ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 4, April 2015

A Novel Steganography Scheme via the use of Alpha channel

Prof. ArjunNichal[1], Mr.Aniket Jadhav[2], Mr. Krishna Pingale[3], Mr.Chaitanya Mohite[4], Mr. Sachin Ponde[5]

Assistant Professor, Electronics & Telecommunication Department, AITRC, Vita, India [1]

Student, Electronics & Telecommunication Department, AITRC, Vita, India [2,3,4,5]

Abstract: Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. It is the art and science of communicating in such a way that the presence of a message cannot be detected. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. In this paper we proposed steganography based on alpha channel.

Keywords: Steganography, Alpha channel, Data hiding.

I. INTRODUCTION

Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible.

Alpha Channel:

Alpha channels are masks through which you can display images. The alpha channel is an 8-bit channel, which means it has 256 levels of gray from 0 (black) to 255 (white). White acts as the visible area; black acts as the transparent area (you see the background behind the image when displayed). The level of gray in between determines the level of visibility. For example, 50 percentgray allows for 50 percent visibility. Alpha channels are usually used with 16.8M color RGB images. The resulting image is called RGBA (RGB+A, A means alpha channel) [1].

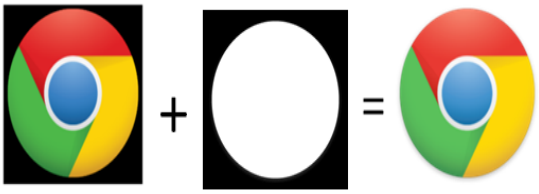

Fig1. Transparency of image by adding alpha channel

Literature Review:

Basically there are main four mediums in which steganography is to be carried out. Imagesteganography plays important role in stenographic field. Image steganography is divided into spatial domain and Transform domain. Spatial domain further divided into simple LSB (least significant bit) substitution, LSB matching and PVD (pixel value difference). Transform domain is one of most significant domain in image steganography. In transform domain DCT (discrete cosine transform) and DWT (discrete wavelet transform) are used. DCT belongs to a lossy compression field. DWT is used for both lossy as well as lossless compression [2,3].

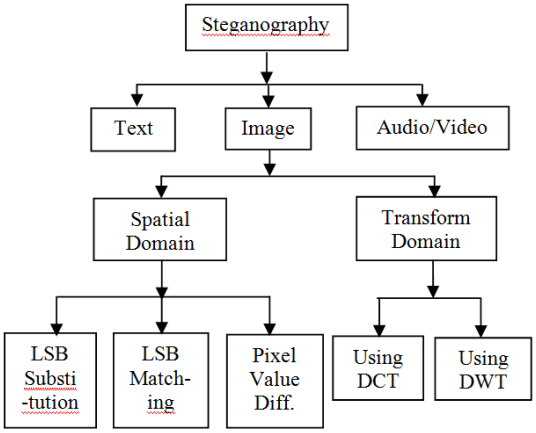

Fig2. Basic types of steganagraphy

Types ofSteganography:

1.Spatial Domain steganography:

Basically spatial domain is divided into LSB (least significant bit) substitution, LSB matching and PVD (pixel value difference). In this domain all operations are directly concerned with the image pixels.

Least Significant Bit (LSB) Substitution:

The principle involved in this method is to replace all LSB bits of pixels of the cover image with secret bits. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels. Although this technique is Simple, it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three.

Least Significant Bit (LSB) Matching:

The principle involved in this methodis to modulate the pixel value by adding ±1 to match the least significant bit with the secret message bit.

Pixel Value Difference (PVD)

The principle involved in this method is to calculate the difference of two consecutive pixels to determine the depth of the embedded bits. After determining embedding depth secret bits are embedded into pixels.

