STEGANOGRAPHY IN COMPRESSED VIDEO STREAM

Kartik Rai, Ayush Sharma, Mohit Tanwar
Student, Dronacharya College Of Engineering, Gurgaon

Abstract: Steganography is the art of hiding information in ways that avert the revealing of hiding messages. In this paper, a steganographic algorithm in MPEG compressed video stream was proposed. Data extraction was also performed in compressed video stream without requiring original video. On a GOP by GOP basis, control information in I frame should be extracted firstly, then the embedded data in P and B frames can be extracted based on the control information. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, a novel steganographic approach called tri-way pixel-value differencing (TPVD) is used for embedding.

Index Term: architecture, Adaptive Rules to Reduce Distortion, the extraction algorithm, Embedding

INTRODUCTION

Steganography is the art of hiding information in ways that prevent the detection of hiding message whereas cryptographic techniques try to conceal the contents of a message. In steganography, the object of communication is the hidden message and the cover data are only the means of sending it. Secret information as well as cover data can be any multimedia data like text, image, audio, video etc. The former is mainly used for copyright protection of electronic products, while steganography, as a new way of covert communication, as a new way of covert communication, the main purpose is to convey data secretly by concealing the very existence of communication. Data embedding in videos seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media. Since videos contain more sample number of pixels or the number of transform domain coefficients, a video has higher capacity than a still image and more data can be embedded in the video. Also, there are some characteristics in videos which cannot be found in images as perceptual redundancy in videos is due to their temporal features. Here data hiding operations are executed entirely in the compressed domain. On the other hand, when really higher amount of data must be embedded in the case of video sequences, there is a more demanding constraint on real-time effectiveness of the system. The method utilizes the characteristic of the human vision’s sensitivity to color value variations. The aim is to offer safe exchange of color stego video across the internet that is resistant to all the steganalysis methods like statistical and visual analysis. Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later. The other, which is more difficult, tries to embed data directly in compressed video stream. The problem of the former is how to make the embedded message resist video compression. But because the video basically exists in the format of compression, the research of the latter is more significative. A steganography algorithm for compressed video is introduced in this paper, operating directly in compressed bit stream. In a GOP, control information is embedded in I frame, and in P frames and B frames, the data are repeatedly embedded in motion vectors of macro-blocks, for the purpose of resisting video processing.

Architecture

A steganographic algorithm for compressed video is introduced here, operating directly in compressed bit stream. In a GOP, secret data’s are embedded in I frame, and in P frames and in B frames. This proposed secure compressed video Steganographic architecture taking account of video statistical invisibility.
1. For each P and B frames, motion vectors are extracted from the bitstream.

2. The magnitude of each motion vector is calculated as follows:

\[ |MV_j| = (H_j^2 + V_j^2)^{1/2} \]

where \( MV_j \) the motion vector of the jth macroblock, and \( H_i \) is horizontal and \( V_j \) is the vertical components of the MV respectively.

3. This magnitude is compared with a threshold

4. Select the block with maximum magnitude and embed the data using PVD method

Adaptive Rules to Reduce Distortion

Although the proposed approach is feasible for embedding secret data, embedding large amount of bits can still cause serious image distortion easily. Since most distortion is generated from the offsetting process, the following two conditions are further designed to avoid too much offset described by

1) embed_bit(P0) ≥5 and 1 embed_bit(P1) ≥4
2) embed_bit(P0) < 5 and 2 embed_bit(P0) ≥6

Where embed_bit(Pi) represents the total embedding bits along the direction of Pi. If either one of above two conditions is satisfied, the current block being processed can probably result in higher distortion. Then we use two pixel pairs, P0 and P3\( = P(x,y+1), P(x+1,y+1) \) and adopt the original PVD method to individually process those two pairs along one direction. If neither of the conditions is satisfied then PVD is applied to three pixel pairs P0, P1 and P2 in three directions. Here, we name those two conditions as “branch conditions”.

The Extraction Algorithm

To retrieve the embedded secret data from the stego-image, the extraction algorithm is described in the following steps.

1) Partition the stego-image into 2x2 pixel blocks, and the partition order is the same as that in the embedding stage.

2) Calculate four difference values \( d^*(i,x,y) \) for four pixel pairs in each block given by

\[ d^*0,(x,y) = P(x+1,y) - P(x,y) \]
\[ d^*1,(x,y) = P(x,y+1) - P(x,y) \]
\[ d^*2,(x,y) = P(x+1,y+1) - P(x,y) \]
\[ d^*3,(x,y) = P(x+1,y+1) - P(x,y+1) \]

3) Using \( |d^*(i,x,y)| \) (i=0,1,2,3) locate a suitable Rk.i. Also find the number of bits ti that was embedded. If ti satisfies the branch conditions, two independent pixel pairs are selected. Otherwise, three pixel pairs are used for further processing.

4) The secret message \( b^* \) is to calculate for stegoimage is not altered \( b^* \) is same as \( b \). Finally \( b^* \) is converted to binary to obtain the original secret message.

Embedding control information in I frame

I frame is the first frame in a GOP, data hiding in I frame is to facilitate the extraction of embedded data. The data that need to be actually transmitted were embedded in P frames and B frames, and the embedding is fulfilled by a slight modification to motion vectors. Furthermore, redundant embedding is adopted to increase the algorithm’ security. So control information includes the embedding capacity of the GOP, the position of the start and the end of each segment after dividing the GOP, to the data that embedded in P frames and B frames, the amount of control information is relatively small, but is critical and should be extracted accurately. Consequently, higher robustness is required. I frame is compressed using intra-frame DCT encoding, the algorithm is similar to JPEG, so data embedding in I frame is similar to the algorithm for still images. We embed the information in middle frequency of quantized DCT coefficients, for the sake of obtaining the tradeoff between imperceptibility and robustness. Firstly we should get the quantized DCT coefficients, which can be achieved by variable length decoding after the minimal parsing of the video stream. Then we embed control information into quantized DCT coefficients. The embedding is realized by modifying the least significant bits of quantized DCT coefficients[7]. The modified coefficients are variable length encoded and placed back into bit stream to form embedded bit stream of I frame.

CONCLUSIONS:

A new Video Steganographic Scheme was proposed in this paper, operating directly in compressed domain. For data hiding tri-way pixel-value differencing (TPVD) algorithm has been used. This algorithm provides high capacity and imperceptible stego-image for human vision.
of the hidden secret information. Here I frame with maximum scene change blocks were used for embedding. The performance of the steganographic algorithm is studied and experimental results shows that this scheme can be applied on compressed videos with no noticeable degradation in visual quality.

REFERENCES:


