

SECURE LSB STEGANOGRAPHY FOR COLORED IMAGES USING CHARACTER-COLOR MAPPING

1.SHIKHA TIWARI

Research Scholar, Department of Computer Science,

Institute of Engineering & Technology, Dr.R.M.L Awadh University, Ayodhya, U.P. India.

AKANKSHA TIWARI

Research Scholar, Department of Computer Science,

Institute of Engineering & Technology, Dr.R.M.L Awadh University, Ayodhya, U.P. India.

NEHAL AGRAWAL

Research Scholar, Department of Computer Science,

Institute of Engineering & Technology, Dr.R.M.L Awadh University, Ayodhya, U.P. India.

RITIMA VISHVASH

Research Scholar, Department of Computer Science,

Institute of Engineering & Technology, Dr.R.M.L Awadh University, Ayodhya, U.P. India

Abstract : In Steganography is the science of embedding the secret messages inside other medium files in a way that hides the existence of the secret message at all Steganography can be applied to text, audio, image, and video file types. In this study, we propose a new steganography approach for digital images in which the RGB coloring model was used. The efficiency of the proposed approach has been tested and evaluated. The experimental results show that the proposed approach produce high-quality

stegano images that resist against visual and statistical attacks.

Keywords: Secure Reversible Data Hiding, Digital Image Steganography, Reversible data hiding

Secure Reversible Data Hiding (SRDH) has been seriously considered in the group of data handling. Additionally eluded as invertible or lossless information concealing, Reversible Data Hiding (RDH) is to install a snippet of data into a host flag to produce the stamped one, from which the first flag can be precisely recouped subsequent to removing the inserted information. The procedure of RDH is valuable in some delicate applications where no perpetual change is permitted on the host flag. In the writing, the greater part of

I. INTRODUCTION

the proposed calculations is for computerized pictures to implant undetectable information or a noticeable watermark. Computerized sight and sound is the most widely recognized kind of data transmission over the Internet. In the most recent decade, the appearance of the advanced period the expansion of PCs and the boundless use of the Internet have made the computerized sight and sound a host for solid information transmission. These days, information installing in computerized sight and sound has been connected in

numerous security applications running from advanced watermarking, mystery correspondences, copyright assurance, to content confirmation. Steganography alludes to the strategy of concealing data in advanced media to hide the presence of the data [2].

In steganography, there are two sorts of segments: the mystery information, and the computerized media (i.e. the bearer that will hold the

message). The media with and without shrouded data are called stego media and cover media, separately [22]. Picture Steganography is the field of steganography in which a computerized picture is utilized to convey the mystery information. Current steganography tries to be distinguishable just if the mystery data is known, mystery keys are shared between the sender and beneficiary [3].

II. LITERATURE REVIEW

1. Z Ni, YQ Shi, N. Ansari, W Su - Reversible data hiding, IEEE, 2006 The computational multifaceted nature of our proposed procedure is low and the execution time is short. The calculation has been effectively connected to an extensive variety of pictures, including regularly utilized pictures, restorative pictures, surface pictures, aeronautical pictures and the majority of the 1096 pictures in CorelDraw database. Trial results and execution examination with other reversible information concealing plans are displayed to show the legitimacy of the proposed calculation.

2. D. Coltuc and J.-M. Chassery - Very quick watermarking by reversible complexity mapping, IEEE, 2007 A spatial area reversible watermarking giving high information implanting bit-rate at a low numerical many-sided quality has been examined. The proposed scheme does not require extra information pressure. As far as installing bit-rates, the proposed scheme to a great extent beats the majority of the reversible watermarking plans revealed in the writing and gives nearly a similar piece rate as the distinction development plan and its augmentations. As far as scientific multifaceted nature, the proposed reversible watermarking shows up just like the most reduced intricacy plot proposed up until now. The computational multifaceted nature is lessened for both checking and disentangling by utilizing LUT access for each match of pixels and some low unpredictability bit control. This makes our plan extremely proper for constant applications. At long last, by appropriating the area delineate by putting away the spared genuine qualities near the relating pixel combines, the RCM scheme gives strength against editing.