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 4, April 2015

2. Transform Domain steganography

Basically transform domain is classified on the basis of which kind of transform used for transformation. Mainly transform domain comprises two types 1) Using Discrete Cosine Transform (DCT) and 2) Using Discrete Wavelet Transform (DWT). In transform domain transformed coefficients are used for embedding secret bits. Image is transformed by using DCT (Discrete Cosine Transform) or DWT (Discrete Wavelet Transform) and then embedding process is applied on coefficients. Basically DCT based steganography conveniently applied in the JPEG (Joint Photographic Experts Group) compression standards. DWT based steganography conveniently applied in the JPEG2000 (Joint Photographic Experts Group 2000) compression standards.

Using Discrete Cosine Transform (DCT)

Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. After transformation steganography is to be applied. This method modifies the DCT coefficients for obtaining final stegocodestream.

Using Discrete Wavelet Transform (DWT)

Principle involved in this method is to modify quantized wavelet coefficients for obtaining final stegocodestream. Wavelet transform gives us four sub-bands LL, LH, HL and HH. LL sub-band contains most useful coefficients. These coefficients are don't take part in steganography process. After quantization process quantized coefficients are modified for embedding secret data. Basically discrete wavelet transform is used in JPEG2000 compression standard. DWT domain based data hiding scheme applied conveniently in JPEG2000 compression standard.

II. STEGANOGRAPHY TRANSMITTER

Steganography transmitter gives output as a stego image which includes security image or security massage with cover image [4].

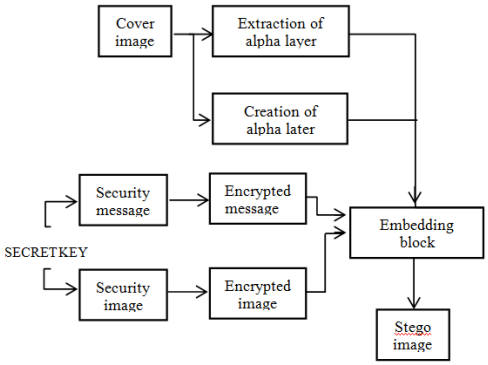

Fig3: Proposed Steganography transmitter Block Diagram

Block Explanation:

Cover Image:

Cover image is the source image. If alpha layer is present in the colour image then extraction of alpha layer takes place and if alpha layer is absent then creation of alpha layer takes place.

Security Image:

Security image is the main image which we want to secure. For the security purpose we have to do the encryption of the image.

Security Message:

Security message is the main message which we want to secure. For the security purpose we have to do the encryption of the message.

Embedding Block:

Embedding block is the main block of the transmitter system. All embedding process is done in this block to produce the stego image.

Stego Image:

Stego image is the image in which security image or security message is present in such a format that is not understandable to others.

III. STEGANOGRAPHY RECEIVER

Steganography receiver receives the stego image and separates the security massage or security image from cover image with the help of secret key which should be exactly same as transmitter side [5].

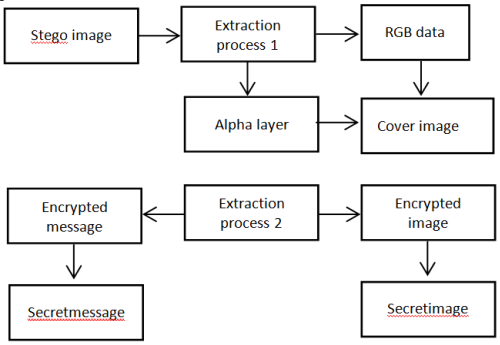

Fig4. Receiver Block Diagram

Block Explanation:

Stego Image:

Stego image is the main image in which secret message or secret image is present.

Extraction Process 1:

Extraction process 1 is the process in which separation of alpha layer and RGB data takes place. RGB data and alpha layer forms the cover image.

Extraction Process 2:

Extraction process 2 is the process in which separation of encrypted message and encrypted image takes place. We get the security message and security image from encrypted message and encrypted image with the help of secret keys.

IV. RESULT ANALYSIS AND DISCUSSION

1. Quality Parameters:

Following are the some quality parameters

PSNR:

This term is mainly used to measure the quality of reconstruction of lossy compression. It is mostly defined

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

IJIREEICE

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 4, April 2015

through MSE (mean square error). PSNR is basically expressed in the logarithmic decibel scale [6].

