Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200201

An Efficient Data Hiding Approach on Digital Color Image

Sreesubha S [a] Babu R [a] Vijayakumar R [b] and Vijay K [b]
[a]*Assistant Professor, Departmentt of IT, Rajalakshmi Engineering College*
[b]*Assistant Professor ,Department of CSE,Rajalakshmi Engineering College*

Abstract. A concealing picture is worked of various assortments of a comparative scene, one for each repulsive section. These dim level picture gives the gathering of light, each at the unequivocal awful part and at the circumstance of every pixel. Red, Green and Blue are three frightful gatherings. Each image is created of three diminish measurement pictures, three gatherings.We'll conceal the substance in diminish pictures. Using Image improvement methodology, when we change the power estimations of basic tones by then the disguised substance is undeniable. From the preliminary outcomes we get 96% exactness

Keywords.RGB color model, Steganography and Demosaicking

1. Introduction

Two Greek words-Steganos specifying "made sure about or secret" and Graphein which designating "forming or drawing" that is the methods by which the term Steganography was gathered[1-5]. Here riddle making is the which methods for Steganography. Private substance is merged with spread picture to make stego-picture. Private substance is encoded what's more, decoded using stego key Figure 1 shows how the check recipient thinks the substance which is concealed.

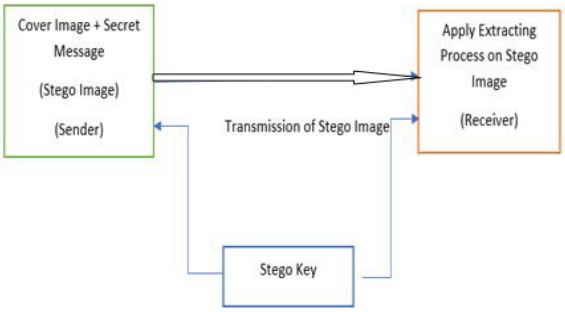


Figure 1. Steganography

Stego picture = Embedded message + Cover picture + StegoUsing the RGB concealing model propelled pictures are gotten and taken care of in structure as pixel which are the humblest unit of an image. Each pixel's capacity is addressed through three shades (RGB)[6-7]. The composing audit shows that there has been a lot of

[1]SreesubhaS ,Assistant Professor , Departmentt of IT, Rajalakshmi Engineering College,
Email :sreesubha.s@rajalakshmi.edu.in

investigate here, anyway all of the methods are complicated and need high plan and progressively computational time. Right now framework is proposed to hide content in pictures. The substance can be recuperated by controlling estimations of RGB.

2. Literature Survey

Zhi-Hong Guan [7] proposed a picture encryption technique in which areas are reordered and dull suspicions of the picture pixels are connected with the plain picture and the stego picture. Praloy [8] concentrated on calculations of cryptography that were made by applying methods of reasoning from an earlier time. Long Baoa [9] introduced unordered structure demonstrating temperamental practices. To grandstand its noteworthiness in picture development, another picture encryption stream utilizing the introduced unordered structure. Seetaiah Kilaru [10], this paper recommended that wellbeing is the need in any field. It is a significant test for the customers to make sure about the pictures moving over web as a result of dreary assault. For this portrayed Solitary Value Decomposition (SVD). It is introduced by Wavelets, unnoticeable watermark that fit into the principal watermark. Hassan [11] introduced design of a safe transmission. To move embedded substance hyper disordered frameworks are utilized. Haroun [12] proposed a technique on remote dissolving mediums dependent on creation of key

3. Implementation

3.1. Novelty of the Image Enhancement Algorithm

Various systems are inspected in all of these papers for scrambling a given picture and thus covering substance. In any case, here right now have presented a novel methodology which uses astoundingly clear system for picture improvement strategy to disguise the substance in a diminish picture.

