Descrambling Privacy Protected Information for Authenticated users in H.264/AVC Compressed Video

R.Hemanth Kumar
Final Year Student, Department of Information Technology,
Prathyusha Institute of Technology and Management ,
Poonamalee - Thiruvallur road, Thiruvallur - 602025, Tamilnadu, India
K.Praveen
Final Year Student, Department of Information Technology,
Prathyusha Institute of Technology and Management ,
Poonamalee - Thiruvallur road, Thiruvallur - 602025, Tamilnadu, India
Dr.M.P.Sivaram Kumar
Professor, Department of Information Technology,
Prathyusha Institute of Technology and Management ,
Poonamalee - Thiruvallur road, Thiruvallur - 602025, Tamilnadu, India

Abstract:

The sensitive or private information in frames, which should not be viewable by the general public or regular users, will be scrambled by directly modifying or removing the related data in H.264/AVC compressed bit streams. A privacy protection mechanism in H.264/AVC videos is proposed, in order to allow the authorized users to recover the partially scrambled video frames, the methodology of information hiding is employed; that is, the correct information is embedded and transmitted along with the video bit stream. After retrieving the data, the authorized users can descramble the protected areas in frames. The conventional information hiding methods in the compressed video domain, focusing on the H.264 video compression standard is being used. Our study is based on Discrete Wavelet Transform (DWT) which is based on H.264/AVC intra prediction.

Keywords: Discrete Wavelet Transform (DWT), H.264/AVC compression standard, Intra prediction blocks.

Introduction:

The main aim of this process is that the sensitive or private visual information in frames, which should not be viewable by the general public or regular users, will be hidden. The methodology of information hiding is employed. The correct information is embedded and transmitted along with the video bit stream. After retrieving the data, the authorized users can descramble the protected areas in frames with a secret key. It uses the Discrete Wavelet Transform (DWT) algorithm for sampling of the wavelets.H.264 video compression standard is used for video compression. It mainly focus on the H.264 video compression standard. In the proposed method, use **Discrete Wavelet Transform (DWT)** which is based on H.264/AVC intra prediction and it is lossless compression.

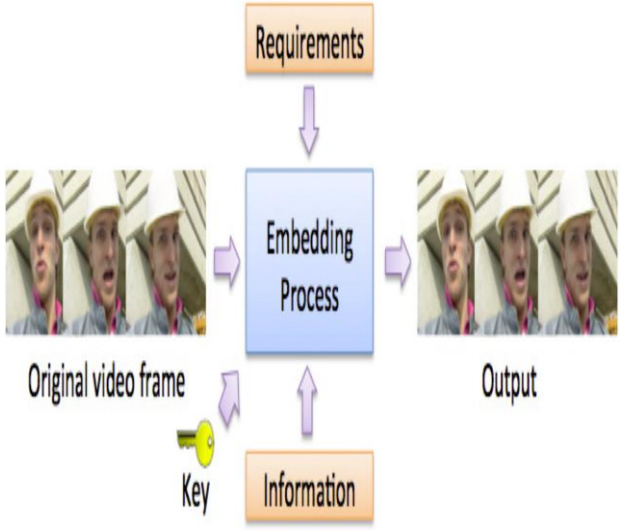

Fig-1a: General framework of information hiding

Firstly the prediction error blocks are computed and then the error values are slightly modified through shifting the prediction errors. The modified errors are used for embedding the secret data.

2. Related works:-

2.1 Macro Block Classification:

Two types of redundancy are responsible for compression. Redundancy between the pixels called spatial redundancy. Redundancy between frames called temporal redundancy. Spatial redundancy, also known as Intra-frame redundancy is achieved using techniques of DWT, Quantization and Entropy coding. Temporal redundancy, also known as Inter-frame redundancy is achieved using techniques of motion estimation. An MPEG video is sequence of still digital images. Two successive frames in video have minor difference. Motion estimation is the process, which tracks such changes in order to reduce this inter-frame redundancy. Motion estimation is the process by which a macro block in a picture is best correlated to macro block in previous or next picture by the estimated amount of motion. The motion vector stores the amount of motion. Correlation with previous image is stored in forward motion vector and correlation with future image is stored in backward motion vector. Background of images generally does not change position while object in the foreground moves a little with relative to reference frame. Motion estimation is used to determine the displacement of an object in frame. Displacement of an object with reference to another frame is coded. In industry many motion estimation algorithm are implemented. Block matching algorithms are most effectively used for motion estimation.

