International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 3, May-Jun-2022, ISSN (Online): 2395-566X

Wavelet Compression Techniques for Video Data Using Bit-Plane Complexity Segmentation

Ismail Hassan Farah, Dr. K. Juliana Gnanaselvi
Dept. of Information Technology, Dept. of Computer Science
Rathinam College of Arts and Science,
Coimbatore, Tamil Nadu, India -641021
ismailhassanfarah.mit20@rathinam.in, hod.it@rathinam.in

Abstract- This project presents a steganography method using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and bit-plane complexity segmentation (BPCS) steganography. In wavelet based video compression methods such as 3-D set partitioning in hierarchical trees (SPIHT) algorithm and Motion-JPEG2000, wavelet coefficients in discrete wavelet transformed video are quantized into a bit-plane structure and therefore BPCS steganography can be applied in the wavelet domain. 3-D SPIHT-BPCS steganography and Motion-JPEG2000-BPCS steganography are presented and tested, which are the integration of 3-D SPIHT video coding and BPCS steganography, and that of Motion-JPEG2000 and BPCS, respectively. Experimental results show that 3-D SPIHT-BPCS is superior to Motion-JPEG2000-BPCS with regard to embedding performance. Steganography is the art and science of communicating in a way which hides the the existence of the secret message communication. It aims to hide information/covered writing. Information to be protected is hidden in another data known as cover or carrier. Data containing hidden message are called as Stefano's or Stegos. Steganos look like cover data and it is difficult to differentiate between them. Steganography based communication over easily accessible platforms to prevent leakage of information.

Keywords- Lossy Compressed Video, SPHIT-BPCS, Steganography, Motion-JPEG2000 -BPCS,

I. INTRODUCTION

The recent finalization of mpeg-4 will make this standard very attractive for a large range of applications such as video editing, internet video editing, internet video distribution, and wireless video communications. These applications are likely to get great benefit from watermarking technology, since it can be enable a number of innovative services, such as conditional access policies data annotation, content authentication to be implemented at a low price.[5]

This application lets you embed or hide important or private messages or files into wmv and mpg without affecting the quality of actual data or files. It achieves this by using the least significant bits of these files for embedding data which are not used by the Image viewers or Image editors. It allows you to embed the messages or files in encrypted form using 32 bit DES algorithm which means that once encrypted, the message or file could be retrieved (or decrypted) from a Master file only after specifying the correct password which was used at the time of encryption. It allows embedding messages and files in compressed form using ZIP compression format. And gives you a choice of compression level to be used-low, normal or high.

II. SYSTEM STUDY

1.Existing System
The existing system is one in which the image can only be hidden and sent to another system through internet and the transfer is not secure. In the existing system they do not followed the steganography concepts.

2.Disadvantages of the Existing System:
1. Poor security.
2. Security of information is low.
3. Less clarity.
4. No accuracy in image.
5. The image can be compressed with loss of the clarity and loss of pixels.

3. The Proposed Work*:*
The drawbacks, which are faced during existing system, can be eradicated by using the proposed system. The main objective of the existing system is to provide a user-friendly interface. In this proposed system the image, audio and video are encrypted more securely and also receiver side retrieving more securely.

Advantages of the proposed system:
1. Security is assured.
2. Maintenance of file is flexible.
3. Images stored are updated instantly.
4. Using embed the messages or files in encrypted form using DES algorithm.

III. SYSTEM ENVIRONMENT

1. Watermarking- Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time.In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark

2. Applications

Digital Watermarking can be used for a wide range of applications such as:

- Copyright protection
- Source Tracking (Different recipients get differently watermarked content)
- Broadcast Monitoring (Television news often contains watermarked video from international agencies)
- Covert Communication.

3. Watermarking life-cycle phases

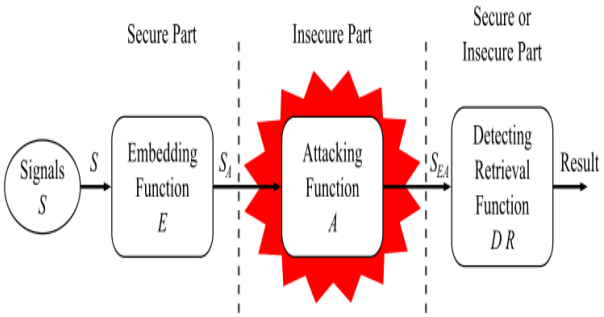

Fig.1 Life cycle.

