International Journal of Embedded Systems, Robotics and Computer Engineering.
Volume 1, Number 1 (2015), pp. 13-21
© International Research Publication House
http://www.irphouse.com

Embedded Hiding and Extracting Secret Data in Compress Video File

Rohit Nagargoje, Manish Raka, Amrut Pol and Prof. B.Gite

[1,2,3]UG Student, [4]Assistant Professor, Department of Computer Engineering
Sinhgad Academy of Engineering, Pune, India.

Abstract

The Security has become an essential part of our daily life, and many organizations realize that the Security can be a major issue to protect data from unauthorized person. In this project, we are going to deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain. We target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their macro block prediction error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bit stream is embedded in the least significant bit of both components of the candidate motion vectors. The method is implemented and tested for hiding data in natural sequences of multiple groups of pictures and the results are evaluated. The evaluation is based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size. Based on the criteria, the proposed method is found to perform well and is compared to a motion vector attribute-based method from the literature.

Keywords— Encryption, Compression, Authentication,LBS method, Password, LZW, AES.

I. INTRODUCTION

DATA hiding and watermarking in digital images and raw video have wide literature. This paper targets the internal dynamics of video compression, specifically the motion estimation stage. We have chosen this stage because its contents are processed internally during the video encoding/ decoding which makes it hard to be detected by image stag analysis methods and is lossless coded, thus it is not prone to quantization distortions. In the literature, most work applied on data hiding in motion vectors relies on changing the motion vectors based on their attributes such as their magnitude, phase angle, etc. In the data bits of the message are hidden in some of the image whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). A single bit is hidden in the least significant bit of the larger component of each CMV. In the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. Using the variable macro block sizes used every 2 bits from the message bit stream to select one of the four sizes for the motion estimation process. The message bit stream is encoded as phase angle difference in sectors between CMV. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold. The methods in focused on finding a direct reversible way to identify the CMV at the decoder and thus relied on the attributes of the motion vectors. In this paper, we take a different approach directed towards achieving a minimum distortion to the prediction error and the data size overhead. This approach is based on the associated prediction error and we are faced by the difficulty of dealing with the nonlinear quantization process.

II. PROPOSED SUSTEM

We proposed system where users that are willing to hiding data in Compress Video that are expected to be computer users with minimal computer knowledge. Proposed I frame encoding adopts wavelet transform and set partitioning in hierarchical trees (SPIHT) algorithm; for P frames, each frame sets the reconstructed frame of its previous frame as a reference frame, and then P frames proceed to code with ME and M C. Eugenie Belayed et al. Proposed a new spatial scalable and low complexity video compression algorithm based on multiplication free three dimensional discrete pseudo cosine transform. This paper shows an efficient results compared with H.264/SVC as well as it can be used for robust video transmission over wireless channels. --

R. Reengineer, J. Gibson et al. the distribution of DCT-coefficients in the field of image compression is examined and an approximation of the AC-coefficients with Laplace distributions is proposed.

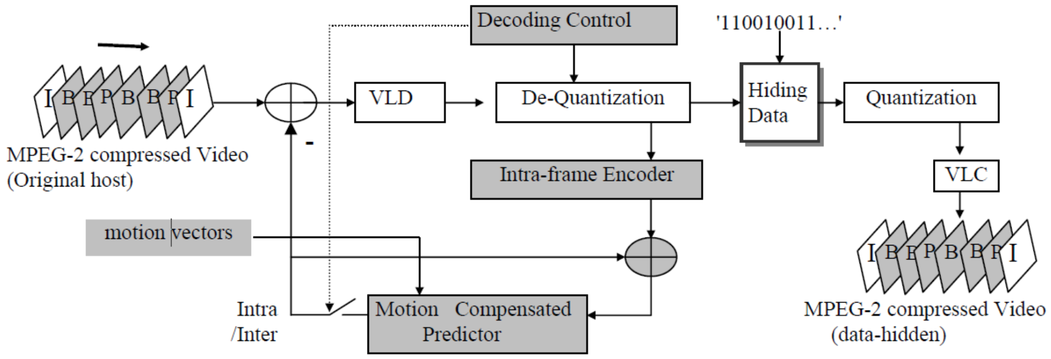
Lai-Man Po and Wing-Chung Ma et al.have proposed “A Novel Four-Step Search Algorithm for Fast Block Motion Estimation” in 1995. The proposed algorithm has given based on the centre-based global minimum motion vector distribution characteristic of real world image sequence, a new Four-Step Search algorithm for fast block-based motion estimation. F. Mueller et al. proposed the work of introduces the generalized Gaussian distribution to model the DCT-coefficients more accurate than with Laplace distributions.