2.2 Motion Estimation:

We have described a new computer environment for evaluation of ME algorithms for video compression. We also examined multi-criteria analysis of algorithms for video compression. The new integrated parameter (C) and a Pareto approach for performance comparison can be used in many other situations (e.g., R-D and complexity-distortion (C-D) codec controls for decision making in ME operations). Our work is only a first step in multi-criteria analysis. Many other algorithms for multimedia can be investigated on this basis. Motion estimation uses the Motion vector to store the movement of the macro block. So, the amount of data to be stored for image difference is greatly reduced. That motion predicted difference image stores very less data compared to normal difference image. Hence, motion estimation is very efficient way for data compression .P frames and B frames are inter-coded frames. P frames are forward predicted from either previous I frame or previous P frame. P frame encoding would require motion estimation. Motion vector and prediction error are generated, and only these information is encoded and transmitted. Inter-frame coding achieves more compression than intra-frame coding as it exploits temporal redundancy. B frames carry difference from previous reference frame as well as next reference frame. Thus B frames achieve the highest compression.

2.3 Motion Compensation:

Multi-frame motion-compensated prediction extends the spatial displacement vector utilized in block-based hybrid video coding by a variable frame reference permitting the use of more frames than the previously decoded one for motion-compensated prediction The multi-frame buffer stores frames at encoder and decoder that are efficient for motion-compensated prediction. The use of multiple frames for motion compensation in most cases provides significantly improved coding gain. The frame reference parameter has to be transmitted as side information requiring additional bit-rate. To control the bit-rate budget, rate constrained motion estimation is utilized.

2.4 Wavelet Transform based Data hiding:

Wavelet-based image compression method using in is the new standard for still image compression. It provides a new framework and an integrated toolbox to better address increasing needs for compression. It also provides a wide range of functionalities for still image applications. Lossless and lossy coding embedded lossy to lossless, progressive by resolution and quality, high compression efficiency, error resilience and lossless color transformations are some of its characteristics. Comparative results have shown that JPEG2000 is indeed superior to existing still image compression standards. Work is still needed in optimizing its implementation performance. Application of wavelet transform in image processing is one of the active areas in wavelet studies. Two dimensional wavelet transform can be considered as an extension of 1D wavelet transform. M dimensional wavelet transform is a natural extension of 2D wavelet transform. It is applied in problems such as system modeling used in control systems and construction of autoregressive models. The reason bi orthogonal wavelets are often used in image analysis is due to human visual system where they are more tolerant

of symmetric errors than asymmetric ones, it is desirable that wavelet and scaling functions be symmetric.

2.5 Key Generation:

The key generation module is the most secret component of a cryptosystem. For security, an architect of a cryptosystem may want to develop his own RNGs instead of using other people's programs or designs. This paper provides a practical guide for the design and testing of cryptographic RNGs. Section 2 describes various kinds of RNGs and their characteristics. We recommend combining outputs of at least four generators of different kinds, including an unpredictable one. Section 3 describes the most well known sets of statistical tests of randomness. These tests check whether the outputs of an RNG are uniformly distributed and independent. We suggest that at least two component RNGs in the combined generator shall pass all these tests. Section 4 describes how to use the collision test to ensure that the seed space of an RNG is not trivially small. If the seed space of an RNG is too small, an attacker will be able to regenerate a key by initializing the RNG with all possible seeds one by one exhaustively. Section 5 suggests practical measures that protect the key generation module against system attacks. It also includes ways that minimize the leakage of secret when the computer that runs the module has been seized. Section 6 provides a checklist for auditing a secure RNG. Redundancy that safeguards the security has been built-in.

3. Model:

We observe from the diagram that the trend of information hiding is related to the release of new image/video compression standard. The number of publications related to information hiding in JPEG does not increase until some years later after its standardization. Among all the information hiding techniques, block size, and intra-prediction type selections offer simple ways to encode information by associating the indices (i.e, states) with groups of bits (i.e., meaning). These techniques maintain coding efficiency with insignificant fluctuation in bit rate, but cause video bit stream size increment in general .On the other hand, hiding information in block size selection provides minimal impact on video quality and bit rate. The current approaches merely divide the block size selection into two groups and offer minimal payload. Hence, a straightforward improvement is to extend the selection groups (to four or eight groups) to encode more information.