3.2. Module 1: Image Encryption

Encryption is a procedure which utilizes a limited arrangement of guidance called a calculation to change over unique message, known as plain content, into figure message, its encoded structure In a grayscale picture, each pixel is given by single entire number regard. 0 suggests full scale dull, 255. strategies hard and fast white. Each character of substance is addressed by ASCII regards that continue running from 0 to 128. The widely inclusive ASCII is 8-piece and matches with the pixels' power run, which is 0 to 255. So encryption using these two should be conceivable all around essentially just by seeing them as common entire numbers and doing any action which limits the encoded an impetus inside 0 to 255, the mixed result can in like manner be addressed as a pixel or as a character. Encoding a message or data so that lone approved gatherings can get to it and the individuals who are not approved can't. Here, we are picking the info picture that we need to scramble. The picture to be scrambled is picked as an information document.

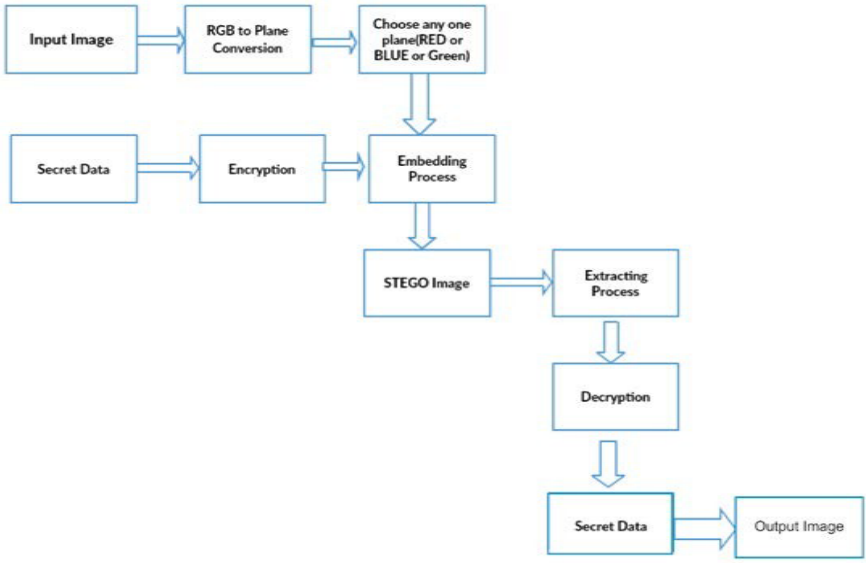


Figure 2. Architecture Diagram

3.2.1. Chaos Encryption and Decryption Algorithm

Cryptography can be characterized as the specialty of mystery composing or securing data by changing it (scrambling it) into an indiscernible arrangement, called figure content and afterward transmitting it across unreliable systems, with the goal that it can't be perused by anybody aside from the expected beneficiary.

3.2.2. Encryption Algorithm

The real picture of .jpeg or .bmp or .jpg or .png group is picked for encryption method.

1. Pixel qualities ought to be created from input picture by utilizing measurements of picture.
2. Pixel rearranging method is done on input picture
3. Chaotic Pseudo-Random key qualities are created
4. Sorting activity is finished
5. After arranging real lists of the arranged key qualities ought to be put away
6. Pixel rearranging is done again on Arnold Cat picture by utilizing bit xor activity
7. Encrypted picture is produced when all the above advances are finished.

3.2.3. Decryption Algorithm

The real picture of .jpeg or .bmp or .jpg or .png group is picked for encryption method.

