Review Article

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology

2020
Vol.8 No.2:51

DOI: DOI: 10.36648/2349-3917.8.2.51

Image Steganography Using Bit Differencing Technique

Mudasir Rashid* and Bhavna Arora

Department of Computer Science and Engineering, Central University of Jammu, Samba, 181143, India

***Corresponding author**: Rashid M, Department of Computer Science and Engineering, Central university of Jammu, Samba, 181143, India, E-mail: mudasircse28@gmail.com

Received date: May 28, 2020; **Accepted date:** June 11, 2020; **Published date:** June 17, 2020

Citation: Rashid M, Arora B (2020) Image Steganography Using Bit Differencing Technique. Am J Compt Sci Inform Technol Vol.8 No.2: 51

Abstract

The swift progression of evidence correspondence in contemporary time demands protected communication of data. Steganography obscures personal material in numerous record organizations, for example, photograph, content, sound, and audio-visual, impalpability, payload and vigour are the key complications on the way to steganography.

This proposed work would give a nascent procedure that could be used for storing imperative data inside some cover metaphors by means of most significant bits (MSB) of the cover metaphors has been presented. The Pixel indicator method is used for storing confidential information in most significant bits (MSB) of the original photograph. Here, the picture is fragmented into red, green and blue components where red components used for signalling on the way to store information in green or blue components of the portrait. The proposed method built on Most significant bits (MSB) is used for safeguarding the organization from unauthorised admittance and the interlopers would not be intelligent to admittance the intimate data.

Keywords: Steganography; Algorithm; Memorandum; Data

Introduction

Information safekeeping is imperative for the broadcasting of top-secret evidence. Steganography is a substantial zone of investigation in image processing together with numerous outcomes. Steganographic techniques are the ways of using original pictures for storing essential and important information though there is not any change in the original image's appearance.

Methodology

Steganography and cryptography are the procedures for making certain about the cataloguing and anonymous information. In cryptography, anonymous content is reformed into figure content, even though in steganography, the anonymous content endures as formerly nevertheless it is set in one more association of information. Currently, within the view of absurd correspondence outlines, defending the anonymous information from the interlopers is a problematic task. The anonymous data that is to be taken from the developers is a tough task. Steganography obscures existence of the information and safeguard anonymous information from an unapproved get to. The information hiding structure encompasses the following subcomponents: the important message to be stored, an original image in which to store the data, and the resulted hidden image or text [1]. Mystery data to be encoded is known as plain content. Original document can be content, picture, sound or video in which information is hidden **Figure 1**. Steganographic records the yield of the steganographic framework that contains the concealed data. The three central merits of a steganographic structures are: (1) Safekeeping, (2) Payload Capacity, and (3) Strength.

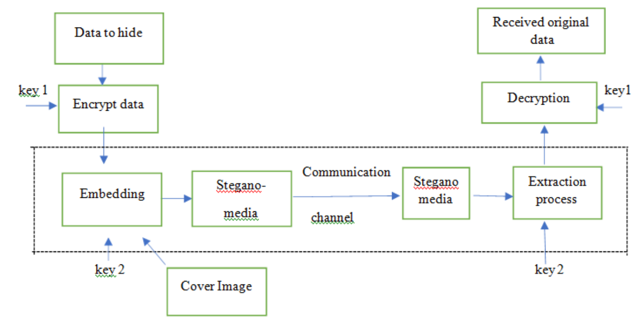

Figure 1: Block Diagram of Image Steganography.

Image Steganography Techniques

Keeping overview of the scrutiny of steganography implemented procedures, all tools are panelled into two groupings:

- Spatial domain-based steganography
- Transform domain-based steganography

Spatial domain based steganography

Spatial steganography fundamentally integrates LSB (Least Significant Bit), this form of addition is a representative, straight forward mode to pact with implanting information in a concealment portrait. The least significant bit (the eighth bit) of a rare or the total of the bytes inside a portrait is altered to a bit of the secret memorandum.

Pixel: (101011111110100110101000)

(101001110101100011101001)

(110110001000011101011001)

Secretmessage: 01000001

Result: (101011101110100110101000)

(101001100101100011101000)

(110110001000011101011001)

Transform domain based steganography

Principally, there are frequent categories of intensity level changes that occur to transfer a portrait to a reappearance range, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform. Transform Domain policies have an ideal location over LSB structures is nice they obscure information in regions of the portrait that are a lesser amount of offered to pressure, trimming, and picture preparing.

