World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:10, 2008

Novel Security Strategy for Real Time Digital Videos

Prakash Devale, R. S. Prasad, Amol Dhumane, and Pritesh Patil

***Abstract*—**Now a days video data embedding approach is a very challenging and interesting task towards keeping real time video data secure. We can implement and use this technique with high-level applications. As the rate-distortion of any image is not confirmed, because the gain provided by accurate image frame segmentation are balanced by the inefficiency of coding objects of arbitrary shape, with a lot factors like losses that depend on both the coding scheme and the object structure. By using rate controller in association with the encoder one can dynamically adjust the target bitrate. This paper discusses about to keep secure videos by mixing signature data with negligible distortion in the original video, and to keep steganographic video as closely as possible to the quality of the original video. In this discussion we propose the method for embedding the signature data into separate video frames by the use of block Discrete Cosine Transform. These frames are then encoded by real time encoding H.264 scheme concepts. After processing, at receiver end recovery of original video and the signature data is proposed.

***Keywords*—**Data Hiding, Digital Watermarking, video coding H.264, Rate Control, Block DCT.

I. Introduction

SPREADING of real time video data have changed the views and aspects related to the security, accuracy and efficiency on online transmission. Because of the easy availability of real time video data online and by some other means one should think about providing security in terms of access control, authentication and protection against piracy of video data. Uses of watermarks are almost as old as paper manufacturing.

Today most developed countries also watermark their paper, currencies, and postage stamps to make forgery more difficult. The digitization of world has expanded the concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests.

Watermarking for Protection against piracy needs very few bits of the size of the source video. The signature data used in watermarking can be the characters or can be video information. The purpose of digital watermarking is to find the ownerships by verifying the signature or watermarks. It is desirable that the embedding and recovery methods are form a logical shield in front of signal processing operations which includes compression, different attacks to vanish signature data.

A rate control algorithm dynamically adjusts encoder parameters to achieve a target bitrate. It allocates a budget of bits to each group of pictures, individual picture and/or sub-picture in a video sequence. Rate control is not a part of the H.264 standard, but the standards group has issued non-normative guidance to aid in implementation.

This paper discusses about to keep secure videos by mixing signature data (video) with negligible distortion in the original video, and to keep steganographic video as closely as possible to the quality of the original video. In this discussion we propose the method for embedding the signature data into separate video frames by the use of block Discrete Cosine Transform. In this discussion we consider the applications which require comparatively and significantly larger amount of embedding. Because of redundancies introduced during embedding in the data, hiding large amount of data will enable robustness in the watermarks. To differentiate our process from typically available watermarking, we use the notations video in video, data hiding, and digital watermarking. Let us consider an example, while the real time video data transfer where in many cases the watermarks can be accepted, to make the overall communication secure the signature data to which we are going to embed in the videos should not be visible to attackers.

II. Early Works

Recent research for embedding is the object based coding method for images. Actual idea is to distribute the key data over the frequency of the source video data. Discrete Cosine transform is used by many of the peoples who are doing research on this concept. Watermarking was the initial task to achieve in those methods. As much of the initial task was on watermarking image data [3,4], recently many methods have been proposed for embedding audio and video information in video standards. For example, Swanson [6] proposed a data hiding algorithm to embed compressed video and audio data into video. The message data is embedded in the DCT domain, by modifying the projections of the 8x8 host block

Prakash Devale is with IT department of Bharati Vidyapeeth University, Pune-43 (phone: +91-20-24220697; e-mail: prakash_devale@yahoo.com).

R. S. Prasad is with computer Engg. Dept. of Vishwakarma institute of Information Technology Pune (phone: +91-9823369180; e-mail: rsprasad_viit@yahoo.com).

Amol Dhumane is with Computer Engg. Dept. of Vishwakarma Institute of Information Tech. Pune (phone: +91-9011043041; e-mail: amol.dhumane@gmail.com).

Pritesh Patil is with Computer Engg. Department of Bharati Vidyapeeth University, Pune-43 (phone: +91-9975850134; e-mail: p.patil.k@gmail.com).

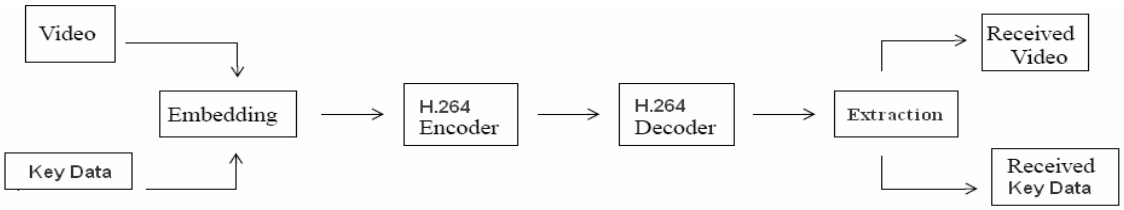


Fig. 1 Block diagram of data hiding scheme

DCT coefficients. The data hiding rate is two bits per 8x8 block. H.263 video coding [1,2] can be used as the key component of embedding system, but it does not support all kind of bitrates. More recently, Mukherjee [5] presented a technique for hiding audio in video. They used multidimensional lattice structures to embed the 8 KHz speech signal, and the data hiding rate is about 1%.

