Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Use of Least Significant Bit Technique at Various Color Spaces for secure Steganography with Performance Evaluation

R.Meenakshi
M. phil Research Scholar,
Department of Comp. Sci. & Engg.
Alagappa University,
Karaikudi, India

Dr.K.Kuppusmay
Professor,
Department of Comp. Sci. & Engg.
Alagappa University,
Karaikudi, India

Abstract*—Steganography is the art and science of information hiding behind other text, image, and audio as well as the video formats. Most probably images are considered as the secure way to hide the secret data. The images are categorized into different forms at different color spaces. The color model is basically a mathematical model, which represents the color spaces as tuples of numbers, typically as three or sometimes four values called as color components. In this paper, we, propose the implementation of Least Significant Bit technique functioning at different color spaces such as YIQ,XYZ,HSV,$YC_bC_{r,,}$ except the RGB and calculate their Peak Signal Noise Ratio (PSNR) value for the image at every color space. According to the PSNR value the performance analysis is made and justification is made upon the color space usage. The PSNR value is taken, since the level of noise of the image will holds the amount of pixels get noised or changed. Furthermore, the experimental results are compared with the existing available techniques. Apart from the PSNR values the Mean Square error, Normalized cross correlation, Average difference, Structural content, maximum difference and normalized absolute error also measured.

Index Terms: — Color spaces, Image Steganography, Least Significant Bit Technique, peak signal noise ratio.

I. INTRODUCTION

Various techniques are in use to protect the image transmission in the communication media. Some of them are, Steganography, image encryption, visual cryptography and watermarking. Steganography is used to hide the secret data within some embedded media like text, image, audio, and video, etc. But the most commonly used media for Steganography is an image file. For Stenographic technique keys are important process. The keys are classified as keyless performance, public key and Secret key [8]. Hiding secret information depends upon the three major factors namely capacity, security, and robustness of the image [3].Image Steganography is categorized into two division's namely spatial domain and frequency domain.

Stenographic overall functionality can be simply stated as follows. Initially the plain text which is to hide into images will be provided. The Cover image refers to the carrier to embed the message into. Stego key means a key refers to hide and retrieval of message. Embedding algorithm means to hide the message. Extracting algorithm used to unhide the message. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. Typically there are several stenographic techniques used in current trends. Such as LSB, DCT, DFT and DWT method, Multiple Bit-planes Based Steganography, Prediction Error Based Steganography, and Quantization Based Steganography, Pixel Value Differencing (PVD), and Modified Kekre Algorithms (MKA). Steganalysis is, from an opponent's perspective, is an art of deterring covert communications while avoiding affecting the innocent ones.

The color model is basically a mathematical model, which represents the color spaces as tuples of numbers, typically as three or sometimes four values called as color components. **(**e.g. RGB and CMYK are color models). Adding a certain mapping function between the color model and a certain reference color space results in a definite "trail". This trail is known as a combination with the color model, defines a new color space.

The user can actually only detect three of these visible colors - red - blue and green. These colors are called primary color space. A color space is a method of representing each color in terms of a combination of several numeric values. It is a method by which the user can specify, create and visualize color. Different color spaces are better for different applications. All these color spaces are the category of primary spaces: It is based on the trichromatic theory which states that any color can be expressed as a mixture of three primaries.

Luminance-chrominance: It represents colors in terms of luminosity and two chromaticity components. Perceptual spaces: It is based on the human visual system and commonly strives for being perceptual uniform. Independent axis spaces: It esults from other spaces by applying mathematical operations that aim at decor relating individual components.

The rest of the paper is organized as follows. Section 2 brings out views on the related works to the proposed area. Section 3 comes out with our proposed work of LSB technique applied in various color spaces. Section 4 contains experimental results and the comparative results from the proposed work. Section 5 contains the conclusion based on the performance value retrieved from every color space.

II. RELATED WORK

S. M. MasudKarim, et al., [9] proposed a new approach based on LSB using a secret key. The secret key encrypts the hidden information and then it is stored in different position of LSB of the image. This provides very good security. XIE Qing et al.,[15] proposed a method in which the information is hidden in all RGB planes based on HVS (Human Visual System). An algorithm in which binary images are considered to be secret images which are embedded in the cover image by taking the HSV (Hue, Saturation, Value) values of the cover image into consideration[2]. KapreBhagyashri et al [7], a new singular value decomposition (SVD) and DWT based watermark technique is proposed in full frequency band in YUV color space.

