Video Steganography Technique using Skin Tone based Embedding in Chrominance Component of YCbCr Color Space

Sameer M. Khupse
Student
J.D.I.E.T. Yavatmal.

Sneha K. Deshmukh
Assistant Professor
IOKCOE, Pune.

ABSTRACT

Steganography is defined as the process of hiding information in a multimedia carrier. Ultimate objectives of steganography are undetectability and robustness of the secret data. It is known as adaptive steganography as the data is embed in to the specific Region of Interest (ROI) of the cover image for the purpose of safety of the inserted data. The assurance of both imperceptibility and robustness requirements are the main objectives of developing an image-hiding technique. The main focus is on embedding the data in the skin region of a video frame. Thus we concentrate on the skin detection algorithm to extract the skin region. This acts as the region of interest for embedding the secret message. To perform embedding the video frames are converted to YCbCr colour space. The frame having least MSE is selected to embed secret data. The secret data is then inserted into the chrominance component (Cr or Cb) of YCbCr of a frame which has least MSE. After embedding secret data, steganoflage video is created by transforming the data into RGB colour space. Secure transmission of secret message can be achieveed through steganoflage video. Steganoflage video satisfies the main objective of steganography that is undetectability and robustness of hidden data.

Keywords

Adaptive steganography, MSE, region of interest, YCbCr color space.

1. INTRODUCTION

The secrecy of digital information sent across an open communication medium like the internet is always questionable. This is due to the easy availability of computation power that can break cipher-text codes. Message secrecy is enhanced by using different approaches to hide certain communications. While a message in cipher text is sure to arouse suspicion, an invisible" message created with careful use of steganography methods, hidden under an inoffensive cover image are likely to slip through Steganography and cryptography are cousins in the spy craft family [1].

The definition of Steganography given as, "the science and art of writing hidden messages in such a way that no one apart from the intended receiver knows about the existence of the hidden message". Almost certainly encryption is performed to the data which use for practical purposes, that is to be embedded in a digital image, before applying steganography methods, thus allowing a greater level of secrecy. Adaptive steganography attempts to secure greater stealth for the message by ensuring that the changes introduced into the cover image remain consistent with the natural noise model associated with cover images. The purpose of steganography is to keep others from thinking that a secret message even exists within stego files.

Digital images are the most widespread cover files used for steganography due to the insensitivity of the human visual system (HVS). Furthermore, digital images can easily be used as cover files without any suspicion because of their presence everywhere on the Internet.

Image steganography systems have two fundamental characteristics, which must be investigated, in order to evaluate the efficiency of such systems. These are the security and capacity of the steganography system. Moreover, designing steganography algorithms that are statistically undetectable and yielding a large capacity is the main goal of steganography.

Image steganography systems can be considered secure if it is impossible for attackers to detect the presence of a hidden message in the stego image by using any accessible means. Therefore, the hidden message must be invisible both perceptually and statistically in order to avoid any suspicions of attackers. Moreover, a steganography system is perfectly secure if the statistics of the cover image and the stego image are identical. However, a steganography system fails if an attacker is able to prove the existence of a secret message or if the embedding technique arouses suspicions of attackers.

JPEG compressed images are the most suitable cover images to be used for steganography. [4]A grayscale image can be defined as a continuous-tone image that has only one component (i.e. luminance).However, the color image is a continuous-tone image that has more than one component (i.e. luminance and chrominance). Almost always the color space (Y-Cb- Cr) is used to store JPEG images. The luminance component (Y) represents the intensity of the image. However, the chrominance components (Cb and Cr) specify the blueness and redness of the image respectively. Using only the (Y) component in such a color model (Y-Cb-Cr) produces a grayscale representation of the color image. Therefore, grayscale images represent special cases of color images As a result; color images can be used as cover images in steganography. Both color and grayscale images are used as cover images. This paper investigates the limitations of the existing methods of steganography and explains a new method of steganography known as "Steganoflage" for videos.

2. LITERATURE SURVEY

Existing steganography methods fall into three main categories, namely methods exploiting image format, methods embedding in the spatial domain and methods embedding in the frequency domain. Essentially, Steganography is achieved by modifying the image's Least Significant Bits (LSBs) in such a way that the carrier image remains intact visually.