1. Pixel qualities ought to be created from input picture by utilizing measurements of picture

2. Pixel rearranging method is done on input picture
3. Chaotic Pseudo-Random key qualities are created
4. Sorting activity is finished
5. After arranging real lists of the arranged key qualities ought to be put away
6. Pixel rearranging is done again on Arnold Cat picture by utilizing bit xor activity
7. Encrypted picture is produced when all the above advances are finished

3.3. Module 2: Data Hiding

Information covering up is a product improvement method explicitly utilized in object-arranged programming to shroud interior article subtleties. Information concealing guarantees elite information access to class individuals and ensures object respectability by forestalling unintended or expected changes. The scrambled picture shows up as red, blue and green plane. From these three planes we pick any of the plane to conceal the information. The plane is picked dependent on the histogram esteem that is got from the chart that depends on the recurrence of hues from 0 to 255 pixels.. Data concealing just covers class data portions, however data exemplification covers class data parts and private procedures. Subsequent to picking the plane the picture that will be covered up is picked. The key for the procedure is entered by the client and a similar key is shared to the recipient with the goal that he/she can decode the document or information. The secret key is entered as a solitary digit numerical worth. In this way, how the mystery information is covered up. Watermarking simply expands the spread source with additional data. Steganographic procedures are utilized to store watermarks in information.

3.4. Module 3: Embedding Process

Inserting is where the scrambled picture and the encoded information or document is consolidated. The key for the information or record that will be covered up is picked as a four digit numerical worth. The inserting system process is utilized to alters the first spread article so as to install the message. A similar four digit numerical worth is shared to the beneficiary with the goal that he can decode the information or document when he needs. After the installing procedure is finished, the scrambled picture (Stego-Image) is got. From the underlying advance to the inserting procedure the sender is associated with all the exercises that happens. For installing the mystery record we have to give a four digit key.

3.5. Module 4:-Extraction Process

Extraction is where the collector is answerable for all the exercises that happens. At the point when the beneficiary wishes to unscramble the information picture that send by the recipient he/she enters the one digit numerical worth that has been shared by the sender. Subsequent to entering the key, the beneficiary gets back the first picture without getting any misfortune in the information picture. For the procedure of unscrambling of information[14] or record he/she enters the mystery four digit numerical worth shared by the sender. When the key is right, the recipient gets the

information or record covered up in the information picture. We can get input picture that we utilized for encryption just as the mystery information that we utilized.

4. HVS System to RGB Format

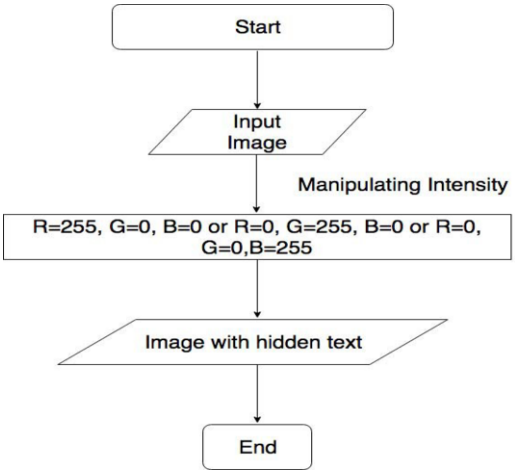
Most indispensable components of human visual systems(HVS) are rehashed by cutting edge camera's image taking care of. Figure 2 is a chart of a point of reference chain. If the camera is in a modified setting, self-modify, auto introduction, and customized white altering counts (all in all implied as "A*") will have identified the scene edge content, quality level, and illuminant concealing and have adjusted the relating camera get parameters before the shade get has been crushed. Demosaicking [13] is the most intriguing movement performed by automated cameras.

5. Proposed Workflow

The method for the proposed work process is according to the accompanying:

1. The substance which ought to be concealed should be behind the light source by thenrevolve around the light source suitably and get the image. The disguised substance should be in context on camera while getting the image. The image can be of any size and setup
2. To expel covered substance, accept the lit up picture as a data
3. Manipulate the power of RGB, R=255, G=0, B=0 or then again R=0, G=255, B=0
   or R=0, G=0, B=255
4. In the establishment of the lit up picture the disguised substance will be perceived

