Journal of Naval Science and Engineering
2016, Vol. 12, No.2, pp.79-92
Elektronik Mühendisliği/Electronic Engineering

IMPLEMENTATION OF A DISTINCT RGB ENCODING TECHNIQUE FOR DATA HIDING IN IMAGES

Feyzi AKAR
Faculty of Electrical and Electronics Engineering,
Naval Academy, Tuzla, 34940, Istanbul, Turkey
feyziakar@dho.edu.tr

Date of Receive: 19.09.2016 **Date of Acceptance: 01.11.2016**

ABSTRACT

A new R−weighted Coding Method (RCM) is improved in this study. This Method offers high data hiding capacity and PSNR values. Experimental results show the usefulness and advantage of the proposed method over its classical counterparts, providing high performance, in terms of PSNR and particularly data hiding capacity. RCM has been adopted from an earlier study that well known the LSB (Least Significant Bit) coding technique. This information hiding/embedding method can be used for protecting of any secret data.

Keywords: Data embedding, data hiding, steganography, RGB Image coding.

ÖZ

Bu çalışmada yeni bir R ağırlıklı kodlama tekniği geliştirilmiştir. Bu metod yüksek veri gizleme kapasitesi ve PSNR değeri sağlar. Deneysel sonuçlar özellikle gömme kapasitesi ve PSNR açısından çalışmanın klasik rakiplerine göre kullanışlılık ve avantaj sağladığını göstermektedir. RCM metodu LSB (Least Significant Bit ; En düşük değerlikli bir kodlaması) olarak bilinen kodlama tekniğinden geliştirilmiştir. Bu bilgi gizleme/gömme metodu herhangi bir gizli bilginin korunması amacıyla kullanılabilir.

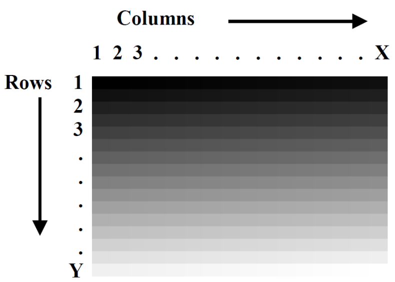
I. Introduction

Data hiding methods have become increasingly more sophisticated and widespread. Which is a discipline that conceals data in a carrier to deliver secret messages. Embedding applications are mostly based on computer software where a vast variety of many complicated algorithms are improved and implemented [1]. Steganography is a technique that conceals the secret messages in innocuous cover objects by means of various information hiding methods. Data hiding, a form of steganography is a technique to embed the original secret image to another cover image by some encryption/encoding techniques, which has potential applications in multimedia and information security. The objective of this research is to propose a different data hiding method for secret data or critical information in images [2].

Any convenient digitized content (picture, audio, and video, etc.) can be used as carriers The digital images are often used as carriers as following reasons. First of all they can be easily delivered over the puplic or through a managed, private network, thus it may take attention with little suspicion when the secret information is embedded. Another reason is that, pixels are highly correlated for most natural images and therefore this situation is very suitable for hiding information. Also, digital images are much easier to be presented in documents than the other types of digitized content. [3]. Data hiding methods have recently made a challenging progress together with the new developments in computer technologies. A lot of data hiding methods and their applications have been proposed since the beginning of 1950s. On the other hand, their initial applications in many domain were unable to ensure a critical secure level of information in time. Thus, both new data hiding techniques and their development have always received ever−increasing interest in parallel to the emerging computer technologies and algorithms [4].

II. Digital Image and Data

In any digital image, a pixel is the smallest item of information in an image that is represented by a series of Y rows and X columns (Fig. 1). Pixels are normally showed in a 2−dimensional grid and are frequently represented using squares or rectangles for gray images. Each pixel is a part of an original image, where the more samples typically provide the more accurate representations of the original. The intensity of each pixel is variable; for example in color systems, each pixel has typically three components and 3−dimensions, e.g., RGB (red, green and blue) [2,5].



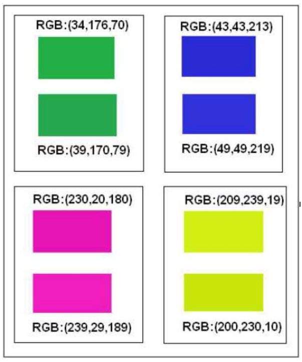


Figure 1. Digital image structure

In order to represent each pixel, number of bits assigns how many colors can be produced. For example, in an RGB color mode, the color monitor uses 24 bits each pixel (8 bits for each channel), allowing displaying 2^{24} (16,777,216) different colors. The number of colors can be obtained when bit depth is increased. This condition is an important circumstance and required for data hiding [4,5].

