IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Information Hiding Based On Message Prediction inMPEG VideoFiles

[1]K.Jayanthi and [2]R.Shankar

[1]Department of Computer Science and Engineering,
Anna university, Indira Institute of Engineering and Technology, Chennai, TamilNadu, India.
[2]Associate professor, HOD / CSE
Department of Computer Science and Engineering, Anna university,
Indira Institute of Engineering and Technology, Chennai, TamilNadu, India.

Abstract

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copyright protection, access control and transaction tracking. Some data hiding techniques to assess the quality of compressed video in the absence Of the original reference. The existing solution rely on hiding message bits in discrete cosine transform (DCT) coefficients, motion vectors(MV), quantization scale or prediction modes. Data hiding using DCT coefficients include the use of the parity of the quantized coefficients to hide a message. They utilized Zero-length codes to insert a dummy value at certain locations to indicate message bits. In this paper two data hiding approaches using compressed MPEG Video. The first approach the quantization scale of a CBR video is either incremented and decremented according to the underlying message bit. A second-order multivariate regression is used to associate macro block level features with the hidden message bit. However, the message payload is restricted to one bit per macro block. The second approach proposed in this paper work for both the CBR and VBR coding and achieves a message payload of 3 bits per macro block. The FMO was used to allocate macro blocks to slice groups according to the content of the message. Apart from the advantage of increase message payload, excessive bit rate and quality distortion the proposed solution overcome the packet loss and provide security to the hidden message in MPEG Video.

Key words—*Data hiding,flexible macroblock ordering,MPEG coding, multivariate regression,packet loss.*

1.Introduction

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copyright protection, access control and transaction tracking. Some data hiding techniques to assess the quality of compressed video in the absence Of the original reference. The existing solution rely on hiding message bits in discrete cosine transform (DCT) coefficients, motion vectors(MV), quantization scale or prediction modes. Data hiding using DCT coefficients include the use of the parity of the quantized coefficients to hide a message. They utilized Zero-length codes to insert a dummy value at certain locations to indicate message bits. In this paper two data hiding approaches using compressed MPEG Video. The first approach the quantization scale of a CBR video is either incremented and decremented according to the underlying message bit. A second-order multivariate regression is used to associate macro block level features with the hidden message bit. However, the message payload is restricted to one bit per macro block. The second approach proposed in this paper work for both the CBR and VBR coding and achieves a message payload of 3 bits per macro block. The FMO was used to allocate macro blocks to slice groups according to the content of the message. Apart from the advantage of increase message payload, excessive bit rateand quality distortion the proposed solution overcome the packet loss and provide security to the hidden message in MPEG Video.

The Internet and the world wide web have revolutionized the way in which digital data is distributed. The wide spread and easy access to

multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Much of the recent work in data hiding is about copyright protection of multimedia data. This is also referred to as digital watermarking. Such data hiding techniques can also be used for other purposes. In general the existing solutions rely on hiding message bits in discrete cosine transform (DCT) coefficients, motion vectors (MVs), quantization scale or prediction modes.

Examples of data hiding using DCT coefficients include the use the parity of the quantized coefficients to hide a message. Additionally zero-length codes to insert a dummy value at certain locations to indicate message bits. Examples of using MVs for data hiding include, where phase angles of MVs are used to hide messages. The quantization scale is also used for data hiding a recent publication in proposed to divide the quantization scale of a macro block by a certain factor.

the presence of hidden message in multimedia. Steganalysis can be applied to digital images and to digital video. The use of intraprediction modes to hide message bits. It was shown that one bit can be hidden in each candidate 4×4 intra block.The quality is estimated based on computing the degradation of the extracted hidden message. A new method of data hiding based on H.264 encoded video sequences system used the DCT coefficients which include the parity of the quantized coefficients to hide a message.

The existing solution rely on the two data hiding techniques to hide the data in the MPEG video files. The two data hiding techniques are the quantization scale modulation and the flexible macro block ordering. In the existing system the message bits are hidden directly into the video, so the packet loss occurs. In this paper by using the same algorithm quantization scale modulation and the flexible macro block ordering efficiently the packet loss can be overcome. The packet loss creates loss of message bits so that data cannot be retrieved properly. It creates big drawback in the process of hiding message bits in the Moving picture experts group (MPEG) video file.

