International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 2, Mar-Apr-2022, ISSN (Online): 2395-566X

A New Approach for Image Steganography Using Inter Pixel Value Difference and Quantized Range Table Method

M.Tech. Scholar Ashma Naz, Associate Prof.Shrikant Zade
Department of Computer Science Engineering
Oriental Institute of Technology Bhopal,MP, India
naz.ashma@gmail.com

Abstract- In the time of data, secret communication is quite possibly the main issues in the present communication framework. The improvement of computerized communication with information mystery becomes one of the fundamental reasons for the analysts. Among the information security methods, steganography is a way to deal with conceal the presence of mystery message in a transporter without being caught by the intruders. As of now, it is essential to conceal information and innovate systems by moving them so that the intruders cannot get the message. There are different information concealing strategies that utilization different advanced media. Digital images are the most well-known among the transporter designs on account of their recurrence on the web. In this paper, another methodology of image steganography with least significant bit substitution is proposed where the data inserted in the arbitrary bit position of a pixel. The test result implies the significance of the proposed technique.

Keywords- Software Fault Prediction, Prone Detection, SVM, Prediction Techniques, ACO, Neural Network.

I. INTRODUCTION

Communication in secret ways with others has generally been one of the notable errors from the old times. These days, in spite of the fact that cryptography and steganography are utilized for secured communication yet they are different in nature [1]-[6]. As cryptography changes a message, it can't be perceived while steganography conceals the message so it shouldn't be visible. The major aim of steganography is to install the communication content in a public cover media [2], [3], [6]. Accordingly, the presence of covered message can be covered up. Digital steganography is the study of moving data with secret message inserted in it. In this way, steganography is a type of safety method where the presence of a message is kept concealed between the sender and the intended beneficiary. Steganography is grouped into 3 classes [2], [8]-[10].

- Pure steganography with no stego-key. Here, the conveying parties expect that no other party knows about the communication.
- Secret-key steganography with the stegano-key. Here, the imparting parties trade the key preceding communication. This is generally helpless to interference.
- Public-key steganography with a public-key and a private-key. Here, the both keys are utilized for secure communication.

In general, Steganography centers around concealing the secret messages in transporters with inconspicuous and less alluring way. Practically all digital document organizations can be utilized as a transporter, yet the reasonable configurations are those which have a serious level of overt repetitiveness. There are different strategies and calculations of concealing information in various kinds of digital document designs. Numerous appropriate steganographic strategies which are being utilized to get security relying upon the sort of the transporter [2], [8]-[10]

- Image Steganography: When an image utilized as a cover object in steganography, it is known as image steganography. For the most part, pixel forces of the image are utilized to conceal the data in these procedures.
- Network Steganography: Taking network convention, for example, TCP, UDP, ICMP, IP and so on as cover object, is known as network convention steganography. Here, steganography can be accomplished by utilizing unused header bits of network conventions.
- Video Steganography: In video Steganography, the transporter for buried data is video (mix ofpictures). To conceal the data in every one of the images in the video, regularly, discrete cosine transforms (DCT) strategy is utilized. Different video organizations, for example,

H.264, Mp4, MPEG, AVI and so forth are utilized in video steganography.

- Audio Steganography: While involving audio as a transporter for concealing data, it is called audio steganography. Due to fame of voice over IP (VOIP), it has become vital medium. Digital audio organizations like WAVE, MIDI, AVI MPEG or and so on are utilized for this steganography.
- Text Steganography: To accomplish data stowing away in text steganography, various methods, for example, capital letters, blank areas, number of tabs, very much like Morse code and so on is utilized.

II.IMAGE STEGANOGRAPHY

In this day and age, practically in each page on the web, digital images can be seen as because of the easiest distribution. Consequently, image documents are the most generally involved conditions for steganography applications, despite the fact that they differ as per the configurations utilized [2], [8]-[10]. The human visual framework has a shortcoming that is; it has a low awareness towards irregular pattern changes and luminance. The human eye can't recognize the little changes in shading or examples and because of this shortcoming, text or realistic records can be embedded into the transporter image without being identified.