III Embedding a byte in a Pixel Cell

A pixel-cell constitutes the smallest building stone in an image. Image is occurred by means of uniting these pixels. The smallest color-cell occurs to uniting with three colors, those are called RGB; red, green and blue. These main colors constitute other intermediate colors with mixing a certain ratio. Each main color signify eight-bits (one byte) and so it has between 0 to 255 decimal numbers corresponding with its density. Accordingly, total size has equivalent three bytes or 24-bits. If a color-cell have a (RGB) weighted: (34,176,70) that indicates R=34, G=176, B=70. The obtained RGB dispersion and eight-bits equivalents are shown in Figure 2.

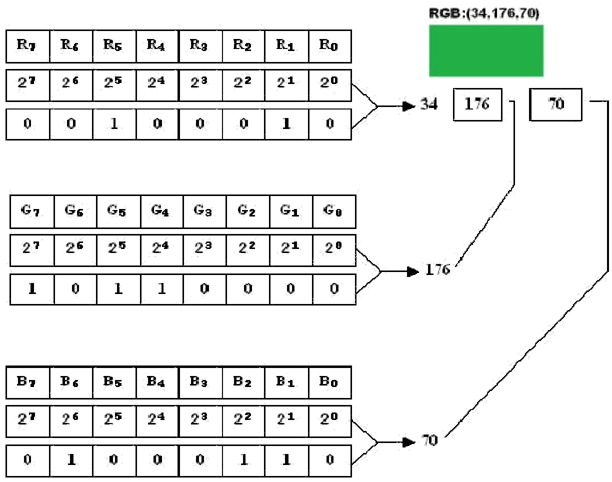


Figure 2. The obtained RGB dispersion as eight-bits equivalents.

For an ASCII code that has equivalent value “154” $(10011010)_2$ is embedding in a color-cell which have a (RGB) weighted (34,176,70). These processes are executed step-by-step in Fig. 3.

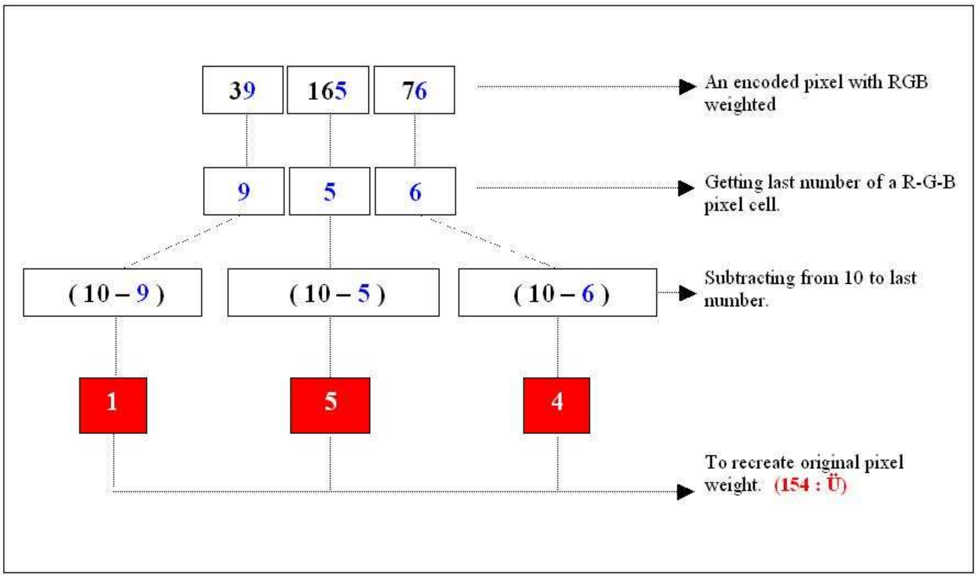


Figure 3. The Processes of Embedding an ASCII Code in a Pixel Cell

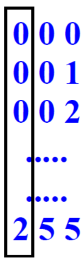


Figure 4. Recreating an ASCII Code where is Embedded a RGB Pixel Cell.

There are two different colors which have RGB: 34,176,70 and RGB: 39,165,76 for a pixel. These colors signify before and after of data hiding or embedding processes. The loss is available but it isn't perceived by the human sense. Now, our first privileged aim is that to provide an embedding without deterioration on the image. Furthermore, it has to embed in image as the biggest sized data. It can be stored to one-byte data for one pixel. Consequently, an image which has sized (310 × 220) pixel or (10,94 × 7.76) cm, that can be, stored (310 × 220) 68200 Byte, thus approximately 66.6 Kbyte data can be embedded in the image. The obtained capacity and the outcome are being quite satisfied for image, which has small sized.