Cong Dao Han et al. implemented a novel search algorithm which utilizes an adaptive hexagon and small diamond search to enhance search speed. Simulation results showed that the proposed approach can speed up the search process with little effect on distortion performance compared with other adaptive approaches.

III. SYSTEM ARCHITECTURE

Since a video can be viewed as sequences of still images, video watermarking is an extension of image watermarking. The applications for still image watermarking can thus be extended to video watermarking by embedding data in single frames. In order to minimize the color distortion in the watermarked video, the Y component of the YUV color space isused for the data embedding process. Embedding the watermark into the U and the V components may result in undesirable color distortions. As enlightened by [10] and [11], we can use the similar data hiding method for video. The Y component of MPEG-2 intraframes (I frames) is used to embed the watermark signal. Fig. 1 outlines the embedding process. In order to avoid strong reduction of the video quality, due to concatenation of MPEG-2 coding, the embedding stage is not carried out on the fully decompressed data. Only data extracted directly from the compressed stream is used. The complete data hiding process is outlined in the sequel. First, the candidate I frame for data hiding is extracted. Then the Variable Length Code (VLC) of the intracoded block is obtained. The VLC of AC components of the selected block is decoded to get the quantized values which are integer numbers. The watermark is embedded in these AC components by applying the following modulation rule:

To embed the bit '1', the value of the selected AC component is changed to the nearest even number. To embed bit '0', the value of the selected AC component is changed to the nearest odd number. Finally, the modulated AC component is encoded back using variable-length coding as shown in Fig. 2.



NB: VLC=variable-length coder ,VLD =variable-length decoder .The grey parts above are not used during hiding data.

Fig. 1: Embedding information in I frames of the MPEG-2 compressed video

Since embedding the same amount of data in different I frames (or in different macroblocks of the same I frame) has different effect on the introduced distirtion, adaptive masking is applied. Frames in the Group of Pictures (GOP) which the largest motion entropy are skipped. P an B macroblocks within a I frame are also sensitive to distortions. If the number of motion vectors is larger than a threshold N1, the number of macro types B and P are larger than a threshold N2 and the quantization coefficient is larger than a parameter K1, then the I frame within the GOP will not be used to embed data. The parameters N1, N2 and K1 are set experimentally. Once the candidate blocks of the I frame are selected, they are classified by calculating the energy of their DCT coefficients. This process is carried out using the following template according to the frequency distribution:

d d h h h . . . E*h* = horizontal energy summed over h elements
d d h h h . . . . E*d* = diagonal energy summed over d elements
v v d d . . . . E*v* = vertical energy summed over *v* elements
v v d d . . . . E*a* = average high frequency energy
v v . . . . . . E*m* = minimum value of E*h* ,E*d* ,E*v*
. . . . E*M* = maximum value of E*h* ,E*d* ,E*v*
. . . . E*m/M* = ratio between E*m* and E*M*
. . . .

d, h and v refer to the diagonal, horizontal and vertical terms, respectively. Since E*a* represents the average high frequency energy of a block, it is used to segment the blocks into low activity and high-activity blocks. High-activity blocks are further classified according to their texture and edgeness using E*m* and E*m/M.*

This classification is performed as follows:

- Uniform block: E*a* <T1
- Textured block: E*a* ≥T1 and E*m* ≥T2 and E*m/M* >T3

T1, T2 and T3 are parameter determined experimentally.

IV. CONCEPT OF STEGNOGRAPH

A. Requirement of Steganography

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of Requirements so that steganography can be applied correctly .

The following is a list of requirements that steganography techniques must satisfy.