Juan José Roque, Jesús María Minguet, propoes "SLSB: Improving the Steganographic Algorithm LSB", a novel steganographic algorithm based on the spatial domain: Selected Least Significant Bits (SLSB). It works with the least significant bits of one of the pixel color components in the image and changes them according to the message's bits to hide[6]. The rest of bits in the pixel color component selected are also changed in order get the nearest color to the original one in the scale of colors. This new method has been compared with others that work in the spatial domain and the great difference is the fact that the LSBs bits of every pixel color component are not used to embed the message, just those from pixel color component selected[6]. Hemalatha S, U Dinesh Acharya, Renuka A, explains about comparison of secure and high capacity Color image steganography techniques in RGB and YCBCR domains. According to their comparison, they show that the quality of the stego images is good in RGB domain by comparing the PSNR values. But RGB method may be detected more easily than YCbCr method since RGB is the normal standard representation for color images. And RGB steganography method requires more execution time than YCbCr method. The PSNR values show that the quality of extracted secret images are good in YCbCr method[5]. Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, have shown the use of LSB technique in Image and Audio Steganography. They have shown, the method is a very high watermark channel capacity. The obvious disadvantage is the extremely low robustness of the method, due to fact that random changes of the LSBs destroy the coded watermark. Since no computationally demanding transformation of the host signal in the basic version of this method needs to be done, this algorithm has a very small algorithmic delay. This algorithm is a good basis for steganographic applications for audio signals[1]. Bhavana.S,and K.L.Sudha, extends their views on LSB technique in text Steganography along with the chaos theory. They, describes about a Steganography techniques, for hiding text message using the concept of non-linear dynamic system (chaos). The chaos system is highly sensitive to initial values and parameters of the system. Their algorithm provides security and maintains secrecy of the secret message and provides more randomness since using chaos which is sensitivity to initial conditions [4].

III . PROPOSED METHODOLOGY

A. LSB Algorithm

One of the flexible and efficient images Stenographic Technique is Least Significant Bit embedding technique. The magic of the LSB technique is when hiding the information in the image, the user can't find information hosts inside the secret image. The data can be hidden in the least significant bits of the cover image to the hidden image in the cover file. This process is looping when decomposition of least significant bit of each pixel is replaced with secret message bits until message end. So the message is hidden even in the second to least significant as well as in the least significant bit then too. The main advantage of LSB method is Integrity of secret hidden information with High Capacity.

LSB Algorithm to embed text message:-

- Read the cover image and text message which is to be hidden in the cover image.
- Convert text message into a binary file.
- Calculate LSB of each pixel of the cover image.
- Replace LSB of the cover image with each bit of secret message one by one.
- Write the stego image

LSB Algorithm to retrieve text message:-

- Read the stego image.
- Calculate LSB of each pixel of stage image.
- Retrieve bits and convert each 8 bits into a character.

B. LSB Alogrithm YIQ color space

YIQ is used in JPEG image compression and MPEG video compression. It is a rotation of the RGB color space such that the Y axis contains the luminance information; the chrominance information is contained in I (orange-blue) and Q (purple-green) which are roughly orthogonal. The conversion of RGB to YIQ is taken place such that, Y' is similar to perceived luminance; 'I and Q' carry color information and some luminance information. Since pixel values are highly correlated in RGB color spaces, the watermark embedding in YIQ color space is preferred for Watermarking. The result of the conversion is presented in the figure (7a) and the stego image in 7b.

C. LSB Algorithm in XYZ Color Space

The XYZ color space was derived from a series of experiments in the study of the human perception by the International Commission on Illumination. It works as a standard reference against where the other color spaces can be used. When non negative values arrives the conversion becomes succeed, the conversion is presented in the figure 5a and the stego image is given in 5b.

D. LSB Alogrithm in HSV Color space

HSI means Hue, Saturation ad Intensity Value for human perception. It represents colors similarly to the human eye perception. The working procedure is given as, finding the point on one of the bottom three faces of the RGB cube which has the same hue and chroma as defined color. Finally, add equal amounts R, G and B to reach the proper lightness or value. The result is given in the figure 3a and the stego image is given in 3b.

E. LSB Alogrithm in YCbCr Color space

YC_bC_r color space is used for color images cryptography. In this color space, the Y denotes the luminance component. It means that Y shows the brightness (luma). Also both of Cb and Cr represent the chrominance actors. It means that Cb is blue color minus luma and Cr is red color minus luma. The difference between YCbCr color space and RGB color space is that YCbCr color space represents color as brightness and two color difference signals, while RGB represents color as red, green and blue. The conversion of the image is presented in the figure 6a and the stego image is given in 6b.

