International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 92-96
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

IMAGE STEGANOGRAPHY IN YUV COLOR SPACE

Hiriyanna G.S.
Department of CS & E
JNN College of Engg., Shimoga,
Karnataka, India

G.R.Manjula
Department of CS & E
JNN College of Engg., Shimoga
Karnataka, India

Niharika M R
Department of ISE
NMIT, Bangalore
Karnataka, India

***Abstract*— Presently there is a rapid development of the internet and the telecommunication techniques. Importance of information security is increasing. Cryptography and steganography are the major areas which work on information hiding and security. In this paper a method is used to embed a color secret image inside a color cover image. A 2-3-3 LSB insertion method has been used for image steganography. The important quality of a steganographic system is to be less distortive while increasing the size of the secret image. Use of cryptography along with steganography increases the security. Arnold CATMAP encryption technique is used for encrypting the secret image. Color space plays an important role in increasing network bandwidth efficiency. YUV color space provides reduced bandwidth for chrominance components. This paper demonstrates that YUV color space can also be used for security purposes.**

Keywords— **Watermarking, Haar Wavelet, DWT, PSNR**

I. INTRODUCTION

Cryptography and Steganography are the major areas which work on Information Hiding and Security. Steganography is a process of hiding information. It conceals the communication taking place therefore when using steganography there is always secret information being transmitted and we try to make this information to be discovered just by the intended receiver. The sender hides a message into a cover file like for e.g. (image, audio,vedio) and tries to conceal the existence of that message, later the receiver gets this cover file and detects the secret message and receives it.

G.R.Manjula and AjitDanti's paper titled "A Novel Hash based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain" describes implementation of a Hash based insertion technique[2]. In this paper a method is proposed to embed a color secret image into a color cover image. A 2-3-3 LSB insertion method has been used for image steganography.

Arvind Kumar, K M Pooja's paper titled "Steganography-A Data Hiding Technique", International Journal of Computer Applications, Vol. 9-No.7 [1], describes Steganography as a useful tool that allows cover transmission of information over the communications channel.

Ajit Danti, G. R. Manjula and R. B. Sushma's paper titled " Steganography using Randomized Index Channel with Arnold Cat Map Encryption" [3], describes the usage of randomized selection of index channel for deciding the image carrier. In this paper the algorithm uses LSB principle for embedding a secret color image in RGB 24-bits color image carrier either in one or two channels depending on the third one (index channel).

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

A. Design Architecture

Proposed system includes 3 modules. In first module the secret image to be embedded is changed to YUV color space. In second module the secret image is encrypted using Arnold Catmap Encryption technique to get encrypted image. In third module encrypted image is embedded inside the cover image using the stego system encoder to get stego image. Obtained stego image can be communicated over network. At the receiver end, stego system decoder is a program module that retrieves the embedded secret image.

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 92-96
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