The proposed system has consists of two hiding techniques for hiding data in MPEG Video files. The first technique is the Quantization scale modulation and the second technique is the Flexible Macro block ordering. The first technique is the quantization scale of a CBR Video is either incremented or decremented according to the underlying message bit. A second-order multivariate regression is used to associate macro block level features with the hidden message bit. However, the message payload is restricted to one bit per macro block. The second technique proposed in this project work for both the CBR and VBR coding and achieves a message payload of three bits per macro block. The Flexible Macro block ordering was used to allocate macro blocks to slice groups according to the content of the message. In this proposed system the splitting up of MPEG video files takes place. The MPEG video files are separated into the video files and the audio files. From the video file the image is separated and from the image the chunks are separated. In the chunks only the process of hiding the data takes place these methods are done in the encoding side. And while in the decoding part again the separation of the video and audio files takes place and from the particular chunk the hidden data is extracted by using the same methodology which has been done in encoding part.

The proposed system has the advantage of the high message payload, less video distortion and excessive overhead. The methods used in proposed system are very efficient in hiding data and extracting the data. Apart from the advantage of increase message payload, excessive bit rate and quality distortion the proposed solution overcome the packet loss in MPEG Video.

In the existing system the message bits are hidden directly into the video, so the packet loss occurs but in the proposed system the packet loss has been overcome by slicing the video and audio then splitting the video into frame and images. Then the message bits are hidden in the chunks of the image. By doing

This paper is organized as follows. Section II introduces message hiding using quantization scale modulation and multivariate regression. Section III introduces message hiding using FMO. Experimental results and comparisons with existing work are reported in Section IV. Lastly, Section V concludes the paper.

2. Message hiding using Quantizationscale Modulation

To hide a message using quantization scale modulation, the message is first converted into a binary stream of bits. During the MPEG encoding of individual macroblocks, the message bits are read one at a time. For each coded macroblock, the quantization scale is either incremented or decremented based on the corresponding message bit.

Clearly, if the original quantization scale was either the lowest or largest allowable values then no modification is applied. This simple process of hiding a message bit in a macroblock is illustrated in Fig. 1.Although the message hiding procedure is straightforward, nonetheless, the question that remains is how to extract the message from the bitstream.

This problem can be solved by extracting macroblock-levelfeature variables during the encoding process. Once the whole message is hidden we end up with a fea-ture matrix and a message vector. We will then treat the feature matrix as predictors and the message bits as a response variable and use multivariate regression to compute a prediction model. Once computed, the prediction model can be used to predict the message bit hidden in a given macro block based on its feature variables. In Sections 3-5 we elaborate on the extraction of macroblock features from an MPEG -2 video, consequently, we formulate the message extraction as a regression problem.

2.1. Macroblock Level Features Variables

The following feature variables are extracted or computed from a MPEG-2 video stream for each coded macroblock.The first feature is the virtual buffer discrepancy from uniform distribution model. This discrepancy is computed

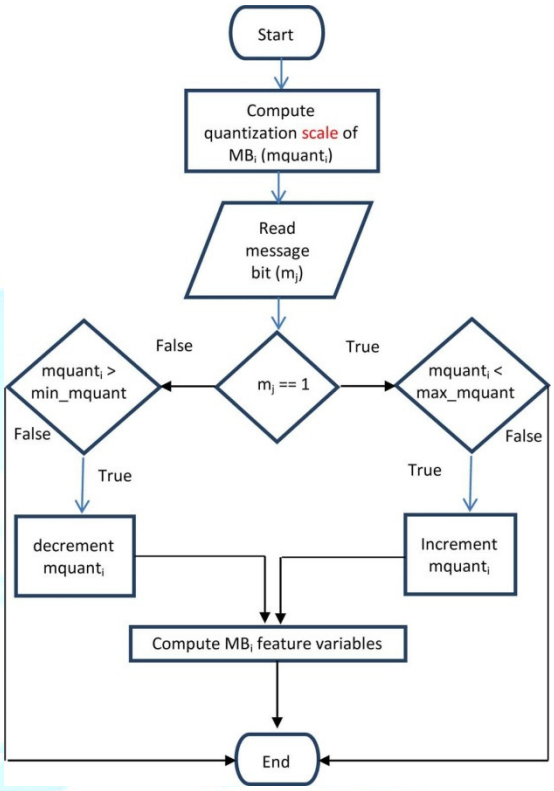


Fig. 1 Message insertion flowchart for one macro block.

For completeness, an example of message hiding using the proposed approach follows. A message is generated and a video sequence is encoded while hiding the message bits. Two consecutive message bits are values 1 and 0. These bits are hidden into two consecutive MBs, say MB*i*and MB*i*+1.In this example, the quantization scale of the first MB is incremented by one to become nine and the quantization scale of the second MB is decremented by one to become five. The encoder stores the feature variables of the two MBs with the values shown in Table 1.

