

embedded algorithm). Figure 1 shows an indispensable map of reflection steganography with stego-key, where the embedding algorithm needs a swath reflection with a hidden message for the embedding course of action. The embedded algorithm's output is a stego-image, which is sent to the extracting algorithm as soon as possible.



(a) **Stego Image Generated at dispatcher Side**



(b) Message extraction at receiver side

Fig.1. Concept of Steganography

III.PRIOR APPROACHES

Several principles and algorithms for data hiding using steganography will be addressed during this survey.

Gandharba Swain (2016) - In this paper, the author proposes steganography strategies that combine least significant bit (LSB) replacement and pixel value differencing (PVD) to increase the concealing limit and peak signal-to-noise ratio (PSNR). Using both LSB substitution and PVD within a block, this paper proposes a stegano graphic technique. In a non-covering configuration, the image is divided into 22 pixel obstructs. The upper-left pixel is implanted with k-pieces of information for each 22 pixel obstruct using LSB replacement. After that, the latest pixel calculation is used to calculate three pixel value contrasts with the square's upper-right, base-left, and base-right pixels Then, in three different ways, these three contrast esteems are used to hide knowledge bits. Even and vertical edges are considered. In 22 pixel squares, a steganographic method based on LSB replacement and three-directional PVD is proposed. This proposed treatment comes in two flavours. When the two variants of the desired modus operandi are compared, deviation-1 is preferred for higher PSNR, while variant-2 is preferred for higher hiding power. This technique can be further extended to 3×3 pixel blocks.[2]

Tripti Dhruw,Dr. Namita Tiwari(2016)- The author of this research paper addressed different PVD (pixel value differencing) methods. PVD methods were the most common method that was investigated. It is based on the concept that edge areas can handle more changes than smooth areas. From 2003 to the present, this paper shows how different PVD approaches have progressed. PVD with the LSB system yields good results in terms of power and PSNR. However, combining the PVD approach with other methods such as MP and MPD is expected to improve hiding ability and PSNR. Since all other approaches used a grey image as a cover media, the PVD method uses a colour image as a cover media for the data embedding process. And if able to embed more data at edge area then increase the tolerance of steganalysis attacks. This paper represents the results of various PVD with different parameters. Lena, baboon and peppers each having size 512×512.The comparisons have been drawn by conducting tests on gray scale images. PSNR and embedding capacity have been complied[26].

Pulkit Khandelwal,Neha Bisht(2015)- The author of this paper discussed the plethora algorithm, which, according to the author, is a universal work on enabling mystery correspondence of extremely secret data among various groups in interactive media frameworks. A steganography system must be formulated in order to complete such a task. Another information concealing plan based on Energy and Cost of the Image has been suggested, in addition to the numerous calculations configurations to cover mystery information in pictures. The relation between contiguous pixels depicted by a picture's vitality is determined by its latent power. Dynamic Programming branches are used to calculate the picture's cost, and irregular crossing is used to choose the pixels in which information is to be implanted. The data is inserted as parts in each of the chosen pixels in a predetermined order. To assess the nature of the spread and the acquired stego photo, the mean square blunder and pinnacle sign to clamour proportion were calculated alongside a simple similitude list. A robust steganography approach is achieved with

the least amount of computing time. Due to the randomness of data hidden in the cover image, Dynamic Programming assisted in the creation of an Image Steganography scheme that provides high protection against unwanted intruders in a digital communication channel. The proposed algorithm was built on the foundation of the Markov Random Field. The grayscale cover image's energy and cost estimation offered the best solution for random traversal through the image. Extensive experimental findings back up the current technique's validity. Stego image was created with no compromises in terms of quality and computational complexity. Higher PSNR values obtained than existing schemes along with the SSIM calculation further backs up the proposed proposal in its aim to provide better imperceptibility. [1]

Praveenkumar, P., G. Ashwin, S.P.K. Agarwal,(2014)-

The author of this research paper addresses RGB-based image encryption. The RGB segments were initially distinct to each plane, so strategic planning was used. Following that, the stage was completed for the number of emphases provided by the client, and the bit planes were consolidated from a single image. The permuted pixels were pushed left/right or up/down in a round transfer operation. Finally, bitwise tasks based on two keys for line and section are implemented. Unified Average Changing Intensity, Number of Pixels Change Rate, and histogram tests were used to determine the strength of the proposed work relation esteems. The final encrypted image is created using a chaotic logistic map on individual bit planes of the image, followed by the rubick encryption principle. Top computer scientists have turned image encryption into a battleground, and encrypted image secrets are securely hoarded and transmitted. The computed horizontal, vertical, and sloping connection importance show that the original and shuffled images have no association. To provide shuffling, chaotic logistic mapping was applied to the RGB planes of the original image, and rubick cube encryption was applied to the shuffled image to obtain the final encrypted output[14].

