Pixel Value Differencing Method Based on CMYK Colour Model

Shobana Manoharan, Deepika RajKumar

(Corresponding author: Shobana Manoharan)

Department of Electronics and Communication Engineering Karpagam College Of Engineering
Coimbatore, Tamil Nadu, India
(Email: divyashobana.m@gmail.com)

(Received June 4, 2016; revised and accepted JUly 18 & July 24, 2016)

Abstract

Due to tremendous improvements in the technology, all the confidential information are flying over the internet and most of the secured data are in the form of digital content. In this situation, data hiding techniques like Steganography stands in the position to protect the data in efficient manner from attackers. The style of embedding covert image over the cover image is termed as Image-Image Steganography. Here the methodology used for image-image steganography is modified form of pixel value differencing. Here, the secret image gets hidden in the cover object(image) in which the size of the message image is equivalent to the cover image and it is achieved by using CMYK colour model. Thus, the proposed algorithm provides a stego image with good quality measures and this algorithm is implemented with the help of matlab. Here the disturbance in the resultant image is calculated with the help of its PSNR and MSE values.

Keywords: Data Hiding; Encoding Algorithm; Network Security; Steganography

1 Introduction

Steganography is nothing but the approach of embedding and transmitting information via seemingly harmless covers in an attempt to obscure the presence of the message. The term "steganography" is an extract from Greek language, exactly means buried writing that comprises a huge array of approaches of covert communications that mask the presence of a secret object. Though steganography is an old skill, the commencement of computer technology has given it new birth. Computer based stenographic approaches announce alteration that covers medium to hide foreign data to the local carriers. That kind of message may be communicated in the form of text, binary files or produce extra information about the carrier and its authority such as digital watermarks or fingerprints. Steganography can be seen as cousin to cryptography. These two techniques have been used completely to insert elements of security to communication.

Cryptographic methods purposely disturb a message, so that, if it is interrupted, it cannot be cleared. This process is known as encryption and the encrypted message is termed as cipher text. Steganography in core "Camouflages", a message to skin its existence and make it seems unnoticed thus hiding the fact that a message is being sent in total. A cipher text message may capture attention while invisible messages will not [5].

One of the most popular cover objects used for steganography is an image. Cover images may be gray scale images or color images. Color images have large space for information hiding and therefore color image steganography is more popular than gray scale image steganography. Color images can be represented in various formats such as RGB (Red Green Blue), HSV, YUV, YIQ, YCbCr etc. Color image steganography can be done in any color space Domain [4].

Varieties of steganography is based on the kind of secret information gets embedded inside the cover medium. If the covert image gets hidden on the cover image then it is termed as Image steganography. If the message is text then it is called as text steganography and so on. Image steganography methods are broadly splitted into spatial domain based [3] and transform domain based methods [11] where the spatial domain hides the message bits in spatial intensity data by substitution and the transform domain techniques is used to hide the data on transform domain coefficients. Steganographic approaches are divided into 6 methods on the basis of the changes take place on the carrier medium. They are Transform domain, substitution, Statistics, Distortion, Spread spectrum and Cover generation based methods.

The Image-Image steganography based on Least Significant bits Substitution [9], Pixel Indicator [12] then Pixel Image intensity variation methods [10] need an image as the cover to hide the covert information which can be taken by altering the pixel values or by altering the intensity value of the pixel. The most common approach in the data hiding field is least-significant bits (LSBs) substitution where the fixed-length secret bits is embedded in the same fixed-length LSBs of pixels but it produces visible disturbance in the carrier medium. To minimize the disturbance led by LSBs substitution, several adaptive methods such as Optimal Pixel Adjustment Process [2] have been introduced. On the other hand, such adaptive methods differ from the others in the case of number of embedded bits in each pixel which owns good image quality [1]. Still, this can be attained by the capacity of lessening in the hiding capability.