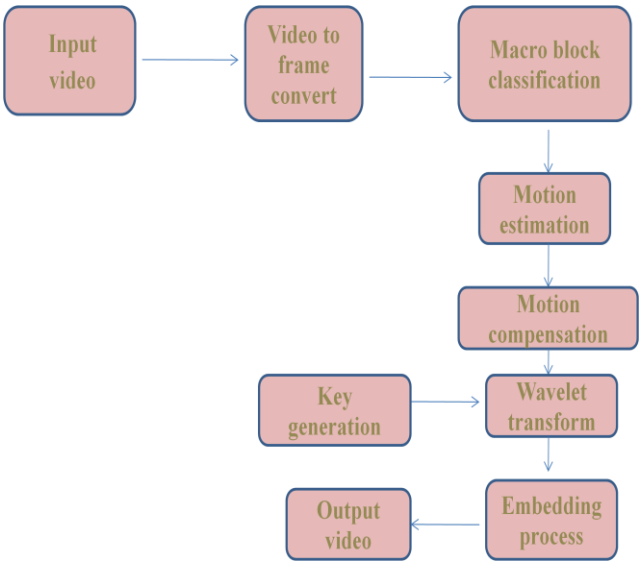

Fig: 3a- The process of information hiding

UML Activity Diagram

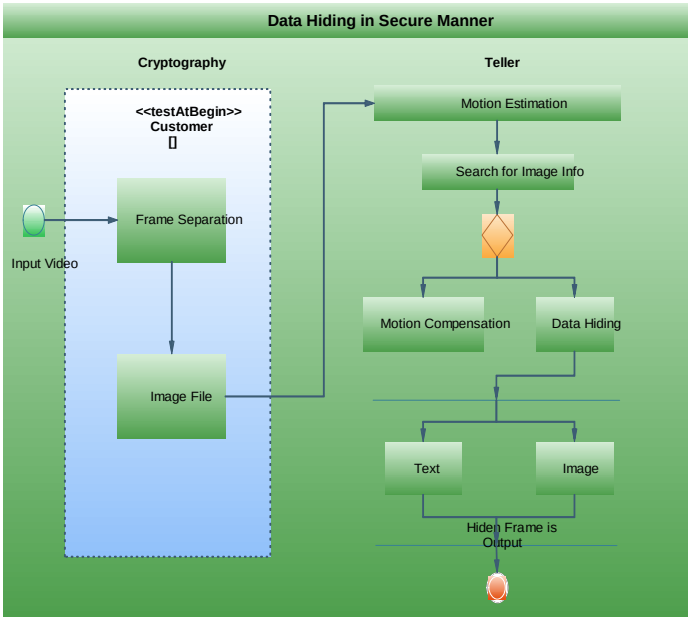

Fig: 3b –UML Activity diagram

since the motion vectors suggested by the compliant encoder do not precisely reflect to the real motion experienced by a macro block, the actual displacement information is embedded for motion tracking purpose. With the embedded motion information, the actual displacement of each macro block is readily available for precise and efficient motion tracking.

Conclusion:

In this paper, we surveyed the conventional information hiding methods in the compressed video domain, focusing on the H.264 video compression standard. 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 bit rate 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) as well as the security issues involved also be investigated in this work. In addition, We used new information hiding opportunities in the latest H.265 video compression standard.

References:

[1] An Overview of Information Hiding in

H.264/AVC Compressed Video

Yiqi Tew and KokSheik Wong (2014)

[2] MPEG-2 to HEVC Video Transcoding With Content-Based Modeling

Tamer Shanableh, Eduardo Peixoto, and Ebroul Izquierdo (2013)

[3] Block Partitioning Structure in the HEVC Standard

Il-Koo Kim, Junghye Min, Tammy Lee, Woo-Jin Han, and JeongHoon Park (2012)

[4] Architectures for Fast Transcoding of H.264/AVC to Quality-Scalable SVC Streams

Jan De Cock, Stijn Notebaert, Peter Lambert, and Rik Van de Walle (2009)