Table 1
Example macroblock-level feature variables

Feature	MB i	MB i+1
Buffer occupancy	9.903725	0.580925
MB spatial activity	0.741272	9.870142
Quantization scale	9	5

In general, during the encoding process, the encoder stores the feature variables for all MBs, expands them to the second order as described and computes the model weights as described. The model weights for this particular example and the expanded feature vectors of MB_i and MB_{i+1} are shown in Table 2.

Table 2
Example model weights and expanded feature vectors

Model weights	Feature vector of MB i	Feature vector of MB i+1
0.8560	1	1
-219.1380	0.741272	0.580925
-219.5450	9.903725	9.870142
-219.1190	9	5
-0.4380	0.549484	0.337474
0.3030	98..08377	97.4197
-0.3190	81	25
219.4780	19.645	15.45107
186.2050	385.9259	238.7355
-186.3590	14.56229	8.975911
186.5070	194.5586	152.5042
185.8970	176.805	77.25534

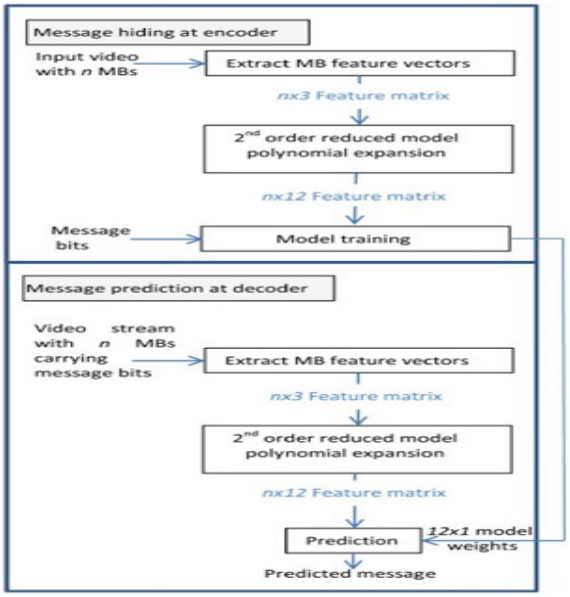


Fig. 2 Block diagram of message hiding and prediction.

To decode the message, the decoder computes the feature variables of the MBs from the encoded bitstream, expands them to the second order and uses the model weights to predict the message bits. The predicted message bits for the above example are 0.77 and 0.061. With rounding, the predicted bits become 1 and 0, respectively.

It is worth mentioning that one of the reasons for the success of this solution is that the set of feature vectors used at the en-coder to generate the model weights is replicated at the decoder. exception is the macroblock activity feature variable as explained previously. Therefore, the decoder uses the same model weights and very similar feature vectors to predict the hidden message bits. This results in high prediction accuracy as shall be elaborated upon in the experimental results section.

Lastly, it is worth pointing out that message hiding using this proposed solution can be extended to allow the encoder to hide message bits in selective macroblocks. This is possible if the message extraction process is modified to predict the

quantization scale at the decoder. For a given macro block, if the predicted quantization scale is the same as the one received in the bitstream, then no bits are hidden in that particular macroblock. On the other hand, in typical techniques that use the least sig-nificant bits of DCT coefficients to hide message bits, such a selective approach cannot be implemented.

3. Message hiding using flexible macroblockordering (FMO)

One of the limitations of the quantization scale modulation solution of the previous section is related to the message payload where only one message bit can be hidden per macroblock. This section introduces a second solution that benefits from a higher message bitrate through the use of FMO of the H.264/AVC video coding standard.

In general, a coded picture is divided into one or more slices. Slices are self-contained and can be decoded and displayed in-dependently of other slices. Hence, intraprediction of DCT co-efficients and coding parameters of a macroblock is restricted to previous macroblocks within the same slice. This feature is important to suppress error propagation within a picture due to the nature of variable length coding. In regular encoding, when FMO is not used, slices contain a sequence of macroblocks in raster scan order. However, FMO allows the encoder to create what is known as slice groups. Each slice group contains one or more slices and macroblocks can be assigned in any order to these slices. The assignment of macroblocks to different groups is signaled by a syntax structure called the “slice group id”. This syntax structure is available in the picture parameter set header and therefore can be altered on picture basis. Notice that the H.264/AVC standard allows for a maximum of eight slice groups per picture. The idea behind the use of FMO in H.264/AVC is to spread the errors caused by burst packet losses to a larger portion of the picture. As such, error concealment becomes easier and more effective. There are a number of predefined slice group types in H.264/AVC that are designed for that purpose. Examples include interleaved slice groups, dispersed slice groups, fore-ground/background slice groups, box-out and wipe slice groups . The H.264/AVC standard also allows for a sixth type for the explicit assignment of macro blocks to slice groups.