Dr. Diwedi Samidha and Dipesh Agrawal (2013)- In this paper, the author illustrates various picture steganography procedures in terms of spatial area and pixel values in a double configuration. The physical area of pixels in an image defines the spatial area. Generally, an eight-piece dim level or shading picture can be used as a spread to conceal detail. Again, paired representations of these pixels are thought to mask the mystery message. Irregular bytes from these bytes are used to replace the mystery message's bits. Many steganography techniques may be used, such as Least Significant Bit (LSB), executive plans, and replacing only l's or only zero's from the lower snack of the byte are all considered for disgorging. Along with these strategies, some new ones are suggested, which are based on randomly selecting pixels from an image and hiding hidden data in random bits of these randomly selected pixels. As a result, various limits of a picture are examined, such as the physical area of pixels, pixel power estimation, and so on. In addition to current picture steganography methods, several new techniques for concealing information in pictures are discussed. Pixels have the ability to hide information. The methods described in this paper can be used to choose the physical area of these pixels. After selecting random pixels, the secret data can be hidden in random bits, which are represented in the bytes of binary digits. While selecting these pixels, many parameters from an image are considered for example. Color of pixels, physical location of pixels etc [3].

Xianhua Song, Shen Wang and Xiamu Niu, (2012)- A picture steganography technique based on number DCT and relative change is depicted by Creator. While number DCT is suitable for steganography because it is invertible and lossless, the difference in DCT coefficients will cause its Laplacian-shape-like dispersion to be harmed. Use relative change to recover the Laplacian-shape-like distribution of the whole number DCT coefficients to ensure the technique's security. Exploratory findings show that, even with a large payload, the proposed strategy can keep the stego image outwardly and factually imperceptible. The authors propose a new image steganography algorithm based on affine transformation and integer DCT. Some affine transformations are applied to the picture before or after LSB replacement in integer DCT coefficients, preserving the Laplacian-shape-like distribution of DCT coefficients histogram. As a consequence of the invertible affine transformation, the information bits can be extracted fully and safely. Experiments on real images illustrate the algorithm's efficacy, and the final stego image's DCT coefficients histogram is close to the original. In the future, attempt to demonstrate the histogram recovery theory after affine transformation.

Xin Liao, Qiao-yan Wen, Jie Zhang (2011)- In this paper, the author introduces a novel stenographic strategy based on four-pixel differencing and modified least critical piece (LSB) replacement to improve the implanting limit and offer an indistinct visual quality. A four-pixel square's standard contrast estimation is abused to classify the square as a smooth territory or an edge zone. The k-bit shift LSB replacement procedure

covers up mystery details into any pixel, where k is determined by the degree to which the usual distinction esteem falls. Rearrangement will be carried out to ensure that the perceptual contortion is kept to a minimum and that the natural contrast esteem has a position when implanting. A hypothetical verification is provided to legitimise the technique's success in implanting and extricating by showing that the rearranging system works. The test results showed that the proposed technique produces reasonable image quality and has a broad inserting limit [23].

Bin Li, Junhui He(2011) - This paper provides an overview of steganography and steganalysis for advanced images, focusing on the fundamental concepts, the evolution of steganographic techniques for images in spatial representation and JPEG architecture, and the development of the corresponding steganalytic plans. Some widely used systems for improving steganographic protection and enhancing steganalytic capability are summarised, as well as potential inspection trends. Review the basic concepts and notions as well as some common techniques in steganography and steganalysis for digital images in this paper. The embedding locations are selected in an adaptive manner. For the sake of avoiding perceptual manufactured posts, author has seen a number of stegano-graphic methods that use adaptive embedding policy to embed statistics into the composite vicinity of an icon. On the other hand, the rims and asymmetrical texture vicinity can be stiff to assemble an arithmetical model, causing the steganalytic scheme to lie on your front, leading to a false inference. As a result, selecting areas for inserting adaptively is still a promising arrangement in steganography. It's worth noting that the adaptive technique should be safeguarded as well, such as by encrypting it with a key to ensure its randomness.

Thanikaiselvan V,Santosh Kumar(2011)

A novel steganographic technique has been proposed in this research work to improve the protection of inserted information with a high limit and intangible visual quality. The proposed strategy is based on four-pixel square differencing, modified LSB substitution, and Knights visit. Hidden data is randomly inserted in each 8x8 pixel block of the cover image using knights tour, and n-bit changed LSB substitution has been used to boost the quality of the stego image, where n is calculated by the point where the usual disparity rate cascades into, and then it uses a readjustment technique to cut the perceptual buckle. The proposed method adaptively implants mystery knowledge into a spread picture by separating the edge and smooth regions, allowing for the installation of a greater number of mystery parts without perceptual twisting. The results show that our proposed system provides improved protection, a higher inserting cap, and better picture quality. Imperceptibility, robustness, and high data ability are understood to be the most important criteria for data hiding, so this approach was created with these requirements in mind. We used four pixel block differencing methods, as well as n-bit Adjusted Least Significant Bit (MLSB) substitution, Knight's tour, and other techniques.

Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang (2008)- The author of this research paper proposes a new image steganography technology that creates a mystery inserted picture that is completely indistinguishable from the original picture to the naked eye. Furthermore, by using pixel-esteem differencing and the modulus work, the new technique avoids the tumbling off-limit problem. To begin, use the pixel-esteem differencing procedure to obtain a distinction esteem from two continuous pixels (PVD). The separation regard plays a role in concealing the two nonstop pixels' farthest reaches. As it stands, the smoother the terrain, the less mystery information can be concealed, while the more edges zones there are, the more mystery information can be added. In these lines, the degradation of stego-picture quality is more intangible to the naked eye.

H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang(2005)

A novel stenographic technique based on least-huge piece (LSB) substitution and pixel-esteem differencing (PVD) strategy is implemented to increase the limit of the veiled mystery details and to provide a vague stego-picture quality. Using the PVD technique, an alternative reward from two back to back pixels is obtained first. A small distinction worth can be found on a smooth surface, while a wide one can be found on a ridged zone. The mystery in sequence is covered up into the spread image in the smooth regions by the LSB technique, while the PVD modus operandi is used in the periphery regions. The protection standard for the proposed strategy is similar to that of a single using the PVD strategy since the array width is variable and the territory where the mystery information is disguised by LSB or PVD technique is difficult to find out. According to the trial results, as compared to the PVD strategy used alone, the proposed technique will encase a lot more data while maintaining a good stego-picture visual nature.

Chi-Kwong Chan, L.M. Cheng (2003)- A facts thrashing format is proposed in this research work using

Table 1 – Shows the comparison of different previous methods

Year	Method	Advantage	Draw backs
2016	A steganographic method combining LSB substitution and PVD in a block.	Improved Data Hiding Capacity and PSNR. Using both LSB substitution and PVD within a block	Implement only at 2X2 block size
2015	Randomly Hiding Secret Data using Dynamic Programming for Image Steganography	Higher PSNR vales and lower MSE error. Energy Matrix based pixel detection.	Random data hiding
2014	Rubik's cube blend with logistic map on RGB	Tests Unified Average Changing Intensity, Number of Pixels Change Rate and histogram	Rubik's cube blend has high complexity
2013	Random Image Steganography in Spatial Domain	LSB layout schemes replacing only l's or only zero's from lower nibble from the byte.	Visual quality is not well. Quality of Stego image low
2012	An Integer DCT and Affine Transfor mation Based Image Steganography	system is invertible and lossless, but the alter of the DCT coefficients will harm its Laplacian contour in the vein of distribution.	Degrade quality of Stego image, not well PSNR and MSE
2011	A steganographic method for digital images with four-pixel differencing and modified LSB substitution.	The method acceptable image quality, also provides a large embedding capacity	Higher Level of complexity
2008	A top notch steganographic strategy with pixel-esteem differencing and modulus work	Difference value from two consecutive pixels by utilizing the PVD technique. Secure against the RS detection attack	PVD is secure but SSIM is low of Color image.
2005	Image steganographic scheme based on pixel-value differencing and LSB replacement methods	Smooth areas in the cover image and has a better image quality by using PVD method	SSIM is very low of Color image.
2004	Image Quality Assessment: From Error Visibility to Structural Similarity	Develop a Structural Similarity Index and demonstrate its promise through a set of intuitive also images compressed with JPEG and JPEG2000.	JPEG image compressed contain low pass filter that is destroy the image data.
2003	Hiding data in images by simple LSB substitution	Simple LSB substitution is proposed. By applying an most advantageous pixel tuning process to the stego-image obtained by the simple LSB changeover method,	LSB has un-sufficient data hiding capacity

a simple LSB substitution technique. Try an optimal pixel fine-tuning modus operandi on the stego-icon created by the LSB substitution technique, and the stego-icon image's eminence can be restored with minimal additional computational complexity. Extensive trials give you an indication of how elective the desired approach is. In terms of iconoclasm and numerical efficiency[25].