For instance, an image record with an encoded text put away in it results another image document, called "stegano image", that is really and outwardly not the same as from the first. Subsequently, an eavesdropper just sees an image that is moved between the two gatherings when a communication occur between them, yet they know nothing about the secret informing really happens by this image. Be that as it may, an image is aassortment of individual places, alluded to as pixels that establish different light powers in various region of the image. In an image, the pixels are introduced evenly column by line. Different shading plans utilize different number of bits for every pixel, called the bit depth. The littlest bit profundity in current shading plans is 8, or at least, to address the shade of every pixel 8 bits are utilized (comparing to 2^8 = 256 tones).

8 bits are utilized in monochrome and grayscale images for every pixel and can show 256 unique shades of grey. Digital shading images utilize 24-bit for every pixel and utilize the RGB shading model, otherwise called true color. Unique strategies can be utilized to conceal data in images. These techniques can be ordered under two headings, considering the information they use during inserting.

- Spatial or Image Domain Technique.
- Frequency or Transform Domain Technique.

In Spatial Domain or Image Domain, the pixels of the image document are straightforwardly different for installing secret information in it. An illustration of this strategy is the Least Significant Bit Insertion (LSB) technique, which is ordinarily utilized. In Transform Domain or Frequency Domain, the covered image is transformed in frequency domain from spatial domain and afterward its frequencies are utilized to conceal the secret data. In the wake of stowing away, the item is again transformed into spatial domain. An illustration of the Transform Domain procedure is the discrete wavelet transform (DWT) execution that utilizes a discrete arrangement of the wavelet scales and interpretations. To assess the nature of the strategy utilized for data stowing away, this exploration takes on various Standard boundaries to quantify the nature of images. The most well-known measures used to decide the nature of image are Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) measurements. MSE is to appraise the mean of the squares of the error between stego image and the first image [11].

PSNR is frequently utilized a s a quality estimation to decide the corruption in the implanting image as for the cover image, that is to say, the distinction between the first and the stego image [11].

Where Xij is the pixel in the first image (cover image) in ith line and jth segment, $X'ij$ is the pixel in the stego image in ith line and jth segment, MN is the size of the image where M is the height and N is the width also, I is the reach pixel esteem. For 8-bit images, I=255.

III.LITERATURE SURVEY

[1] In this paper, author utilize a two-layer security. From the beginning, information encryption is accomplished by the strategy for RSA algorithm of unbalanced cryptography, and later the encoded information is concealed into have picture by an inventive inserting method. To conceal our encoded information into have picture, we alter the current LSB method and utilize a mapping function that guarantees a secure and classified picture steganography coming about in a stego picture. Here cryptography is mixed with steganography as well asprovides two-level security in the private information transmission over the web.

[2] In this project, author presented point by point near study is performed between the proposed approach and the other best in class draws near. This examination depends on perception to identify any debasement in stego picture, trouble of extricating the inserted information by any unapproved watcher, Peak Signal-to-Noise Ratio (PSNR) of stego picture, and the installing algorithm CPU time. Test results shows that the proposed approach is safer contrasted and the other conventional methodologies.

[3] In this paper expected execution assessment of secrete picture steganography procedures involving LSB technique for information and picture security, its correlation on various size and images(.bmp; .jpg; .png) and work out its boundaries like PSNR and MSE for its to examine its hiding capacity with that of MATLAB execution, which is a strong strategy for information and picture security.

[4] In this paper, proposed work for the space area picture steganography. Here, alteration of least significant piece (LSB) of picture component of carrier-images (CI) is finished by the mean significantbit (MSB) of secret images (SI). Here, alongside data hiding, security is given by the powerful key cryptography. The unique element of key is empowered by turning the key and every revolution of key delivers new key. In this method, pixel determination of transporter picture and secret picture is done based on pseudo-random number (PRN) that provide twofold-layer security to provide the stegano-scientific-attack.