2 Existing Method

The existing method is on the basis of pixel value differencing technique and modulus function. In the first step, the cover object is divided into Red, Green and Blue colour layers [6]. In this method, modulus function of 3 is applied to all the pixel value of the three colour planes. Let us consider the pixel value be p. The secret message is converted into base 3 digits. Let us consider this message value be m. During embedding process the value of p is compared to m. If the value of p is equal to m, then without any modification the cover pixel is considered as the stego pixel. If the value of p is greater than m, then increase the value of the cover pixel by 1 and that value is considered as a stego pixel. If the value of p is lesser than m, then decrease the value of the cover pixel by 1. This operation is carried out sequentially for all the three colour planes [7].

3 The Proposed Method

In this method, the cover image is splitted into cyan, magenta, yellow and black(key) colour for security purpose [8]. Because, most probably, all colour image steganography is based on red, green and blue layers. Here, modulus of 4 is applied for all pixel's value in the carrier image. By this, each cover pixel is capable of holding each pixel of message image. All pixels in the carrier image are involved in the process of embedding. The secret message is gray scale image and its size is equal to the cover image.

4 Algorithm

4.1 Embedding Method

Input: cover image(I), grayscale secret image(g);
Output: Stego image(s);

1) Convert RGB image to CMYK colour model.

2) Split the cover image in to cyan, magenta, yellow, and black layer (C, M, Y, K) respectively.

3) Take modulus function of 4 to all pixel values in the four layers as follows:

   N be the number of pixels in the secret image;

   For i =1 to N;

   C(i) mod 4 = C1(i);

   M(i) mod 4 = M1(i);

   Y(i) mod 4 = Y1(i);

   K(i) mod 4 = K1(i).

4) Convert all pixel values of secret image to base 4 such that each pixel value is of digits as mentioned as follows:

$$\begin{aligned} (0)10 &= (0000)4(d1, d2, d3, d4) \\ (1)10 &= (0001)4(d1, d2, d3, d4) \\ &\vdots \quad\quad \vdots \\ (255)10 &= (3333)4(d1, d2, d3, d4). \end{aligned}$$

5) The secret bit d1 will get embedded in C, d2 in M, d3 in Y and d4 in K.The Embedding process is carried out using Algorithm 1.

6) Convert the resultant image in to RGB image.

Algorithm 1 EMBEDDING ALGORITHM

```
for j = 1 to N do
  if C1[j] = d1[j] then
    C[j] ← C[j]
  else if C1[j] < d1[j] then
    C[j] = Function f1(C1[j],d1)
  else
    C[i] = Function f2(C1[j],d1)
  end if
  if M1[j] = d2[j] then
    M[j] ← M[j]
  else if M1[j] < d2[j] then
    M[j] = Function f1(M1[j],d2)
  else
    M[j] = Function f2(M1[j],d2)
  end if
  if Y1[j] = d3[j] then
    Y[j] ← Y[j]
  else if Y1[j] < d3[j] then
    Y[j] = Function f1(Y1[j],d3)
  else
    Y[j] = Function f2(Y1[j],d3)
  end if
  if K1[j] = d4[j] then
    K[j] ← K[j]
  else if K1[j] < d4[j] then
    K[j] = Function f1(K1[j],d4)
  else
    K[j] = Function f2(K1[j],d4)
  end if
end for
```

4.2 Functions Used in Embedding Algorithm

Here r1 is corresponding pixel sent to the following functions. It may be C, M, Y or K.

```
Function f1(r1,d)
If(r1 == 1)
        r1 = r1 + 1;
If(r1 == 2)
        r1 = r1 + 2;
If(r1 == 3)
        r1 = r1 + 3;
End
End

Function f2(r1,d)
If(r1 == 0)
        r1 = r1 - 3;
If(r1 == 1)
        r1 = r1 - 2;
If(r1 == 2)
```

```
        r1 = r1 - 1;
End
End
```

4.3 Extraction Method

Input: Stego image (S);
Output: Message image (g);

1) Convert Stego image from the RGB layers into CMYK colour layers.
2) Split the stego image into cyan, magenta, yellow, and black layer (C, M, Y, K respectively).
3) Take modulus function of 4 to all pixel values in the four layers and store it in separate array as A.
4) Split the array A such that each sub array equals to 4 digits.
5) Convert all 4 digits value in to its equivalent decimal value.
6) Arrange all the decimal value in sequential manner to form secret image(g).