1. The integrity of hidden information after it has been embedded inside the Stegano object must be correct. The secret message must not be changed in any way such as additional information being added, loss of information or changes to the Information after it has been hidden. If secret Information is changed during steganography, it would defeat the whole point of process.
2. The Stegano object must remain unchanged or almost unchanged to the naked eye. If the Stegano object changes significantly and can be noticed, a third party may see that information is being hidden and therefore could attempt to extract or destroy it.
3. Steganography Changes in the Stegano object must have no effect on the message. 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 Stegano inside the image must survive these manipulations.

4. Otherwise the attackers can be very easily removing the Stegano and point of steganography will be broken.
5. Finally, we always assume that the attacker knows that there is hidden information inside the steno object.

B. Techniques of Steganography

There are many techniques for hiding information or messages in images. Common approaches are including.

1) Least significant bit insertion (LSB)

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least Significant bit does not result in human perceptible difference because the amplitude of the change is small.

2) Masking and filtering

Masking and filtering techniques**,** usually restricted to 24 bits and gray scale images, hide information by masking an image in a manner similar to paper watermarks. The techniques Performs analysis of the image, thus embed the Information in significant areas so that the hidden message is more integral to the cover image than Just hiding it in the noise level.

3) Transform techniques

Transform techniques embed the message by modulating coefficients in a transform domain, Such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or Other variants.

V. DATA HIDING TECHNIQUE

The following figure shows data hiding technique in Compressed video. The input video is separated into frames. Then the frames are subjected to DCT and Huffman Coding to compress the frame. Using the secret key and LSB Algorithm data is inserted. This generated video is stego video. The secret data can be extracted using inverse LSB and secret Key.

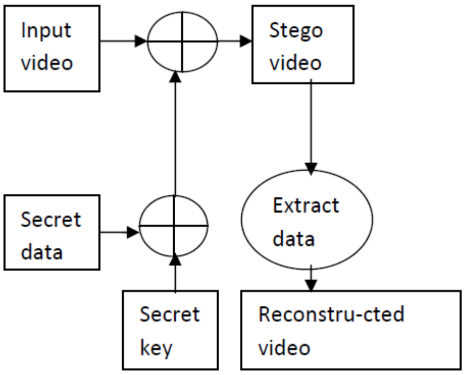


FIGURE 1.Data hiding technique

A. LSB algorithm

Embedding message is performed for two pixels *X* and *Y* of a cover image at a time and then adjusting one pixel of the (*X*, *Y*) to embed two secret bits message *s1 s2*. The embedding flowchart is shown in Fig.2 and the embedding procedure is described as following:

Step 1. If the LSB of *X* is the same as *s1*, go to step 2.Otherwise, go to step 3.

Step 2. If the value of *f* (*X*, *Y)* is the same as *s2*, do not change any pixel. Otherwise, the value of pixel *Y* is increased or decreased by 1.

Step 3. If the value of *f* (*X* −1, *Y) is* the same as *s2*, the value of pixel *X* is decreased by 1. Otherwise, the value of pixel *X* is increased by 1.Where the function *f*(*X*, *Y*) is defined as since this new LSB matching method just only increase or Decrease 1 in two adjacent pixels, the difference of the two neighbourhood pixel between cover image and stego-image is very small. Hence, it can keep high quality while hiding data.

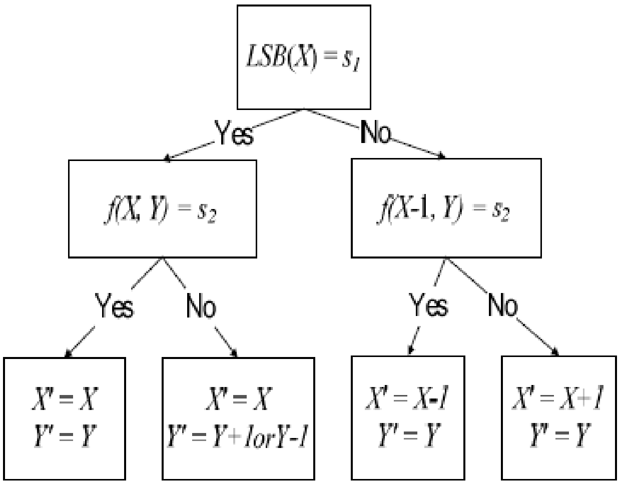


FIGURE 2: The LSB matching embedding procedure.