[5] In this paper, author propose an original system for generative steganography in view of autoregressive model, or rather, Pixel CNN. Hypothetical inference has been taken to demonstrate the security of the edge work. An improved-on variant is likewise proposed for double installing with lower intricacy, for which the examinations show that the proposed technique can oppose the current steganalysis strategies

[6] In this paper, author propose another picture steganography plot in view of a U-Net design. In the first place, as matched preparing, the prepared deep brain network incorporates a hiding organization and an extraction organization; then, at that point, the shipper utilizes the hiding organization to insert the secret picture into another regular picture with next to no alteration and sends it to the collection part. At last, the recipient utilizes the extraction organization to recreate the secret picture and unique cover picture accurately. The exploratory outcomes show that the proposed plot packs and disseminates the data of the installed secret picture into all suitable bits in the cover picture, which tackles the conspicuous viewable prompts issue, yet in addition builds the inserting capacity.

[7] In this paper, author's work centers around picture steganography which means hiding a picture (secret picture) inside one more picture of a similar size (cover picture). Preparation plot is proposed to accelerate the preparation stage. Through broad trials, it has been confirmed that the new organization design, joined with the new preparation technique, can brought about lower mean-square error of pixel distinguish though the preparation time is diminished considerably.

[8] In this paper, author make following three significant commitments: (I) Author propose a deep learning based conventional encoder-decoder design for picture steganography; (ii) Author present another misfortune function that guarantees joint start to finish preparing of encoder-decoder organizations; (iii) Author perform broad observational assessment of proposed engineering on a scope of testing openly accessible datasets (MNIST, CIFAR10, PASCAL-VOC12, ImageNet, LFW) and report cutting edge-payload capacity at higher PSNR as well asvalue of SSIM.

[9] In this paper, author consolidates late deep convolutional neural network strategies with picture into-picture steganography. Author shows that with the proposed strategy, the capacity can go up to 23.57 bpp (bits per pixel) by changing just 0.76% of the cover picture. Author applied a few conventional steganography investigation algorithms and figured out that the proposed strategy is very powerful.

[10] In this paper, author joins late deep convolutional brain network techniques with picture into-picture steganography. It effectively conceals a similar size picture with an unravelling pace of 98.2% or bpp (bits per pixel) of 23.57 by changing just 0.76% of the cover picture by and large. Our technique straightforwardly advances start to finish mappings between the cover picture and the implanted picture and between the secret picture and the decoded picture. Author further shows that our inserted picture, while with uber payload capacity, is as yet strong to factual investigation.

IV.PROPOSED METHODOLOGY

Various steps involved in image steganography such as image pre-processing, PVD algorithm, secret message hiding or embedding and decoding of secret message. These steps are illustrated in Fig 1.

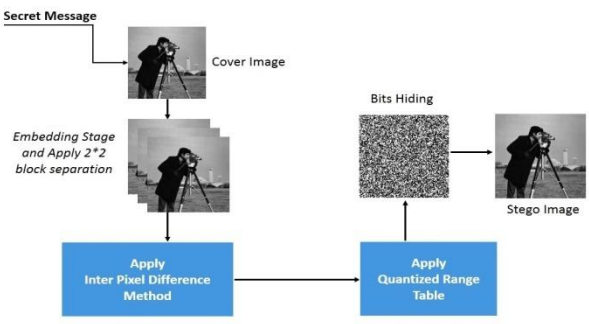

Fig. 1. Shows the sender side image steganography system architecture

1. Pixel Value Differencing Algorithm

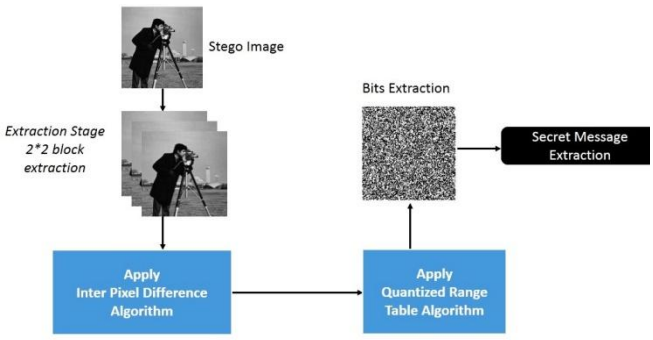

Fig. 2. Shows the receiver side image steganography system architecture

PVD used to hide secret information using 256 grey values images. PVD algorithm is so flexible that it can hide large amount of information without any degradation in image quality and thus the changes made by algorithm is hardly visible by human eyes. It depends on the way that natural eyes can undoubtedly notice little changes in the dim upsides of smooth regions in the picture however they can't notice somewhat bigger changes at the edge's regions. Fig. 3 and Fig. 4 shows the embedding process of PVD algorithm.