5 Results and Discussions

In this method, for embedding purpose four Cover images were used. They are Lena, Gandhi, Mother Teresa and temple. Secret image is Baboon. Both of the secret image and cover image size is 256×256. The disturbance in the Stego image is calculated using PSNR and MSE.Let M and N be the rows and columns of the matrix of the image's pixels and R be the maximum error occurs in the stego image. Table 1 describes the PSNR and MSE values for the four stego images which are obtained with the help of proposed embedding algorithm. Figure 1 is the Secret image which is hidden in the cover images. Figures 2, 4, 6, 8 are the cover images used for embedding. Figures 3, 5, 7, 9 are the stego images. Figures 10, 12, 14, 16 are the histograms of the original images (Figures 2, 4, 6, 8 respectively). Figures 11, 13, 15, 17are the histogram of the stego images (Figures 3, 5, 7, 9 respectively.)

Table 1: The MSE and PSNR values for the proposed method

Stego-Image	**Red -PSNR**	**Red-MSE**	**Green-PSNR**	**Green-MSE**	**Blue-PSNR**	**Blue-MSE**
Lena	60.3030	0.0606	58.9794	0.0822	60.1428	0.0629
Gandhi	60.2606	0.0612	55.9256	0.1662	56.1500	0.1578
Mother Teresa	57.9897	0.1033	56.6041	0.1421	58.4761	0.0924
Temple	58.7836	0.0860	57.4020	0.1183	59.8987	0.0666

Figure 1: Secret image (Baboon)

Figure 2: Cover Image (Lena)

Figure 3: Stego Image (Lena)

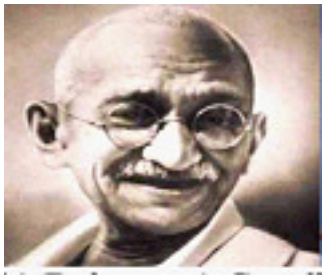

Figure 4: Cover Image (Gandhi)

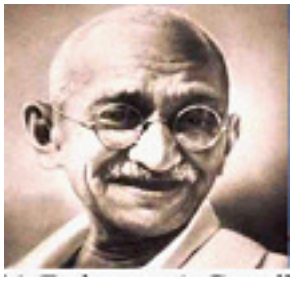

Figure 5: Stego Image (Gandhi)

Figure 6: Cover Image (Mother Teresa)

Figure 7: Stego Image (Mother Teresa

Figure 8: Cover Image (Temple)

Figure 9: Stego image (Temple)

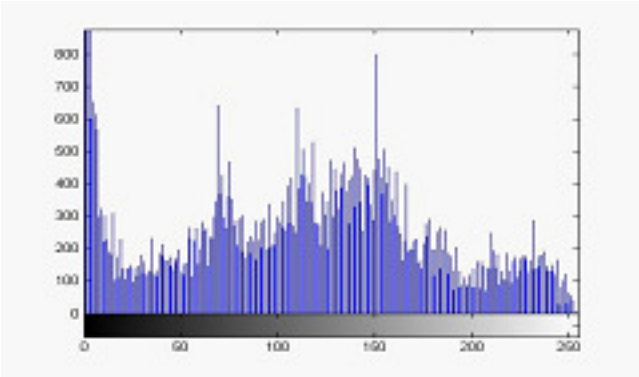

Figure 10: Histogram of CoverImage (Lena)

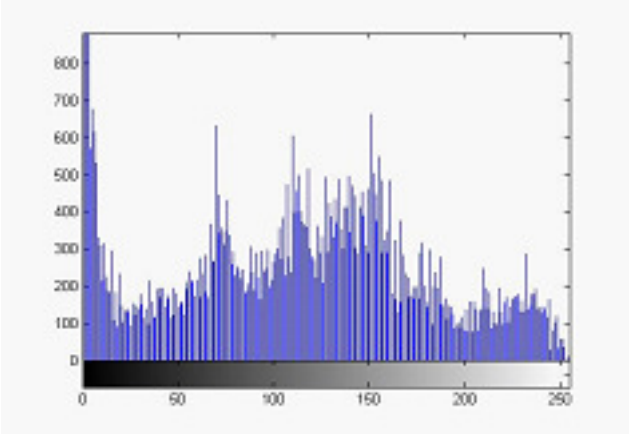

Figure 11: Histogram of Stego Image (Lena)

