World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:4, No:10, 2010

Implementing Adaptive Steganography by Exploring the Ycbcr Color Model Characteristics

Surbhi Gupta, Alka Handa, Parvinder S.Sandhu

***Abstract*—**Stegnography is a new way of secret communication the most widely used mechanism on account of its simplicity is the use of the least significant bit. We have used the least significant bit (2 LSB and 4 LSB) substitution method. Depending upon the characteristics of the individual portions of cover image we decide whether to use 2 LSB or 4 LSB thus it is an adaptive stegnography technique. We used one of the three channels to behave as indicator to indicate the presence of hidden data in other two channels. The module showed impressive results in terms of capacity to hide the data. In proposed method, instead of using RGB color space directly, YCbCr color space is used to make use of human visual system characteristic.

***Keywords*—**Stegoimage, steganography, Pixel indicator, segmentation, YCbCr..

I. Introduction

STEGANOGRAPHY deals with embedding information in a given media (called cover media)without making any visible changes to it [4].cryptography is about screening the matter or the material of the message while stegnography is about concealing the presence of the message. For many years Information Hiding has captured the imagination of researchers. Digital watermarking and steganography techniques are used to address digital rights management, protect information, and conceal secrets. Information hiding techniques provide an interesting challenge for digital forensic investigations. Information can easily traverse through firewalls undetected. We can use digital images, videos, sound files, and other computer files that contain redundant information as covers or carriers to hide secret messages. After embedding a secret message into the cover images, we obtain a so-called stego-image. It's important that the stego-images don't contain any detectable artifacts due to messages embedding. A third party could use such artifacts as an indication that a secret message is present. Once a third party can reliably identify which images contain secret messages, the steganographic tool becomes useless. Obviously, the less information we embed into the cover.

Parvinder S. Sandhu and Alka Handa are associated with the Rayat & Bahra Institute of Engineering & Bio-Technology, Mohali-Sahauran14004. E-Mail: parvinder.sandhu@gmail.com,

Surbhi Gupta is working as a Assistant Professor with the Rayat & Bahra Institute of Engineering Technology, Railmajra-140001.

cover_medium + hidden_data + stego_key = stego_medium

Message embedding is performed in spatial or frequency domain. One of the representative data hiding methods in spatial domain is to use the least significant bit (LSB), such as LSB replacement or LSB matching. Transform domain steganographic methods employ the well-known transformation techniques such as Discrete Cosine Transform (DCT), Fourier Transform (FT), or Discrete Wavelet Transform (DWT). Spatial domain methods are simpler and have a large capacity while transform domain methods are more robust compared to spatial domain method.

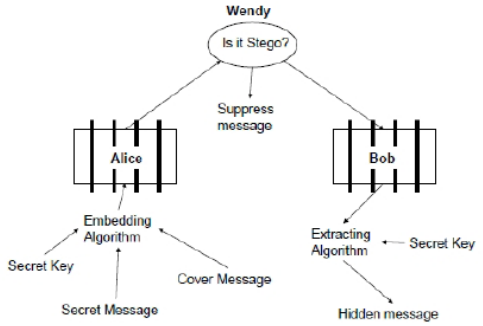

Fig. 1 General Model of Steganography

Images typically use either 8-bit or 24-bit color. When using 8-bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8-bit value. A 24-bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pixel is represented by three bytes, each byte representing three channels Y (luminance)Cb and Cr (croma).

A. Constraints for concealing information

Many different protocols and methods are available that enables us to enclose data in a given object. However, all of the protocols and techniques must satisfy a number of constraints so that steganography can be applied correctly. The following is a list of main constraints or requirements that steganography methods must satisfy:

• In case of images, after hiding the data in the cover image we get stego image and this stego image must remain unchanged. If there is significant amount of change in the stego image then it will become noticeable, thus third party can detect the existence of hidden data and can corrupt or destroy it.

• There should be no alterations to the data to be hidden, such as extra data being added, loss of secret data or changes to data. The integrity of the hidden information after it has been embedded inside the stego image must be correct. If secret data changes then there is no point doing steganography.

• In watermarking, changes in the stego object must have no effect on the watermark. Imagine if you had an illegal copy of an image that you would like to manipulate in various ways. These manipulations can be simple processes such as resizing, trimming or rotating the image. The watermark inside the image must survive these manipulations, otherwise the attackers can very easily remove the watermark and the point of steganography will be broken.

B. YCbCr model

YCbCr is also called (YUV) colorspace .it contains three variables ,also known as components or channels Y=Luma (black and white or lightness) and CbCr =Chroma (or color),where Cb =blue minus 'black and white' and Cr ='red minus black and white '.The advantage of YCbCr is fast computation .the principal advantage of the model in image processing is decoupling of luminance and color information .The importance of this decoupling is that the luminance component of an image can be processed without affecting its color component. In proposed method, instead of using RGB color space directly, YCbCr color space is used to make use of human visual system characteristic. Many different protocols and methods are available that enables us to enclose data in a given object. However, all of the protocols and techniques must satisfy a number of constraints so that steganography can be applied correctly.