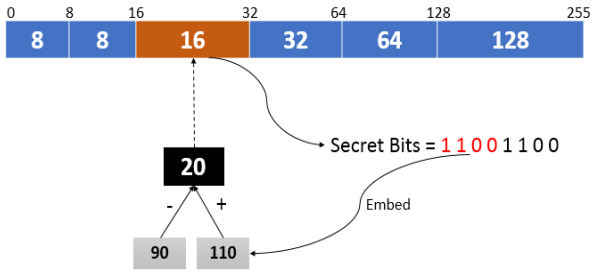

Fig. 3 Embedding Process Using PVD - Part-1

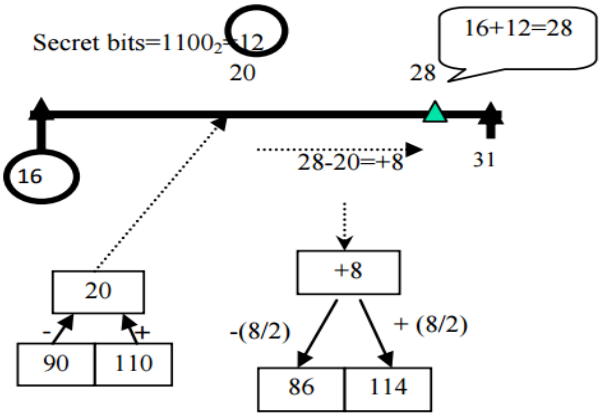

Fig. 4. Embedding Process Using PVD – Part-2

Algorithm PVD
Input: Cover-image C_i, secret data S.
Output: Stegano-image S_i.

Step 1. The cover-image is dividing into non-overlapping two-pixel blocks
$B = \{ B \mid i = 1, 2,3,\ldots(W \times H)/2 \}$. In every block, there consistsof two neighboring pixels p_i and p_i+1, and their respective gray values are g_0 and g_1, respectively.
Step 2. Transform S into a binary bit stream S'.
Step 3. $H_r(R_1, \alpha)$ and $H_c(R_2, \beta)$ are used to generatetwo binary sets K_r andK_c, respectively.
Step 4. Calculate Q as follows:

$$Q = (\alpha + \beta)$$

Step 5. For the first pixel p_i in the block, S_Q = Q bits of binary bit stream S'. After that, this SQ is divided into two sub-sets S_{Q1} and S_{Q2}, where S_{Q1} has α bitsand S_{Q2} has β bits.
Step 6. Find the metrics i and j utilizing $S_{Q1} = K_{ri}$ and $S_{Q2} = K_{cj}$, where K_{ri} and K_{cj} are ith and jth binary elements in K_r andK_c sets, respectively.
Step 7. Compute y as follows:

$$y = 2^{\beta} \times (i-1) + j$$

Step 8. Generate a pixel group G which is a subset of the pixel intensity set

$G = \{g_i \mid i = 1, 2, 3\ldots n\}$ and is generated as follows:

$f(p_i) = p_i \bmod n$, where $n = 2^Q$

Thus, the pixel group G is an ordered set
Step 9. For reducing perceptual distortion between the cover and stego images,we use "error reducing process". Let $L \in [-1, 0, 1]$ and $n = 2^Q$.
Step 10. Until now, we embed Q bits in the first pixel in the block B_i. Now,compute the difference value between p_i' and the second pixel p_i+1 in Bi.
Step 11. Find the corresponding sub-range R for the resulted differencevalue di from the dividing range table.
Step 12. If R_i belongs to the lower-level, then 3 secret data bits will be embeddedin the second pixel p_i+1. Unless 4 secret data bits will be embedded in thesecond pixel p_i+1. By considering t_i is the number of embedded secret data bits,then, read t_i bits from the binary bitstream S' and convert it into its decimal value.
Step 13. Compute the new difference value dd_i

$dd_i = l_i + s_i$

Step 14. Now, we are getting the stego-block consisting p_i' and p_{i+1}'. After that, repeat the steps from 5 to 14 for the next block until all secret data bits are completely embedded and the stego-image is obtained.