Formula:

$$PSNR = 10log_{10}\left(\frac{max_I^2}{msf}\right)$$

AMBE:

The proposed method is trying to preserve brightness mean, more & more possible by considering value of absolute mean brightness error (AMBE). AMBE is calculated from equation below [7].

$$AMBE = |E[Y] - E[X]|$$

Where,

E[Y] & E[X] are mean of new & original gray level of image respectively.

MSE:

The MSE is cumulative squared error between the compressed and the original image whereas PSNR is a measure of the peak error.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - k(i,j)]^2$$

StructuralContent (SC):

Structural Content is defined as,

$$SC = \frac{\sum M,N[I1\ m,n .* I1(m,n)]}{\sum M,N[I2\ m,n .* I2(m,n)]}$$

The large value of Structural Content (SC) means that image is of poor quality.

Average Difference (AD):

Average Difference (AD) is defined as,

$$AD = \frac{\sum M,N[I1\ m,n\ - I1\ m,n\ ]}{M * N}$$

The large value of AD means that the pixel values in the reconstructed image are more deviated from actual pixel value. Larger value of AD indicates image is of poor quality.

Contrast:

Contrast defines the difference between lowest and highest intensity level. Higher the value of contrast means more difference between lowest and highest intensity level.

2. Result:

For color image

Following results are obtained for Lena image with the binary image Ani as a secret image. The terms in the table are EC = Embedding capacity, NBE = No. of bits embedded, PSNR = Peak signal to noise Image

(a) (b) (c)

Fig5.(a) original image (b) secret image (c) stego image

Parameters	Value
PSNR in db of RGB	100
PSNR in db of alpha	53.9185
MSE of alpha	0.263775
No. of bits embedded	20000
Embedding capacity	2.09715e+006
Structural content alpha	255
NCC alpha	0.998966
AD alpha	0.263775

For png image

Following results are obtained for Chrome image with the binary image Ani as a secret image. The terms in the table are EC = Embedding capacity, NBE = No. of bits embedded, PSNR = Peak signal to noise Image

(a) (b) (c)

Fig6. (a) Original image (b) secret image (c) stego image

Parameters	Value
PSNR in db of RGB	100
PSNR in db of alpha	53.9185
MSE of alpha	0.263775
No. of bits embedded	22000
Embedding capacity	2.09715e+006
Structural content alpha	255
NCC alpha	0.998966
AD alpha	0.263775

3. Matlab implementation:

By using matlab, steganography of the image in alpha layer is done. We have steganography transmitter and steganography receiver. In transmitter window we do the embedding process to form the stego image. Stego image consist of cover image and secret image.

At the receiver window we have stego image to which extraction process is applied. We can separate secret image and cover image with the help of secret key.

The following are the three windows which shows main steganography window along with its transmitter and receiver.

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 4, April 2015

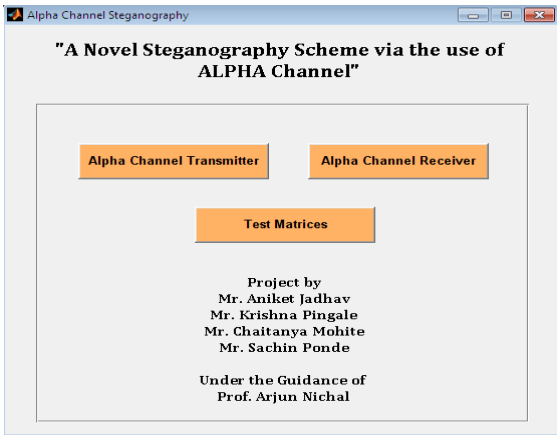

Fig7. Steganography main GUI window

Steganography transmitter consist of selection of color image or png image as a cover image and selection of secret image. After embedding we can save stego image.