F. LSB Algorithm in CMYK Color space.

CMYK is widely used for the printing process, since it describes the links for the reflection of the colors. One starts with a white substrate and uses ink to subtract color from white to create an image. CMYK stores ink values for cyan, magenta, yellow and black. There are many CMYK color spaces for different sets of inks, substrates, and press characteristics. The conversion is shown in the figure 2a and the stego image is given in 2b.

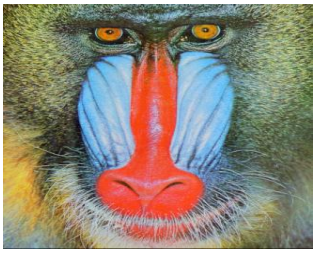
G.LSB Algorithm in L*a*b* Color Space

A L*a*b* color space is a color opponent space with the light dimension at L, a, b for the color – opponent dimensions, based on non linear space coordinates. The conversion of the image to Lab is presented in the figure 4a and the stego image is described in 4b.

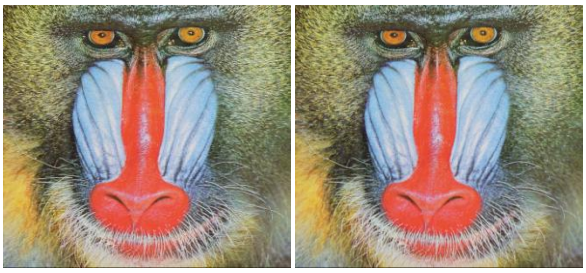
IV. EXPERIMENTAL RESULTS

The following section shows various performance metrics such as the peak- signal- noise- ratio, Mean Square Error, were calculated for the given input image. It comprises of the LSB technique spaces applied at various color and their performance analysis. The performance parameters calculated here are explained as follows: An important property of Peak signal noise ratio value will cause the noise distortion rather than the visual degradation of the image. The Mean Square Error value should remains minimized such that the effectiveness of the original image will be high.

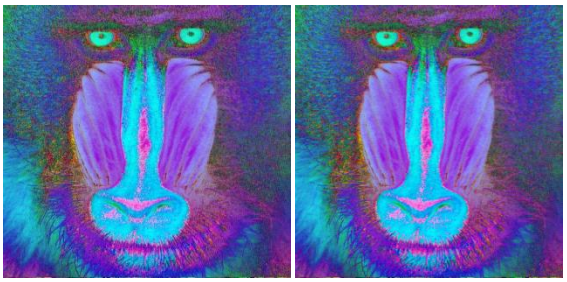
The Average difference shows the clear image as the noise will be reduced from the image. The maximum difference ends in poor quality of the resultant image. The closeness between two images can be calculated using the correlation terms. They are the similarity measures between the images before and after the conversion. Normalized absolute error is a measure of the conversion image from the original image with the value of zero being the perfect fit, whereas the larger values indicates the poor quality of images. The Structural content is given and if it is spread at 1, then the converted image is of better quality and large value of Structural content means that the image is in poor quality.