IV. Changing of "R" Coding Weighted

The embedding process of last two-bit of part of eight-bit "R"

So far, we have discussed a novel embedding method that is changed all of RGB weighted with the same method. In this section we will discuss the other encoding way in which a data hiding can be embedded using last two-bits of R; R_1 AND R_0. It is necessary that must be minimal deterioration on the embedded image. Thus, the coded image become increasingly resembles original image. Because of this, it will apply a distinct encoding technique for part of R.

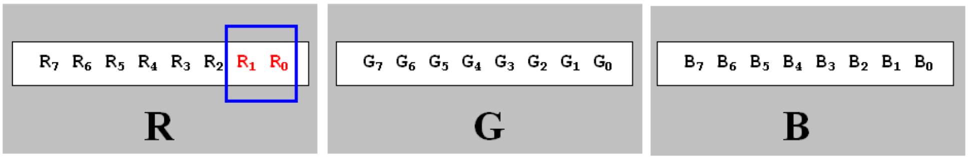


Figure 5. The embedding process of last two-bit of part of eight-bit "R"

In an extended ASCII, alphanumeric characters are represented by numbers ranging from 0 to 255 and are translated into an 8-bit binary code, hence first digit of 0 to 255 (MSB) can be 0 or 1 or 2. It can't be 3 to 9 numbers. This situation can be used as a useful advantage. In a data hiding application using RGB weighed coded technique that is constituted 3 distinct RGB colors weighed with each one 8 bit. The last two-bit of the first eight-bit (MSB), R1 and R0 are being used for this aim. Figure 5 illustrates this technique. For instance we assume a pixel that has RGB values (34,176,70) and "A", ASCII (065) character is desired to embed in this pixel. .Figure 5 graphically illustrates the concept of this novel technique. The operation process is as follows.

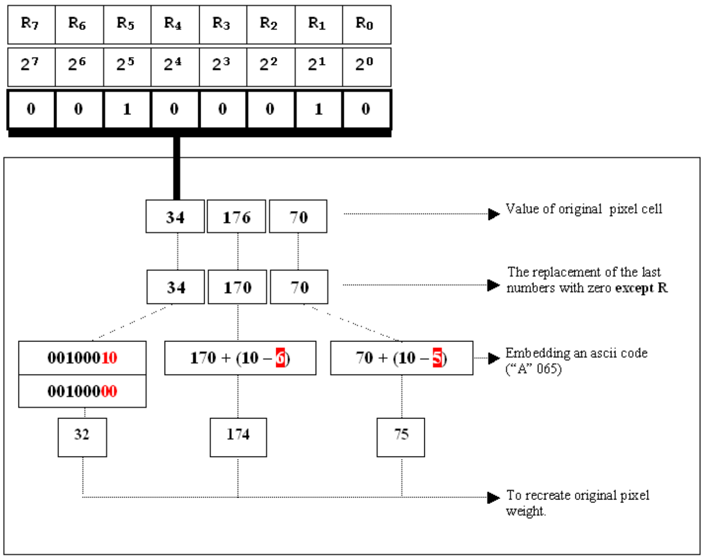


Figure 6. The Processes of Embedding an ASCII Code with R and GB in a Pixel Cell

A pixel that has RGB (34,176,70) value, its weight of R has 34. The value of BCD (34) has equal (00100010) as 8-bit binary. The last two-bit of the first eight-bit (MSB), R1 and R0 replace with "00" bits. Thus the result of new eight-bit is "001000 + 00". In an extended ASCII, first digit of 0 to 255 (MSB) can be 0 or 1 or 2. These equal "00", "01", "10". Character of "A" equals 065 values as ASCII; accordingly first digit of number of 065 is "0". The last two-bit of the first eight-bit (MSB), R1 and R0 are replace value of "00". In this way, value of eight-bit binary 00100000 is obtained. This eight-bit equal 32 as BCD; $32=(00100010)_2$.

Embedding technique of both G and B are applied same old method. Because, both can have zero-nine number in an extended ASCII. This method can be applied last four bits for G and B; merely this situation is caused a lot of deterioration in an image.