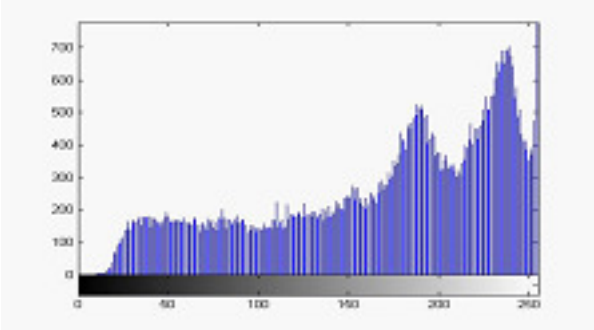

Figure 12: Histogram of CoverImage (Gandhi)

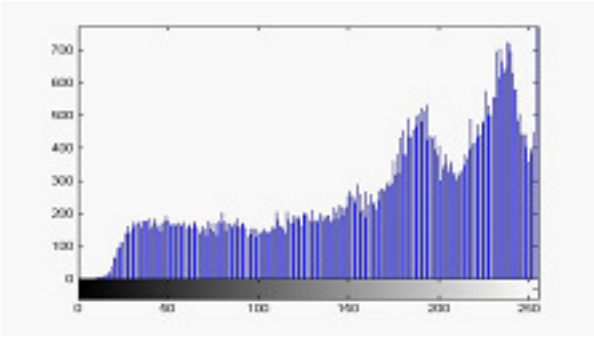

Figure 13: Histogram of Stego Image (Gandhi)

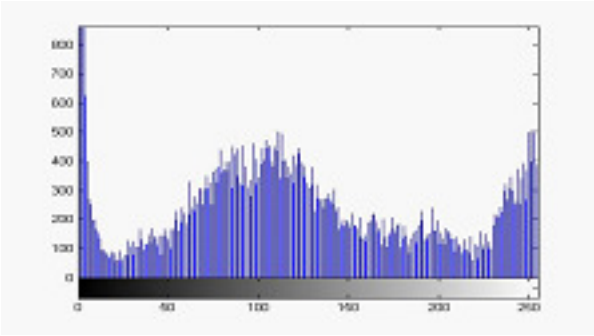

Figure 14: Histogram of Cover Image (Mother Teresa)

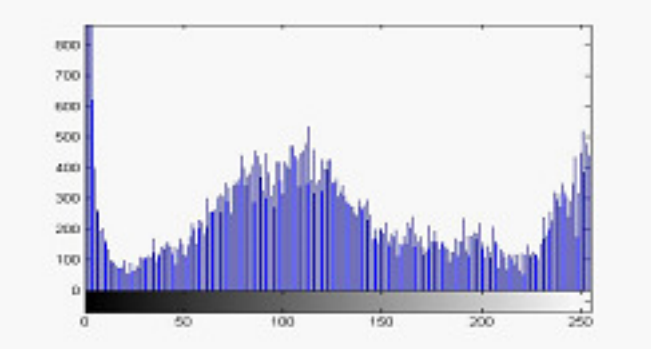

Figure 15: Histogram of Stego Image (Mother Teresa)

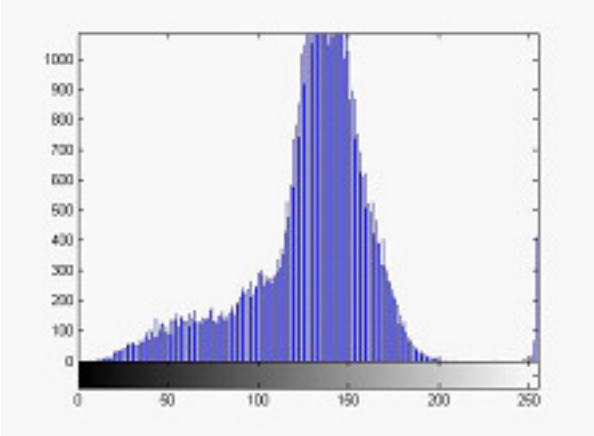

Figure 16: Histogram of Cover Image (Temple)

