Information Hiding in H.264/AVC using Digital Watermarking

Praveen.M[1], Raj Vikram.R[2], Sasi Kumar.K[3], Sathish Kumar.S[4], Delhirani.S[5]

[1,2,3,4]*UG Scholar, Department of Computer Science Engineering, Kingston Engineering College, Tamilnadu, India*
[5]*Assistant Professor, Department of Computer Science Engineering, Kingston Engineering College, Tamilnadu, India*

Abstract - *Information hiding refers to the process of inserting information into a host to serve specific purpose(s). In this article, information hiding methods in the H.264/AVC compressed video domain are surveyed. First, the general framework of information hiding is conceptualized by relating state of an entity to a meaning (i.e., sequences of bits). This concept is illustrated by using various data representation schemes such as bit plane replacement, spread spectrum, histogram manipulation, divisibility, mapping rules and matrix encoding. Venues at which information hiding takes place are then identified, including prediction process, transformation, quantization and entropy coding. Related information hiding methods at each venue are briefly reviewed, along with the presentation of the targeted applications, appropriate diagrams and references. A timeline diagram is constructed to chronologically summarize the invention of information hiding methods in the compressed still image and video domains since year 1992. Comparison among the considered information hiding methods is also conducted in terms of venue, payload, bitstream size overhead, video quality, computational complexity and video criteria. Further perspectives and recommendations are presented to provide a better understanding on the current trend of information hiding and to identify new opportunities for information hiding in compressed video.*

KeyWords: **Information hiding, Compression, Watermarking, AVC, Encryption.**

1. INTRODUCTION

DATA hiding techniques can be used to embed a secret message into a compressed video bit stream for copyright protection, access control, content annotation and transaction tracking. Such data hiding techniques can also be used for other purposes. Data hiding techniques to assess the quality of compressed video in the absence of the original reference. The quality is estimated based on computing the degradations of the extracted hidden message. The authors of used data hiding 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. Data hiding is also used for error detection and concealment in applications of video transmission. Edge orientation information and number of bits of a block are hidden in the bit stream for that purpose

1.1 Existing System

In the Existing System, Digital Watermarking technique is used to provide data protection to text documents only. It provides copyright protection and ownership protection to text documents. This system makes use of data mining to explore the properties of text documents so as to embedded the secret message into it. Hence it helps in providing high robustness with high imperceptibility.

In some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. some parameters are embedded into a small number of encrypted pixels, and the of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

1.2 Disadvantage

It can hide secret message only into the Text documents. It is vulnerable to formatting attacks. The visual watermark on a digital file is rather simple: you can make an image that has your copyright symbol or other identifying visual on the picture itself. If people copy the picture, you can still see it's yours. You can choose to put a huge mark in the middle, or you can put a more subtle mark on the side. While it's easier to see the entire image when using a small mark, the disadvantage is that it can be easily removed by an unscrupulous person using a simple image editor. While this is nearly impossible with a larger mark in the middle of the image, the strong disadvantage is that it's harder to see the image itself.

2. PROPOSED SYSTEM

In this paper, we survey on information hiding methods designed specifically for compressed video, illustrate possible hiding venues within the H.264 coding structure for information hiding, and review their applications. We considered H.264 (instead of the latest compression standard, i.e., H.265) because of its rich literatures in various applications. Here, we emphasize on the techniques that manipulate the underlying coding structure of H.264 to realize data embedding and how each of the techniques affects the payload (i.e., the number of bits that can be inserted into the host video), bitstream size overhead, video quality and computational complexity. Nevertheless, at times, information hiding methods designed for image are also reviewed since they can be readily applied to compressed video.

3. SYSTEM ARCHITECTURE

This Architecture diagram includes AES Encryption, ASCII to Binary Conversion, Slicing, Motion Compensation, Motion vector prediction & estimation, Block Transformation and Encoding. The input is the frame that is extracted from the video and the ouput produced will be of bitstream image.

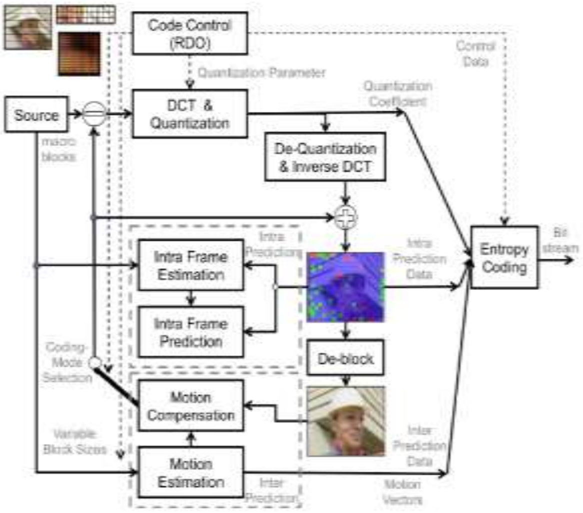


Fig -1: System Architecture

3.1 Slicing

In general, a coded picture is divided into one or more slices. Slice is a portion of a picture composed of macro blocks. This feature is important to suppress error propagation within a picture due to the nature of variable length coding

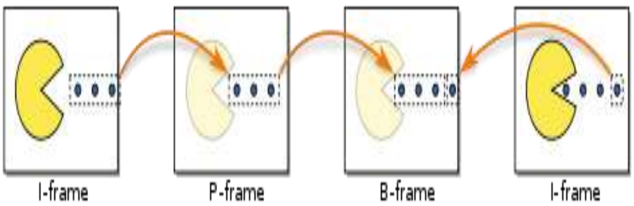


Fig -2: Slicing

An I-frame (Intra-coded picture) is a complete image, like a JPG or BMP image file. P-frame (Predicted picture) holds only the changes in the image from the previous frame. B-frame (Bidirectional predicted picture) saves even more space by using differences between the current frame and both the preceding and following frames to specify its content.

3.2 Motion Compensation

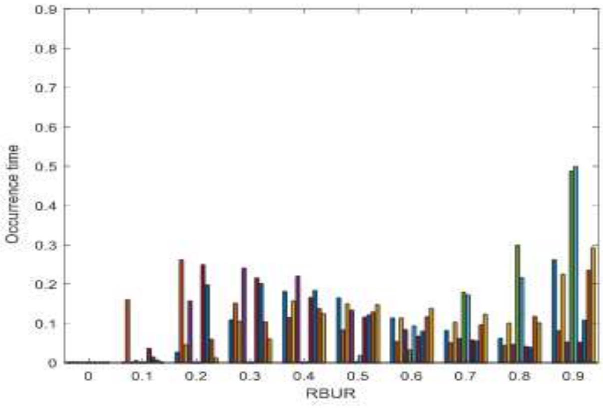
Since MPEG-1, motion compensation is a standard coding tool for video compression. Using motion compensation, motion between frames can be encoded in a very efficient manner. A typical P-type block copies an area of the last decoded frame into the current frame buffer to serve as a prediction. If this block is assigned a nonzero motion vector, the source area for this copy process will not be the same as the destination area. It will be moved by some pixels, allowing to accomodate for the motion of the object that occupies that block. Motion vectors need not be integer values: In H.264, motion vector precision is one-quarter pixel (oneeighth pixel in chroma). Interpolation is used to determine the intensity values at non-integer pixel positions. Additionally, motion vectors may point to regions outside of the image. In this case, edge pixels are repeated.

3.3 Motion Vector Prediction

Because adjacent blocks tend to move in the same directions, the motion vectors are also encoded using prediction. When a block's motion vector is encoded, the surrounding blocks' motion vectors are used to estimate the current motion vector. Then, only the difference between this prediction and the actual vector is stored

3.4 Macro Block ordering

In this paper, we make use of the explicit assignment of macroblocks 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.



4. CONCLUSION

In this work, we surveyed the conventional information hiding methods in the compressed video domain, focusing on the H.264 video compression standard. Commonly considered data representation schemes and the hiding venues were summarized. The general trend of information hiding in the compressed video domain were presented. Then, we categorized the existing information hiding methods based on the venues at which they operate and highlighted their strengths and weaknesses. Video criteria such as motion alleviation, GOP size and bitrate were recommended as guidelines to select appropriate technique for information hiding, and future research directions were suggested. This survey is limited to the techniques that manipulate the underlying coding structure of H.264 to realize data embedding. The decoding process (e.g., in multi-bit watermark application) and the detection process (e.g., in zero bit watermark application) as well as the security issues involved will be investigated as our future work.

REFERENCES

[1] Chun-Shien Lu, and Hong-Yuan Mark Liao, "Multipurpose Watermarking For Image Authentication And Protection" 2010.
[2] Chun-Shien Lu, Member, IEEE, Shih-Kun Huang, Chwen-Jye Sze, and Hong-Yuan Mark Liao, Member, IEEE, "Cocktail Watermarking for Digital Image Protection".
[3] Eugene T. Lin, Ahmet M. Eskicioglu, Reginald L. Lagendijk, Edward," Advances In Digital Video Content Protection".
[4] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn," Information Hiding - a Survey".
[5] M.Ezhilarasan, P.Thambidurai, K.Praveena, Sudha Srinivasan, N.Sumathi, "A New Entropy Encoding Technique for Multimedia Data Compression".
[6] M. A. Ansari ; Imran Ullah Khan, "Performance analysis and evaluation of H.263 video codec ".