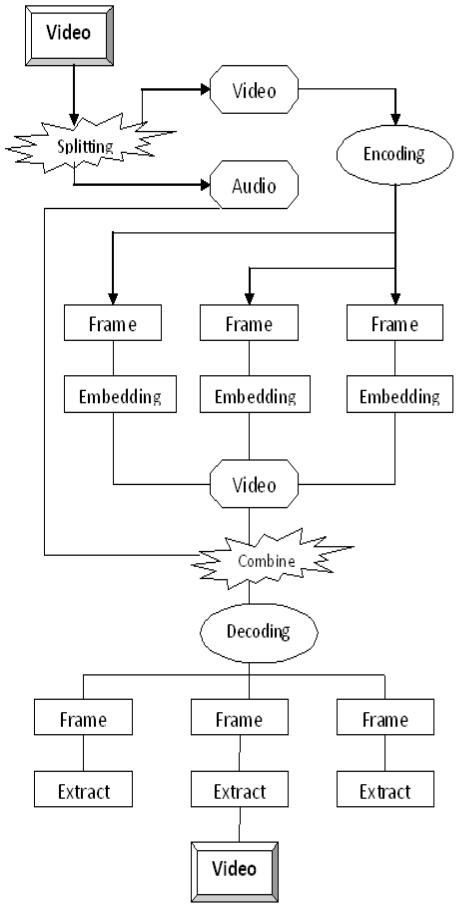
Although FMO was devised for enhancing error resiliency and concealment, nonetheless it has been used for other purposes as well. For instance, proposed the use of FMO to aid video scrambling for privacy protection. FMO has also been used to enhance the efficiency of video transcoding.

In this paper, we make use of the explicit assignment of mac-roblocks to slice groups to hide messages in the video stream. Since macroblocks can be arbitrary assigned to slice groups, we propose to use the slice group ID of individual macroblocks as an indication of message bits. Assume for instance that two slice groups are used, the allocation of a macroblock to slice group 0 indicates a message bit of 0 and the allocation of macroblock to slice group 1 indicates a message bit of 1. Hence, one message bit per macroblock can be carried. Furthermore, since the H.264/AVC standard allows for a maximum of eight slice groups per picture then two or three message bits can be carried per macro block.

Clearly, one can think of other arrangements for assigning message bits to macroblocks. Examples might use eight slice groups yet use a subset of them for data hiding. For instance, one can use slice groups 2 and 5 to indicate a message bit of 0 and slice group 3 and 7 to indicate a message bit of 1. In general, what can be varied is the size of the subset of slice groups that are used to hide information, the message bit values hidden in these slices groups and the order in which message bits are assigned to slice groups. All of these permu-tations can even be altered per frame.Such scenarios indicate that the permutations for message hiding using this approach are very large. In general, to hide a message into the H.264/AVC bit stream, the message is first read into chunks of n bits, where n is either 1, 2, or 3. If m macroblocks are coded per picture, then $m \times n$ message bits can be used to allocate the macroblocks to slice groups. The process of message hiding is illustrated in Fig. 3.

To extract the message bits, each time a picture is decoded, the macroblock to slice group mapping syntax structure is used to read $m \times n$ message bits and append them to the extracted message.

Fig.3. Architecture of data hiding in MPEG Video files



The architecture of this paper Fig. 3.illustrates that the MPEG Video is splitting into video and video. The audio is kept aside without disturbing it. Then the video is encoded by separating the video into frames and embedding message bits and after embedding the embedded video is combined with the audio and sended to the receiver. The receiver decode the embedded video to extract the hidden message bits. The decoding process involves in the separation of embedded video into frames, from the frames the hidden data's are extracted. Finally the video is recombine.

The main aim of this paper is to overcome the packet loss in the video file. The packet loss has been overcome by using the quantization scale modulation and flexible macro block ordering in an efficient manner. In the existing solution the direct hiding of the data into the mpeg video files makes packet loss. Now in the proposed system the MPEG video file is split into video and audio. From the video the images are separated and from images the chunks are separated. So that the hiding process become effective and thus packet loss can be prevented.