3. Jarno Mielikainen, LSB Matching Revisited, IEEE, 2006 This letter proposes a change to the minimum critical piece (LSB) coordinating, a steganographic technique for installing message bits into a still picture. In the LSB coordinating, the decision of whether to include or subtract one from the cover picture pixel is arbitrary. The new strategy utilizes the decision to set a twofold capacity of two cover pixels to the coveted esteem. The implanting is performed utilizing a couple of pixels as a unit, where the LSB of the main pixel conveys one piece of data, and an

element of the two pixel esteems conveys another piece of data. Hence, the adjusted technique permits implanting an indistinguishable payload from LSB coordinating however with less changes to the cover picture. The test consequences of the proposed strategy indicate preferred execution over conventional LSB coordinating as far as twisting and obstruction against existing steganalysis.

4. Shilpa Gupta, Geeta Gujral, Enhanced Least Significant Bit calculation For Image Steganography, IJCEM, 2012 The quick improvement of information exchange through web has made it simpler to send the information exact and speedier to the goal, however to exchange the information safely to the goal with no alterations, there are numerous methodologies like steganography. This paper presents the idea of steganography utilizing another Algorithm "Upgraded LSB Algorithm", which has careless contortion when contrasted with the Least Significant Bit Algorithm.

5. Mamta Jain, Saroj Kumar Lenka, Secret Data Transmission utilizing Vital Image Steganography over Transposition Cipher, IEEE, 2015 The thought behind this paper portrays a methodology about mystery interface over the globalization of the correspondence over the world. To achieve this marvel, two assortments of security component, cryptography and steganography is being connected. At the previous stage, encryption is being given to mystery plain content utilizing Vernam cipher (One-Time Pad) transposition system, since Vernam cipher demonstrate great execution measurements regarding less CPU running time, file estimate same after encryption and solid torrential slide impact contrast and all transposition cipher. Furthermore, at the later stage, it change cipher content into bytes and partitions every byte into sets of bits and relegates the decimal qualities to every match, which is known as ace variable. ace variable esteem range will be change between 0 to 3. Contingent on the ace sketchy esteem, include that cipher message in the vocation picture in any event Significant Bit (LSB) sixth furthermore, seventh bit area or seventh furthermore, eighth bit area or seventh furthermore, sixth or then again eighth furthermore, seventh bit area. Which demonstrates the installing area dynamicity of the

calculation relies on progressively changed ace variable esteem. After fulfillment of installing and sending the stego picture to the recipient side, recovering procedure of the figure content from the said areas will be finished. And afterward unscrambling procedure to recover the mystery plain content will be performed utilizing the Vernam figure transposition calculations. In this we give vigorous picture steganography. Execution investigation watched utilizing MSE and PSNR esteem.

6. Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm, IMECS, 2011 This paper displays the use of Wavelet Transform and Genetic Algorithm in a novel steganography plot. We utilize a

7. Ahmad T. Al-Taani and Abdullah M. AL-Issa, A Novel Steganographic Method for Gray-Level Images, IJCISSE, 2009 In this work we propose a novel Steganographic technique for concealing data inside the spatial space of the dim scale picture. The proposed approach works by separating the cover into squares of equivalent sizes and after that implants the message in the edge of the square contingent upon the quantity of ones in left four bits of the pixel. The proposed approach is tried on a database comprises of 100 distinct pictures. Exploratory outcomes, contrasted and different strategies, demonstrated that the proposed approach shroud all the more vast data and gave a decent visual quality stego-picture that can be seen by human eyes.

8. Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad, Key Dependent Image Steganography Using Edge Detection, IEEE, 2014

III. PROPOSED SYSTEM

To our best learning, there is no current RDH calculation that plays out the undertaking of differentiation upgrade in order to enhance the visual nature of host pictures. So in this examination, we go for designing another RDH calculation to accomplish

IV. SYSTEM ARCHITECTURE

Framework advancement showing is the determined setup that depicts the structure and conduct of a framework. A building design portrayal is a formal depiction of a structure, managed in a way those sponsorships contemplating the central properties of the framework. It depicts the framework segments or building pieces and gives a course

hereditary calculation based mapping capacity to implant information in Discrete Wavelet Transform coefficients in 4x4 squares on the cover picture. The ideal pixel alteration process is connected in the wake of installing the message. We use the recurrence area to enhance the vigor of steganography and, we execute Genetic Algorithm and Optimal Pixel Adjustment Process to acquire an ideal mapping capacity to lessen the distinction along these lines enhancing the concealing limit with low mutilations. Our Simulation blunder between the cover and the stego-picture, comes about uncover that the novel plan outflanks versatile steganography method in view of wavelet change as far as pinnacle flag to clamor proportion and limit, 39.94 dB and half individually.

