International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-8 March-2013

Steganography in MPEG Video Files using MACROBLOCKS

Lathikanandini. M[1], Suresh. J[2]
Student, Coimbatore Institute of Engineering & Technology, Coimbatore, Tamil Nadu[1]
Asst. Professor, Coimbatore Institute of Engineering & Technology, Coimbatore, Tamil Nadu [2]

Abstract

Digital communication has become an essential part of infrastructure now-a-days and the advancement in the field of digital communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of digital Communication. The steganography approach uses the flexible macroblock ordering feature of H.264/AVC to hide message bits. The message to be hidden is encrypted using AES algorithm. The message is hidden twice and predicted using the transitive, reflexive, symmetric properties. The proposed method here evades the copyright infringement and makes the stego video immune to steganalysis.

Keywords

Macroblock, H.264/AVC, Steganography, AES algorithm, transitive, reflexive, symmetric properties.

1. Introduction

Steganography is the art of hiding and transmitting data through apparently harmless carriers in an effort to hide the existence of the data. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection. Therefore, Stenographic methods could be combined with Cryptography in order to enhance the security even more. In cryptography, the sender encrypts the secret message preceding to the overall communication process, and makes more difficult for an attacker to detect embedded cipher text.

2. Literature Review

The data hiding system can be used for copy right protection, scene change detection [1] and also for message passing. Data hiding technique can also be used to assess the quality of compressed video in the absence of the original reference. This quality is calculated by computing the degradations of the extracted hidden message. Data hiding approach can also be used for error detection and concealment in applications of video transmission. To enable real time scene change detection in compressed video, the information is hidden using the motion compensation block sizes of an H.264/AVC video. The H.264/advanced video coding (AVC) is the latest standard for video compression with high compression efficiency and also very well suitable for network transmission where the data could be hidden in quantized discrete cosine transform (DCT) in the I frames of the video [2]. Using DCT coefficients, the data hiding is done which includes the use the parity of the quantized coefficients to hide a message.

Data hiding can be done in motion vector MV which uses the magnitude of MV [3]. This uses the least significant bit of both components of candidate motion vectors to embed a secret message. The candidate MVs are selected which is based on the prediction error of the underlying macroblock. MVs which are associated with high prediction errors are chosen. A 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.

Data hiding based on the quantization scale is also possible [4]. 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. The steganography method used in Tamer Shanableh [5] hides the secret message bits by changing the quantization scale of the video with constant bit rates. The message bits are extracted from the macroblock using the multivariate regression. But the major drawback of this method is that the message payload where only one message bit can be hidden per macroblock.

3. Proposed work

The framework for the proposed work can be divided into parts. Firstly the video is converted into frames which are used to hide the secret message. The message hiding uses the method of flexible macroblock ordering. In general, the frame is divided into slices. These slices are self-contained and be decoded independently of other slices. Each slice group contains one or more slices and macroblocks which can be ordered in any way. There are number of predefined slice group types such as interleaved slice groups, dispersed slice groups, foreground/background slice groups, box-out and wipe slice groups [6].

Table 1: Number of Slice Groups versus Number of Hidden Message Bits per Macroblock, adapted from Tamer Shanableh [5].

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

The obvious assignment of macroblocks can be made used to slice the groups to hide messages in the video stream. Since macroblocks can be randomly assigned to slice groups. The slice group ID of individual macroblocks can be used as an hint of message bits. If there are two slice groups are used, the allotment of a macroblock to slice group 0 indicates a message bit of 0 and the allotment of macroblock to slice group 1 indicates a message bit of 1 which is clearly elaborated in Table 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.

The procedure is as follows. Firstly the message is first read into chunks of n bits, where n is either 1, 2, or 3 according to the values in Table 1. If m macroblocks are coded per picture, then mxn message bits can be used to allocate the macroblocks to slice groups. To take out the message bits, when each time a picture is decoded, the macroblock to slice group mapping syntax structure is used to read mxn message bits and appended to the extracted message.

Packet Loss

Video communication is often afflicted by various forms of losses, such as packet loss over the Internet. Recovering the pixels which are lost in the video frames is an important step. Packet loss can be detrimental to compressed video with interdependent frames because errors potentially propagate across many frames. The latency requirements do not permit retransmission of all lost data. This Flexible Macroblock Ordering in H.264/AVC is used to stretch the errors produced by burst packet losses in a larger portion of the picture frame. Thus the error wrap up becomes easier and more efficient [7, 8].

