Stegnography in video files using Multivariate Regression and Flexible Macroblock Ordering

Anila Chandran

Abstract: *Data hiding is the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer. Data hiding consists of two sets of data, namely the cover medium and the embedding data, which is called the message. In general, there are two types of data hiding for video: one that hides the video content itself (video encryption or scrambling) so that nobody understands what is being transmitted; the other that embeds external information into the video, hence utilizing video as the data host. This paper proposes two data hiding approaches in compressed MPEG video. In the first approach, the quantization scale of a Constant Bit Rate (CBR) video is either incremented or decremented according to the underlying message bit that is to hidden. A second-order multivariate regression is used to associate the macroblock-level features with the hidden message bit. The decoder makes use of this regression model to predict the message bits. However, the message payload is restricted to one bit per macroblock. The second approach of our work is for both constant bit rate and variable bit rate (VBR) coding and it achieves a message payload of three bits per macroblock. The Flexible Macroblock Ordering (FMO) was used to allocate macroblocks to slice groups according to the content of the message bits. In existing network delivery of compressed video, information may be lost if there is the presence of errors or due to attacks. Such losses tend to occur in burst. Thus we can enhance our work to robustness of the existing work against information losses in video steganalysis methods. In this work, we develop an error resilient video encoding approach to help error concealment at the decoder. The existing solutions are very superior in terms of message payload while causing less distortion and compression overhead and the proposed solution reduces the color information losses and thus we can reconstruct the high quality video itself.*

IndexTerms: *Data hiding, flexible macroblock ordering, MPEG coding, multivariate regression, steganography.*

I. Introduction

Data hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academia. It contains two main branches: digital watermarking and stegnography. The former one is mainly used for copyright protection of electronic products, while stegnography, is a new way for sealed communication,its main purpose is to convey data secretly by concealing the very existence of communication. It is the process of hiding and transmitting data through carriers in an effort to hide the existence of the data. The main goal of stegnography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'. They are used for secure secret communication between two parties.

Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer. This technique consists of two sets of data, namely the cover medium and the embedding data, which is called the message. The digital medium or the message can be text, audio, picture or video depending on the size of the message. Although digital video has become a popular multimedia content for both online and offline environments. It is important to consider ways to protect the contents from malicious use, efficient ways to search the desired contents in the database. In general, there are two types of data hiding for video: one that hides the video content itself (video encryption or scrambling) so that nobody understands what is being transmitted and the other that embeds external information into the video, hence utilizing video as the data host. These data hiding techniques are used to embed a secret message for copy-right protection, access control ,content annotation and transcation tracking. The authors of [1] used data hiding methods to assess the quality of compressed video in the absence of host video. Here the quality of the video is obtained based on computing the degradations of the extracted hidden message. Data hiding methods are also used for detecting errors and concealment during video transmission.For that purpose, edge orientation information and number of bits of a block are hidden [2]. To enable real time scene change detection in compressed video,the authors of [3] used data hiding techniques. The information is hidden using the motion compensation block sizes of an H.264/AVC video. Early video data hiding techniques extended to video by hiding the message in each frame independently [4]. Methods such as spread spectrum are used, where the basic idea is to distribute the message over a wide range of frequencies of the host data.Transform domain is generally preferred for hiding data in the videos.

Traditionally, the message bits are hidden in discrete cosine transform (DCT) coefficients, motion vectors (MVs), quantization scale or prediction modes.

Examples of data hiding using DCT coefficients to hide messages include the use the parity of the quantized coefficients.[5]. The authors of [6] used the phase angles of motion vectors for the purpose of data hiding. The work in [7] proposed solutions for using magnitude of motion vectors for data hiding.In this the least significant bit of both components of candidate motion vectors to embed a secret message. The candidate motion vectors are selected based on the prediction error of the underlying macroblock. The motion vectors with high prediction errors are chosen. The prediction error threshold is computed per frame and transmitted in the video bit stream to guide the decoder in recognizing the MVs that carry bits of the secret message. Therefore in the above scenario video is providing the protection for the message from the third party users or simply the hackers. Data hiding based on the quantization scale is also possible [8]. The quantization scale method proposes by dividing the quantization scale of a macroblock by a certain factor. The factor chosen is multiplied by all coefficients in the corresponding macroblock.This process is referred as promoting and exciting a macroblock. The presence of excited macroblock indicates the presence of bit one and else zero. Data hiding can also be applied prior to compression. For example, [9] introduced a method that is robust to heavy JPEG compression. This paper proposes methods to hide information into images that achieve robustness against printing and scanning with blind decoding. The selective embedding in low frequencies scheme hides information in the magnitude of selected low-frequency discrete Fourier transform coefficients. Using the proposed methods, several hundred information bits can be embedded into images with perfect recovery and moreover, the hidden images also survive several other attacks. It is also possible to hide data in the wavelet domain as reported in [10].In this new wavelet transform-based image watermarking system, only significant wavelet coefficients (with large magnitude) are selected to bear a watermark and the message payload is embedded in it.