1a) ***Original Image***

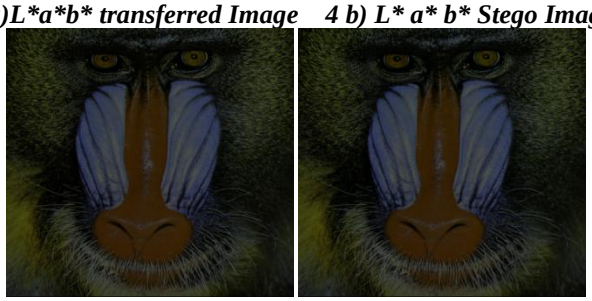


2a)CMYK transferred Image *2 b) CMYK Stego Image*

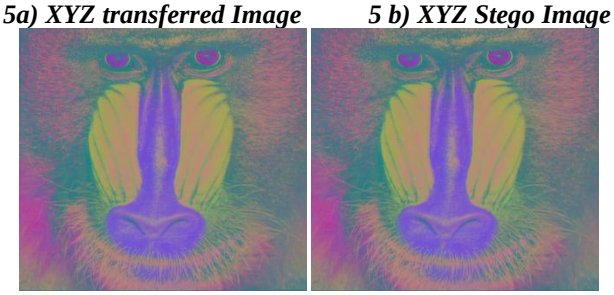


3a)HSV transferred Image *3b) HSV Stego Image*

*4a)L*a*b* transferred Image* *4 b) L* a* b* Stego Image*



5a) XYZ transferred Image *5 b) XYZ Stego Image*



6a) YC_bC_r transferred Image *6 b) YC_bC_r Stego Image*

7a) YIQ transferred Image *7 b) YIQ Stego Image*

Image	Performance Metrics	Values					
		CMYK	**HSV**	**L*a*b***	**XYZ**	**YC_bC_r**	**YIQ**
Baboon Image	Mean Square Error	58.8631	3.4754	1.2306	9.9526	1.0829	7.4711
	Peak Signal Noise Ratio	30.4324	12.7208	17.2297	8.1514	17.7856	9.3970
	Normalized Cross Correlation	1.0495	0.7085	0.9647	0.2716	0.8870	0.3826
	Average Difference	-7.2580	29.4221	-5.0922	96.8927	6.1679	78.8219
	Structural Content	0.9072	1.6558	1.0044	12.7441	1.2015	5.9873
	Maximum Difference	2	178	73	135	95	158
	Normalized Absolute Error	0.0560	0.3690	0.2315	0.7475	0.2094	0.6081

V. CONCLUSION

In this paper, we use the LSB based stego technique, applied at diverse colors spaces. A number of experiments were discussed results were provided. The visual quality of the mixed images is good, it is hardly attracted from eavesdropper by naked eye. As a result, the CMYK color space could be an efficient and robust color space, for text hiding in images. Because, PSNR value indicates the very effective value from the experimental results. Also, hides the text in CMYK color space it does not reflect the perceptual quality of the original image. The future scope for the proposed method might be the development of an enhanced Steganography along with the cryptographic technique. Meanwhile the work can be enhanced for other data format files like video, audio, text.

References

[1] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution", in International Journal of Coputer Applications, Vol77, No 13, September 2013, pp:37-44.

[2] Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of InformationTechnology, Vol. 7, No. 4, October 2010.

[3] Bender, W., D. Gruhl, and N. Morimoto, "Techniques for data hiding", IBM Systems Journal , vol. 35, no. 3/4, 1996, pp. 131-336.

[4] Bhavana.S, K.L.Sudha. "Text Steganography Using Lsb Insertion Method Along With Chaos Theory ".

[5] S.Hemalatha, U.dinesh Achraya, A.Renuka, "Comaprison of secure and high capacity color image steganography techniques in RGB and YCBCR Domains", in International Journal of Advanced Information Technology , Vol. 3, No. 3, June 2013, pp: 1-9.

[6] Juan José Roque, Jesús María Minguet, "SLSB: Improving the Steganographic Algorithm LSB ".

[7] Kapre Bhagyashri, S., " Robust image watermarking based on singular value decomposition and discrete wavelet transform ", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:5),9-11 July 2010.

[8] Low, S. H., and N. F. Maxemchuk, "Performance Comparison of Two Text Marking Methods", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, 1998, pp. 561-572.

[9] Pitas, I., "A Method for Signature Casting on Digital Images," in International Conference on Image Processing, vol. 3, IEEE Press, 996, pp. 215-218.

[10] Prashasti Kanikar,Ratnesh N. Chaturvedi and Vibhishek Kashyap, " Image Steganography using DCT, DST, Haar and Walsh Transform" , International Journal of Computer Applications (0975 – 8887) Volume 65– No.17, March 2013

[11] Rhodas, G. B., "Method and Apparatus Responsive to a Code Signal Conveyed Through a Graphic Image", U.S. Patent 5,710,834, 1998.

[12] Prashasti Kanikar,Ratnesh N. Chaturvedi and Vibhishek Kashyap, " Image Steganography using DCT, DST, Haar and Walsh Transform" , International Journal of Computer Applications (0975 – 8887) Volume 65– No.17, March 2013

[13] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data", in International Journal on Computer Science and Engineering Vol.1(3), 2009, pp:137-141 .

[14] Swanson, M. D., B. Zhu, and A. H. Tewk, "Transparent Robust Image Watermarking", in Proceedings of the IEEE International Conference on Image Processing, vol. 3, 1996, pp. 211-214.

[15] Xie Jianquan,Xiao Yunhua , "A High Capacity Information Hiding Algorithm in Color Image ",e-Business and Information System Security (EBISS), 2010 2nd International Conference on 22-23 May 2010.