V. Reconstruction of embedded data of last two-bit of eight-bit "R"

Firstly, value of R: 32 convert to from BCD to binary form. $(32)10=(00100000)_{2.}$ Getting last two-bit of R, R1 and R0. (R1 R0 = 00) These binary numbers are equal "0" as BCD. The last digit of number of G: 174 is "4" and B: 75 is "5" . Both number are subtracting from 10. (10-4=6 and 10-5=5) Thus, number of 6 and 5 are obtained. Figure 7 graphically illustrates the processes of this technique On the whole, value of BCD (065=A) has attained.

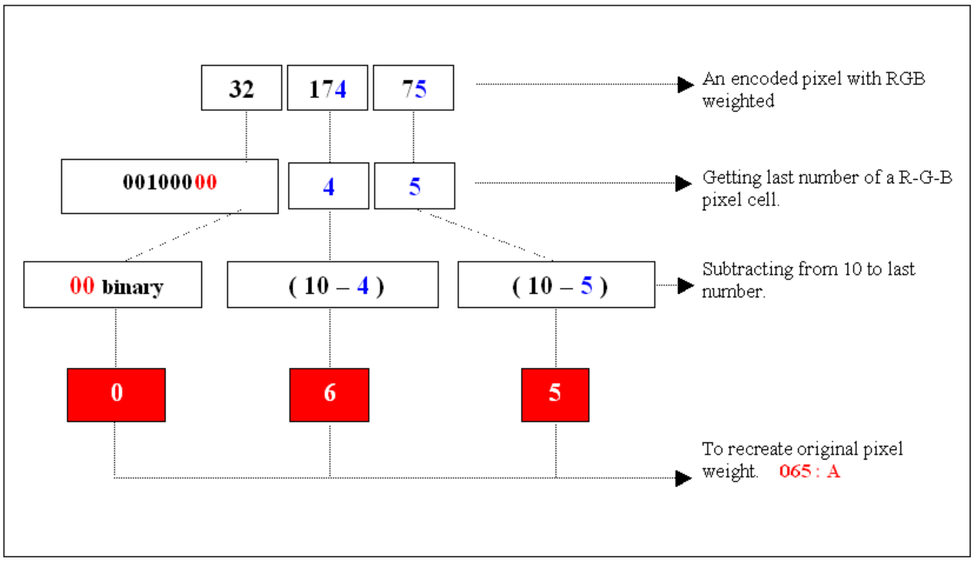


Figure 7. Recreating an ASCII Code where is Embedded a RGB Pixel Cell.

VI. Quality measures

In general terms "Peak Signal to Noise Ratio" (PSNR) and "Mean Square Error" (MSE) parameters are operated for statistical analysis of the image embedding methods. The MSE should be figured out first as given in equation (1) and equation (2). As a second step PSNR can be derived as in equation (3) [12,13], where "O" and "S" are the original and stego image pixel values (binary) respectively to be compared and the image size is "X × Y". PSNR result of the stego images produced by all of the histogram−based data hiding techniques is guaranteed to be above the other classical techniques' performance in terms of statistical and perceptual invisibility. Note that the equations (1) and (2) are defined for only monochrome images, but for color images, the denominator of the equation (3) is multiplied by a factor 3. To compute the PSNR, the block first calculates the mean−squared error using the following equation [4]:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left\| O(i,j) - S(i,j) \right\|^2 \qquad [1]$$

$$MSE = \frac{\sum_{m,n} \left[O(i,j) - S(i,j) \right]^2}{m \times n} \qquad [2]$$

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \qquad [3]$$

TABLE I. Comparison of other methods on bit rate and PSNR for Lena Image

Method	PSNR (dB)	Bit rate (bpp)
Goljan et al. [6]	39.00	0.092
Celik et al. [7]	38.00	0.284
Tai et al. [8]	37.98	0.493
Xuan et al. [9]	34.39	0.600
Tian [10]	34.80	0.671
Jung and Yoo [11]	41.46	0.766
Proposed	39.56	1.469 *

Table I shows that the proposed method not only has improved the data embedding capacity but also the PSNR for the well−known Lena image compared to its counterparts. Proposed method allows in much better the data embedding capacity compared to the classical methods. Data embedding methods are confirmed through well−known quality measures. PSNR value is the primary metric but it does not match with the HVS exactly. In addition to PSNR, some perceptual measures put forward such as Universal Image Quality Index (UQI) [14], Visual Information Fidelity (VIF) [15] and Mean Structural Similarity (M−SSIM) [14] in order to evaluate and analyze the data hiding methods. The UQI, VIF and the M−SSIM are measured as a quality result (Q) that ranges between [−1 and 1], between [0 and 1] and between [0 and 1] respectively, meaning that the best Q value can be 1 for all of them.