This paper is organized as follows. Section II presents the main related work. Section III describes the message hiding using Quantization scale modulation and Section IV introduces message hiding using flexible macroblock ordering. Section V deals with the experimental results. Finally, some conclusions are reported in Section VI.

II. Related Work

[1]. Kaushal Solanki proposed two methods to hide information into images in ‘Print and Scan’ Resilient Data Hiding in Images. The first technique, called selective embedding in low frequencies (SELF), hides data in the selected high magnitude low-frequency coefficients of the host image. The second technique, called Differential Quantization Index Modulation (DQIM) is for hiding data in the phase spectrum of the host image. SELF uses turbo-like codes, which helps for error-free recovery of the embedded bits. Once the image is automatically derotated and the gamma compensation is corrected, it is then used to demodulate and decode the embedded information. Finally, the sum product algorithm is used to decode the hidden information bits, which leads to error-free recovery of the hidden data despite the strong attacks. By using powerful channel codes provides robustness to the embedded data against a variety of other attacks. The robustness of our approach is based on two key components: the use of powerful turbo-like channel codes, and automated algorithms for derotation and correcting gamma compensation at the receiver. The disadvantage of this method is the presence of coloured noise. By reducing the effect of coloured noise , the embedding capacity can be improved by using the mid (or high) frequency coefficients along with the low-frequency ones for hiding.

[2] K. Nakajima, K. Tanaka, T. Matsuoka, and Y. Nakajima, proposed a rewritable data embedding scheme on MPEG coded data domain in [5.]This paper proposes a method that is used for content managements, content controlling and indexing. Here data hiding is achieved by block by block basis, where the length of zero run and the value of dummy AC component of quantized DCT coefficients are used as a data carrier. In the detection process, the correct position of final nonzero AC component is specified and we can reconstruct the MPEG coded data almost the same as close to the original MPEG data by just discarding the attached dummy component. Therefore, a video decoder which includes this code recovery function can playback the content with almost the same quality as that of original MPEG data. Else, a normal MPEG decoder can also playback the data embedded content, but its playback quality may be degraded when compared with the original MPEG data. Although the original MPEG picture quality is not maintained in the data embedded stream when the normal MPEG decoder is used, its quality can be recovered when the normal MPEG decoder is used after MPEG data is reconstructed, or when the MPEG decoder with data reconstruction function is used.

[3].Data hiding is also possible in the motion vectors and it is described in “Data hiding for digital video with phase of motion vector,”of compressed video based on their associated prediction error. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain

which are vulnerable to steganalysis. There is new method to hide the data in motion vectors of MPEG-2 compressed video. The motion vectors are used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video**.** Motion vectors are calculated using macroblock prediction errors. The secret message is encoded in the least significant bit of the block. The results of this paper are evaluated on two metrics: quality distortion to reconstructed video and data size increase of the compressed video.

III. Message Hiding Using Quantization Scale Modulation

Data hiding based on the quantization scale is also possible. This paper discusses methods for hiding data in MPEG video files. The data hiding system can be used for copy right protection, scene change detection and also for message passing. They are also used to assess the quality of compressed video without the presence of original video. The data hiding approach can also be used for error detection and concealment.

In order to hide a message using quantization scale modulation, first convert the message into a binary stream of bits and the, message bits are read one at a time during the MPEG encoding of each individual macroblocks. For each coded macroblock, the quantization scale of it is either incremented or decremented based on the underlying message bit. For a message bit one, the quantization scale is incremented and for a message bit zero,it is decremented. If the original quantization scale is either the lowest or largest value, then it is neither incremented nor decremented.

After all the message bits are hidden up, we end up with a feature matrix and a message vector. We will then treat the feature matrix as predictors and the message bits as a response variable. In order to extract the message bits that are hidden, extract the macroblock-level feature variables and compute a second order regression model.