C. LSB technique

The least significant bit insertion method is simple and the most well known Stenography technique. . It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision when applying 4LSB techniques to each bytes of a 8-bit image, one bit can be encoded to each pixel. Any changes in the pixel bits will be indiscernible to the human eye. The main advantage of 4LSB insertion is that data can be hidden in the last four least significant bits of pixel and still the human eye would be unable to notice it. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image.

C. Adaptive steganography

Adaptive steganographic techniques have become a standard direction taken when striving to complicate the detection of secret communication. This method takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The technique is driven by separate functions: adaptive excerption of the place to conceal, Adaptive excerption of number of bits per pixel to conceal

II. RELATED WORK

Anderson, patitcolas in their paper clarified what steganography is and what it can do. They contrast it with the related disciplines of cryptography and traffic security, present a unified terminology agreed at the first international workshop on the subject, and outline a number of approaches-many of them developed to hide encrypted copyright marks or serial numbers in digital audio or video. They then presented a number of attacks, some new, on such information hiding schemes. This leads to a discussion of the formidable obstacles that lie in the way of a general theory of information hiding systems (in the sense that Shannon gave us a general theory of secrecy systems). However, theoretical considerations lead to ideas of practical value, such as the use of parity checks to amplify covertness and provide public key steganography. Finally, we show that public key information hiding systems exist, and are not necessarily constrained to the case where the warden is passive

Abbas et al. discussed a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. Their paper concluded some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, is not the focus of their survey but nonetheless they briefly discussed

S.K Moon, R.S Kawitkar used the least significant bit (4LSB) substitution method . The 4LSB method is implemented for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media. They explained that by using the proposed algorithm, we can hide their file of any format in an image and audio file. We can then send the image via e-mail

Adnan Gutub et.al discussed that LSB is a commonly used technique in this filed. Several scenarios of utilizing least significant bits within images are available. They mixed the ideas from the random pixel manipulation methods and the stego-key ones to propose their work, which uses the least two significant bits of one of the channels to indicate existence of data in the other two channels. Their work showed attractive results especially in the capacity of the data-bits to be hidden with relation to the RGB image pixels.

Rattanapitak and Udomhunsakul presented comparative efficiency of color models for multi-focus color image fusion in their paper. The objective of these experiments was to finding the proper color model for using in multi-focus color image fusion. In their research study, firstly they transformed RGB color model of source images into four color models that are YIQ, YCbCr, HSV and HSI color models. Next, the intensity or luminance component was only used in fusion process using Spatial Frequency Measurement based fusion method compared with Stationary Wavelet Transform with

Extended Spatial Frequency Measurement. Finally, the fused image results were transformed back to RGB model to get the final results. The experiments showed that the YCbCr color model outperforms other color models in term of objective quality assessment.

III. Proposed Technique

A. Pixel Indicator Technique

Our module discusses Pixel indicator technique for YCbCr image stegnography .This technique uses either two least significant bits or four least significant bits of the channels .The decision of whether to use 2 or 4 is based on the cover image characteristics. For this the cover image selection is very important. We should choose such image in which color variations are less. Experimentally we will find out the color value of each channel and then depending upon the color range we will use either 2 or 4 bits .thus lower the color value ,more number of bits can be use to store the data.

Four LSB's of channels can be used in random fashion. Our technique resolves the problems of static technique. This technique is based on adaptive steganography where technique adapts itself according to characteristics of the cover image.

B. Algorithm

- First consider the cover image to check the color value of each pixel (color value of three channels Y, Cb, Cr).
- According to the segmentation method we will find how many LSB's of each channel we can use (to be used as pixel indicator and to store the data bits).
- From the matrix generated by segmentation scheme, select the first occurrence of 4 as pixel indicator and use other two channels to store the secret information.
- The selection of the pixel indicator and amount of data bits to be stored is not static. It depends on the color resolution of cover image.

C. Segmentation method

In proposed algorithm, segmentation technique is based on the color value of individual channel. Let the color value is represented by cv. For Cb, Cr the channel having 16>=cv<85 allows 4 bit changes and 85>=cv<160 allows 2 bit changes and no data will be hidden in channels having value 160>=cv=<240. For channel Y the range differs, 16>=cv<130 allows 2 bit changes and 130>=cv <=235 does not allow any changes. Thus we can't use Y as pixel indicator because we can use only 2 LSB's bits. The technique is different for Y(luma) because it is the main component of this model. Large variations to color value results in drastic changes to stego image.

TABLE I
MEANING OF INDICATOR VALUES WHEN REFERRING TO FOUR LEAST SIGNIFICANT BITS.