6. Result



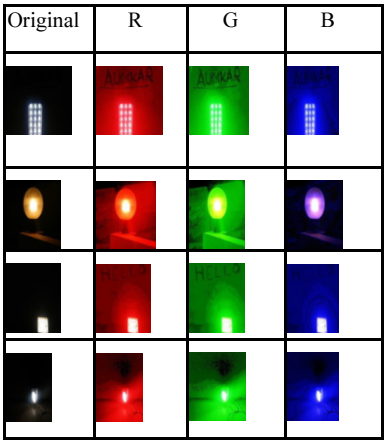


Figure 3. Proposed work flow

7. Conclusion

In this paper, we have proposed a calculation to conceal message in a picture which is enlightened utilizing white light or Yellow light. The outcomes depend on the assessment acquired from some contextual investigations attempted on various pictures. It is obviously appeared that the delivered yield pictures which are obvious by controlling the distinctive shading forces demonstrate the covered up message out of sight. The calculation is simple and easy to execute and still fills its need. Just the credible client will realize the calculation to unscramble the message from the scrambled picture. We tried on 50 pictures and accomplished 96% precision. Therefore, our proposed calculation when thought about to other steganography approaches is straightforward and viable. Hence this strategy is recommendable for genuine applications.

Reference

[1] Fridrich, Jiri. "Applications of data hiding in digital images." Signal Processing and Its Applications, 1999. ISSPA'99. Proceedings of the Fifth International Symposium on. Vol. 1. IEEE, 1999.

[2] Petitcolas, Fabien AP. "Introduction to information hiding." Katzenbeisser, S and Petitcolas, FAP (ed.) (2000): 275-290.

[3] Bender, Walter, et al. "Techniques for data hiding." IBM systems journal 35.3.4 (1996): 313-336.

[4] Silman, Joshua. "Steganography and steganalysis: an overview." Sans Institute 3 (2001): 61-76.

[5] Dugelay, Jean-Luc, and Stephane Roche. "A survey of current watermarking techniques." Information hiding techniques for steganography and digital watermarking (1999): 121-148.

[6] Guan, Zhi-Hong, Fangjun Huang, and Wenjie Guan. "Chaos- based image encryption algorithm." Physics Letters A 346.1-3 (2005): 153-157

[7] De, Praloy Shankar, and Prasenjit Maiti. "DEDD Symmetric- Key Cryptosystem." International Journal of Advanced Computer Research (IJACR) 3.8 (2013)

[8] Bao, Long, et al. "A new chaotic system for image encryption." System Science and Engineering (ICSSE), 2012 International Conference on. IEEE, 2012.

[9] Kilaru, Seetaiah, Yojana Kanukuntla, and K. B. S. Chary. "An effective algorithm for Image security based on Compression and Decomposition method." International Journal of Advanced Computer Research (ISSN(IJACR) 3.8 (2013).

[10] Hassan, Mohamed Fahim. "Synchronization of hyperchaotic systems with application to secure communication." Systems Conference (SysCon), 2015 9th Annual IEEE International. IEEE, 2015.

[11] Li, Chun-Ta, Chin-Wen Lee, and Jau-Ji Shen. "A secure three-party authenticated key exchange protocol based on extended chaotic maps in cloud storage service." Information Networking (ICOIN), 2015 International Conference on. IEEE, 2015

[12] Haroun, Mohamed F., and T. Aaron Gulliver. "Secret key generation using chaotic signals over frequency selective fading channels." IEEE Transactions on Information Forensics and Security 10.8 (2015): 1764-1775.

[13] A. Vignesh, T. Yokesh Selvan, Ganesh Krishnan, Arjun N. Sasikumar, V. D. Ambeth Kumar, "Efficient Student Profession Prediction Using XGBoost Algorithm", Lecture Notes on Data Engineering and Communications Technologies, Volume 35, pp 140-148, 2020.

[14] N. Hari Keshav, H. Divakar, R. Gokul, G. Senthil Kumar, V. D. Ambeth Kumar, "Real Time Categorical Availability of Blood Units in a Blood Bank Using IoT", Lecture Notes on Data Engineering and Communications Technologies, Volume 35, pp 503-510, 2020.