2.1 A spatial domain steganography

In spatial domain methods a Steganographer modifies the secret data and the [5]cover medium in the spatial domain, which is the encoding at the level of the LSBs. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as "non-natural". Potdar et al. used this technique in producing fingerprinted secret sharing Steganography for robustness against image cropping attacks. The logic behind is to divide the cover image into sub-images and compress and encrypt the secret data. [2]The resulting data is then sub-divided and embedded into those images portions. To recover the data a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The load of computational was high, but the parameters of algorithm, specifically the number of sub-images (*n*) and the threshold value (*k*) were not set to optimal values leaving the reader to guess the values. Color palette based Steganography exploits the smooth ramp transition in colors as indicated in the color palette. Here the LSBs are modified according to their positions in the said palette index. Johnson and Jajodia were in favour of using BMP (24-bit) instead of JPEG images. The LSB encoding is enormously sensitive to any kind of filtering or manipulation of the stego-image. Cropping, rotation, Scaling, lossy compression to the stego-image and addition of noise, is very likely to destroy the message. Moreover an attacker can easily take out the message by removing the entire LSB plane with very little change in the perceptual quality of the modified stego-image". Almost every filtering process changes the values of many of the LSBs.

2.2 A frequency domain steganography

New algorithms keep promising prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced system for security. [2] The discovery of the LSB embedding mechanism is actually a big success. Although it is perfect in not misleading the HVS, it's fragile to attacks left researchers wondering where to apply it next until the successful application within the frequency domain. DCT is used comprehensively in Video and image (i.e., JPEG) lossy compression. Each block DCT coefficients obtained is quantized using a specific Quantization Table (QT). Most of the techniques here use a JPEG image as a vehicle to embed their data. JPEG compression uses DCT to transform successive sub-image blocks (8x8 pixels) into 64 DCT coefficients. Insertion of the data is done into these coefficients insignificant bits. On the other hand, altering any single coefficient would affect the entire 64 block pixels. Since the change is operating on the frequency domain instead of the spatial domain there will be no visible changes in the cover image. The JSteg algorithm was among the first algorithms which uses JPEG images. Even though the algorithm stood strongly against visual attacks, examination of the statistical distribution of the DCT coefficients yields a proof for existence of secret data. *X2-test* easily detect the JSteg, which is a non- statistical algorithm used in order to detect whether the intensity levels scatter in a uniform distribution throughout the image surface or not. Whether detecting one similar intensity level like it, then the pixels related with this intensity level is considered as corrupted pixels or having a higher probability of containing embedded data. Moreover, since the DCT coefficients need to be treated with sensitive care and intelligence, the JSteg algorithm leaves a serious statistical signature. Wayner stated that the coefficients in JPEG compression normally fall along a bell curve and the hidden information embedded by JSteg distorts this. Manikopoulos et al discussed an algorithm that utilizes the Probability Density Function (PDF) used to generate discriminator features fed into a neural network system to detect hidden data in this domain. OutGuess, developed by [8] Provos and Honeyman, was a better alternative as it uses a pseudo-random-number generator to select DCT coefficients. The randomly distributed data will not be detected by X2-test. Provos and Honeyman, suggest applying an extended version of X2-test to select Pseudo-randomly embedded messages in JPEG images. Andreas Westfeld based "F5" algorithm on subtraction and matrix encoding.

2.3 An Adaptive steganography

Adaptive steganography is one of the special cases of steganography. It is also known as "Statistics-aware embedding", "Masking". This method of steganography takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. [2]The statistics will state that, where to create the changes and It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local (STD), standard deviation. Finally it aimed to avoid smooth areas and areas of uniform color. This action makes adaptive steganography seek images with existing or deliberately added noise and images that demonstrate color complexity.

Edge embedding follows edge segment locations of objects in the host gray-scale image in a fixed block fashion each of which has its centre on an edge pixel. Although simple, this method is robust to many attacks and it follows that this adaptive method is also an outstanding means of hiding data while maintaining a good perceptibility. Chin-Chen proposes an adaptive technique applied to the LSB substitution method. The idea behind it is to exploit the relationship between neighbouring pixels to estimate the degree of smoothness.