The Discrete Cosine Transform (DCT)

These measured transforms translate the pixels so as to stretch the effect of "scattering" the portion of the pixel over representation [2]. The DCT fluctuates a symbol from a portrait illustration into a replication illustration, by gathering the pixels into 8 × 8-pixel squares and altering the pixel barricades into 64 DCT. DCTs operated in steganography as- image is fragmented into 8×8 squares of pixels. Working from left to right, top to bottom, the DCTs are useful to each square. Each square is jam-packed through quantization table to scale the DCT coefficients and message is implanted in DCT coefficients.

The Discrete Wavelet Transform (DWT)

Wavelets transformation (WT) varies over spatial space information to the reappearance range information. Wavelets are useful in the portrait steganographic model on the estates that the wavelet alteration purely parts the high -relapse and low-relapse statistics on a pixel by pixel premise. This structure injects important files or information in the control and point areas of the portrait. When all is said and done, the human eye is more and more quick-tempered to disorder in the horizontal quarters of a portrait.

Results and Discussion

In the paper, summary of image steganography, its applications and procedures are presented. Most of the strong and weak points related to important image files with diverse procedures of storing messages are given in which one method deficient in payload dimensions whereas other deficient in robustness but together upsurges the possibility recognition [3].

The authors Chandramoul R et al. [4] provides new and efficient ways of steganography using least significant bit (LSB) of image pixels. This paper also provides the detection capability for the number of bits being used for embedding prior the user can make difference between hidden image and cover image.

The paper presents the overview investigation to discuss the various effective parameter of the given techniques. The effectiveness of the parameters is assessed using Mean square error[5].

(MSE) and Peak Signal to Noise Ratio (PSNR), Processing time, security. The results disclosed that Discrete cosine transform is superlative technique.

The paper [6] gives some important standards and guidelines computed using the overview investigation and provides up-to-the-minute appraisal and scrutiny of the methods used by steganography. The conclusion of the paper provides acclamation for the object-oriented technique.

This paper [7] presents the procedures used for Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) and the authors have provided various practices used for hiding information or some undisclosed files in the image file formats. The evaluation of results has been performed to know which procedure is good for image hiding.

The authors Islam et al. [8] has presented technique for hiding essential information using most significant bits (MSB) of image pixels. The difference between bit number 5 and bit number 6 is calculated and if the outcome is unalike from that of secret data bit. Then, value of bit number 5 is altered. The consequences generated from the above investigation reveals that the projected method advances signal to noise ratio. The paper assesses several methods and techniques used in stegano scrutiny, notions and techniques used in spatial representation [9]. Altogether the probable imminent exploration drifts related to steganography safekeeping and substantiation abilities are summarised.

The Josh et al. [10] recommends novel technique of image coding by loading data in the carefully chosen pixel and on the succeeding value of the designated pixel. selected pixel is used to accumulate the primary bit of the data and pixel+1 value is used to store another bit of the data. The pixel+1 variable is generated by applying mathematical function on the 7th bit of image data.

This paper [11] analyses the existing image steganographic techniques and its types. Moreover, contribution of various modalities of these techniques are concerned. General procedure, necessities, different characteristics, different categories and their routine estimations regarding to image steganography are overviewed.

The authors Xaozhong, et al. [12] overviews all the steganographic approaches (current steganographic methods, such as F5, Outguess, Steghide, JPhide and Jsteg) used for several JPEG images and their suitable arrangement has been done. Furthermore, the cataloguing of wholly varieties of steganographic images has been performed by the proposed algorithm to detect 109 features and trans SVM. Coloured steganography created on DCT and a universal adaptive-reg ion (GAR) is presented in paper [13]. in this method, the same area under unique image coefficients and mystery data is realised. The main advantages of using this method is increased payload capacity among most steganographic techniques is gained. Histogram technique is used for data hiding in the paper [14]. In this paper, pixels are mainly characterised based on image characteristics. From the smooth region, a smaller number of pixels are selected whereas huge fidelity requires large number of pixels.

The authors in paper [15] has proposed the called as speeded up robust features (SURF) used for detecting the important regions in the cover image. Steganography process is completed by modulating the secret data by using wavelet coefficients. A genetic scheme for detecting the optimum regions from the cover image is used in the paper [16]. Then secret bit embedded randomly based key using steganography based on LSB replacement. In the paper [17], The reduction in the difference between cover image and steganographic image is done by using pixel modification algorithm whereas LSB method is used for embedding secret data.

The new and amended method has been proposed in the paper [18] which is used for addressing the various problems related to data hiding which were not addressed yet like step of security, key size and pay-load capacity. The authors in the paper [19] has proposed a novel algorithm known as Blowfish encryption algorithm which is used for improving proficiency and safekeeping. The undisclosed data is encoded using blowfish algorithm formerly implanting the message.

