Dithering Technique for Digital Image Steganography

K. Jyothsna
Post Graduate Student
Department of CSE,
KSRM College of Engineering, Kadapa,
YSR District, AP (INDIA)

V. Lokeswara Reddy, PhD
Associate Professor
Department of CSE
KSRM College of Engineering, Kadapa,
YSR District, AP (INDIA)

ABSTRACT
Image Processing is a generally examined branch of sciences. Digital Image is a spot, where one can save data and can be recovered by normal vision handling. Considering the general properties of images, there are numerous strategies and procedures connected in this Image Processing. Steganography alludes to the investigation of imperceptible correspondence. Unique from cryptography, where the objective is to secure communications from a spy, yet the steganographic systems endeavor to conceal the very vicinity of the message itself from an observer. The general thought of concealing some information in advanced substance had a more extensive class of uses that go beyond steganography. This paper proposes a creative method for concealing and afterwards recovering a secret image. One can blend two branches of innovation of image processing and stenography. The system comprises of two procedures i.e encoding and decoding . The primary phase in the encoding stage is to shroud the secret RGB color image in a cover picture and get a few shares which are to be transmitted to the receiver. The main focus in the decoding stage is to get back the recovered picture to the original picture quality. However much as could reasonably be expected from the shares in the receiver end.

Keywords
Steganography**,** Dithering, Filtering, Encoding and Decoding, Cover image, Secret image.

1. INTRODUCTION
Steganography alludes to the investigation of imperceptible correspondence. In this undertaking the most part is to concentrate on computerized image steganography, which is about utilizing advanced pictures to shroud pictures. The word steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying "written work" characterizing it as "secured writing". This is expert through concealing picture in other picture, accordingly concealing the presence of the imparted picture. In picture steganography, the picture is shrouded usually in pictures. Advanced Image Steganography framework permits a normal client to safely exchange pictures by concealing them in a computerized picture document.

Given the expansion of advanced pictures and having the high level of repetition persevere in a computerized representation of a picture (despite compression), there has been totally expanded enthusiasm for utilizing advanced pictures as spread items with the end goal of steganography. Steganography is the science that includes conveying mystery information in a suitable mixed media bearer, e.g., picture, sound, and feature documents. Some of the basic methods of image restoration techniques[1] and analysis of digital image steganography methods[2] are presented. Subsequently this paper concentrated on pictures and steganography with computerized pictures.

This paper is organized as follows. Section I provides the introduction part. Section II provides proposed system. Encoding and decoding process is given in section III. Experimental work is provided in section IV. Finally conclusion is given in section V.

1.1 Image Steganography
Image Steganography has broad scope and a number of technologies are used in making this to work[3]. Some applications of this are sending passwords in images, sending logos in images and finally passwords or logos are extracted in the end of the process from a image. Steganography technique is good, however this technique is difficult to find and to crack it[4].

2. PROPOSED SYSTEM
This paper presents an innovative method, which uses already existing image algorithms. Firstly, split the secret image into three channels corresponding to the red, green and blue color channels respectively[5]. Then combine these shares individually with the cover image and forming a total of six shares. The next step deals with the retrieval of the secret image i.e., the decoding of the hidden image from the shares corresponding to the three color channels[6]-[7]. Some basic principles of visual cryptography, which involves applying the process of pixel expansion to a Visual Cryptography Scheme (VCS) [8]-[12]. A (n, n) VCS is defined as a scheme which encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. Finally, undithering and retrieving the secret image is done and merging it to get the required secret image.

Actually steganography means hiding the information in the cover images. The proposed technique can be done by hiding the secret image into a cover image. In this method the dithering technique is used, which is a process of creating factory of colors from RGB set of colors. The person, who wants to transfer the image to the receiver then the following fields should be registered by him. The fields are name, password, email id, and mobile number. After login, the image which sender wants to transfer is to be selected. First the cover image is selected and then the secret image, which is to be sent secretly to the receiver.

The procedure is given as follows:

Step 1: Select the cover image.

Step 2: Select the secret image to transfer.

Step 3: Embed the secret image into cover image .