In the existing systems, two novel solutions for data hiding are obtained. The first approach is hiding the message bits by modulating the quantization scale of a macroblock. The quantization scale is either incremented or decremented based upon the message bit. The macroblock-level feature variables are extracted and a second order regression model is computed, and using this regression model, decoder computes the hidden message bit. In the second approach, message bits are hidden and extracted using flexible macroblock feature of H.264/AVC video. Here macroblocks are assigned according to the content of the message bit. But in existing network, delivery of compressed video, packets may be lost if the channel is unreliable. Such losses may tend to occur in burst.So, a new block shuffling scheme is introduced to isolate erroneous blocks caused by information losses. This proposed solution reduces the information loss during video transmission.

A. Macroblock Level Features Variables

The following feature variables are extracted or computed from MPEG video for each coded macroblock.

- The first feature is the virtual buffer discrepancy from uniform distribution model and it is recalculated at the decoder for each macroblock.
- The second feature is the spatial activity of the underlying macroblock. This activity is computed from the four original(i.e., noncoded) luminance blocks of the current macroblock.
- The third feature is the actual quantization scale of the current macroblock and it is available from the macroblock header in the video bit stream. Using these feature variables, the decoder computes the hidden message bits.

B. Message Prediction and Extraction

It is formulated using a second order multivariate regression. Here the response variable is message binary bits denoted by vector. As, each macroblock has three feature variables, the predictors or the feature vectors of macroblocks are arranged into one matrix and is referred to as the feature matrix. To perform a mapping between the predictors and the response variable , the dimensionality of the rows or the feature vectors in matrix is expanded. The feature variables of each macroblock are computed from the bit stream inorder to extract the hidden message in the coded video. The feature vectors are arranged into a feature matrix and expanded to the second order, and this feature matrix is multiplied by the model weights to generate the predicted hidden message.

The process of message hiding and prediction is summarized. Notice that the feature extraction and polynomial expansion steps are repeated at both stages of message hiding and prediction. As such, the feature vector need not be transmitted with the bit stream.

One of the reasons for the success of this solution is that the set of feature vectors used at the encoder to generate the model weights is replicated at the decoder. This results in high prediction accuracy. The main limitations of the quantization scale modulation solution is related to the message payload where only one message bit can be hidden per macroblock.

IV. Message Hiding Using Flexible Macroblock Ordering(Fmo)

The limitations of the previous section are 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 this work we explicitly assign macroblocks to slice groups to hide messages in the video stream. Since macroblocks can be arbitrary assigned to slice groups, we use the slice group ID of individual macroblocks as an indication of message bits. Assume that if two slice groups are used, then 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 macroblock as shown in Table I.

Table I. Block Size

Number of slice groups	Potential Message bits/MB	Message bits
2	0,1	1
4	00,01,10,11	2
8	000,001,010,011,100, 101,110,111	3

Inorder to hide a message into the H.264/AVC bit stream, first we need to read the message into chunks of n bits, where n is 1, 2, or 3 according to the values in Table I. If m macroblocks are coded per picture, then mxn message bits can be hidden into the video stream.

In order to extract the message bits, we need to decode the picture every time, the macroblock to slice group mapping syntax structure is used to read message bits and append them to the extracted message.

In existing network, during the delivery of compressed video, the information may be lost due to the presence of errors, or due to any kind of attacks. Such losses may tend to occur in burst or it will tend to degrade the quality of the original video at the decoder.

So we proposes a robust error resilent approach for MPEG video files transmission. Here we are enhancing our work to robustness of the existing work against information losses in video steganalysis methods.

In this work, we develop an error resilient video encoding approach to help error concealment at the decoder. We introduce a new block shuffling scheme to isolate erroneous blocks caused by information losses. The existing solutions are superior in terms of message payload while causing less distortion and compression overhead and the proposed solution reduces the information loss in the video stream and identifies the quality of decoded video . Here we aim to reconstruct the original video at the decoder, without any loss of color information at the encoding stage.

Block Shuffling in source coding can be analogue to bit (block) interleaving in channel coding, which aims to break burst error into random bit errors. The difference lies at decoder: source decoder makes use of the remaining natural. Several shuffling patterns redundancy to recover random block error, while channel decoder uses explicit Forward Error Correction (FEC) code to recover the random bit error. Because the structure of MPEG video usually leads bit error to block error, and there is always some redundancy left in the coded video, source block shuffling can be more effective than channel interleaving in dealing with burst error.

