www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11972-11976

Image steganography for hiding videos

Ms.A.Lavanya , Mr.D.Jayakumar M.Tech.,

Pg Student,

Department Of Computer Applications,

Ifet College Of Engineering,

Villupuram

Assistent Professer,

Department Of Computer Applications,

Ifet College Of Engineering,

Villupuram.

Abstract: Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding isachieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stegoimage(generated image which is carrying a hidden message). In proposed we are embedding video file in the image for secret sharing of data and also keen on obtaining the same quality of image after decoding.This paper intends to give an overview of to hide videos inside image, its uses and techniques. In this project video hidden inside the image for which video get compressed and stored inside the image.features are extracted before encryption for effective re-construction.

Introduction:

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. We compute the structure of each micro-pattern with the aid of a compass mask that extracts directional information, and we encode such information using the prominent direction indices (directional numbers) and sign—which allows us to distinguish among similar structural patterns that have different intensity transitions. We divide the face into several regions, and extract the distribution of the LDN features from them. Image features like LDN(binary code), edge detection, histogram generation.

In digital signal processing, **video compression**, **source coding**,[1] or **bit-rate reduction** involves encoding information

using fewer bits than the original representation.[2]Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it.[3] The process of reducing the size of a data file is referred to as data compression. In the context of data transmission, it is called source coding (encoding done at the source of the data before it is stored or transmitted) in opposition to channel coding.[4]

Compression is useful because it helps reduce resource usage, such as data storage space or transmission capacity. Because compressed data must be decompressed to use, this extra processing imposes computational or other costs through decompression; this situation is far from being a free lunch. Data compression is subject to a space–time complexity trade-off. For instance, a compression scheme for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage. The design of data compression schemes involves trade-offs among various factors, including the degree of compression, the amount of distortion introduced (when using lossy data compression), and the computational resources required to compress and uncompress the data.

Algorithm used:

Lossless video compression:

Lossless data compression is a class of data compression algorithms that allows the original data to be perfectly reconstructed from the compressed data. By contrast, lossy data compression permits reconstruction only of an approximation of the original data, though this usually improves compression rates (and therefore reduces file sizes).

Lossless data compression is used in many applications. For example, it is used in the ZIP file format and in the GNU tool gzip. It is also often used as a component within lossy data compression technologies (e.g. lossless mid/side joint stereo preprocessing by the LAME MP3 encoder and other lossy audio encoders).

Lossless compression is used in cases where it is important that the original and the decompressed data be identical, or where deviations from the original data could be deleterious. Typical examples are executable programs, text documents, and source code. Some image file formats, like PNG or GIF, use only lossless compression, while others like TIFF and MNG may use either lossless or lossy methods. Lossless audio formats are most often used for archiving or production purposes, while smaller lossy audio files are typically used on portable players and in other cases where storage space is limited or exact replication of the audio is unnecessary.

Edge detection algorithm:

Edge detection is the name for a set of mathematical methods which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed *edges*. The same problem of finding discontinuities in 1D signals is known as step detection and the problem of finding signal discontinuities over time is known as change detection. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction.

Binary code (LDN Generation)

LDN encodes the directional information of the image textures (i.e., the texture's structure) in a compact way, producing a more discriminative code than current methods. We compute the structure of each micro-pattern with the aid of a compass mask that extracts directional information, and we encode such information using the prominent direction indices (directional numbers) and sign—which allows us to distinguish among similar structural patterns that have different intensity transitions. We divide the face into several regions, and extract the distribution of the LDN features from them. Then, we concatenate these features into a feature vector.

Steganography:

steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of security. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal.[2] Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Video files are hidden inside the image using steganography scheme video get compressed before it get and encrypted inside the image. For video compression lossless compression technique is used for compressing the video. Image features are extracted for effective reconstruction of image during decryption process image features are extracted before hiding the video inside the image.

Sender part functional diagram represented

Fig 1.1

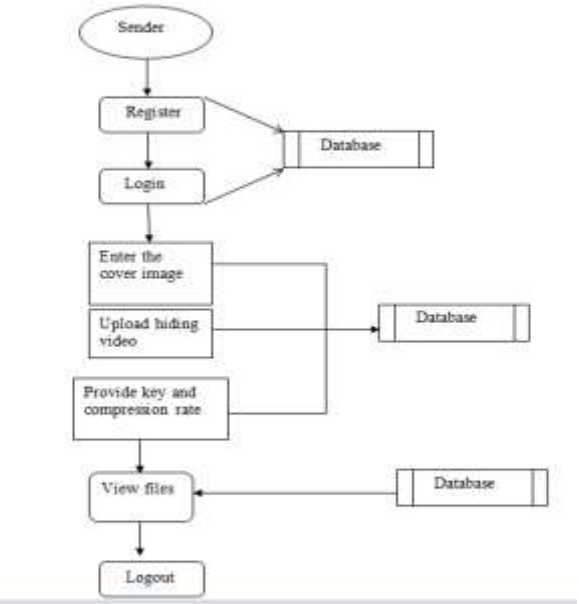


Fig 1.1

Receiver part functional diagram represented in fig 1.2

Conclusion:

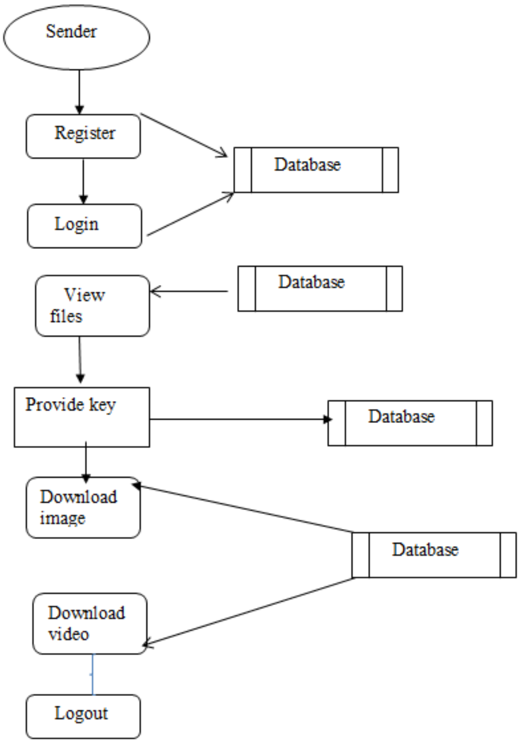
We are embedding video file in the image for secret sharing of data and also keen on obtaining the same quality of image after decoding. We have extracted the image features and stored before binding with image and video is compressed and encrypted inside the image.Steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

References:

[1]http://en.wikipedia.org/wiki/Steganography

[2]http://cs.gmu.edu/~astavrou/courses/ISA_785_F11/sing_stego.pdf

[3] algorithm and technique on various edge detection: a survey Rashmi1 ,Mukesh Kumar2 , and Rohini Saxena2



[4]http://www.eetimes.com/document.asp?doc_id=1275884

[5]http://classic.www.axis.com/products/video/about_networkvideo/compression.htm

[6]http://www.ijceronline.com/papers/Vol2_issue5/BX02516201623.pdf

[7] Jiri Fridrich ,Du Dui, "Secure Steganographic Method for Palette Images," 3rd Int. Workshop on InformationHiding, pp.47-66, 1999.

[8] KafaRabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) - 2004.

[9] A. Ker, "Improved detection of LSB steganography in grayscale images," *in Proc. Information Hiding Workshop*, *vol. 3200*, Springer LNCS, pp. 97–115, 2004.

[10] Keissarian, F. Hiding secrete data in compressed images using histogram analysis. *In* the 2nd International Conference on Computer & Automation Engineering
(ICCAE), Singapore, 2010, 2, pp. 492-96.

[1]http://en.wikipedia.org/wiki/Steganography

[2]http://cs.gmu.edu/~astavrou/courses/ISA_785_F11/sing_stego.pdf

[3]ALGORITHM AND TECHNIQUE ON VARIOUS EDGE DETECTION: A SURVEY Rashmi1 ,Mukesh Kumar2 , and Rohini Saxena2

[4]http://www.eetimes.com/document.asp?doc_id=1275884

[5]http://classic.www.axis.com/products/video/about_networkvideo/compression.htm

[6]http://www.ijceronline.com/papers/Vol2_issue5/BX02516201623.pdf

[7] Jiri Fridrich ,Du Dui, “Secure Steganographic Method for Palette Images,” 3rd Int. Workshop on

InformationHiding, pp.47-66, 1999.

[8] KafaRabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) - 2004.

[9] A. Ker, “Improved detection of LSB steganography in grayscale images,” *in Proc. Information Hiding Workshop*, *vol. 3200*, Springer LNCS, pp. 97–115, 2004.

[10] Keissarian, F. Hiding secrete data in compressed images using histogram analysis. *In* the 2nd International Conference on Computer & Automation Engineering
(ICCAE), Singapore, 2010, 2, pp. 492-96.