ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Secured Image Transmission Using Videos

R. Saranya Devi
Research Scholar
Department of Computer Science
Mother Teresa Women's University,
Kodaikanal, India.

Dr. M. Pushpa Rani
Professor and Head
Department of Computer Science
Mother Teresa Women's University,
Kodaikanal, India.

***Abstract* :** The internet is always vulnerable to interception by unauthorized people over the world. The importance of reducing a chance of the information being detected during the transmission is being an issue now days. These issues to overcome with the help of steganography and can be used different method (text, audio, image and video). In that, videos can be stored in a large amount of data that can be in any form of information such as images. The most of the color image stored in the RGB color model, but three primary colors is not sufficient to reproduce all colors and also medical researchers proved the human eye has different sensitivity to color and brightness. So, RGB color transform to YCBCR color model. It is a best representation in the image or video steganography. Because the human eye is sensitive to small changes in luminance but changes in chrominance part cannot alter the image quality. In the proposed method, an image hiding and extraction procedure in using YCBCR color transformed Mosaic image. Skillfull techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly losslessly.

***Keywords*:** YCBCR Color Transformation, Data Hiding using RSA Encryption, Huffman Encoding, Video Steganography.

INTRODUCTION

Steganography is a method of sharing secret information by making it inconspicuous to non authenticated users. Steganography has been originated from the Greek word Steganos and graphics. Steganos means covered or hidden and graphics means writing. Greek People used steganography to convey secret messages through different methods. Steganography is the art of hiding the information in some other host object[1].

Most of the research work in video steganography is the extension of image steganography. Video can be considered as combination of audio and a collection of still images which moves in constant time sequence. Videos are getting popular as a cover object in steganography due to high embedding payload than a digital image and temporal features of video also provide perpetual redundancy, which is not available in digital images. Due to availability of a large number of frames secret data can be easily disguised inside a video. Disguising secret information on some network protocols is known as protocol steganography[3]. Video steganography is still explored by the researcher for better performance. The advantage of this method is its robustness. The loss of data after applying the geometric transformation is very less in this method. The security of this method is also very strong and difficult to break.

LITERATURE REVIEW

- **Ya-Lin Lee** et .al .discussed about the mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image[1].
- **Ramandeep Kaur** et .al .talk about video steganography has become a strong tool to hide a large amount of data rather than image steganography. An idea about a hybrid approach for video steganography to achieve high capacity data & high quality of stego video on the basis of quality metrics like PSNR, MSE and BER. In this method hide text message inside of the all layers RGB color frames of video[2].
- **Hemalatha.S** et .al .conversed different techniques have to be used for color image steganography and grey scale image steganography since they are stored in different ways. The color image is normally stored with 24 bit depth and gray scale images are stored with 8 bit depth. Color images can hold a large amount of secret information since they have three color components[3].

PROPOSED SYSTEM

Recently video steganography has become a strong tool for hiding a large amount of the information. Existing work, implemented RGB color model for image hiding, but it's not more, the secure and storage level is not enough. So move on to the YCBCR color transformation is a best method for image hiding[4]. YCBCR color transformed image hides in the videos that has recommended for hiding image imperceptibility inside the stego video. It contains the various techniques such as color transformation, image tiling, random location hiding, RSA encryption, Huffman encoding. It hides the images efficiently from the intruders through internet[2]. The steganography, video files can store large amount of data in all frames. The experimental results are analyzed in MATLAB software and information embedded video that term is stego video.