Basic steganography model:

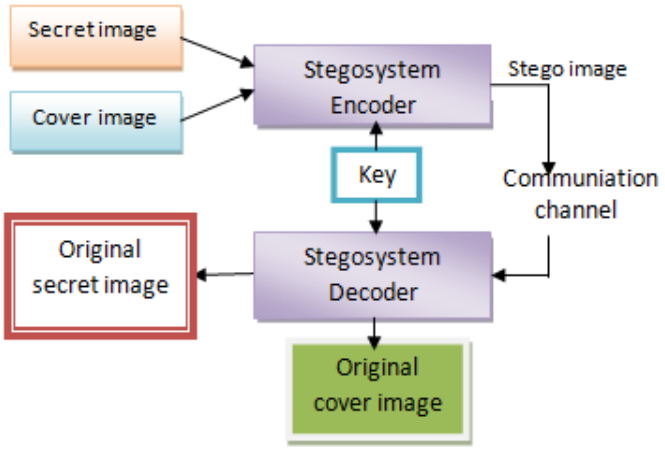


Figure 1: Steganography model

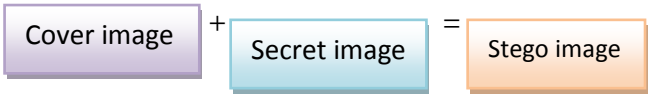
3. ENCODING AND DECODING PROCESS

The images which are going to transfer to the receiver are to be encoded and then decoded after the image is received to the receiver. The images which are to be transferred are encoded before embedding.

3.1 Embedding process

It is the process of combining the secret image and the cover image into a single file and save the file to the server and transfer that to the receiver .

This can be given as



a. Encoding Algorithm

Input : Cover and secret images.
Output : Original secret image.

Step 1: Get the rotation number ‘r’.

Step 2: Do the rotation to the secret image for ‘r’ number of times.
Step 3: Find the edge pixels in the cover image.
Step 4: Convert the secret image to binary equivalent.
Step 5: Calculate the length of payload.
Step 6: Calculate the pixel number required for embedding.

Table 1: Transformations on LSB

Condition	Action to be taken
$X_1=a_1 \oplus a_3$	No change required
$X_2=a_2 \oplus a_3$	
$X_1=a_1 \oplus a_3$	Change component G to match conditions(3)& (4)
$X_2 \neq a_2 \oplus a_3$	
$X_1 \neq a_1 \oplus a_3$	Change component R to match conditions(3)& (4)
$X_2=a_2 \oplus a_3$	
$X_1 \neq a_1 \oplus a_3$	Change component B to match conditions(3)& (4)
$X_2 \neq a_2 \oplus a_3$	

Step 7: For each pixel in the edge and upto required number of pixels, embed secret image into those pixels using the transformations on least significant bits.

Step 8: Transfer the stego image to the receiver.

The encoding algorithm is divided into two phases. The phases are mapping and embedding.

3.2 De- embedding process

It is the process of extracting, the hidden image from the cover image. In the extraction process it gives the output of the image that was sent by the sender. Some filters are used in image restoration phase to decode the secret image from the cover image[1]. By using these filters one can get back the original secret image sent by the sender.

b. Decoding Algorithm

Input : Two images
Output : Original secret image

Step 1: Get the secret key length.
Step 2: Apply edge detection algorithm.
Step 3: Get Edge pixels.
Step 4: Get all the pixels in the order in which they are embedded aginst the length of secret image.
Step 5: Mix all bits to form a binary sequence.
Step 6: Get characters from binary sequence.
Step 7: Rotate the secret image as the same number of times encoding.
Step 8: Decrypt the secret image.
Step 9: Get the original secret image.

The secret image is going to be placed in the cover image , then the two images are embedded[3] and the replacement of the secret image is done in cover image by using the RGB colors. The above process can be seen in the following image.

The replacement technique used is

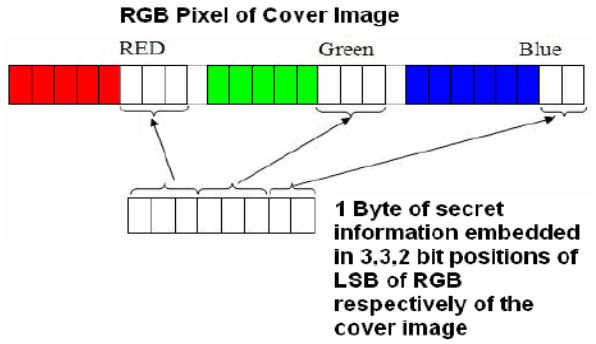


Figure 2: Replacement technique

In the above technique replacing a few bits from original file with secret code file and the order is as shown in the image.