A novel technique has been proposed in the paper [20] which is resulted from the grouping of steganography and cryptography. Cipher scheme is used for coding the data and the resultant data is implanted inside image via LSB method. In the paper [21], the author has proposed a new method by grouping steganography and cryptography. In this technique, Jamal encryption algorithm has been used as crypto-graphic algorithm and LSB technique with 128 bit sego-key has been used as stegano-graphic algorithm.

A new technique for hiding the confidential data has been proposed in the paper [22] which addresses the pixel values of every image that has been used in the experiment.

Problem statement

In the new era of communication and expertise, perception of steganography is a very decisive and vital idea to be understood by the innovators and programmers. To explore the security and substantiation concerns in the communication, first concept known as LSB based hiding was introduced due to its easiness of usage. Though, the idea has several numbers of drawbacks regarding to the security, this concept is applicable all over the world to get the evidence conveyed from one user to other. To upsurge the efficiency and security of the system, most significant bit (MSB) based image steganography procedure has been proposed which uses 16-bit image file to store and hide the significant data. By the applications and calculations of the proposed system, the hidden data could be shifted from one user to other user lacking the intervention of any other unauthorised third party. In the prosed system, the surreptitious data would be warehoused in the calculated MSB of the cover file.

Demerits of LSB based image Steganography: The information being transferred using this concept could be easily attacked by the attackers. The attackers could get the LSBs of the original file to generate image.

This concept was used since other efficient techniques were not discovered yet and it is very less efficient as compared to other techniques.

In case of LSB based image hiding, if several number of LSBs are used for storing the important information, the quality may get decreased so it is not preferably used.

- The MSB based image hiding is preferred as compared to LSB based image hiding because the interlopers cannot decrypt the Image or file simply by generating MSB of the picture.

This encryption technique is more difficult to use in image hiding because it was made to remove the complexity of the LSB based image hiding so the interlopers could not attack this type of encoding.

This technique removes the drawback of the LSB based image hiding because more than one MSBs can be used to store the data files without degrading the original image's quality Based on the existing solutions, we highlight the advantages and disadvantages of classification methods in **Table 1** and various image steganography techniques in **Table 2**. These solutions make balance between different attributes like Security, Payload capacity, Data Capacity etc So, depending on the situations, the best feasible solution must be chosen.

Table 1: Comparison of various steganographic classification method.

References	Classification Technique	Method Explanation	Advantages	Disadvantages
Rabe and Kame[13]	Region based - Transform domain-DCT	Coloured steganography is built on DCT and universal adaptive-region (GAR).	Sophisticated payload dimensions.-Adequate noiselessness	Deprived security. - reduced amount of corroboration for pictures being used.

Q n et al.[14]	Region grounded-Spatial domain-Histogram Alteration	-Histogram move technique is used for data hiding. The estimate model used is based on image inpainting.	As the reference points on the receiving end are correctly identified so accuracy is guaranteed.	Lower payload capacity. Geometric and compress ion attacks are less concerned.
Hamd et al.[15]	Regi on based-Transform domain-DWT	-Detecting the most important regions in the cover image, the method called as Speeded Up Robust Features (SURF) is used.	Even if the image is modified by the attacks, The SURF can be used to identify the points.	-The total keeping data capacity is not as per requirement.
Shah and Bichkar [16]	Spatial domain-LSB- Genetic Algorithm	A genetic scheme for detecting the optimum reg ions from the cover image is used then secret bit embedded randomly based key using steganography based on LSB replacement.	Higher state of being imperceptible Number of cryptographic techniques are used to increase security.H18	High complexity
Bandyopadhyay [17]	A -Spatial domain-LSB- GA	The reduction in the difference between cover image and steganographic image is done by using pixel modification algorithm whereas LSB method is used for embedding secret data.	Higher state of being imperceptible.More Robust against histogram and	it is least concerned about the geometric modifications.

Table 2: Review of various image Steganography Techniques.

	Technique	Advantages	Disadvantages
Spatial domain	Least Significant bit (LSB)	Simpler to use for encoding and decoding of data. Good payload capacity	Poor defence against geometric, compression and statistical attacks. Lack of security
	Pixel valuedetector (PVD)	High encoding capacity.	Poor defence against geometric, compress on and statistical attacks.
	Difference Expansion	Better embedding capacity. Better visual quality compare to previous techniques.	Need large location data for extracting secret data. Poor control of capacity
Transform Domain	Discrete Fourier Transform (DFT)	Simple transform domain that used in data hiding Technique	Poor embedding capacity Less visual quality Lack of security
	Discrete Cosi ne Transform (DCT)	Better visual quality than DFT	Poor embedding capacity Lake of security Poor robustness against attack

Conclusion

In this work, we have studied fundamentals of steganography, several classification approaches and dissimilar steganographic procedures. in addition, this effort presents a steganographic policy using grey-colour image as a concealment medium. MSBs are used to obscure surreptitious message inside cover image to upsurge the safekeeping of the procedure as an alternative of entrenching message inaugural after maximum leftward crook or lowest right, dominant port on is carefully chosen for implanting. providing more robustness to the technique.

