Design and Implementation of an Stegnography Algorithm Using Color Transformation

Sonia Sharma, Anjali Dua

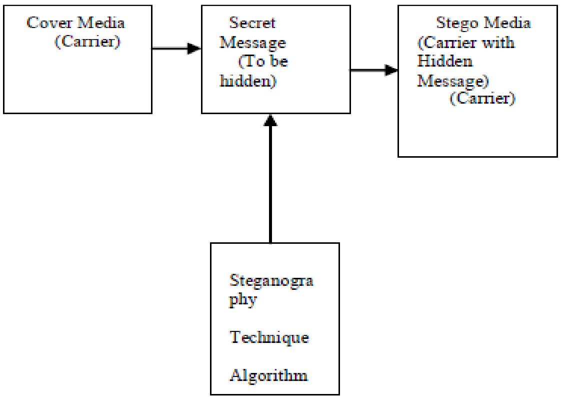
***Abstract:** In a computer, images are represented as arrays of values. These values represent the intensities of the three colors R(ed) G (reen) and B (lue), where a value for each of the three colors describes a pixel. Through varying the intensity of the RGB values, a finite set of colors spanning the full visible spectrum can be created. In an 8-bit gif image, therecan be 28 = 256 colors and in a 24-bit bitmap, there can be 224 = 16777216 colors. Large images are most desirable for steganography because they have the most space to hide data in. The best quality hidden image is normally produced using a 24-bit bitmap as a cover image. Each byte corresponding to one of the three colors and each three-byte value fully describes the color and luminance values of one pixel. The cons to large images are that they are cumbersome to both transfer and upload, while running a larger chance of drawing an "attacker's" attention due to their uncommon size. Our main focus to introduce the stegnography using color transformation.*

***Index Terms:** Stegnography, Color Transformation, RGB,Data Hiding, Imperceptibility.*

I. INTRODUCTION

Though the fields of steganography and cryptography are associated with one another, there is a distinction to be made. Cryptography is the art of jumbling a message so that a would-be eavesdropper cannot interpret the message. Steganography, on the other hand, is the art of hiding a message so that a would-be eavesdropper is unaware of the message's presence. While steganography has been around for centuries, the Digital Revolution has sparked a renewed interest in the field. For instance, the mass media industry has shown increasing interest in steganography to fight piracy.

STEGANOGRAPHIC PROCESS


Cover Media (Carrier)
Secret Message (To be hidden)
Stego Media (Carrier with Hidden Message) (Carrier)
Steganography Technique Algorithm

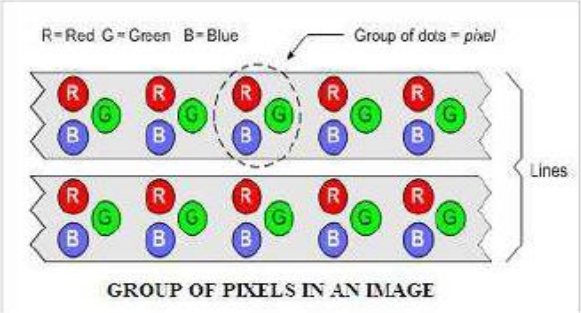
In the above figure cover media is the carrier medium - such as text ,image ,audio, video and even the network packet. The secret message is the private message that is to be hidden in the cover media.

II. WHY IMAGE AS CARRIER?

Images are a good medium for hiding the data. The more detailed an image ,the fewer constraints there are on how much data it can hide before it becomes suspect. Digital images are a preferred media for hiding information due to their high capacity and low impact on visibility.

III. COLOR TRANSFORMATION OF RGB COMPONENT

Techniques used so far focuses only on the two or four bits of a pixel in a image ,(at most five bits at the edge of an image.) which results less peak to signal noise ratio and high root mean square error i.e. less then 45 PSNR value.



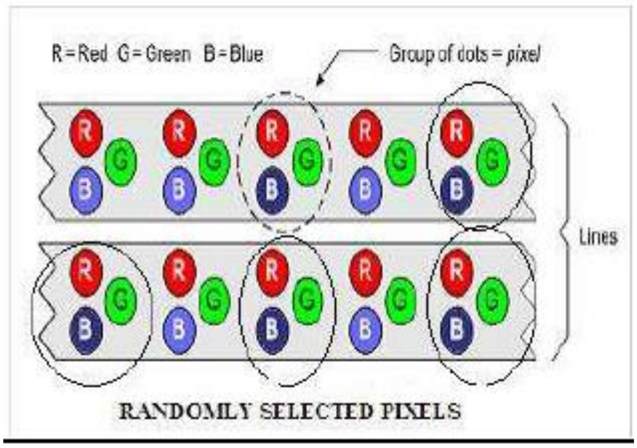
Revised Manuscript Received on 30 June 2012.
* Correspondence Author

Assistant Professor Sonia Sharma*, Department of Computer Science and Engg., JMIT Radaur, Yamunanagar, Haryana, India

Scholar Anjali Dua, Department of Computer Science and Engg., JMIT Radaur, Yamunanagar, Haryana, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Pixels of an image



My proposed work concentrate on 8 bits of a pixel (8 bits of Red,blue Green component of a selected pixel in a 24 bit image), resulting better image quality. One can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:

(00100111 11101001 11001000) (00100111 11001000 11101001)

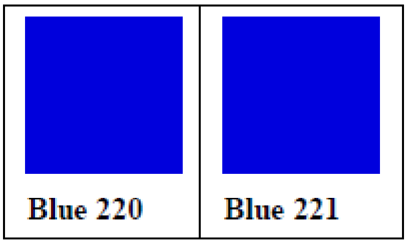
(11001000 00100111 11101001)

To hide the letter "A" which has a position 65 into ASCII character set and have a binary representation

"01000001", by altering the first component (blue channel) bits of randomly selected pixels

(00100110 11101001 11001000) (01000001 11001000 11101000) (11001000 00100111 11101001)

For example; we can see the difference resulting by varying the value of first component (blue channel) of an pixel :



Only First component (Blue component) is selected because a research was conducted by Hecht, which reveals that the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.

IV. DATA HIDING USING FIRST COMPONENT ALTERATION TECHNIQUE ALGORITHM

To insert the different matrices we have to take different perception as per the human visualization vision for the color Identification

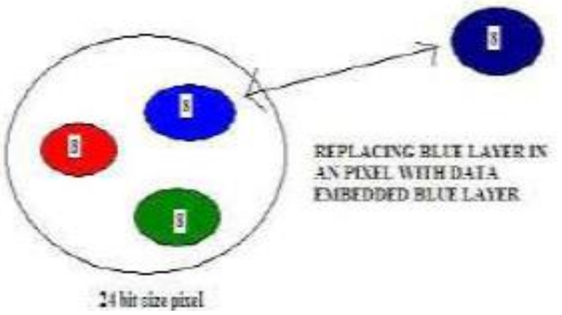
1) Let R represents the Red Color matrix for the image :
|R1 R2 R3……..Rn| be cells for Red color matrix

2) Let B represents the Blue Color matrix for the image :
|B1 B2 B3……..Bn| be cells for Blue color matrix

3) Let G represents the Green matrix for the image
|G1 G2 G3……..Gn| be cells for Green color matrix
R1(0),R2(0),R3(0) ………………………… Rn (0) be total first channels in all pixels
G1(0),G2(0),G3(0) …………………………Gn (0) be total Second channels in all pixels
B1(0),B2(0),B3(0) ………………………… Bn (0) be total third channels in all pixels

4) Input the characters that has to be hidden in the image .
Let ch1,ch2,ch3………………………………chm be total character that has to be inserted in the image :

5) Find the numeric value for the characters
Therefore total character that has to be inserted is given by:-
Dividing Characters into three format


REPLACING BLUE LAYER IN AN PIXEL WITH DATA EMBEDDED BLUE LAYER
24 bit size pixel

Let V is the value
V = Chi -

for blue Chi = Chi-16; and Bi= Chi;
for Red Ri | Chi
for Green Gi | Chi Where i = 0,1,2…….n (total character to be hidden)

V. MEASURING IMAGE QUALITY

In objective measures of image quality metrics, some statistical indices are calculated to indicate the reconstructed image quality. The image quality metrics provide some measure of closeness between two digital images by exploiting the differences in the statistical distribution of pixel values. The most commonly used error metrics used for comparing compression are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) .

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the

PSNR, the better the quality of the compressed or reconstructed image.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (1)$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \qquad (2)$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc.