2.4 S-Tools

S-Tool is a particular method which involves changing the least significant bit of each of the three colors in a pixel in a 24-bit image e.g. a 24-bit BMP file. It involves a pre-processing step to reduce the number of color entries by using a distance measurement to identify neighbour colors in terms of intensity. After this stage each color of the dithered image would be associated with two palette entries one of which will carry the hidden data. [1]The software for S-Tools can reduce the number of colors in the image to 256. The software uses the algorithm developed by Heckbert to reduce the number of colors in an image in a way that will not visually disrupt the image. The algorithm plots all the colors in three dimensions (Red, Green, and Blue - RGB). It searches for a collection of *n* boxes, which contains all of the colors in one of the boxes. The process starts with the complete 256*256*256 space as one box. The boxes are then recursively subdivided by splitting into the best possible way. Splitting continues until there are *n* boxes representing the space. When it is finished the program chooses one color to represent all the colors in each box. The color may be chosen in different ways: the centre of the box, the average box color or the average of the pixels in the box. The system interface is easy to use. It supports a drag and drop method to load images. Once the cover image is dragged in; the system will advise the user on how much data in bytes the image can hold.

2.5 Limitations of previous methods

- F5 and S-Tools scatter the secret message over the whole carrier medium.
- In Direct spatial LSB techniques large payload but often offset the statistical properties of the image.
- Direct spatial LSB techniques are not robust against lossy compression and image filters.
- Transform domain techniques cannot resist attacks based on multiple image processing techniques.

3. METHODOLOGY

The method of video steganography "Steganoflage" is explained by using following block diagram shown in Fig. 1.

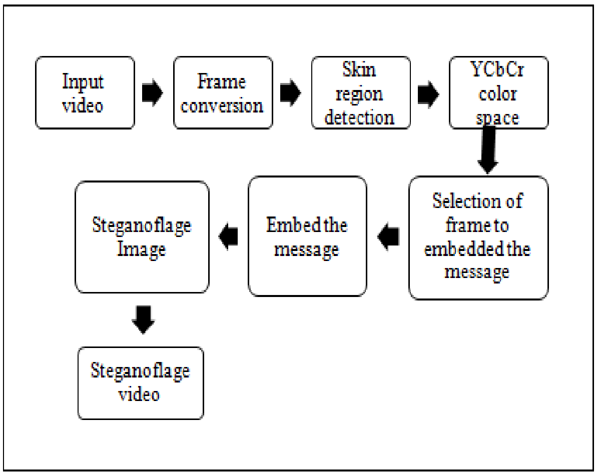

Figure 1: Block Diagram of Steganoflage Algorithm (Encoding).

The steps involved in the discussed "Steganoflage" method are given below.

3.1 Frame conversion

- Image sequences (video) are considered as four-dimensional arrays. Each separate image of a video is called as frame; all frames are having same size, and are concatenated along the fourth dimension. aviread function will be used for loading and showing the input video sequence. The frames stored in a data structure called as cell array. Fig. 2 shows frame of input video.

Figure 2: video is converted to frames.

3.2 Skin region detection

- Skin region is detected by converting to hsv color space and segmenting the foreground image.
- Morphological dilation and filling operation have applied to extract the face region. The extracted face region from frame of a video is shown in Fig. 3.

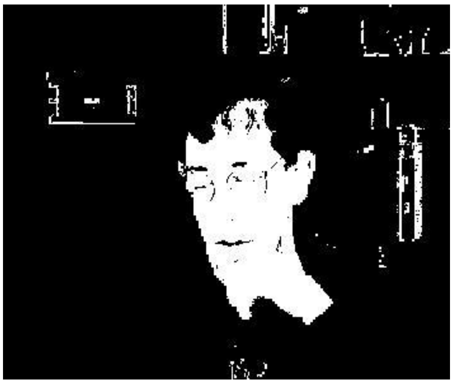

Figure 3: Skin region detection

3.3 Select a frame to embed

- The video frames are transformed to YCbCr color space to perform embedding.
- The frame which has least MSE is selected to embed a secret data.
  Fig. 4 shows YCbCr components of selected frame for embedding.