4. EXPERIMENTAL WORK

When the machine is executed the user interface is displayed. The following is the Figure of the main window which shows the home page. Where the login and registration page will appear.

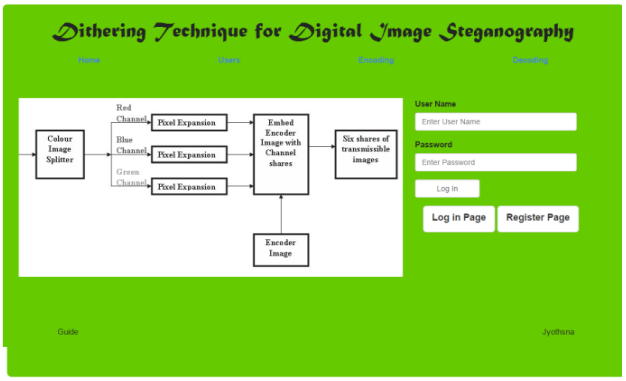


Figure 3: Home page.

The Figure of encoding page is shown in Figure 4. For embedding the images click on the "embed" button. The embedding process involves choosing of the images for cover image and secret image. The cover image is normal image which is visible to all and the secret image is hidden image to keep in the cover image. After that, click on the embed for embedding the two images.

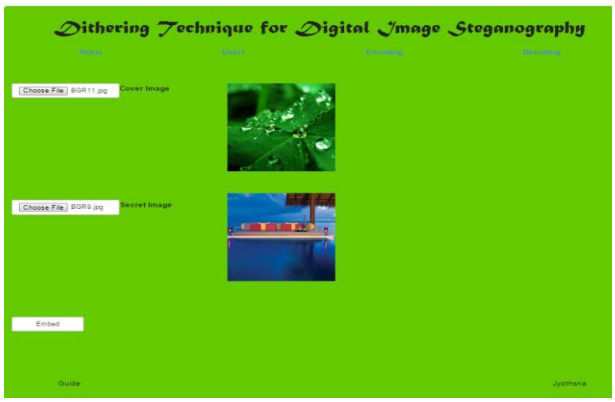


Figure 4: Encoding process.

The window of decoding phase is shown in Figure 5. The images which the sender sent to receiver is selected for the decoding process.

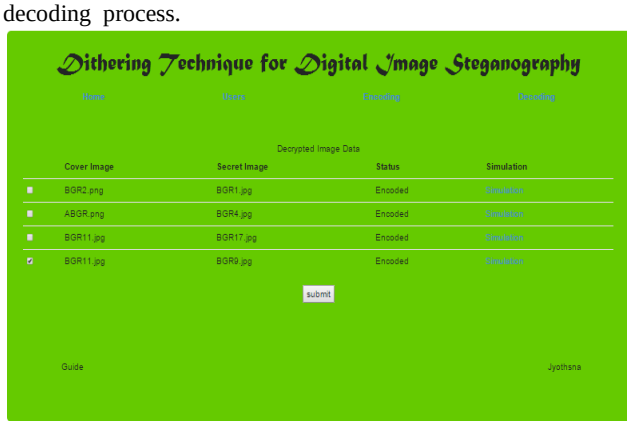


Figure 5 : Decoding process.

The simulation process is shown in the Figure 6. In the simulation process the filters are applied to the file, which is received from the sender. After applying the filters the original secret image is obtained.

Figure 6: Simulation process.

The extraction of the secret image is shown in Figure 7. Where the secret image is extracted from the embedded image.

Figure 7: Secret image is extracted.

The cover image is taken for the encoding is shown below.

Figure 8: Cover image.

The secret image is taken for transferring to the receiver is shown below.

Figure 9: Secret image.

The stego image, which is sent to the receiver by the sender is shown in Figure 10, where the cover and secret images are embedded.