3.1 Advantages and Disadvantages of Proposed FMO Solution

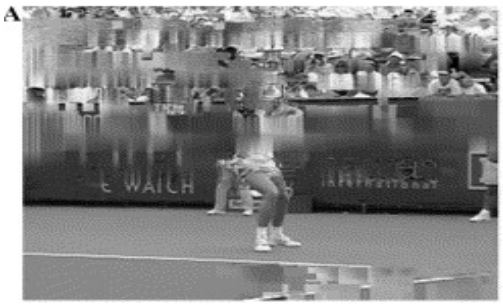
The proposed approach has a number of advantages. It is simple and it is fully compliant with the H.264/AVC syntax using the baseline or the extended AVC profiles. Another advantage is that message hiding works for both coded and skipped macroblocks. The proposed solution also works independent of picture type being I (intra), P (predicted) or B (bidirectionally predicted).
In terms of message hiding capacity, if three message bits are hidden per macroblock, a message payload of 35.64 Kb/s message payload of 121.5 Kb/s is achieved at a 720 × 480, 30 Hz video resolution. Apart from the above mentioned advantages of the FMO User cannot find the original data.It is not easily cracked. It increase the Security. It increase the size of stored data. We can hide more than one bit.

4. Experimental results

This section reports the experimental results of the proposed message hiding solutions and compares them to existing. In the existing the data hiding process with high message payload is done. Now in the proposed system the Flexible Macro Block Ordering technique is efficiently used to overcome the packet loss in the MPEG video files. The loss of packet has been overcome by splitting up the selected video rather than directly hiding the data into to the MPEG video files. After the splitting up of the mpeg video files the audio has been kept aside without any disturbance to the audio, the video is again splitted into the frames and from the frames the images are separated and finally the chunks are obtained. The message bits which has to be hide is placed in the chunk. The reverse process is done to extract the

hidden message bits. By doing like this the message bits cannot be loss.

Fig .4. 5% packet loss, no B slices, high quality.



No FMO

FMO

The above given two pictures illustrates that how the packet loss is overcome by using FMO and without using FMO. In the picture A there are more packet loss since FMO was not used there. But in the picture B the packet loss is considerably reduced by using the FMO. This proves that by using FMO efficiently the packet loss can be overcome.

5. Conclusion

This paper used the quantization scale modulation and flexible macro block ordering to increase the message payload by 3 bits per macro block and to provide less video distortion. Apart from these achievements by efficiently using the flexible macro block ordering the packet loss can be overcome by separating the mpeg video into audio and video. Further video has been separated into frames and images. Finally, the message bits are hidden in the chunk. In the existing the message bits are hidden directly to the video but in the proposed solution the message bits are hidden in the chunk of the mpeg video files so that the packet loss is considerably reduced. Future work includes the work against channel bit errors.

References

[1] S. Kapotas and A. Skodras, "A new data hiding scheme for scene change detection in H.264 encoded video sequences," in *Proc. IEEEInt. Conf. Multimedia Expo ICME*, Jun. 2008, pp. 277–280.

[2] A. Yilmaz and A. Aydin, "Error detection and concealment for video transmission using information hiding," *Signal Processing: ImageCommunication*, vol. 23, no. 4, pp. 298–312, Apr. 2008.

[3] Tamer Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macro block ordering"IEEE*Transactions on information forensics ans security, vol.*7,no.2,april 2012.

[4] Y. Li, H.-X. Chen, and Y. Zhao, "A new method of data hiding based on H.264 encoded video sequences," in *Proc. IEEE Int. Conf. SignalProcessing, ICSP*, Oct. 2010, pp. 1833–1836.

[5] K. Nakajima, K. Tanaka, T. Matsuoka, and Y. Nakajima, "Rewritable data embedding on MPEG coded data domain," in *Proc. IEEE Int.Conf. Multimedia and Expo, ICME*, Jul. 2005, pp. 682–685.

[6] D.-Y. Fang and L.-W. Chang, "Data hiding for digital video with phase of motion vector," in *Proc. IEEE Int. Symp. Circuits Systems, ISCAS*, Sep. 2006.

[7] C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in *Proc. Int. Conf. Innovative Computing, Information andControl, ICICIC'06*, 2006, vol. II, pp. 803–806.

[8] H. A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error," *IEEE Trans. Inform. ForensicsSecurity*, vol. 6, no. 1, pp. 14–18, Mar. 2011.

[9] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 19, no. 10, Oct. 2009. Y. Hu, C. Zhang, and Y. Su, "Information hiding based on intra pre-diction modes H.264/AVC," in *Proc. IEEE Int. Conf. Multimedia andExpo, ICME*, Jul. 2007, pp. 1231–1234.