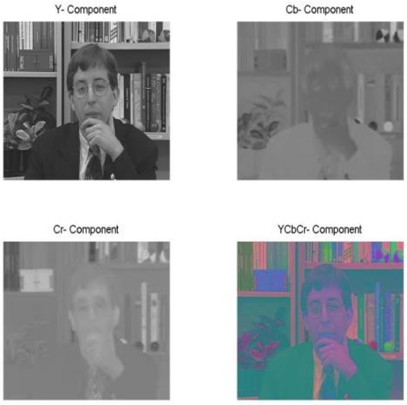

Figure 4: Y, Cb, Cr and YCbCr component of video frame.

3.4 MSE calculation

MSE Calculation for Each Frame

- In a sense, any measure of the centre of a distribution has associated with some measure of error. Suppose the number *t* is a superior measure of centre, then presumably *t* represents the entire distribution superiorly, in some way, than other numbers.
- In this circumstance, measuring the quality of *t*, the centre of distribution is better explained by the mean square error.

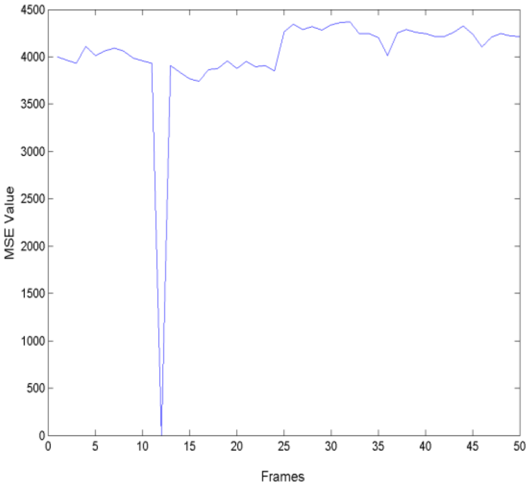

Figure 6: MSE Graph for "Video".

3.5 Steganoflage image

- The message data is embedded into a frame with least MSE.
- The least MSE frames have decomposed into YCbCr component.
- The data have embedded into the Cb component alone.
- Later the embedded component will be concatenated with the remaining components. Fig. 5 shows the frame obtain after embedding secret message inside it.

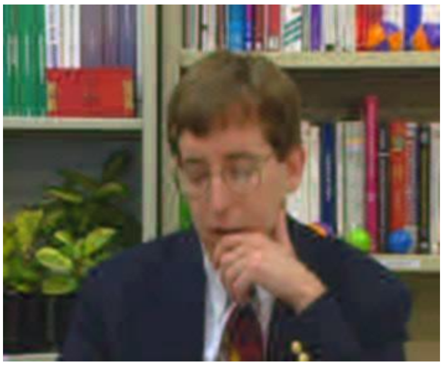

Figure 7: Stego image formed by "Steganoflage".

3.6 Steganoflage video

- The Steganoflage image will be replaced in the YCbCr frame set.
- Then those frames will be converted to RGB color space.
- An object variable will be initialized to reconstruct the frames into video.
- Finally Steganoflage video is obtained.

The decoding process is exactly opposite to the encoding process. The block diagram of decoding process is shown in Fig. 8.

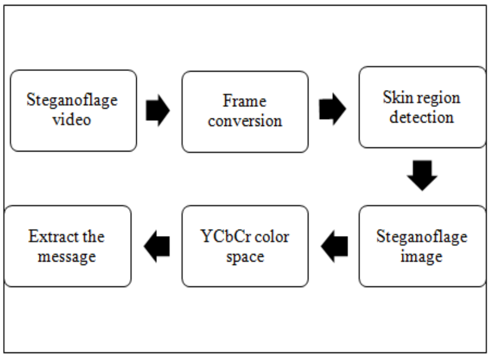

Figure 8: Block Diagram of Steganoflage Algorithm (Decoding).

