Abstract—Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The data-hiding is an application of the steganography. Its purpose is to embed a large amount of data in images in an invisible way. Steganography is firstly encrypted by some traditional means and then a cover text is modified in some way to contain the encrypted message, which results in a stego text. In the present paper, we have used the least significant bit substitution method. According to the characteristics of the individual portions of cover image we decide whether to use 2 LSB or 4 LSB thus it is an adaptive steganography technique. In this, 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—Stego image, ycbcr, stegnography.

I. INTRODUCTION

A. Steganography

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another. STEGANOGRAPHY deals with embedding information in a given media (called cover media) without making any visible changes to it. cryptography is about screening the matter or the material of the message while steganography is about concealing the presence of the message.

Hiding information into a media requires following elements:

- The cover media (C) that will hold the hidden data
- The secret message (M), may be plain text, cipher text or any type of data
- The stego function (Fe) and its inverse (Fe-1)
- An optional stego-key (K) or password may be used to hide and unhide the message.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course, be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.

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. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files.

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.
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) color space. 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.

C. LSB technique

Least Significant Bit steganography: An image is nothing more than strings and strings of bytes, each byte representing a different color. The last few bits in a color byte, however, do not hold as much significance as the first few. This is to say that two bytes that only differ in the last few bits can represent two colors that are virtually indistinguishable to the human eye. For example, 00100110 and 00100111 can be two different shades of red, but since it is only the last bit that differs between the two, it is impossible to see the color difference. LSB steganography, then, alters these last bits by hiding a message within them.

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 exception of the place to conceal, Adaptive exception of number of bits per pixel to conceal.

II. RELATED WORK

Anderson and Patitcolas[3] 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 coveryness 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.[7] 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.

Gutub[2] 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 [11] 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 World Academy of Science, Engineering and Technology 70 2010767 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 steganography. 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.

IV. CONCLUSION

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

REFERENCES