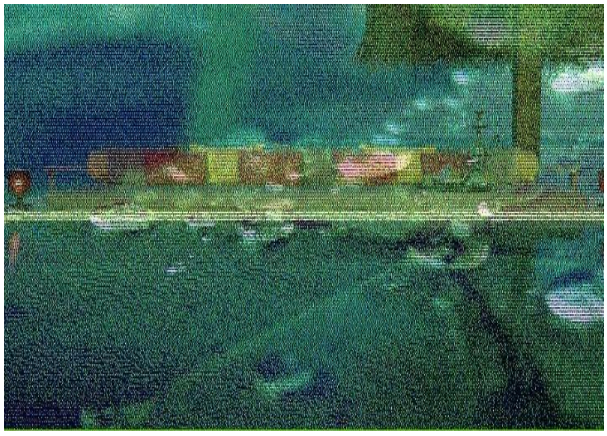


Figure 10: Stego image.

5. CONCLUSION

Information hiding is a technique that is currently being used by most countries and big companies for transferring of sensitive information. In the above procedures discussed we have tried to mix some of the conventional techniques so as to hide the image as far as possible. However, unlike general decoding schemes, we have tried to bring back the secret image as near to the original quality as possible. However lots of work left to be done. In future, we shall be trying to develop newer and better algorithms based upon the above theoretical knowledge. We shall also try to reduce loss in image quality as far as possible.

6. REFERENCES

[1] Reginald L. Lagendijk and Jan Biemond, "BASIC METHODS FOR IMAGE RESTORATION AND IDENTIFICATION", Information and Communication Theory Group, Faculty of Information Technology and Systems Delft University of Technology,The Netherlands.

[2] Abbas Cheddad Joan Condell, Kevin Curran Paul Mc Kevitt Digital image steganography: Survey and analysis of current methods School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, UK.

[3] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography and authentication." Journal of Systems and software 73.3 (2004): 405-414.

[4] T. Morkel , J.H.P. Eloff M.S. Olivier An Overview Of Image Steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[5] Marvel, Lisa M., Charles G. Boncelet Jr, and Charles T. Retter. "Spread spectrum image steganography." Image Processing, IEEE Transactions on 8.8 (1999): 1075-1083.

[6] D. Biswas, S. Biswas, P. P. Sarkar, D. Sarkar, A. Pal, S. Banerjee, S. Polle, F. K. M. Nawaz, K.Das, "Embedding Watermark byPixel Bit Manipulation", IEEE conference on Scientific Paradigm Shift in Information Technology and Management (SPSITM),2011.

[7] G.Langelaar, I. Setyawan, and R. Lagendijk. Watermarking digital image and video data. IEEE Signal Processing Magazine, 17:20–46, 2000.

[8] Houmansadr , Shahrokh Ghaemmaghami , "A Digital Image Watermarking Scheme Based on Visual Cryptography" Electrical

[9] Engineering Department, Sharif University of Technology, Azadi St., Tehran, Iran.Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme" Centre for IT Education, Biju Pattanaik University ofTechnology, Orissa 751010, India, Department of Computer Science & Engineering

[10] R. J. Hwang, " A Digital Copyright Protection Scheme Based on Visual Cryptography", Tamkang Journal of Science andEngineering, vol. 3,no. 3, 2000.

[11] N.Naor and A.Shamir, "Visual Cryptography", Advances in cryptology: Eurocrypt'94, Springer- Verlag, Berlin,1995,pp.1-12.

[12] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Visual cryptography for gray-level images by dithering techniques." Pattern Recognition Letters 24.1 (2003): 349-358.

7. AUTHOR PROFILE

Dr. V. Lokeswara Reddy received his Ph. D in Computer Science and Engineering from JNTUA, Ananthapuramu in the year 2015. Received his M. Tech (CSE) degree from SRM University, Chennai in the year 2005. Received his M.C.A degree from S.V. University, Tirupati in the year 2000. He has a total of 13 years of experience in teaching. Currently he is working as Associate Professor at K.S.R.M College of Engineering, Kadapa. He has presented 9 papers in International, National Conferences and published 13 papers in International journals.

K. Jyothsna received her B.Tech degree in computer science and engineering from JNTUA, Ananthapuramu in the year 2013. She is pursuing her M.Tech at K.S.R.M College of Engineering, Kadapa from JNTUA, Ananthapuramu, Andhra Pradesh. Her current research interests include hiding techniques.