Steganography is the exploration of imperceptible correspondence. It goes for concealing touchy data in advanced media in an approach to disguise the presence of data. In this paper, we intended to propose an enhanced secured picture steganography conspire as of late given by Chen et al. The enhanced plan is mystery key based irregular LSB substitution. It likewise takes the upsides of edge recognition based pixel reliance to accomplish high installing information limit. The analysis comes about demonstrate that the proposed conspire likewise accomplishes high inserting limit. High scores of PSNR uncover that there is no discernible contrast between cover picture and stego-picture. Also, the proposed enhanced plan is powerful and can shield adequately the inserted message from being steganalysis because of the commencement of irregularity, pixel reliance and key reliance.

the property of difference improvement rather than simply keeping the PSNR esteem high. Consequently this task will conceal mystery information in computerized pictures utilizing histogram strategy. The concealed information can be separated from stegano picture without influencing the visual nature of the picture.

of action from which things could be gotten, and structures built up, that will take an interest to execute the general framework. The System design is demonstrated as follows.

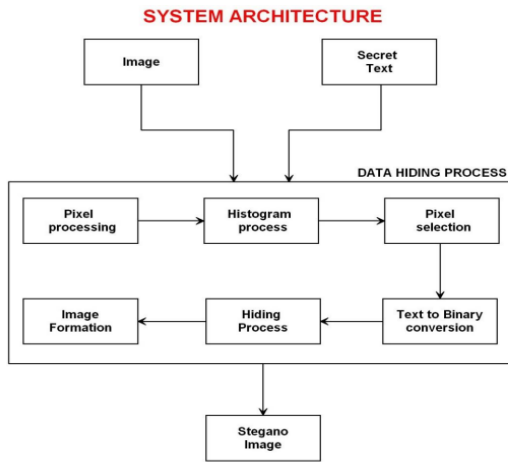


Figure 5.1: System Architecture

Fig 01: Working Model of Proposed System

V. DATA HIDING

The user selects the original image in which the user wishes to embed data. The user uploads the image as well as the secret text the user wants to store in the image. Image is scanned completely on the x-axis and y-axis to find out the pixels which contain the highest histogram value (value ranges from 0-255). Pixels having the highest histogram values are selected for hiding the data, the data is hidden in the LSB bits of the pixels. Secret message is converted into its equivalent ASCII and then into its binary

values. Each character requires 4 pixels to store. Before hiding of image a key is used which

tells us about the no of pixels we need to read in order to retrieve back the data so that we do not waste timing in reading all the pixels to search for the characters. After the key and the secret text is embedded in the image the user is provided with a stegano image which is the image which can be transferred without any information leak and the image quality is retained.

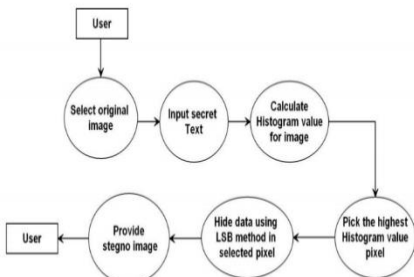


Figure 5.3: Flow diagram on Data Hiding

VI. DATA RETRIVAL

In order to retrieve back the text, the user needs to provide both the original image and stegano image. Both the images are scanned and the pixels of both the images are compared. The pixels with the highest histogram values are selected and then first the key is retrieved which tells us how many pixels

we need to read in order to retrieve back the text. The Pixels which have highest histogram are selected and the last two bits are retrieved and combined from the next 3 subsequent to retrieve and single character and similarly the entire message is retrieved back and the image quality is retained.