Data Extraction Process

The extraction engineering of the proposed framework for text record/picture document is same.
1. Parcel the stego-picture into the (2 x 2) sub-pixel blocks.
2. Parcel the stego-picture into the (2 x 2) sub-pixel blocks.
3. Observe the inserting pieces in view of the quantization range table of pixel distinction esteem.

4. Proceed with the process until we track down every one of the secret pieces as indicated by encoded record length. Exit from the extraction process.

V.RESULT AND DISCUSSION

We have analyzed image cameraman, Barbara girl image using Pixel Value Differential algorithm method by using range table quantization method. We have adjusted perfect square to hide secret data. The output of 2X2 segmentation generated are given in table II presents various metrics for validating performance of proposed steganography method.

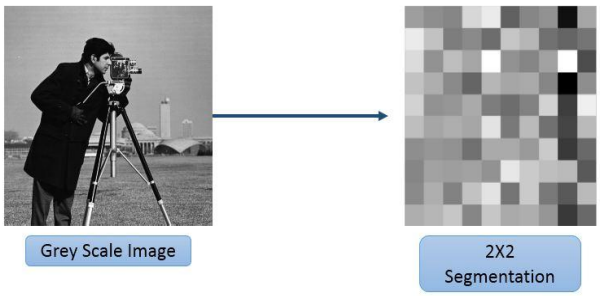

Fig. 5. Shows the 2X2 segmentation of image cameraman

The output image quality is calculated by the PSNR. The PSNR formula is defined as

$$\mathbf{PSNR} = -10 log_{10} \frac{e_{MSE}}{S^2}$$

Where MSE is the mean square error between the cover and stego images. For a cover image, whose width and height are w and h, then MSE is defined as

$$e_{MSE} = \frac{1}{MN} \sum_{n=1}^{M} \sum_{m=1}^{N} [\hat{g}(n,m) - g(n,m)]^2$$

Where $s(i, j)$ denotes pixel value from stego images and $c(i, j)$ denotes pixel values from cover images respectively. PSNR and MSE values of the 70,827 bytes (70KB) image capacities for embedding data by using the cover Images. All images are 512x512 and 256x256 and two set of width ranges are used for gray values (Table II).

Table 2. Shows PSNR value and time required for execution of algorithm

Image	Size	Execution time	PSNR
cameraman.tif	256 X 256	20.191 sec	37.9908 dB
barbara.png	512 X 512	20.54 sec	71.0068 dB

The experimental results shows that our proposed algorithm effectively process our images and transform it into another form where the secret bits are hidden. We also have computed the computation time of our algorithm to show how much time is required for processing of job. We have validated our work with PSNR value. The PSNR describes about image quality. The higher is the PSNR value, the higher will be the quality of image.

VI.CONCLUSION

We have proposed a novel method by combining two different method namely, Pixel Value Differencing and Range Table Quantization. Both method tries to hide secret bits into image in more efficient and robust way. Traditionally the data bits are hidden only using Pixel Value Differencing method, which helps hacker to bypass the algorithm by hit and trial method. In combination with range table quantization method, the hacker need to do some extra effort to break the algorithm. Due to the time limit, several interesting ideas have not been implemented yet. However, it will be worthwhile trying them in the future. One of the foremost thing I would like to improve is to apply steganography for 3D images using for Pixel Value Differencing Algorithm.