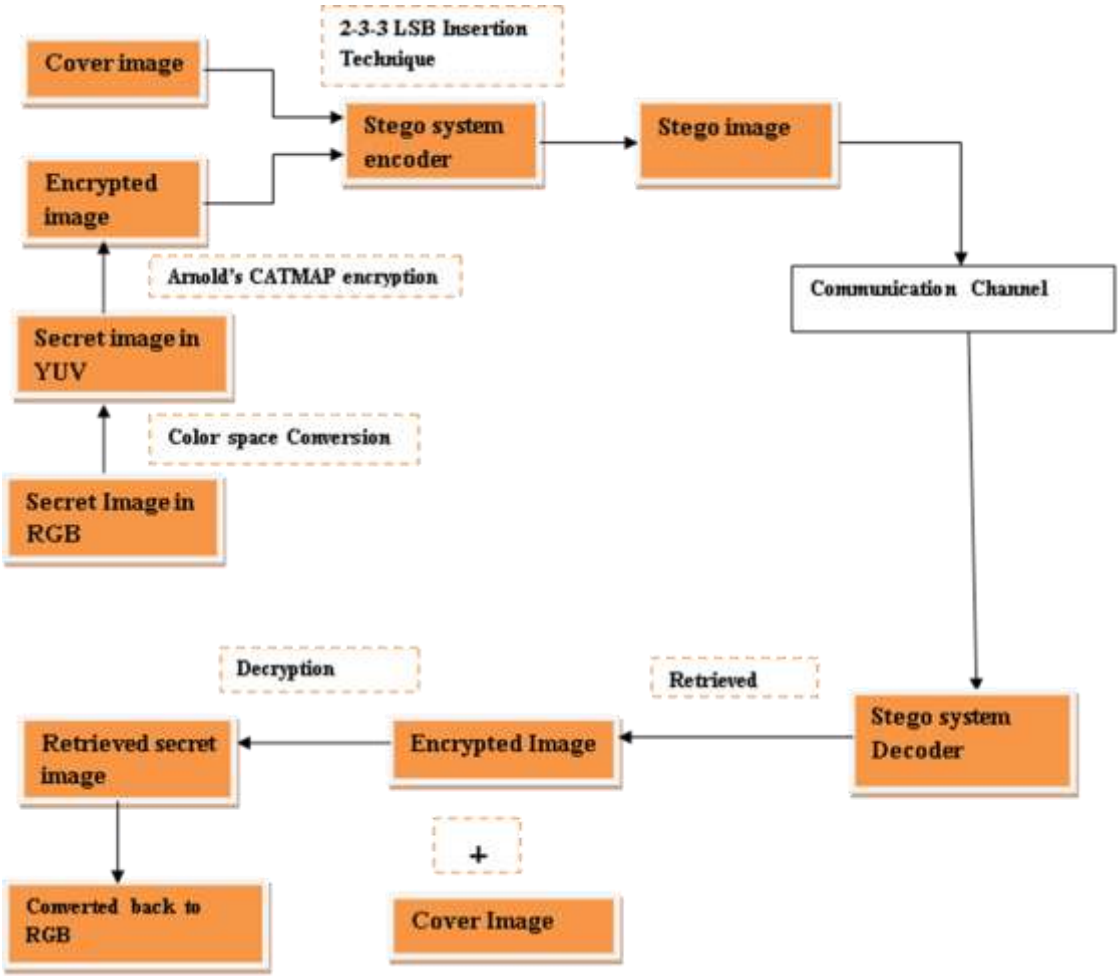


Fig. 1.Design Architecture

B. Embedding algorithm

Step1: Read the Secret image.
Step 2: Change color space of secret image from RGB to YUV.
Step 3: Encrypt the secret image using Arnold Cat Map.
Step 4: Read cover image.
Step 5 : Embedd each byte of secret image inside 3 pixels of cover image using 2-3-3 LSB technique.
Step 6: Output the stego image.

C. Extraction algorithm

Step 1: Retrieve secret image from stego image using 2-3-3 LSB technique.
Step 2: Decrypt the secret image using Arnold Cat Map.
Step 3: Change the secret image from YUV to original color space RGB.

III. EXPERIMENT AND RESULT

The test set for this evaluation experiment of steganography images are randomly selected from the internet. Matlab 2010 software platform is use to perform the experiment.

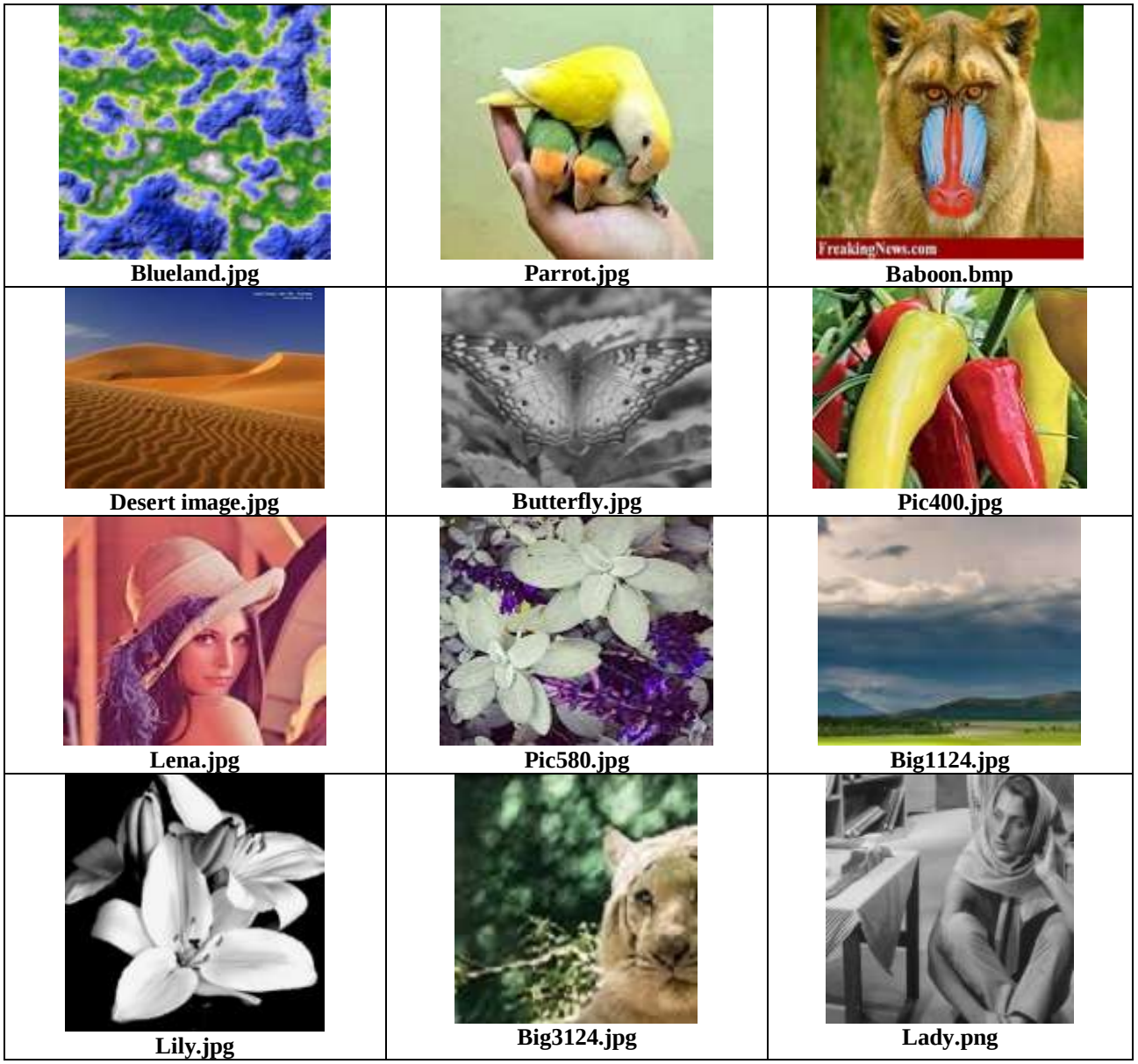
Steganography techniques are measured by two attributes, imperceptibility and capacity. Additionally, as an objective measure, the Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Normalized Absolute Error (NAE) are considered. The quantities are as given below. The PSNR is calculated using the equation (2).