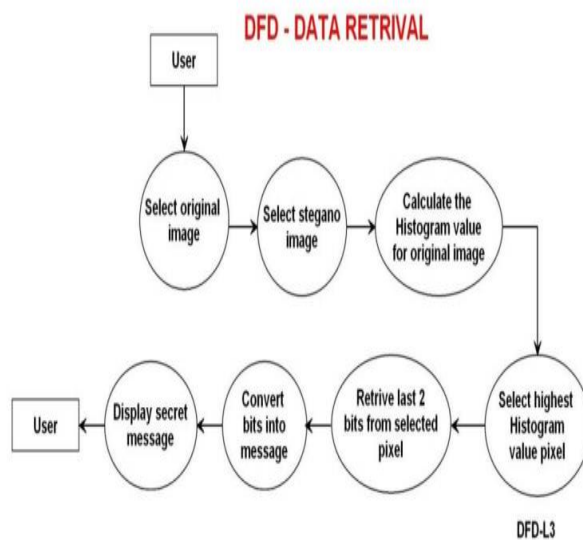


Figure 5.4: Flow diagram on Data Retrieval

VII. RESULT AND DISCUSSION

The accompanying depictions layout the outcomes or yields that we are going to get once regulated execution of the considerable number of modules of the framework. Another reversible information concealing calculation has been proposed with the property of differentiation upgrade. Essentially, the two tops in the histogram are chosen for information implanting with the goal that histogram evening out can be all the while performed by rehashing the procedure. The information is put away in the LSB of the pixels and each character is put away in four pixels. Changing the LSB of the pixels does not influence much in the complexity or the nature of the pictures since a slight variety in the RGB esteem would not influence or be seen by the client. In our undertaking a safe method for transmission of a mystery message is accomplished in which no gatecrasher can think about the data being traded. The trial comes about have demonstrated that the picture complexity can be upgraded by part various histogram tops match by combine. Contrasted and the other existing procedures, the visual nature of the complexity upgraded pictures produced by our calculation is better saved. In addition, the first picture can be precisely recouped with no extra data. Subsequently the proposed calculation has influenced the

picture to differentiate upgrade reversible and there is most extreme recovery of information.

VIII. REFERENCES

- [1] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
- [3] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

- [4] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversiblecontrast mapping," IEEE Signal Process. Lett., vol. 14, no. 4, pp.255–258, Apr. 2007.
- [5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversiblewatermarking algorithm using sorting and prediction," IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
- [6] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking basedon adaptive prediction-error expansion and pixel selection," IEEETrans. Image Process., vol. 20, no. 12, pp. 3524–3533, Jan. 2011.
- [7] Z. Zhao,H.Luo,Z.-M. Lu, and J.-S. Pan, "Reversible data hiding basedon multilevel histogram modification and sequential recovery," Int. J.Electron.Commun.(AEÜ), vol. 65, pp. 814–826, 2011.
- [8] H. T.Wu and J. Huang, "Reversible image watermarking on predictionerror by efficient histogram modification," Signal Process., vol. 92, no.12, pp. 3000–3009, Dec. 2012.
- [9] Y. Yang, X. Sun, H. Yang, C.-T.Li, and R. Xiao, "A contrast-sensitivereversible visible image watermarking technique," IEEE Trans. CircuitsSyst. Video Technol., vol. 19, no. 5, pp. 656–667, May 2009.
- [10] J. A. Stark, "Adaptive image contrast enhancement using generalizationsof histogram equalization," IEEE Trans. Image Process., vol. 9,no. 5, pp. 889–896, May 2000.
- [11] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W. J.Rucklidge, "The emerging JBIG2 standard," IEEE Trans. Circuits Syst.Video Technol., vol. 8, no. 7, pp. 838–848, Jul. 1998.
- [12] The USC-SIPI Image Database [Online]. Available: <http://sipi.usc.edu/database>
- [13] Kodak Lossless True Color Image Suite [Online]. Available: <http://www.r0k.us/graphics/kodak/>
- [14] M.-Z.Gao, Z.-G.Wu, and L.Wang, "Comprehensive evaluation forHEbased contrast enhancement techniques," Adv. Intell. Syst. Applicat.,vol. 2, pp. 331–338, 201