References

1. Khan Z, Shah M, Naeem M, Mahmood T, Khan SNA, et al. (2016) Threshold based Steganography: A Novel Technique for improved Payload and SNR", International Arab J inform Technol 13: 380-386.
2. Ankur MM, Lanz sera S, Krstofer SJP (2016) Steganography Wireless Communication 802: 15: 4.
3. Morkel T, Eloff JHP, Oliver MS (2015) An over view of image steganography. Information and Computer Security Architecture (CSA) Research Group.
4. Chandramoul R, Memon (2014) Ananalysis of lsb based image steganography techniques. IEEE :7803-6725.
5. Kaur G, Kochhar A (2012) ASteganography implementation based on LSB & DCT", International Journal for Science and Emerging Technologies with Latest Trends 4: 35-44.
6. Cheddad A, Condell J, Curran K, McKett P (2010) Digital image steganography: Survey and analysis of Current methods. Signal Processing ELSEIVER 90727–90752.
7. Kaur N, Bansal A (2014) A review on Digital image Steganography (JCST). International J Comput Sci inform Technolo 5 :8135-8137.
8. Islam AUl, Khalid F, Shah M, Khan Z , Toqeer Mahmood, et al. (2016) An improved image Steganography Technique based on MSB using Bit Differencing IEEE 978-98.
9. Bn L , Junhu H, wu Huang J, Qngsh Y (2017) A Survey on image Steganography and Steganalysis J Inform Hiding Multimedia Signal Process 2.
10. Josh K, Gill S, Yadav RA (2018) New Method of image Steganography Using 7th B it of a Pixel as indicator by introducing the Successive Temporary Pixel in the Gray Scale image. Hindaw J Comput Networks Commun 2018.
11. Kadh m NJ, Premaratne P, Vial PJ, Halloran, B (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research Neurocomputing 335 : 299–326.
12. Xaozhong P, Yan BT, Ke NU (2010) Multiclass Detect of Current Steganographic Methods for JPEG Format Based Re-stegnography IEEE :4244-5848.
13. Rabe T, Kamel B (2017) High-capacity steganography: A global-adaptive-region discrete cosine transform approach Multimedia Tools Applications. Springer Science 76 :6473–6493.
14. Cheng PH , Chang KC , L u CH (2017) A reversible data hiding scheme for VQ ndces using histogram shifting of prediction error. Multimedia Tools Applications 76 :6031–6050

15. Hamd N, Yahya A, Ahmad AB, Al-Qersh O (2012) Characteristic Region Based image Steganography Using Speeded-Up Robust Features Technique 2012. Int: Conference on Future Communication Networks.

16. Prat k D. Shah , Bichkar RS (2018) A Secure Spatial Domain image Steganography Using Genetic Algorithm and Linear Congruential Generator. International Conference on intelligent Computing and Applications, Advances in intelligent Systems and Computing 632.

17. Prasad BD, Dasgupta KK, Mandal JK, Dutta P, Ojha VK, et al. (2014) A Framework of Secured and Bio- inspired image Steganography Using Chaotic Encryption with Genetic Algorthim Optimization (CEGAO) Proceedings: of the Fifth international. Conference on innovations. in Bio- inspired Computing. and Applications. B CA 2014, Advances in intelligent Systems and Computing 303.

18. Rahna E, Govindan VK (2013) A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage. Int J Adv Engineer & Technol 6: 1263.

19. Barhoom TS, Abo Mousa SM (2015) A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm. Int J Res Engineer Sci 3: 61-66.

20. Laskar SA and Hemachandran K High (2012) Capacity data hiding using LSB Stegano- graphy and Encryption. Int. J. Database Manag. Syst 4.

21. Al-Qwider WH, Bani Salameh JN (2017) Novel Technique For Securing Data Communication Systems By Using Cryptography And Steganography. Jordanian J Comput Inform Technol 3.

22. Khan Z, Shah M, Naeem M, Mahmood T, Ali Khan SN, et al. (2016) Threshold-based Steganography: A Novel Technique for Improved Payload and SNR.