Pixel indicator	**Pixel(1)**	**Pixel(2)**	**Pixel(3)**	**Pixel(4)**
0000	No hidden data	No hidden data	0-bits of data	0-bits of data
0100	No hidden data in 1st Channel	Contains hidden data in 2nd channel	0-bits of data	2-bits of data
0101	No hidden data	Contains hidden data in 2nd channel	0-bits of data	4-bits of
1000	Hidden data in 1st channel	No hidden data	2-bits of data	0-bits of data
1100	Hidden data in 1st Channel	Hidden data in 2nd channel	2-bits of data	2-bits of data
1101	Hidden data in 1st Channel	Hidden data in 2nd channel	2-bits of data	4-bits of data
1010	Hidden data in 1st Channel	No hidden data	4-bits of data	No hidden data
1110	Hidden data in 1st channel	Hidden data in 2nd channel	4-bits of data	2-bits of data
1111	Hidden data in 1st Channel	Hidden data in 2nd channel	4-bits of data	4-bits of data

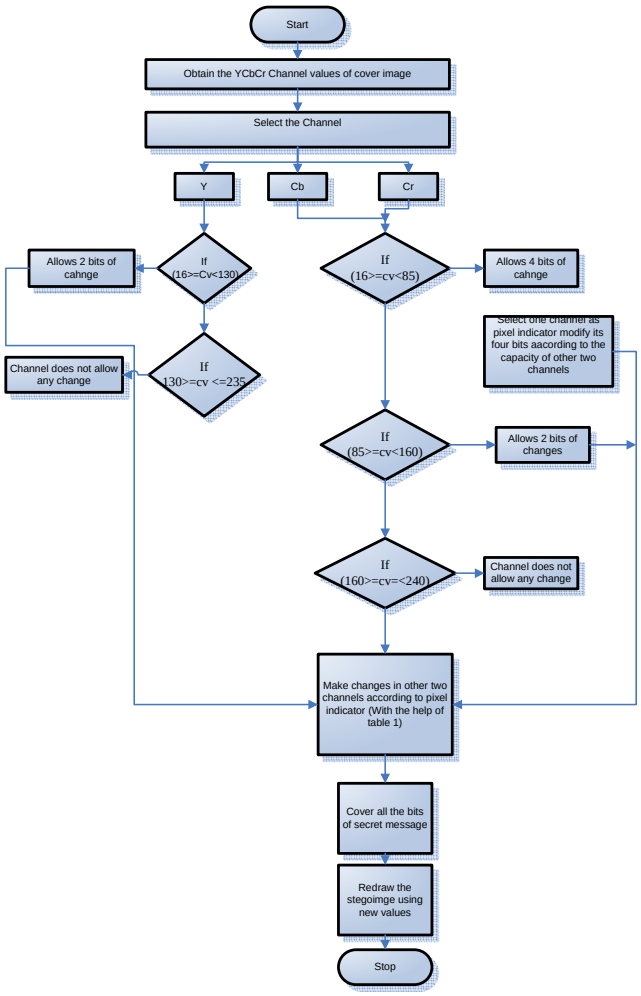

Fig. 2 Process of Stego image creation

IV. Conclusion

The proposed method is more secure and also provides good results in terms of capacity.

References

[1] Abbas Cheddad,A. Joan Condell,J. Curran,K. and Kevitt,P.M., "Digital image steganography: Survey and analysis of current methods", in the Signal Processing Journal,vol 90 ,pp.727–752.

[2] Abu-Marie,W., Gutub,A. And Abu-Mansour, H. (2010), "Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator", International Journal of Signal and Image Processing, vol.1, no. 3, pp. 196-204.

[3] Anderson, R.J. and Petitcolas, F.A.P. (2001), "On the limits of the Stegnography", IEEE Journal Selected Areas in Communications, vol. 16, no. 4, pp. 474-481.

[4] Avcibas, I.,Menon, N. and Sankur,B. (2003), "Steganalysis Using Image Quality Metrics", IEEE transactions on image processing, vol. 12, no. 2, pp.221-223.

[5] Channali, S. and Jadhav,A. (2009), "Steganography An Art of Hiding Data" , International Journal on Computer Science and Engineering, vol.1, no. 3, pp. 137-141.

[6] Fridrich, J.,Goljan, M. and Du, R.(2001), "Detecting LSB Steganography in Color and Grayscale Images", Magazine of IEEE Multimedia Special Issue on Security, vol. 15, no. 1, pp. 22-28.

[7] Gutub, A., Ankeer, M., Ghalioun, M.A., Shaheen, A. and Alvi, A. (2008), "Pixel indicator high capacity technique for RGB image based Steganography", WoSPA 5th IEEE International Workshop on Signal Processing and its Applications, U.A.E, pp.234-239.

[8] Naoe,K. and Takefuji,F.(2004), "Damageless Information Hiding using Neural Network on YCbCr Domain", IJCSNS International Journal of Computer Science and Network Security, vol.8 ,no.9,pp.81-84.

[9] Neil, F.J. and Jajodia, S. (1998), "Exploring steganography: Seeing the unseen", IEEE Transaction on computer practices, Washington, vol. 31, no. 2, pp.26-34.

[10] Rattanapitak, W. and Udomhunsakul,S., "Comparative Efficiency of Color Models for Multi-focus Color Image Fusion", Proceddings of the intenational multiconference of engineers and computer scientists,Hong Kong,vol II.

[11] Sallee,P.(2003), " Model-based steganography" , in Proceedings of the 2nd International Workshop on Digital Watermarking, Seoul, Korea, LNCS, vol. 2939, pp. 254-260.