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, video) 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 Ajit Danti’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.

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.
B. Embedding algorithm
Step 1: 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: Embed 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).

\[
PSNR = 10 \log_{10} \frac{L^2}{MSE}
\]  

(2)

Where L is peak signal level for an image.

The value of MSE is calculated by Equation (3)
\[ \text{MSE} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (P(i,j) \times S(i,j))^2 \]  \tag{3}

Fig 2: Test bed of Cover and Secret Images
Where H and W are height and width, P(\textit{i}, \textit{j}) represents the original image and S(\textit{i}, \textit{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).

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

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 blue1and.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 stego image with and without Yuv conversion.

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