PROPOSED SYSTEM MODEL

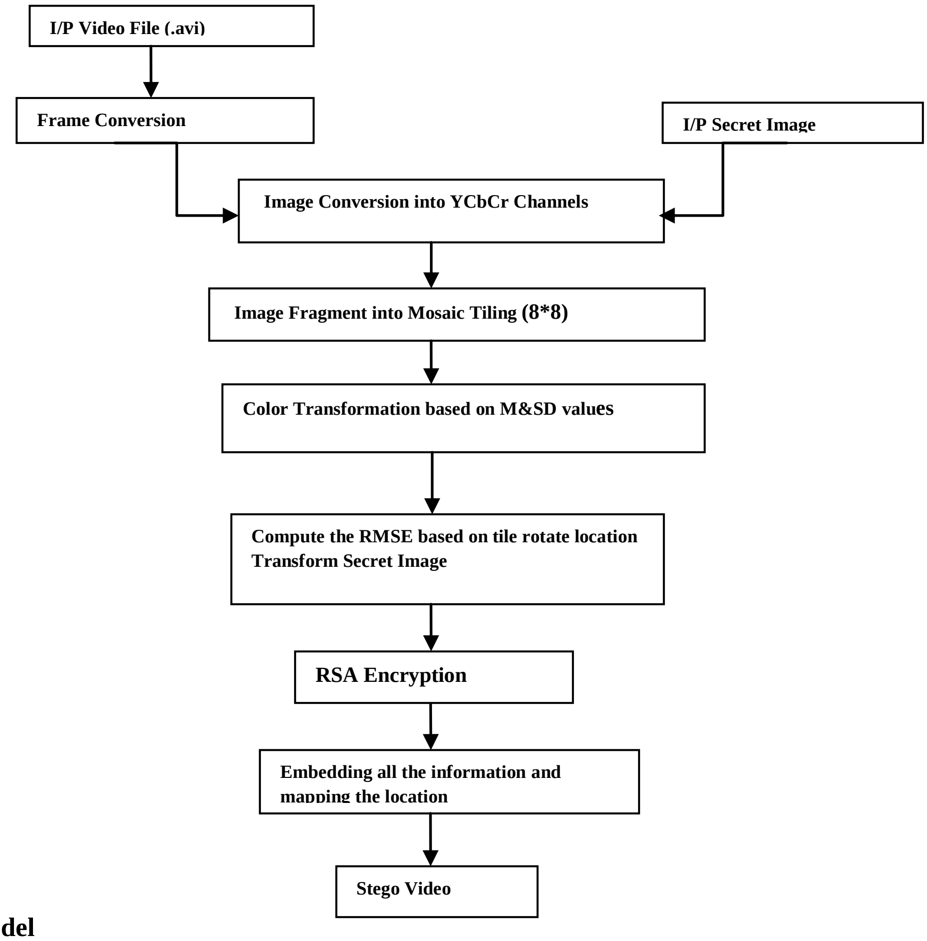

I/P Video File (.avi)
Frame Conversion
I/P Secret Image
Image Conversion into YCbCr Channels
Image Fragment into Mosaic Tiling (8*8)
Color Transformation based on M&SD values
Compute the RMSE based on tile rotate location
Transform Secret Image
RSA Encryption
Embedding all the information and mapping the location
Stego Video

Figure 1: Data Flow Model

PHASES OF PROPOSED WORK

A) Frame Conversion

First, select the cover video (.avi file) any formats of cover video. The basic .avi format video provides per second, 20-25 frames, but our video time are three second in that 50 frames are produced. *vid.NumberOfFrames;* a function used in MATLAB for converting the video into a number of frames and converted frames are stored in 'n' variable. Here, randomly select a video frame (Figure.3) at the same time select a secret image (Figure.2).

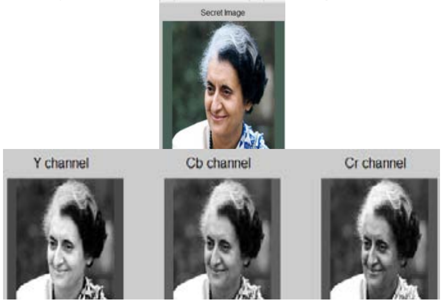
Fig: 2. Secret Image.

Fig: 3. Target Image.

After selecting, the images are resized equally that is 256 * 256. So it's useful for image tiling and also equal size gives a high imperceptibility[5].

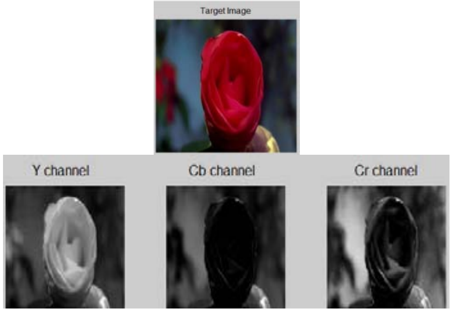
B) YCBCR Color Channels

Video steganography can be done in any color space domain. One of the best representations for steganography is YCBCR. The human eye is very sensitive to changes in luminance but not in chrominance. So small changes in chrominance part cannot alter the overall image quality much[4,5]. Luminance component is Y and Cb, Cr are the blue and red chrominance components respectively. These are shown in Figure 4 & 5.



(a) (b) (c) (d)

Figure 4: (a) is a secret image, (b) represents Y Luminance, (c) and (d) represent Cb & Cr is the components of blue and red chrominance.



(a) (b) (c) (d)

Figure 5: (a) is a target image, (b) represents Y Luminance, (c) and (d) represent Cb & Cr is the components of blue and red Chrominance.

The conversion formulae are used to convert values from one color space to another color space. The conversion to YCBCR from RGB is as follows:

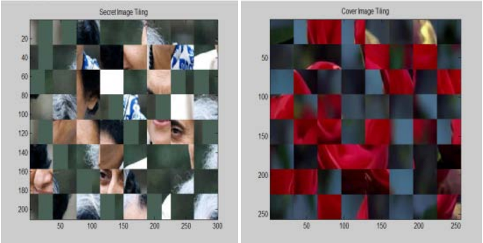
Y = (77/256) R + (150/256) G + (29/256) B (1.1)

Cb =− (44/256) R − (87/256) G + (131/256) B + 128 (1.2)

Cr = (131/256) R − (110/256) G − (21/256) B + 128

C) Image Tiling

The propose work, both target frame and secret image are converted into equal size such as 256*256. So that provides 1024 blocks for the image tiling process like 8*8 matrixes.