REFERENCES

[1]. Lee YP, Lee J-C, ChenW-K, Chang K-C, Su I-J, Chang C-P, "High Payload Image Hiding With Quality Recovery Using Tri-Way Pixel Value Differencing," Information Sciences, vol. 191, pp. 214-225, 2012.

[2]. Hsien-Wen Tseng and Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Journal of Applied Mathematics, 2013.

[3]. Wu D-C and Tsai W-H., "A Steganographic Method For Images By Pixel Value Differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.

[4]. El Sayed M. El Alfy and Azzat A. Al-Sadi, "Improved Pixel Value Differencing Steganography Using Logistic Chaotic Map," Innovations in Information Technology, 2012.

[5]. H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic Scheme Based On Pixel-Value Differencing and LSB Replacement Methods," IEEE Proceedings-Vision, Image and Signal Processing, vol. 152, No. 5, pp. 611- 615, 2005.

[6]. Weiqi Luo, Fangjun Huang, Jiwu Huang, "A More Secure Steganography Based On Adaptive Pixel-Value Differencing Scheme," Multimedia Tools and Applications, vol. 52, pp. 407-430, 2011.

[7]. C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, "A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Function," Journal of Systems and Software, vol. 81, pp. 150-158, 2008.

[8]. C.Y. Weng, H.K. Tso and S.J. Wang, "Steganographic Data Hiding in Image Processing

using Predictive Differencing," Opto-Electronics Review, vol. 20, pp. 126-133, 2012.

[9]. J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain," International Journal of Information Sciences and Techniques, vol. 2, 2012.

[10]. Yuan-Yu Tsai, Jian-Ting Chen, and Chi-Shiang Chan, "Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding," International Journal of Network Security, vol. 16, pp. 363-368, 2014.

[11]. Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang and Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488-497, 2008.

[12]. S. Pramanik, D. Samanta, S. Dutta, R. Ghosh, M. Ghonge and D. Pandey, "Steganography using Improved LSB Approach and Asymmetric Cryptography," 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), 2020, pp. 1-5, doi: 10.1109/ICATMRI51801.2020.9398408

[13]. K.A.AlAfandy,O.S. Faragallah, A.Elmhalawy, E.-S. M.El-Rabaie, and G.M.El-Banby,‘‘High security data hiding using image cropping and LSB least significant bit steganography,’’ in Proc. 4th IEEE Int. Colloq. Inf.Sci. Technol. (CiSt), Oct. 2016, pp.400–404.

[14]. Arya and S. Soni, ‘‘Performance evaluation of secrete image steganog- raphy techniques using least significant bit(LSB)method,’’*Int.J.Comput. Sci.* Trends Technol., vol. 6, no. 2, pp. 160–165,2018.

[15]. N. Patel and S. Meena, ‘‘LSB based image steganography using dynamic key cryptography,’’ in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 2016, pp.1–5.

[16]. K. Yang, K. Chen, W. Zhang, and N. Yu, ‘‘Provably secure generative steganography based on autoregressive model,’’ in Proc. Int. Workshop Digit. Watermarking. Cham, Switzerland: Springer, 2018, pp.55–68.

[17]. X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ‘‘Reversible image steganography scheme based on a U-Net structure,’’ IEEE Access, vol. 7, pp. 9314–9323, 2019.

[18]. T.P.Van,T.H.Dinh,andT.M.Thanh,‘‘Simultaneousco nvolutionalneural network for highly efficient image steganography,’’inProc.19thInt.Symp. Commun. Inf. Technol. (ISCIT), Sep. 2019, pp.410–415.

[19]. R. Rahim and S. Nadeem, ‘‘End-to-end trained CNN encoder-decoder networks for image steganography,’’ in Proc. Eur. Conf. Comput. Vis. (ECCV), 2018, pp. 1–6.

[20]. P. Wu, Y. Yang, and X. Li, ‘‘Image-into-image steganography using deep convolutional network,’’ in Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland: Springer, 2018, pp.792–802.

[21]. P. Wu, Y. Yang, and X. Li, ‘‘StegNet: Mega image steganography capacity with deep convolutional network,’’ Future Internet, vol. 10, no. 6, p. 54, June 2018