IV. CONCLUSION

The different data hiding processes of images are discussed in this survey article. Discuss data concealment and reversible data concealment systems. Various image steganography methods are investigated

and summarised. A quick look at steganography. In addition, address the literature survey on various image steganography techniques in Table 1, which compares various approaches. Confidential touch and hidden figure storage are two examples of image stegnogrphy applications. Data modification security, access control systems for digital content distribution, Media Database systems, potential ability to conceal the presence of not-to-be-mentioned data Enhancing the mystery of encrypted data. Future studies would propose a modern data hiding approach for the online social age. As the amount of data hacking and attacks grew on a daily basis, a highly secure data hiding technique became essential. One of the true solutions to this problem is image steganography. In the future, a new approach based on a modification of the Algorithm Spatially Desynchronized Steganographic Algorithm will be proposed (SDSA). Due to the generation of vast amounts of data, such as big data, this approach is based on JPEG-based data hiding. JPEG-based data capacity is very high in the proposed future method SDSA, but the same losses occur in the future proposed method SDSA based apply enchantment for minimising the losses and enhancing data hiding capacity.

REFERENCES

[1] Pulkit Khandelwal, Neha Bisht and Thanikaiselvan V, "Randomly Hiding Secret Data using Dynamic Programming for Image Steganography", International Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India.

[2] Gandharba Swain. "A steganographic method combining LSB substitution and PVD in a block", International Conference on Computational Modeling and Security (CMS 2016)

[3] Dr. Diwedi Samidha and Dipesh Agrawal (2013) "Random Image Stegano-graphy in Spatial Domain", IEEE, 2013.

[4] Amirtharajan, R. and J.B.B. Rayappan. "Steganography-time to time: A review". Res. Journal Information Technology, 5: pp 53-66, 2013.

[5] Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan,. Kubera kolam: "A way for random image steganography", Res. J. Inform. Technol., 5: 304-316, 2013.

[6] Bin Li, Junhui He, Jiwu Huang and Yun Qing Shi., "A examination on icon Steganography and Steganalysis", Journal of in sequence thrashing and Multimedia indication Processing. 2(2): 142-172, 2011.

[7] Chan, CK and L. M. Cheng. "thrashing data in descriptions by undemanding LSB substitution. Pattern Recognition". 7: 469– 474. 2004.

[8] Chan, C.K and L.M. Cheng, "Improved hiding information in pictures by ideal decently huge piece substitution Letters. 37 (16): 1017–1018. 2001.

[9] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai and Min-Shiang Hwang, "A great steganographic strategy with pixel-esteem differencing and modulus work". The Journal of Systems and Software. 81:150–158. 2008.

[10] Chung, K.L., C.H. Shen, L.C. Chang, "A novel SVD- and VQ based image hiding scheme" Pattern Recognition Letters. 22 (9): 1051–1058, 2001.

[11] Da-Chun Wu and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing". Pattern Recognition Letters. 24: 1613–1626, 2003.

[12] Hsien-Wen Tseng and Hui-Shih Leng., "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number". Journal of Applied Mathematics.: Article ID 189706, 8 pages, 2013

[13] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu, "A Novel Image Steganographic Method Using Tri-way Pixel- Value Differencing". Journal of Multimedia. 3(2): 37-44, 2008.

[14] Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan. "Rubik's cube blend with calculated guide on RGB: A way for image encryption. Res. J. Inform. Technol"., 6: 207-215, 2014.

[15] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin. 2000. Hiding data in images by optimal moderately significant-bit replacement. IEE Electron. Lett. 36 (25): 2069–2070.

[16] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin. 2001. Picture stowing away by ideal LSB replacement and hereditary calculation. Pattern Recognition. 34(3): 671–683.

[17] Shai Avidan and Ariel Shamir. 2007. Seam Carving for Content-Aware Image Resizing. In Proceedings of ACM SIGGRAPH. 26(3): Article No. 10.

[18] X. Song, S. Wang, and X. Niu. "An Integer DCT and Affine Transformation Based Image Steganography Method," in Proc. of eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '12), pp. 102–105, 2012.

[19] Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

[20] Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini, and Rengarajan Amirtharajan. 2013. A Graph Theory Practice on Transformed Image : A Random Image Steganography. Sci. World J., Vol. 2013. 10.1155/2013/464107.

[21] Wu D.C and W.-H. Tsai. 2003. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters. 24(9-10): 1613– 1626.

[22] Wu, H.C., N. I.Wu, C. S. Tsai, and M. S. Huang. 2005. Picture steganographic plot dependent on pixel-esteem differencing and LSB substitution methods. IEE Proceedings Vision Image and Signal Processing. 152(5): 611–615.

[23] Xin Liao, Qiao-yan Wen and Jie Zhang, " A steganographic technique for computerized pictures with four-pixel differencing and altered LSB replacement", Diary of Visual Communication and Image Representation, 22: 1-8, 2011.

[24] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh and Eero P. Simoncelli. 2004. Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transactions On Image Processing, 13(4): 600-612.

[25] Chi-Kwong Chan, L.M. Cheng 2003 Hiding data in images by simple LSB substitution Published by Elsevier Ltd doi:10.1016/j.patcog.2003.08.007

[26] Tripti Dhruw1,Dr. Namita Tiwari 2016 Different Method Used in Pixel Value Differencing Algorithm IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume