RESEARCH ARTICLE OPEN ACCESS

# Mathematical Approach to Steganography for Embedding RGB Images

**P.Meenakshi Sundari**
Associate Professor,
Department of Computer Science,
Fatima College, Madurai. Tamil Nadu, India

ABSTRACT
The digital world presents opportunities for the art of data concealment. Steganography exemplifies this, enabling the embedding of confidential data, such as images or text, within innocuous digital images. Leveraging non-secret files to transmit secret messages offers a distinct security advantage over cryptography by aiming to avoid the scrutiny of hackers. While the existence of the hidden data remains known only to the intended sender and receiver, this paper proposes a new steganographic approach for concealing an RGB image within another. The method involves choosing three coordinates within the cover image. The red, green, and blue values of each pixel in the secret image are split into three segments and embedded within the middle value of the respective color channels at these three coordinates. A circular formula is used to calculate the subsequent embedding coordinates. To further bolster security, adding noise to the cover image before the embedding process is suggested.
Keywords:- Steganographic, color image

## I. INTRODUCTION

The art of concealing information within other data is crucial in today's digital landscape. Steganography stands out as one such technique for embedding information within digital media. Evading the notice of malicious actors while hiding images presents a significant challenge, making steganography, and especially its combination with cryptography, a potentially stronger security measure. Given the evolving threats in the digital world, continuous research and novel approaches in both steganography and cryptography are essential. This paper contributes to this field by proposing a new method for hiding an RGB image within another, with the primary goal of avoiding hacker detection.

## II. COLOR MODEL

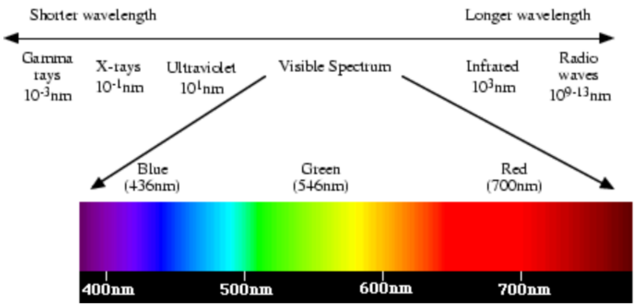


Figure -1 - Standard Wavelength

Three independent image planes are in the RGB model. The primary colours of RGB model are red, green and blue. Figure 1 shows the standard wavelength for the three primaries colours in the RGB model.

Specifying particular colour is a combination of the amount of each primary component.

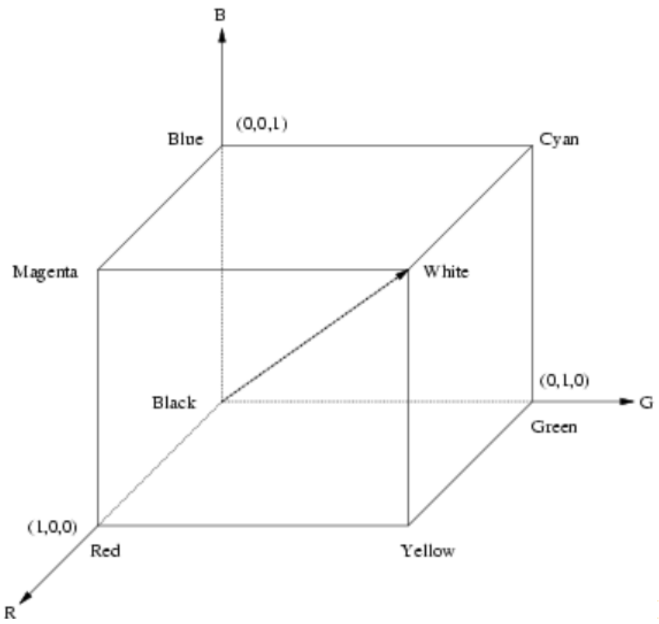


Figure -2 – Geometry of the RGB model

Figure-2 shows the geometry of the RGB colour model Cartesian Co-ordinate system is used for specifying colours in the RGB model. The greyscale spectrum lies on the vertices of line joining black and white vertices. The greyscale colours are made from equal amounts of each primary colours. RGB color model is defined 24-bit color model. Each primary color has 8-bit to store their shades. Combination of red, green and blue shades produces different colors. The maximum integer value for each primary color is 255, which is stored in the 8-bit storage [Table1]. Hence each primary color shades start from 0 to 255. So totally, each primary color has 256 shades. Total number of colors in the RGB model is 256 x 256 x 256.

| **Primary Color** | **Min Value** | **Max Value** |
|---|---|---|
| Red | 0 | 255 |
| Green | 0 | 255 |
| Blue | 0 | 255 |

**Table - 1**

Total number of colors in each primary color has 256 shades, starts from 0 to 255.

In this approach, integer value of primary colors in RGB are splitted into three digits, v1,v2 and v3. For example the value 178 is considered as v1=1, v2=7, v3=8. Table 2 describes range of v1, v2 and v3.

| **Value** | **Min Value** | **Max Value** |
|---|---|---|
| v1 | 0 | 2 |
| v2 | 0 | 9 |
| v3 | 0 | 5 |

**Table - 2**

The maximum value for any shade is 255. Then v1 is in the range [0,1,2], v2 is in the range [0,1,2,3,4,5,6,7,8,9] and v3 is in the range [0,1,2,3,4,5].

## III. PROPOSED APPROACH

In the proposed approach 8-bit image is hiding in 24-bit image.

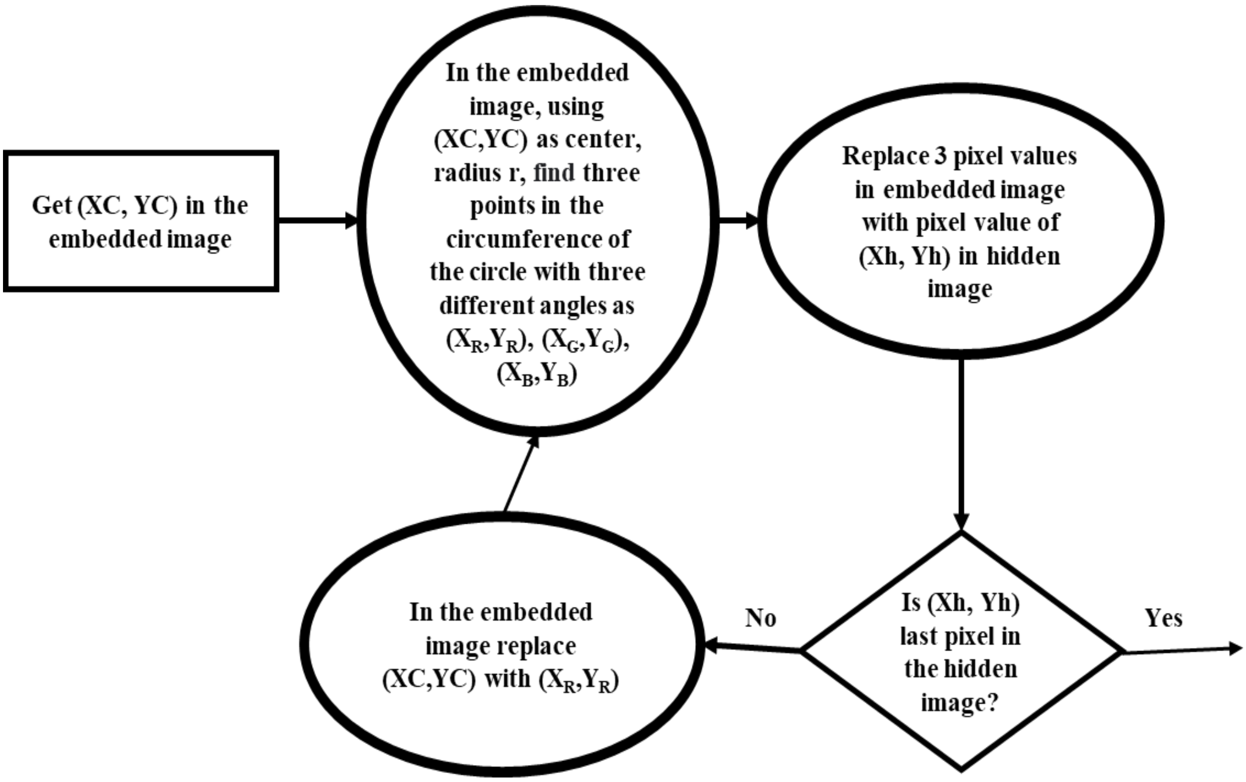

Figure -3 – Proposed Approach

The pixel value of hidden image splits into three digit, that is three parts [v1,v2,v3].

Select a co-ordinate $(X_c,Y_c)$ from the embedded image which is shared by sender and receiver. Then find three co-ordinates$(X_R,Y_R)$, $(X_G,Y_G)$ and $(X_B,Y_B)$ from the circumference of the circle with center .

$(X_c,Y_c)$, radius r (also shared) and angles 45°, 135° (90°+45°) and 225° (180°+45°).

$X_R=X_c+r.cos(45)$ -------------------- [1]
$Y_R=Y_c+r.sin(45)$ ---------------------[2]
$X_G=X_c+r.cos(90+45)$ ----------------[3]
$Y_G=Y_c+r.sin(90+45)$ -----------------[4]
$X_B=X_c+r.cos(180+45)$ ---------------[5]
$Y_B=Y_c+r.sin(180+45)$ ----------------[6]

Next find the pixel value of hidden image $(X_{RGB},Y_{RGB})$. Find the Red, Green and Blue value of $(X_{RGB},Y_{RGB})$ in the hidden image

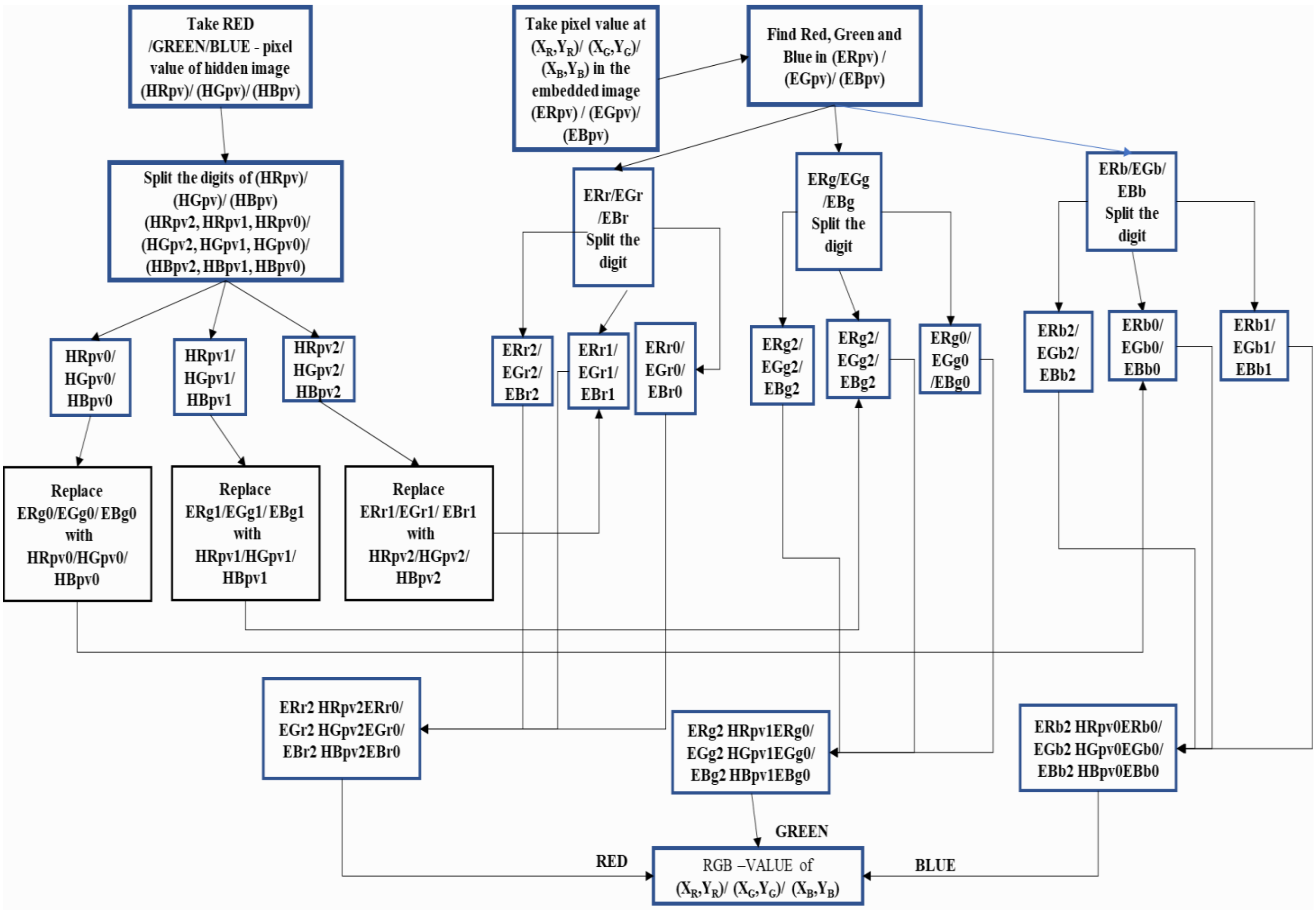


Figure -4 – Replace hidden image RED value in the Embedded Image Embedded image

Replace the middle digit of the red, green, and blue values at coordinate (XR,YR) with the digits of the red value from coordinate (XRGB,YRGB) in the hidden image. Split the digits of the red value in (XRGB,YRGB) into HRr2, HRr1, and HRr0. For example, if the red value is 198, then HRr2=1, HRr1 =9, and HRr0=8. Then, replace the middle digit of the red, green, and blue components at (XR,YR) in the embedded image with these values. For instance, if the original RGB values are red=129, green=080, and

blue=150, after replacement, they become red=119, green=090, and blue=180.

Similarly, store the green and blue values of (XRGB ,YRGB) from the hidden image in the corresponding color components at (XG,YG) and (XB,YB) of the embedded image, respectively, by replacing their middle digits.

If the embedded image is pre-processed by adding noise, it becomes more difficult for hackers to track the hidden image.

Apply this approach to store all pixel values of the hidden image within the embedded image.

## IV. SCOPE OF THE APPROACH

The proposed approach demonstrates significant effectiveness when the embedded image undergoes pre-processing with the addition of noise. The distribution of the hidden image's RGB values across the entirety of the embedded image makes it challenging for malicious actors to retrieve the concealed data.

## V. FUTURE ENHANCEMENT

This approach is only for RGB colour model. This approach should be enhanced for all color models. The pixel values are stored in the embedded image without getting the attention of hackers.

## VI. CONCLUSION

Cryptography's strength lies in concealing message content, but its weakness is its conspicuous existence, which can alert hackers. Steganography, however, provides enhanced security by hiding the very fact that secret data is being transmitted, thus remaining unknown to unauthorized individuals. Despite the array of existing techniques in both fields, the dynamic nature of digital security demands continuous research and innovative solutions. This paper introduces a novel approach for concealing an RGB image within another RGB image, specifically designed to evade the notice of hackers.

## REFERENCES


[1]. M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin "Information Hiding using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia. 2003 IEEE.

[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf

[3] Feng, J.B., Lin, I.C., Tsai, C.S., Chu, Y.P., 2006. Reversible watermarking: current status and key issues. International Journal of Network Security 2 (May), 161–170.

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[5] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science,Springer, 1998. pp. 32-47.

[6] Chan, C.K., Cheng, L.M., 2004. "Hiding data in images by simple LSB substitution". Pattern Recognition 37 (March), 469–474.

[7]. T. Sharp, "An implementation of key-based digital signal steganography," in Proc. Information Hiding Workshop, vol. 2137, Springer LNCS, 2001, pp. 13–26.

[8] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.

[9] Neil F. Johnson, S.C. Katzenbeisser,"A survey of steganography technique"

[10] Chung-Ming Wang a, Nan-I Wu a, "A high quality steganographic method with pixel-value differencing and modulus function", accepted 24 January 2007

[11] Mohammad Tanvir Parvez and Adnan Gutub, "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008 – Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12December 2008

[12] Deepesh Rawat , MTech (DC 2nd Year) , Vijaya Bhandari Asst. Professor (ECE ), BTKIT, DWARAHAT , UTTARAKHAND, INDIA

A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image, *International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, February 2013.*