B. Data hiding algorithm

```
Input: Video
Output: Stego video
Step 1: Read the input Video
Step 2: Perform frame seperation
Step 3: Apply Integer DCT on each 8×8 block.
Step 4: Perform Zigzag Scanning on each 8×8
block.
Step 5: Apply Huffman coding to compress the frame.
Step 6: Apply secret key to hide the data.
Step 7: Apply LSB Algorithm to embed data
Step 8: Generate Stego video
```

C. Data Extraction algorithm

```
Input: Stego video
Output: Hidden data
Step 1: Read Stego video.
Step 2: Perform decoding using IDCT and Inverse
Step 3: Extract hidden data using ILSB and Secret Key.
Huffman coding.
```

D. Secret key generation algorithm

```
Step 1: Take a key which is a prime number
Step2: Generate two prime numbers p, q
Nearer to given key.
Step3: Calculate n=p*q;
Step 4: Calculate m= (p-1)(q-1).
Step 5: Generate e
Assume e=1; x=1;
While (mod(m,e)==0)
e = e+1;
Step 6: Generate d
Take s=1+x*m;
While (mod(s,e) ~= 0)
x = x+1;
s=1+x*m;
d=s/e;
```

VI. Experimental Work and Results

MPEG is the most popular video compression standard, several experiments have been conducted to validate the proposed approach. In these experiment the watermark is embedded in the mid-frequencies bands of compressed video sequences. The watermark remains detectable even when the video undergoes compression ratios at which the host signal is significantly degraded. Since very person has a different visual sensitivity threshold, it is hard to give theoretical limits. The performed experiments show that even the ‘perfect eyes' cannot detect the watermark in a movie unless they do a frame by frame assessment using the original sequences to find the difference.

VII. CONCLUSION AND FUTURE WORK

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. In this paper we give an idea to enhance the security of system by combining the two techniques. It can enhance confidentiality of information and provides a means of communicating privately. Here message is first encrypted and then embed in cover file with help of steganographic system. LSB algorithm is applicable for all kind of cover medium (image, audio, video).LSB algorithm is used for both embedding and extraction process. There are infinite number of steganography applications for digital image including copyright protection, feature tagging, and secret communication. This paper explores a tiny fraction of the art of steganography. The steganography method may be further secured if we compress the secret message first and then encrypt it and then finally embed inside the cover file.

The method is compared to another one from the literature that relies on a motion vector attribute. The proposed method is found to have lower distortion to the quality of the video and lower data size increase. Future work will be directed towards increasing the size of the embedded payload while maintaining the robustness and low distortions.

REFRENCES

[1] Ms. Monika S. Shirbhate, “Hiding Secrete Data in Video File ” Vol. 6, No.2, Apr 2013 ISSN: 0974-1011.

[2] D.-Y. Fang and L.-W. Chang, “Data hiding for digital video with phase of motion vector,” in *Proc. Int. Symp. Circuits and Systems (ISCAS)*,2006, pp. 1422–1425.

[3] Generic Coding of Moving Pictures and Associated Audio, ISO/IEC 13818 (MPEG-2 standard), 1994.

[4] S. Suma Christal Mary, “Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ,” International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397

[5] T. Sravanthi,”An Adaptive Algorithm for video compression” ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue 12, December 2012

[6] Saurabh Singh and Gaurav Agarwal,”Hiding image to video: A new approach of LSB replacement”, International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

[7] Steganography on new generation of mobile phones with image and video

processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244- 7432-5.

[8] Advanced Steganography Algorithm usingencrypted secret message, Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Application (IJACSA) Vol-2 No.3, Page19-24,March(2011).

[9] J. Zollner, H. Federrath, H. Klimant,et al.,“Modeling the Security of Systems”, Steganographic in 2nd Workshop on Informafion Hiding, Portland, April 1998, pp. 345-355. proceeding of IEEE, pp. 1062-1078, July19