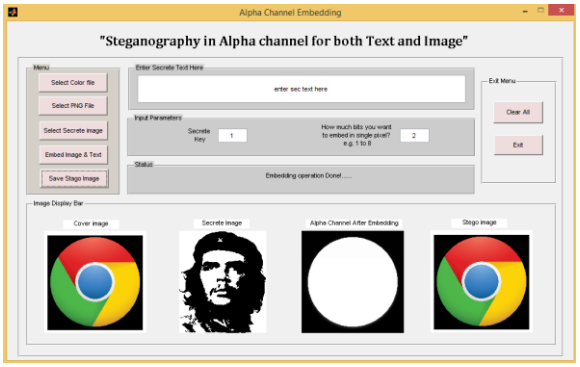

Fig8. Steganography transmitter

Steganography receiver consist of extraction of stego image to separate secret image from color image or png image. It is done with help of secret key.

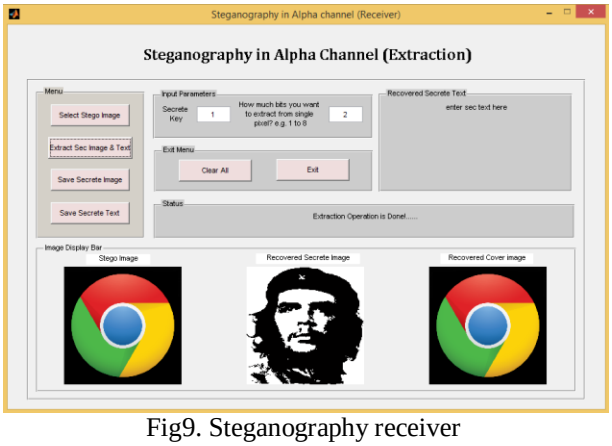

Fig9. Steganography receiver

CONCLUSION

In this work, a novel data hiding scheme for encrypted image with a low computation complexity is proposed, which consist of image encryption, data embedding and data extraction image recovery phases. The data of the original image are entirely encrypted although a data hider does not know the original content; he can embed additional data into the encrypted image by modifying a part of encrypted data.

With an encrypted image containing embedded data, receiver may firstly decrypt it using the encrypted key, and decrypted version is similar to the original image. LSB substitution method is used for embedding purpose. This work gives effective study of simple but strong steganography.

REFERENCES

[1] Message embedding in pngfile using LSB Steganography techniques-January 2013, by WaiWaiZin (university of computer studies Mandalay,Myanmar)
[2] A review of comparision techniques of image steganography(May-June) 2013, by StutiGoel, Arun Rana, ManpreetKaur.
[3] Modelling the Security of Steganographic Systems, in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.
[4] Matsuoka, H., Spread Spectrum Audio Steganography using Sub – band Phase Shifting, Proceedings of the 2006
[5] InternationalConference on Intelligent Information Hiding and Multimedia Signal
[6] Robert Krenn,Steganography and steganalysis, January 2004.
[7] Elshazly, A. R., M. M. Fouad, and M. E. Nasr. Secure and robust high quality DWT domain audio watermarking algorithmWith binary image. Computer Engineering & Systems (ICCES), 2012 Seventh International Conference on. IEEE, 2012

BIOGRAPHIES

Prof. A. R. Nichal Assistant professor in AITRC vita. Received M.Tech in electronics from Walchand College of engineering, Sangli, His area of interest is Digital Image Processing, Digital Signal Processing and Embedded system.

Mr. Krishna Pingale pursuing his B.E degree in Electronics and telecommunication from AITRC, vita. His area of interest is Digital Image Processing.

Mr.Aniket Jadhav pursuing his B.E degree in Electronics and telecommunication from AITRC, vita. His area of interest is Digital Image Processing.

Mr.Chaitanya Mohite pursuing his B.E degree in Electronics and telecommunication from AITRC, vita. His area of interest is Digital Image Processing.

Mr. Sachin Ponde pursuing his B.E degree in Electronics and telecommunication from AITRC, vita. His area of interest is Digital Image Processing.