4. Embedding method

A watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference. A watermarking method is referred to as amplitude modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method but is particularly embedded in the spatial domain.

5.Evaluation/benchmarking

The evaluation of digital watermarking schemes can provide detailed information for a watermark designer or for end users. Therefore, different evaluation strategies exist. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. End users are mostly not interested in detailed information. They want to know if a given digital watermarking algorithm can be used for their application scenario, and if so, which parameter sets seems to be the best.

6.Reversible data hiding

Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the watermark and replacing the image data which had been overwritten. This would make the images acceptable for legal purposes. The US army is also interested in this technique for authentication of reconnaissance images.

7.Watermark (Data Fle)

A watermark stored in a data file refers to a method for ensuring data integrity which combines aspects of data hashing and digital watermarking. Both are useful for tamper detection, though each has its own advantages and disadvantages.

III. SYSTEM IMPLEMENTATION

1.Modules

- Image Steganography
- Audio Steganography
- Video Steganography

2.Image Steganography

In this module for hiding the message in any of the image file format (.jpg, .gif, .tiff, .bmp), the given text will be embedded into the source image using a 8 bit encryption key. To retrieve the embedded message, the file is displayed with the information and a request to retrieve the message. Using the encrypted key the original message is dispatched from the image and displayed in a separate window.

3.Audio Steganography

In this module for hiding the message in any of the audio file format (.mp3, .ram, .wav, .wma) , the given text will be embedded into the source audio file using a 8 bit encryption key. To retrieve the embedded message, the file is displayed with the information and a request to retrieve the message.

4. Video Steganography

In this module for hiding the message in any of the video file format (.mpg, .dat, .wmv, the given text will be embedded into the source video using a 8 bit encryption key. To retrieve the embedded message, the file is displayed with the information and a request to retrieve the message. Using the encrypted key the original message is

dispatched from the video and displayed in a separate window.

5.Symmetric Key Cryptography

The most widely used symmetric key cryptographic method is the Data Encryption Standard (DES), published in 1977 by the National Bureau of Standards. DES It is still the most widely used symmetric-key approach. It uses a fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages.

V. CONCLUSION

This research work has presented a large capacity steganography method applicable to compressed video which is invented based on BPCS steganography and wavelet- based video compression.3-D SPIHT-BPCS steganography and Motion-JPEG2000-BPCS steganography have been presented, which are the integration of 3-D SPIHT video coding and BPCS steganography, and that of Motion-JPEG2000 and BPCS, respectively. The proposed 3-D SPIHT-BPCS steganography achieved embedding rates of around 28% of the compressed video size for twelve-bit representation of wavelet coefficients with no noticeable degradation in video quality.

REFERENCES

[1] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.
[2] M. Niimi, H. Noda and E. Kawaguchi,"A steganography based on region segmentation by using complexity measure," Trans. of IEICE, J81-D-II, pp.1132-1140, 1998.
[3] E. Kawaguchi and R. O. Eason,"Principle and applications of BPCS-steganography," Proc. of SPIE, 3528, pp.464-473, 1998.
[4] J. Spaulding, H. Noda, M. N. Shirazi and E. Kawaguchi,"BPCS steganography using EZW lossy compressed images," Pattern Recognition Letters, 23, pp.1579-1587, 2002.
[5] A.Sivakumar, "A Survey on Wide Area Network Optimization Techniques and it's Applications", International Journal of Innovative Research in Computer and Communication Engineering, Volume 8, Issue 8, e-ISSN: 2320-9801, p-ISSN: 2320-9798, 3006-3012, Aug 2020.
[6] H. Noda, J. Spaulding, M. N. Shirazi, M. Niimi and E. Kawaguchi," Bit-plane decomposition steganography combined with JPEG2000 compression," Lecture Notes in Computer Science, 2578, pp.295-309, 2003.