The new shuffling pattern proposed in this paper disperses the errors over a wide area of the image, thus lowering the probability that the connected important blocks are lost at the same time during the encoding process. We shall call this shuffling pattern \ Error Spreading Shuffling (ESS)", which can more spread errors and minimize the overhead in compression. During the decoding process, we will extract all the data and if all the data and errors are recovered without any loss of information, we can conclude that there is no information loss in the video stream. There are chances for the loss of color information, which leads to reduce the image quality during the decoding process. If there is no loss of information, we can reconstruct the original image at the decoder.

1	8	3	5	2	7	4	6
6	1	8	3	5	2	7	4
4	6	1	8	3	5	2	7
7	4	6	1	8	3	5	2

Figure 1. Error spreading shuffling (ESS)

The error spreading shuffling pattern can be generated as follows. Suppose the image has N rows and M columns of Blocks/macroblocks, and assume M > N. We label the (i; i) blocks as \1" starting with the top left corner. After the N \1" blocks, we label as \2" all the (i, i + N) blocks, starting from the (1; N+1) block. When the labeling reaches the right extreme of the image, it wraps around to the left side. When the label \k" reaches the bottom row, say the (N; j) block, a new label \k +1" begins with the (1; j +1) block.

If the (1; j +1) block has already labeled then \k + 1" is assigned to the (1; j0) block, where j0 is the median of j + 1 and the column index of its greater nearest labeled neighbor. If it also has been labeled, then assign \k + 1" to the (1; j"), where j00 is the median of j + 2 and the column index of its greater nearest labeled neighbor. Continue with this manner until all the blocks have been labeled. This kind of shuffling can isolate error blocks under packet loss. We have noticed that fixed shuffling pattern can cause artifacts in fixed pattern, which can be annoyed for long video streams. In practice, mixing shuffling pattern of different direction can be employed to reduce the artifacts.

Here, during the encoding process we embed the secret message along with some errors,and then during the decoding process, we will extract the message from the video and if we are able to be extract all the datas along with the errors that are embedded. Then we can finalize that, there is no information loss in the video steganalysis method.

V. Experimental Results

When the system is executed, the video is displayed. First select the secret message (Here secret message is a text message) and it is converted into binary stream of bits. Embed the secret message into the video file during the encoding process. There are chances for errors during the embedding process in the video files and during the transmission over the internet. These errors may tend to information loss in the video or packet loss during transmission. During the decoding process, we extract the secret hidden message from the video files and if the errors are also extracted completely from the video, then we can guarantee that there is no information loss in the video. And finally the original hidden message can be extracted without any changes.

VI. Conclusion

In this paper, can enhance our work to robustness of the existing work against information losses in video steganalysis methods. A robust error resilient approach for MPEG video transmission over internet. In this work, we develop an error resilient video encoding approach to help error concealment at the decoder. It introduce a new block shuffling scheme to isolate erroneous blocks caused by data or information losses. And we apply data hiding to add additional protection for motion vectors. The existing solutions are superior in terms of message payload while causing less distortion and compression overhead and the proposed solution reduces the information loss during transmission.

References

[1]. M. Carli, M. Farais, E. D. Gelasca, R. Tedesco, and A. Neri, “Quality assessment using data hiding on perceptually important areas,” in Proc. IEEE Int. Conf. Image Processing, ICIP, Sep. 2005, pp. III-1200-3–III-1200-3.

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

[3]. S. Kapotas and A. Skodras, “A new data hiding scheme for scene change detection in H.264 encoded video sequences,” in Proc. IEEE Int. Conf. Multimedia Expo ICME, Jun. 2008, pp. 277–280.

[4]. 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.

[5]. 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. Signal Processing, ICSP, Oct. 2010, pp. 1833–1836.

[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 and Control, ICICIC’06, 2006, vol. II, pp. 803–806.

[8]. K. Wong, K. Tanaka, K. Takagi, and Y.Nakajima, “Complete video quality-preserving data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 10, Oct. 2009.

[9]. K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, “’Print and Scan’ resilient data hiding in images,” IEEE Trans. Inform. Forensics Security, vol. 1, no. 4, pp. 464–478, Dec.2006.

[10]. X.-P. Zhang, K. Li, and X. Wang, “A novel look-up table design method for data hiding with reduced distortion,” IEEE Trans. Circuits Syst. Video Technol., vol. 8, no. 6, pp. 769–776, Jun. 2008.