(a) (b)

Figure 6: (a) Mosaic tiles of secret image and (b) Mosaic tiles of target image (8*8).

Tiling is useful for calculation. After tilling calculate average the Mean and Standard Deviation for each block in the mosaic tile. Depend on the average values of Mean and standard deviation, a color transformation process made in the secret image[6]. The following formulas for calculating the Mean and Standard Deviation,

$$Mean\ \mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \qquad -------Eq(1)$$

$$Standard\ Deviation\ \sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i-\mu_c)^2} \qquad --------Eq(2)$$

Eq: 1, μ_c represent the mean value of each pixel. Eq: 2, σ_c represent the standard deviation of each pixel. The SD based on the mean value that denote in the equation 2 (c_i - μ_c). Each pixel mean and SD are calculating time is 0.2 seconds and the average of these each block value calculating time is 0.002 or 0.019 seconds depends on the color model values[6,7].

D) Color Transformation

Color transformation performs based on the average mean and standard deviation of cover frame so that secret image color can be changed. The color transformed image again tiling for calculating the root mean square error (RMSE). The color transformed mosaic image rotate four directions are 0^o, 90^o, 180^o, 270^o. In which angle is similar to the cover image based on the rotate degree in that compute the root mean square error and residual value.

Figure 7: Color Transformed Secret Image.

The color transformation process is conducted as some pixel values in the new tile image might have overflowed or underflows. The ranges of possible residual values are unknown, and to solve this problem, record the residual values in the untransformed color space rather than in the transformed one[8]. That is, by using the following two formulas,

$C_s = [(1/q_c)\ (255 - \acute{\mu}_c) + \mu_c];$

$C_L = [(1/q_c)\ (0 - \acute{\mu}_c) + \mu_c]$. (3)

In which, compute first the smallest possible color value *cS* (with *c* = *r*, *g*, or *b*) in a new tile image that becomes larger than 255, as well as the largest possible value *cL* in the new tile image that becomes smaller than 0, respectively, after the color transformation process has been conducted: finally, because the residual values are centralized around zero.

E) RSA Encryption

To make our secret message more secure, we are using RSA asymmetric key based encryption algorithm. It converts the secret message in an unreadable format and increases its security from hackers. In our work, we have used an RSA encryption algorithm instead of symmetric key based encryption. Both sender and receiver are using their own public and private keys to encrypt and decrypt the secret message and key sizes are up to 1024 to 4096 bits and also used a large factorial number for encryption, which is hard to decrypt by attackers. So RSA encryption provides high security to encrypt secret message behind video frames. Huffman encoding give compressed coding of the symbols provided as input[9,10]. Huffman table has prefix free codes and corresponding symbols. Huffman table is used during Huffman decoding.

CONCLUSION

A modern, secure image transmission method has been proposed, which creates meaningful mosaic images and also can transform a secret image into a mosaic one with the same data size for use as a mask of the secret image. The use of proper pixel color transformations as well as the converted values of the pixels' colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images. The proposed methodology is color transformation and tiling the mosaic images and hiding the random location of mosaic image and using Huffman encoding. Also, the original secret images can be recovered nearly losslessly from the created mosaic images. The proposed method achieving high imperceptibility, high security and hiding large amounts of data in all formats of videos. In future, this method of color transformation used in various applications.

REFERENCES

[1] Ya-Lin Lee and Wen-Hsiang Tsai,"A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 24, No. 4, April 2014.

[2] Ramandeep Kaur, Pooja and Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques", IEEE WiSPNET 2016 Conference.

[3] Hemalatha S, U Dinesh Acharya and Renuka A, "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB And YCBCR Domains", (IJAIT) Vol. 3, No. 3, June 2013.

[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[5] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21, no. 3, pp. 749–761, 2004.

[6] Xie, Qing., Xie, Jianquan., Xiao, Yunhua., (2010), "A High Capacity Information Hiding Algorithm in Color Image.", Proceedings of 2nd International Conference on E-Business and Information System Security, IEEE Conference Publications, pp 1-4.

[7] Sachdeva, S and Kumar, A., (2012), "Colour Image Steganography Based on Modified Quantization Table", Proceedings of Second International Conference on Advanced Computing & Communication Technologies, IEEE Conference Publications, pp 309 – 313.

[8] Ramandeep Kaur, Pooja, and Varsha, ―The NonTangible Masking of Confidential Information using Video Steganography‖, International Journal of Computer Applications (IJCA), Vol.119, No.17, June 2015.

[9] Ramandeep Kaur, Pooja, ―XOR Encryption Based Video Steganography‖, International Journal of Science and Research (IJSR), Vol.4, Issue 11, November 2015.

[10] Sunil. K. Moon, Rajeshree. D. Raut (2013), ―Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security‖, IEEE Second International Conference on image information processing (ICIIP- 2013), pg 660-665.