VI. CONCLUSION

In this paper, we proposed a new image steganography Algorithm using Color Transformation and three compone alteration technique, and the proposed scheme is a type of spatial domain technique. In order to hide secret data in a cover-image . The method is an first component alteration of three channels of pixel, altering 8 bits of first component (RGB component) to hide the data in it.To make an algorithm robust enough that it can withstand different transmission parameters e.g. compression filters, Reformat Attack, File an Original copy. To overcome these attacks we placed the key at asymmetric counts of the pixels and hence one can-not find which pixels are used to save the key as well as the hidden text. Thus making this algorithm technique best among other available techniques in terms of data capacity, robustness, fragile. The proposed technique is compatible and can be programmed with latest user friendly languages which are in connection with the latest online, E-Commerce and shopping applications as given in the example. More over the proposed method can be extended to all types of image formats e.g. jpeg, bmp etc.

REFERENCES

1. Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, “Spread Spectrum Image Steganography”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999.
2. Jessica Fridrich, Miroslav Goljan,Binghamton, Department of Electrical Engineering, Binghamton, NY,” Practical Steganalysis of Digital Images – State of the Art”, Conference , San Jose CA , ETATS-UNIS (21/01/2002).
3. Kevin Curran, Internet Technologies Research Group, University of Ulster ,Karen Bailey, Institute of Technology, Letter Kenny , Ireland,” An Evaluation of Image Based Steganography Methods, International
4. Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.
5. Sabu M Thampi,Assistant Professor,Department of Computer Science & Engineering,LBS College of Engineering, Kasaragod,Kerala- 671542, S.India ,” Information Hiding Techniques: A Tutorial Review”, ISTE-STTP on Network Security & Cryptography, LBSCE 2004.
6. Kefa Rabah, Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey,” Steganography-The Art of Hiding Data”, Information Technology Journal 3 (3): 245-269, 2004,ISSN 1682-6027.
7. Mantiuk,R.Myszkowski,Seidel,H.-P.MPI Informatik, Saarbrucken, Germany,“Visible difference predicator for high dynamic range images “, IEEE International Conference on Systems, Man and Cybernetics , Oct. 2004, ISSN: 1062-922X.
8. C. A. Bouman,” The Visual Perception of Images” Digital Color Imaging magazine,April, 2005.
9. 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 Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.
10. Ching-Yu Yang, Department of Computer Science and Information Engineering,National Penghu University Penghu, Taiwan,” Color Image Steganography based on Module Substitutions”, Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication: 2007 ISBN:0-7695-2994-1.
11. S .K. Moon , R.S. Kawitkar,PICT, Pune and SCOE, Pune,INDIA,” Data Security using Data Hiding”, International Conference on Computational Intelligence and Multimedia Applications 2007.
12. Jae-Gil Yu1, Eun-Joon Yoon2, Sang-Ho Shin1 andKee-Young Yoo, Dept. of Computer Engineering, Kyungpook National University Daegu, Korea,” A New Image Steganography Based on 2k Correction and Edge-Detection”, Fifth International Conference on Information Technology: New Generations 978-0-7695-3099-4/08 © April 2008 IEEE.
13. Junhui He, Shaohua Tang and TingtingWu,School of Computer Science and Engineering,South China University of Technology,University Town, Guangzhou 510006, China2008,” An Adaptive Image Steganography Based on Depth-varying Embedding”, Congress on Image and Signal Processing, Steganographic technique is a means of covert communication.Volume 5, Issue , 27-30 May 2008 Page(s):660 – 663.

AUTHOR PROFILE

SONIA SHARMA received her B.Tech degree in Computer Engineering from Seth Jai Parkash Institute Of Engineering and Technology, Radaur, Haryana, India in 2005, and received her M.Tech. degree in Computer Science and Engineering from Seth Jai Parkash Institute Of Engineering and Technology, Radaur, Haryana, India in 2007. Her area of interest include cryptography and data structures.

ANJALI DUA received her B.E degree in Computer Engineering from Anupama College of Engineering, India in 2006, and received her M.Tech. degree in Computer Science and Engineering from Seth Jai Parkash Institute Of Engineering and Technology, Radaur, Haryana, India in 2012. Her area of interest include image denoising and Stegnography