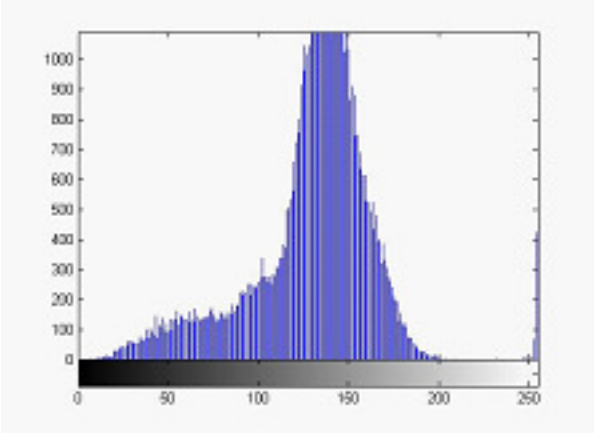

Figure 17: Histogram of Stego Image (Temple)

6 Conclusion

A new way of hiding technique has been proposed by introducing the concept of CMYK colour layers in image in the field of steganography. Hiding the message in CMYK colour layers provides more secure and good image quality rather than its RGB colour layers. The PSNR and MSE value is in good range in the CMYK approach when compared to RGB colour model. In this method, if the attacker tries to break the image into RGB colour layers also he cannot retrieve the message fully.

References

[1] R. Amirtharajan, D. Adarsh, V. Vignesh, and R. Boscobalaguru, "PVD blend with pixel indicator - OPAP composite for high fidelity steganography," *International Journal of Computer Application*, vol. 7, no. 9, p. 31?37, 2010.

[2] C. K. Chan And L. M. Chen, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 8, pp. 469–474, 2004.

[3] A. Cheddad, J. Condell, K. Curran, and P. Mckevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] S. Hemalatha, U. Dinesh Acharya, and A. Renuka, "Wavelet transform based steganography technique to hide audio signals in image," *Procedia Computer Science*, vol. 47, no. 2, pp. 272–281, 2015.

[5] S. Manoharan, "Efficient x-box mapping in stego-image using four-bit concatenation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 29–33, 2014.

[6] K. Muhammad, H. Farman, and M. Sajjad, "A secure method for color image steganography using gray-level modification and multi-level encryption," *KSII Transactions on Internet and Information Systems*, vol. 1, no. 10, pp. 27–32, 2015.

[7] V. Nagaraj, Z. Dr Vijayalakshmi, and G. Dr Zayaraz, "Colorimage steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, no. 11, pp. 17–24, 2013.

[8] M. Shobana, "An efficient image steganographic algorithm using cmyk color model," *International Journal of Research and Innovations in Science & Technology*, vol. 90, no. 12, pp. 25–31, 2015.

[9] M. Shobana, P. Gitanjali, M. Rajesh, and R. Manikandan, "A novel approach for hiding image using pixel intensity," *International Review on Computers and Softwares*, vol. 8, no. 5, pp. 904–908, 2013.

[10] V. Thanikaiselvan, S. Kumar, N. Neelima, And R. Amirtharajan, "Data battle on the digital field between horse cavalry and interlopers," *Journal of Theoritical Technology*, vol. 29, no. 7, pp. 85–91, 2011.

[11] Z. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan, and J. B. BalaguruRayappan, "Wave (let) decide choosy pixel embedding for stego," in *IEEE 2011 International Conference on Computer, Communication and Electrical Technology*, pp. 157–162, 2011.

[12] K. C. Wu, "Steganography using reversible texture synthesis," *IEEE Transactions on Image Processing*, vol. 24, no. 6, pp. 130–139, 2015.

Biography

M. Shobana is working as an Assistant Professor in the Department of Electronics and Communication Engineering in Karpagam College of Engineering Tamil Nadu,India.Her area of interest is Steganography,Internet of Things and network Security.

R. Deepika is working as an Assistant Professor in the Department of Electronics and Communication Engineering at Karpagam College of Engineering Tamil Nadu,India.Her area of interest is Network On Chip,Steganography and network Security.