The volume of the video frame can be expressed using frames. Let $x_j \epsilon R^n$ be a vector formed from pixels of frame j of video sequence, for j=1,2…J where J is the total number of frames. n is the total number of pixels in the frame. let $X=[x_1,x_2,\ldots x_J] \epsilon R^{nxJ}$ be a matrix of dimension nXJ, using the expression the volume of the video is calculated. However to hide the longer message in a video, it is suitable to take the video with the better length.

The slice loss in the error frame is calculated using, $e(t)= \hat{f}(t)-\bar{f}(t)$ by its amplitude and support. Since the slice is controlled by the number of macroblocks, the error depends on it. Let $Y=[y_1,y_{2,\ldots}y_N]$ be a vector of response variable. This Y is expressed by another covariate vector $X=[x_{1,}\ x2,\ _{\ldots}x_p]$ and a vector of unknown regression coefficients β where $\beta=[\beta_0,\beta_1,\ldots\beta_p]^T$.

Let Y^k represent the model with a subset of k covariates. The ith data point Y^k , y_i^k (i=1,2,…N) is given in equation (1).

$$Y_i^k = \beta_0^k + \beta_1^k\ x_{i1} + \beta_2^k\ x_{i2} + \ldots\ldots\ldots.. + \beta_k^k\ x_{ik} + \epsilon_i \quad (1)$$

Where β_0^k is the intercept and β_j^k where j=1,2,…k are the coefficients of x_{ij}.

The correlation between the video frames is denoted using equation (2).

$$I(X;Y) = \sum x \sum y\ p(x,y)\log(\frac{p(x,y)}{p(x)p(y)}) \quad (2)$$

Where p(x,y) are the frame x and frame y i.e. joint probability mass functions of random variables x and y and p(x) and p(y) are the marginal pmf of x and y respectively.

Secondly, the message to be hidden is encrypted using the Advanced Encryption Algorithm (AES). It is a block cipher symmetric algorithm which was intended to replace the DES algorithm. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. These key lengths make it impossible to break by simply trying every key. The overall working process of the proposed system is given in the Figure 1 Architecture diagram.

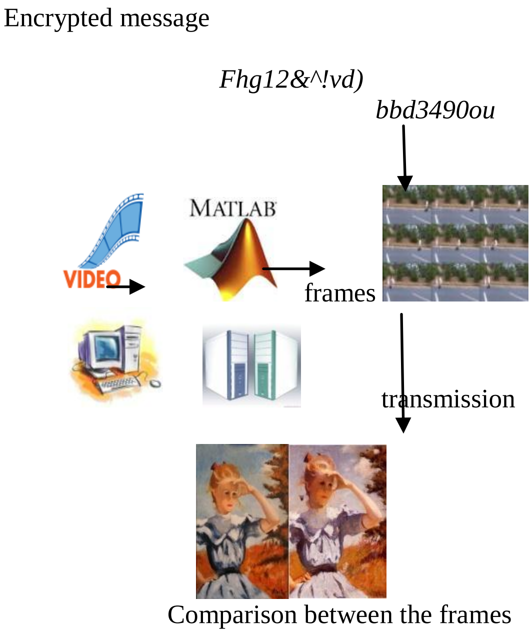

Figure 1: Architecture Diagram

Equivalence Relation

The security is further enhanced by using the equivalence relation. Instead of hiding the message bits once, it is hidden twice i.e. the allocation of macroblock to the slice group, based on the message bit, is repeated again. The equivalence relation is used to implement the idea. In mathematics, an equivalence relation is a relation that, partitions a set so that every element of the set is a member of one and only one cell of the partition. Two elements of the set are considered equivalent (with respect to the equivalence relation) if and only if they are elements of the same cell. The intersection of any two different cells is empty; the union of all the cells equals the original set [9].

The equivalence relation comprises of reflexive, transitive and symmetric properties. These reflexive, symmetric, transitive properties of the pixel relations provide equivalence groupings of adjacent, but not necessarily contiguous, pixels that are similar in chromaticity and luminance. The relationship between all the pixels is calculated using the reflexive, symmetric, transitive closure of the binary relation adjacent-matches between pairs of pixels [10]. The transitive property is defined as, for any macroblocks a, b and c, if a=b and b=c, then a=c. The reflexive property binary relation in which every macroblock is related to itself i.e. for a macroblock a, it is defined as a=a. Finally the symmetric property for macroblocks a and b is defined as, if a=b then b=a.