4. PERFORMANCE MEASURE

As a performance measurement for image distortion, the well known parameter is Peak-Signal-to-Noise Ratio (PSNR), which have classified under the[2] difference distortion metrics, applied to the Stego and the Original images. It is defined as:

$$\text{PSNR}=10\ \log_{10}(\frac{C^2\text{MAX}}{MSE})$$

Where MSE is Mean Square Error which is given by:

$$\text{MSE}=\frac{1}{\text{MN}}\sum_{x=1}^{M}\ \sum_{Y=1}^{N}\quad (Sxy-Cxy)^2$$

It holds the maximum value in the original image, given by example:

$$Cmax \leq \begin{cases} 1, & in\ double\ precision\ intensity\ images \\ 255, & in\ 8-bit\ unsigned\ integer\ intensity\ images \end{cases}$$

x and *y* are the coordinates image, M and N are the image dimensions, S_{xy} is the generated stego image and C_{xy} is the cover image. The PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30dB indicate a fairly low quality (i.e., distortion caused by embedding can be obvious). A high quality Stego should strive for 40dB and above.

5. EXPERIMENTAL RESULT

Several simulations were performed to evaluate the performance of the studied method Steganoflage. An avi video is used for performing the operation and result obtain after operations are stated in following table. For calculating performance measure of S-Tool, the first step is to run the S-Tool software, then drag the particular image frame on S-tool window which act as a carrier. Next step is to drop the image which is supposed to hide, on the particular image carrier frame. After this operation stego image is formed.

The function which calculates PSNR value takes the path of both original image frame and stego image as input and gives PSNR values in decibels as output. The output values are stated in table 1.

The result shows that the discussed method Steganoflage shows better results than S-tool and another method of Steganography using LSB method.

Table 2 shows the results of Performance after embedding in Cb and Cr components of YCbCr. PSNR value calculated by using two different parameters. PSNE using MSE and PSNR using Y component of YCbCr color space.

Table 1: Comparison of Performance with discussed method Steganoflage, S-tool and Steganography using LSB method.

Tool used	PSNR	Embedded Bits	Size Original / Stego
Steganoflage	66.78	2120	20.5kb / 13.0kb
S-Tool	58.3595	2120	297kb / 297kb
Steganography using LSB Method	21.3878	3601	297kb / 36.6kb

Table 2: Result obtain after embedding the secret message in different components of YCbCr

Steganoflage	PSNR_MSE	PSNR_Y
Embedded in Cr Component.	66.7814	77.8000
Embedded in Cb component.	66.7810	77.8003

6. CONCLUSION AND FUTURE SCOPE

The discussed method uses video as a carrier to embed secrete message in a particular region of interest. The particular region of interest is selected by using skin detection algorithm. The secrete message is embed in selected region of interest of a frame having least MSE. This method can avoid many drawbacks occurs in LSB method after rotational distortion, noise and cropping effect of image.

In future the capacity of the secret message can be increased by embedding the secret message in more than one video frame.

7. REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt,*" Enhancing Steganography In Digital Images". Canadian Conference on Computer and Robot Vision. pp. 326-332, 2008.*

[2] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt," Biometric Inspired Digital Image Steganography". *15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems.* pp. 159-167, 2008.

[3] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt**,** "Skin Tone Based Steganography In Video Files Exploiting The Ycbcr Color Space". *ICME Hannover*.pp. 905 – 908, 2008.

[4] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography". Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science University of Pretoria.

[5] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image**".** *Computer Technology and Application.*pp.102-108, 201.

[6] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "Steganoflage - A Novel Approach to Image Steganography".pp.191-194.

[7] Anjali A. Shejul, Umesh L. Kulkarni" A Secure Skin Tone based Steganography Using Wavelet Transform" *International Journal of of Computer Theory and Engineering, Vol.3.* 2011.

[8] Johnson, N. F. and Jajodia, S." Exploring Steganography: Seeing the Unseen". IEEE Computer, 31 (2): 26-34, Feb 1998.

[9] Provos, N. and Honeyman, P."Hide and Seek: An Introduction to Steganography". IEEE Security and Privacy, 01 (3): pp. 32-44, May-June 2003.

[10] Petitcolas, F.A.P. "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC. Watermarking. Norwood: Artech House, INC, 2000.

[11] S-Tool : http://bit599.netai.net/s_tools.htm.