$$PSNR = 10 \log_{10} L^2 / MSE \quad (2)$$

Where L is peak signal level for an image.
The value of MSE is calculated by Equation (3)

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 92-96
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

$$MSE=\frac{1}{HW}\sum_{i=1}^{H}\sum_{j=1}^{W}(P(i,j)*S(i,j))^2 \qquad (3)$$



Blueland.jpg | **Parrot.jpg** | **Baboon.bmp**
Desert image.jpg | **Butterfly.jpg** | **Pic400.jpg**
Lena.jpg | **Pic580.jpg** | **Big1124.jpg**
Lily.jpg | **Big3124.jpg** | **Lady.png**

Fig 2: Test bed of Cover and Secret Images

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 92-96
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

Table -1 Experiment Result

Cover Image	*Secret Image*	*MSE*	*PSNR*	*NAE*
blueland.jpg	*lena.jpg*	*1.2830*	*47.0827*	*0.0028*
blueland.jpg	*big1124.jpg*	*1.1419*	*47.5887*	*0.0028*
blueland.jpg	*desert.jpg*	*1.3064*	*47.0039*	*0.0028*
blueland.jpg	*big3124.jpg*	*1.3491*	*46.8644*	*0.0028*
baboon.bmp	*big1124.jpg*	*3.0327*	*43.3466*	*0.0077*
baboon.bmp	*desert.jpg*	*3.4416*	*42.7972*	*0.0079*
baboon.bmp	*index128.jpg*	*3.7192*	*42.4604*	*0.0079*
baboon.bmp	*pic400.jpg*	*3.7246*	*42.4541*	*0.0079*
butterfly.jpg	*lena.jpg*	*4.5827*	*41.5536*	*0.0117*
baboon.bmp	*lena.jpg*	*3.4448*	*42.7931*	*0.0079*

Where H and W are height and width, P(i, j) represents the original image and S(i, j) represents corresponding stego image.

Maximum payload (bits per byte/bpb) for the technique has also been obtained i.e. maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. In this scheme eight bits of data are embedded in 1 pixel of the cover image.

Normalized absolute error (NAE) computed by Eq. (4) is a measure of how far is the stego image is from the original cover image with the value of zero being the perfect fit. Big value of NAE indicates poor quality of the resulting image after embedding. The value of NAE is calculated using the Equation (4).

$$NAE = \sum_{i=1}^{H} \sum_{j=1}^{W} | P(i,j) - S(i,j) | / \sum_{i=1}^{H} \sum_{j=1}^{W} | S(i,j) | \quad (4)$$

The results in terms of MSE, PSNR and NAE values are provided in the table 1. For example if a secret image lena.jpg is embedded inside the cover image blueland.jpg then the obtained MSE value is 1.2830, PSNR value is 47.0827 and NAE value is 0.0028.

Fig.1 contains Test Bed of cover and secret images used for experimentation.

Table 2 depicts the comparison on consumption of disk space by the secret images in RGB and YUV color spaces respectively. It also shows that lesser disk space is utilized by the cover image when it is converted to a stego image.