	RWB	LSB (2bits)	LSB	HSV	RWB	LSB (2bits)	LSB	HSV
	Lena				Baboon			
VIF	0.9798	0.9802	0.9981	**0.9993**	0.9823	0.9888	0.9930	**0.9997**
UQI	0.9237	0.9440	0.9988	**0.9995**	0.9724	0.9814	0.9945	**0.9998**
M−SSIM	0.9531	0.9654	0.9991	**0.9997**	0.9801	0.9890	0.9980	**0.9999**
	Peppers				Airplane			
VIF	0.9573	0.9786	0.9980	**0.9998**	0.9571	0.9325	0.9976	**0.9997**
UQI	0.9012	0.9435	0.9976	**0.9999**	0.8375	0.9390	0.9950	**0.9997**
M−SSIM	0.9366	0.9703	0.9986	**0.9999**	0.9422	0.9612	0.9980	**0.9998**

TABLE 2. Experimental results for different statistical metrics for different 512×512 gray images.

As mentioned above, only a PSNR analysis is not adequate for a complete quality assessment of any steganography method. In addition to

PSNR; VIF, UQI and M−SSIM visual quality measures are also used for the performance comparisons in this section (Table 2). Considering these parameters, the HSV method gives results that are closer the finest quality.

VIII. Conclusion

In this paper a novel R−weighted Coding Method (RCM) is discussed for protecting of any secret data. It is intended with this method that negligible deterioration in image and maximal storage of secret data. This Method offers high data hiding capacity and PSNR values. Experimental results show the usefulness and advantage of the proposed method over its classical counterparts, providing high performance, in terms of PSNR and particularly data hiding capacity. In this research particularly the deterioration of original image is decrease thanks to changing of "R" Coding Weighted technique.

References

[1] I. J. Cox and M.L. Miller, “The first 50 years of electronic watermarking”, Journal of Applied Signal Processing, vol.16(4), pp. 126–132, 2002.

[2] F. Akar and H.S. Varol, “A new RGB weighted encoding technique for efficient information hiding in images”, Journal of Naval Science and Engineering, vol. 2, pp. 21−36, July 2004.

[3] W. Hang, T. S. Chen, and C. W. Shiu, “Reversible data hiding based on histogram shifting of prediction errors”, International Symposium on Intelligent Information Technology Application Workshops, pp. 292–295, 2008.

[4] Y.Yalman, F.Akar and İ.Ertürk Contemporary Approaches to the Histogram Modification Based Data Hiding Techniques, “Recent Advance in Steganography”, , ISBN 978-953-51-0840-5, InTech, November 11, 2012

[5] Y. Yalman and I. Erturk, “A new histogram modification based robust image data hiding technique”, IEEE 24th International Symposium on Computer and Inf. Sciences (ISCIS’09), pp. 39–43, September 2009.

[6] M. Goljan, J. Fredrich, and R. Du, “Distortion–free data embedding”, Proc. of 4th Information Hiding Workshop, pp. 27–41, 2001.

[7] M. U. Celik, G. Sharman, A. M. Tekalp, and E. Saber, “Reversible Data Hiding”, IEEE International Conference on Image Processing, vol. 2, pp. 1646–1648, 2002.

[8] W. L. Tai, C. M. Yeh, and C. C. Chang, “Reversible data hiding based on histogram modification of pixel differences”, IEEE

Transactions on Circuits and Systems for Video Technology, vol. 19(6), pp. 906–910, 2009.

[9] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, “Reversible data hiding based on wavelet spread spectrum”, IEEE 6th Workshop on Multimedia Signal Processing, pp. 211–214, 2004.

[10] J. Tian, “Reversible data hiding using a difference expansion”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 13(8), pp. 890–896, 2003.

[11] K. H. Jung and K. Y. Yoo, “Data hiding method using image interpolation”, Computer Satandards and Interfaces, vol. 31(2), pp. 465–470, 2009.

[12] Netravali A. N. & Haskell, B. G. (1995). Digital Pictures: Representation, Compression and Standards, Plenum Press, New York, 1995.

[13] Rabbani, M. & Jones, P. W. (1991). Digital Image Compression Techniques, SPIE Optical Engineering Press, Washington, 1991.

[14] Wang, Z.; Bovik, A. C.; Sheikh, H.D. & Simoncelli, E.P. (2004). Image Quality Assessment: From Error Visibility To Structural Similarity. IEEE Transactions on Image Processing, vol. 13, 2004, pp. 600–612.

[15] Sheikh, H. D. & Bovik, A. C. (2006). Image Information and Visual Quality. IEEE Transactions on Image Processing, vol. 15, 2006, pp. 430–444.