The identification of macroblock ordering which contain the same message bit, two properties are used, Adjacency and Chroma-luminance affinity. The reflexive, symmetric and transitive properties of the binary relation adjacent-matches, between the pairs of macroblock slice ordering. The macroblock ordering M1 adjacent-matches with macroblock ordering M2 if and only if it follows the conditions:

- Two macroblocks are CL-similar if their chroma-luminance difference is within a given threshold, ε. It is the measure of difference between the image color models. In RGB model, the chroma-luminance is the difference between the macroblock M1 and M2 and it is calculated using

$$\mathrm{Max}\begin{matrix}|R1-R2|\\|G1-G2|\\|B1-B2|\end{matrix} \leq \varepsilon \quad (3)$$

- Macroblock adjacency can be calculated using the parameter λ. For a given macroblock M, the neighborhood of M, n(M), is defined as all macroblocks within a λxλ square window centered around M. Two macroblocks M1 and M2 are adjacent if and only if *M1ϵ n(M2)*, equivalently *M2 ϵn(M1)*. M1 and M2 need not be nearest frames.

The equivalence relation relates all pixels using the reflexive, symmetric, transitive closure of the adjacent-matches pixels. Macroblocks that satisfy the equivalence relation are not required to be directly connected with immediate frames.

4. Result Analysis

There is no message prediction in the proposed method and the proposed method is compared with the existing result in [5]. The message hiding in the proposed solution is measured using kilobits per second.

The result is based on two cases. The first case uses two slice groups per frame and the later uses four slice groups per frame. The maximum number of message bits to hide in first case is one and the second case is two. The Table 2a represents for two slice groups order and 2b represents the four slice groups order with their average distortion. The sequences that benefit most out of intraprediction across macroblock boundaries are expected to generate higher bitrates in the case of message hiding.

Table 2: Message hiding with distortion for proposed solution

a. Using two slice groups

Sequence name	**2 slice groups**	
	Payload Kbits/s	**Average Distortion [dB]**
Coastguard	11.30	0.26
Container	11.30	0.08
Flowergarden	9.9	0.26
Mobile	11.88	0.22
Average	11.09	0.20

b. Using four slice groups

Sequence name	**4 slice groups**	
	Payload Kbits/s	**Average Distortion [dB]**
Coastguard	23.77	0.42
Container	23.77	0.15
Flowergarden	19.9	0.39
Mobile	23.77	0.45
Average	11.09	0.35

With comparison to hiding message bits using the quantization scale, interframe-coded macroblocks can have more than one MotionVector, and results in higher payload of the embedded secret messages. However, changing the values of the MotionVectors to embed message bits may reduce the quantity of the compressed video. Since there is no alternation in the values of the video frame pixels, this proposed method is can have greater advantage.

5. Conclusion and Future Work

The proposed method finds various advantages. It is quite simple and fully amenable with the H.264/AVC syntax. The allocation of macroblocks to the slice group is according to the content of the message to be hidden. 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 (bi directionally predicted). This method can be used both for Constant Bit Rate CBR and Variable Bit Rate VBR coding and has the message payload of 3 bits per macroblock. The security is further enhanced by encrypting the message using AES algorithm and hiding the message bits twice using the macroblock allocation to slice groups. The future work contains the examining the sturdiness of the proposed scheme and resistance against the digital video steganalysis.

References

[1] Spyridon K. Kapotas and Athanassios N. Skodras, ‘‘A New Data Hiding Scheme for Scene Change Detection In H.264 Encoded Video Sequences’’ in *Proc. IEEE Int. Conf. Multimedia Expo ICME*, pp. 277–280, Jun. 2008.

[2] 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*, pp. 1833–1836, Oct. 2010.

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

[4] 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.

[5] Tamer Shanableh, “Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering”, IEEE Transactions On Information Forensics and Security, Vol. 7, No. 2, April 2012.

[6] S. Wenger and M. Horowitz, Flexible macroblock ordering (FMO) 101 2002 [Online]. Available: http://ftp3.itu.ch/av-arch/jvt-site/2002_07_Klagenfurt/JVT-D063.doc.

[7] P. Lambert, W. De Neve, Y. Dhondt, R. Van de Walle, ‘Flexible macro block ordering in H.264/AVC’, doi: 10.1016/ j.jvcir.2005.05.008.

[8] Yves Dhondt, Peter Lambert, Stijn Notebaert, Rik Van de Walle, ‘Flexible macroblock ordering as a content adaptation tool in H.264/AVC’ Elsevier, J. Vis. Commun. Image R. 17 358–375 (2006).

[9] Nick Feamster and Hari Balakrishnan, ‘Packet Loss Recovery for Streaming Video’, M.I.T. Laboratory for Computer Science Cambridge, MA.

[10] Dana Forsthoefel, D. Scott Wills, and Linda M. Wills,’’Leap Segmentation for Recovering Image Surface Layout’’, IEEE SSIAI 2012.

Lathikanandini M has received under graduate degree in the field of Computer Science Engineering, from Anna University Coimbatore. She is currently pursuing Post graduate from Anna University Chennai. Her research interests include network security and steganography.