Table 2: Comparison on consumption of disk space

Secret Image	**RGB Image in KB**	**YUV Image in KB**	**Cover Image**	**RGB Image in KB**	**Stego Image in KB**
pic400.jpg	9.95	2.29	pepper.jpg	22.9	10.6
big1124.jpg	3.78	1.77	baboon2.bmp	576	31.5
big1124.jpg	3.78	1.77	largeflower.jpg	44.5	23.0
lena.jpg	8.29	2.59	baboon.bmp	432	24.6
index128.jpg	9.96	3.10	butterfly.jpg	35.8	18.7
lena.jpg	8.29	2.59	tulip.jpg	99.4	38.5

Table 3: Comparison on disk space occupied by stego image with and without Yuv conversion.

Cover Image	**RGB Image in KB**	**Stego Image in KB**	**Stego Image without YUV Conversion in KB**
pepper.jpg	22.9	10.6	22.9
baboon2.bmp	576	31.5	576
largeflower.jpg	44.5	23.0	44.5
baboon.bmp	432	24.6	432
butterfly.jpg	35.8	18.7	35.8
tulip.jpg	99.4	38.5	99.4

Table 3 depicts the comparison between the disk space occupied by the stego image with Yuv conversion of secret image and the stego image without the Yuv conversion of secret image. It is clearly visible that without Yuv Conversion, the size of the stego image remains the same as its RGB size whereas it occupies very less disk space when the secret image is converted to Yuv color space.

IV. CONCLUSION

The need for information security is increasing day by day as many people are depending on internet for their daily needs. The proposed 2-3-3 algorithm in YUV color space provides better results compared to previous 3-3-2 method in terms of MSE, PSNR , NAE values. With a comparison between the proposed algorithm and previous technique considered by this study, the proposed technique shows promising results .There is a drastic improvement in MSE and PSNR values. Combining cryptography with steganography provides higher security, cryptographic algorithm Arnold's CATMAP Technique is used for image encryption. Experimental results show that, even though cryptography is used in steganography analysis parameters (MSE, PSNR etc.) are not affected. YUV color space encodes a color image or video taking human perception into account, allowing reduced bandwidth for chrominance components, there by typically enabling transmission errors or compression artifacts to be more efficiently masked by human perception than using a direct RGB-representation. From table 2 and 3 it is clear that a YUV image consumes less space than RGB image. For example, pic400.jpg consumes 9.95 KB when it is in RGB but when it is converted to YUV it consumes only 2.29 KB of disk space. The stego image occupies less space when compared to cover image.. Thus we can conclude that the proposed method provides better results in terms of MSE, PSNR , NAE values as well as the disk space occupied and is therefore very optimized.

V. REFERENCES

[1] Arvind Kumar, KmPooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Vol. 9-No.7, November 2010.

[2] G.R.Manula, Ajit Danti "A novel hash based least significant bit (2-3-3) image steganography in spatial domain" International journal of Security,Privacy and Trust Management Vol 4, No 1, February 2015.

[3] Ajit Danti, G R Manjula, R B Sushma "Steganography using Randomized Index Channel with Arnold Cat Map Encryption" Proceedings of International conference on "Emerging Research in computing, information, communication and applications" ERCICA August 2014 ISBN 9789351072607

[4] Namita Tiwaril, Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal Of Security and Its Applications, Vol. 4, No. 4, October, 2010.

[5] Walaa Abu-Marie, Adnan Gutub, Hussein Abu-Mansour, "Image Based Steganography Using Truth Table Based on Determinate Array on RGB Indicator", International Journal of Signal and Image Processing, Vol. 1-2010/Iss.3, pp. 196-204.

[6] Ali Akbar Nikoukar, "An Image Steganography Method with High Hiding Capacity Based on RGB Image", International Journal of Signal and Image Processing, Vol. 1-2010/Iss.4, pp. 238-241.

[7] Emad T. Khalaf, Norrozila Sulaiman,"Segmenting and Hiding Data Randomly Based on Index Channel", International Journal of Computer Science Issues, Vol. 8, Issue 3,No. 1, May 2011.

[8] Yogendra Kumar Jain, R. R. Ahirwal, "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International journal of Computer Science and Security, vol. 4, issue 1.

[9] Debnath Bhattachryya, Arpita Roy, Pranab Roy, Tai-hoon Kim, "Receiver Compatible Data Hiding Color Image", International Journal of Advanced Science and Technology, vol. 6, May, 2009.

[10] Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, vol. 2,No. 1 Feb 2010.

[11] Koushik Dasgupta et.al "Hash based least significant bit technique for video steganography" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[12] Ajit Danti, G.R.Manjula, Sushma R B " Steganography using Randomized Index Channel with Arnold Cat Map Encryption"published and presented in *Second International Conference on Emerging Research in computing, Information, Communication and Applications (ERCICA2014)* held at Bangalore during Aug-2014. Elsevier Publication 2014 .ISBN:9789351072607.