Video Steganography using Wavelet Transfer

Aditya Basta(19BCE1287), Ayyappan KM(19BCE1410), Naman(19BCE1491)

Abstract

Internet is has grown wildly over the past few years and so has the number of users who use it on a daily basis. Every day 2.5 quintillion bytes of data are generated which is accessed and shared over the internet and hence comes the question of the security of that data that needs to be shared.

This has led to various encryption techniques and protocols being developed to secure data. One of which is steganography. Steganography is the technique of hiding secret data with ordinary data, files, or messages to avoid detection from unintended entities. Video steganography is a method used to hide secret data such as a message or a photo in a cover multimedia file like a video file. Video files are very suitable for hiding data because of the large number of frames and the ability to make minor changes to each frame. We have mainly implemented DWT(Discrete Wavelet Transform) to hide the message(photo) behind the cover multi-media file. We have also experimented with hiding a video in another video using the same technique, which will be part of our further studies.

Introduction

Video Steganography is soon becoming one of the main research areas in data hiding techniques. Human visual senses are less sensitive to the very minor changes to digital media such as videos and hence video steganography is highly effective when used properly. Video Steganography can be classified into 3 main types, Intra-embedding. Pre embedding and post-embedding. Intra - embedding methods are pixel interpolation, motion vectors, etc. Pre embedding methods manipulate the raw video file and perform operations in spatial and transform domains. Post embedding mainly focuses on bitstream. We have worked on the pre-embedding part by using discrete wavelet transform.

Discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time).

In wavelet analysis, the Discrete Wavelet Transform (DWT) decomposes a signal into a set of mutually orthogonal wavelet basis functions. These functions differ from sinusoidal basis functions in that they are spatially localized – that is, nonzero over only part of the total signal length.

We have used DWT to perform operations(addition of secret-frame) in the frequency domain and also used inverse DWT to convert back to spatial domain to store the location which was hidden in the video file using the least significant bit(LSB) hiding.

Literature Survey

V. Saravanan et al [1] "Security Issues in Computer Networks and Steganography"

This paper reduces the detectable distortion in a joint photographic experts group (JPEG) file during the data hiding process, by introducing a new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), the vertical difference (VD), and region size (RS). The JPEG image will be split into several

blocks and each pixel in it will be examined to calculate the variations. Depending upon the variation, the amount of secret information will be hidden in an image. This proposed method of information hiding will help to solve the security issues in computer networks.

Bin Liu et al [2] "Secure Steganography in Compressed Video Bitstreams"

A new compressed feature secure steganography (CVSS) calculation is proposed. In the calculation, implanting and discovery operations are both executed completely in the compacted area, with no requirement for the decompression process. The new criteria utilizing factual imperceptibility of adjoining edges are utilized to modify the installing technique and limit, which builds the security of the proposed calculation. Along these lines, the plot safe properties are acquired. Feature steganalysis with shut circle input way is outlined as a checker to discover evident bugs. Trial results demonstrated this plan can be connected on packed feature steganography with high-security properties.

Balaji, R. et al [3] "Secure data transmission using video Steganography"

It is extremely fundamental to transmit imperative information like saving money and military data safely. Video Steganography is the methodology of concealing some mystery data inside a feature. The expansion of this data to the feature is not conspicuous by the human eye as the change of pixel shading is unimportant. This paper means to give a productive and safe strategy for feature Steganography. The proposed system makes a list for the mystery data and the record is put in a casing of the video itself. With the assistance of this record, the casings containing the mystery data are placed. Consequently, amid the extraction process, as opposed to examining the whole feature, the casings containing the mystery information are investigated with the assistance of a list at the less than desirable end.

Keren Wang et al [4] "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value"

This paper exhibits a strategy for the location of movement vector-based feature steganography. To begin with, the alteration on the minimum noteworthy bit of the movement vector is displayed. The impact of the installing operation on the entirety of outright contrast (SAD) is represented, which permits us to concentrate on the distinction between the real SAD and the by regional standards ideal SAD after the including or-subtracting-one operation on the movement esteem. At long last, taking into account the way that most movement vectors are by regional standards ideal for most feature codecs, two capabilities are extricated and utilized for arrangement.

Mustafa, R.J. et al [5] "A highly secure video steganography using Hamming code"

Because of the rapid advances in web innovation, individuals are getting to be more agonized over data being hacked by aggressors. As of late, numerous calculations of steganography and information stowing away have been proposed. Steganography is a procedure of installing the mystery data inside the host medium (content, sound, picture, and feature). Simultaneously, a large portion of the intense steganographic examination programming projects has been given to unapproved clients to recover the significant mystery data that was inserted in the bearer documents. Some steganography calculations can be effectively recognized by Steg analytical locators given the absence of security and installing productivity. In this paper, we

propose a protected feature steganography calculation in light of the guideline of straight square code. Nine uncompressed feature successions are utilized as spread information and a double picture logo as a mystery message.

Any successful steganography technique must consider some factors like imperceptibility, anti steganalysis, and payload capacity but some factors contradict each other, for example increasing payload capacity leads to distortion of imperceptibility, and distortion of imperceptibility leads to vulnerability to attacks. Hence any steganography scheme can be considered as an optimization problem where the steganography technique hides secret messages inside the cover video frame. Koushik et.al [38] had proposed an optimized technique for basic video steganography technique using a genetic algorithm. The optimizer has been used to optimize a 3-3-2 LSB technique to achieve PSNR between 20 to 40dB and improved image fidelity (IF) as compared to the previously existing method.

Proposed Work

We propose a new method in our project, where implement video steganography using wavelet transform in python using *PyWavelets.* PyWavelets allows us to perform DWT transform on images in python without the help of MATLAB. We embed images as well as videos in a cover video using DWT on a cover frame. This cover frame is chosen at random to further evade any unauthorized personnel finding the *secret* data. The steps to embed an image are discussed below:

1) Splitting the video into frames, and choosing random frames (i.e. 3 for each image) to store the image.
2) The image is resized to the resolution of the video to avoid any further conflict and the image is broken down into red, blue and green channels.
3) For every channel, the assigned frame is broken down into red, blue and green channels.
4) The red channel of the cover frame is then wavelet transformed into four wavelet bands.
5) The HH bands of the cover frame are then replaced by the channel of the secret image. Then all the bands inverse-wavelet transformed back into a frame. In this way, all three channels are stored in 3 different frames of the cover video.
6) After all the channels are embedded, all the frames are stitched back into a frame array.
7) The frame array is used to form the original video back.

The steps explain most of the process in brief. The additional processes are explained hereafter. In order to find *random frames* and to make sure that we don't embed data into a particular, a HashMap data structure is used to store all the frames where we embed data. Before embedding any data, a lookup is performed in the HashMap, to ensure that frame wasn't used before. Another problem with choosing random frames is to find these random frames during extraction. To overcome this problem, we make use of a stego key. This key is just a string containing all the frame numbers of the frames where the data was embedded. This key is then stored in the final video in spatial domain by implementing the LSB method to store data in an image. The key is stored in the first frame of the cover video. After the embedding process, additional encoding process is performed on the frame array

before actually forming the original video back.

The steps to extract an image from the video are :

1) Extract the stego key from the first frame of the video and store the frames.
2) For each combination of frames (i.e. 3 frames), break the frame into red, green and blue channels.
3) Wavelet transform the red channels of the frame and extract the HH bands and store them in individual channels.
4) Merge these individual channels, into an image.

To store a video in a video, most the steps are same except that the data video is broke down into each frame and each frame is stored by the above process.

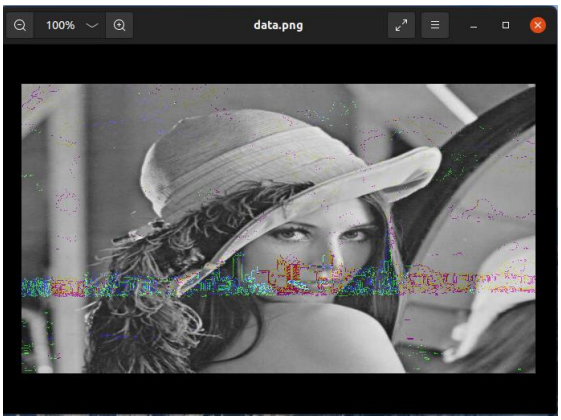
Software - Hardware Needed

RAM – minimum 8GB
Processor – Intel i5 or higher
Python – 3.8 or higher

Results

The results of the steganography process. The screenshots of the images and video frames are attached.

The sample image which we embedded in a video.



The image after extraction.

Summary

The aim of the project was to explore Video Steganography. We employed video steganography in both transfer and spatial domain. The video after the embedding process not only looks alike with the original video but also has the audio intact, which most of the previous works didn't overcome. In the future, Video Steganography will become ever more important as privacy concerns are increasing all over the globe. We can even hope for a mixture of steganography and cryptography for further secure transmission of data.

References

[1] "Security Issues in Computer Networks and Steganography"

[2] "Secure Steganography in Compressed Video Bitstreams"

[3] "Secure data transmission using video Steganography"

[4] "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value"

[5] "A highly secure video steganography using Hamming code"