In this discussion, we propose a data hiding technique. A schematic of our embedding scheme is shown in Fig. 1. A key component of this scheme is the use of H.264 video coder [12]. The signature image and host video frames are transformed using the 8X8 block DCT. The signature coefficients are quantized and then encoded using H.264 encoder shown in Fig. 2 and inserted into the host DCT coefficients. This insertion is adaptive to the local texture content of the host video frame blocks [7]. The embedded video frames are then compressed, and the signature data is recovered from the lossy compressed video.

Embedded source video frames of video information are captured at the source and are encoded or compressed by a video encoder. The compressed stream is transmitted across a network or telecommunications link and decoded or decompressed by a video decoder. The decoded frames then becomes the input to extraction algorithm and finally at the destination side we would receive the secrete information to which we are aiming to send.

A lot of video coding techniques are available each technique is designed for a particular type of application: e.g. JPEG for rigid images, MPEG2 for digital television and H.261 for ISDN video conferencing. But if bit rate is the major concern then the H.264 video coding technique will help us for low bit rates of the video frames: typically 20-30kbps and above of real time video data and also in adjusting the encoder parameter.

III. Hiding RT Video Data

Fig. 2 shows the block diagram of encoder used in the data hiding scheme.

1. The video frame and key image frame are transformed to the DCT domain.
2. The quantization of signature coefficients would be done according to the signature quantization matrix and the resulting quantized coefficients are encoded.
3. The signature codes are then appropriately scaled using the total scale factor and the JPEG quantization matrix. The JPEG quantization matrix helps renormalize the code vectors so that their dynamic range is similar to that of a typical DCT block.
4. The selected host coefficients are then replaced by the scaled signature codes and combined with the original (unaltered) DCT coefficients to form a fused block of DCT coefficients.
5. The fused coefficients are then inverse transformed to produce an embedded frame. Fig. 5 shows embedding method. By applying the inverse operations one can extract the signature data.

By subtracting the previous transmitted frame from the current frame one can reduce the bandwidth so that only the difference needs to be encoded and transmitted. It means that areas of the frame that do not change e.g. background are not encoded. Further reduction of bandwidth is achieved by attempting to estimate where areas of the previous frame have moved to in the current frame termed as motion estimation and compensating for this movement termed as motion compensation. The motion estimation module compares each 16x16 pixel block termed as macroblock in the current frame with its surrounding area in the previous frame and attempts to find a match. The matching area is moved into the current macroblock position by the motion compensator module.

The motion compensated macroblock is subtracted from the current macroblock. The rate-distortion curves presented by Cagnazzo [8] are really helping us in our process to find out cost and spectrum of video frames.

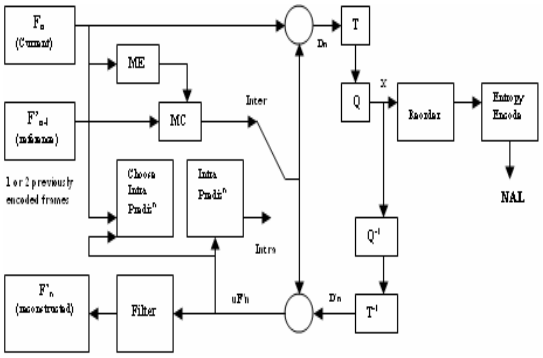


Fig. 2 Encoder of the data hiding scheme of Fig. 1

IV. Entropy Encoding or Coding Control

The coding control e.g. Huffman encoder replaces frequently-occurring values with short binary codes and replaces infrequently-occurring values with longer binary codes. This technique is also used to compress the quantized DCT coefficients. The result is a sequence of variable-length binary codes. These codes are combined with synchronization and control information to form the encoded bitstream.

The prediction error or the input picture is subdivided into 8 X 8 blocks which are segmented as transmitted or non-transmitted. The criteria for choice of mode and transmitting a block are not recommended and may be varied dynamically as

part of the coding strategy. Transmitted blocks are transformed and the resulting coefficients are quantized and variable-length coded. Although not a part of H.264, several parameters may be varied to control the rate of coded video data.

V. Quantizer

The DCT transforms a block of pixel values into a set of spatial frequency coefficients. In H.264 video coder the DCT operates on a 2-dimensional block of pixels rather than on a 1-dimensional signal and is particularly good at compacting the energy in the block of values into a small number of coefficients. This means that only a few DCT coefficients are required to recreate a recognizable copy of the original block of pixels.

For a typical block of pixels, most of the coefficients produced by the DCT are close to zero. The quantizer module reduces the precision of each coefficient so that the near-zero coefficients are set to zero and only a few significant non-zero coefficients are left.

VI. Rate Control and H.264

A rate control algorithm dynamically adjusts encoder parameters to achieve a target bitrate. It allocates a budget of bits to each group of pictures, individual picture and/or sub-picture in a video sequence. Rate control is not a part of the H.264 standard, but the standards group has issued non-normative guidance to aid in implementation.

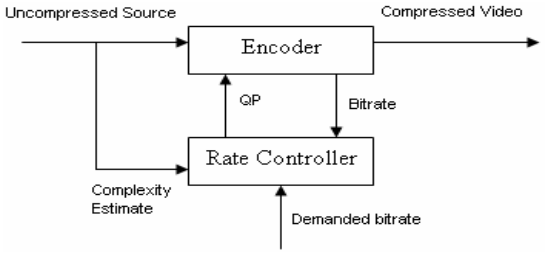


Fig. 3 H.264 video encoder with rate controller

VII. H.264 Rate-Distortion Optimization and Global Rate Control

In H.264, 7 modes are for inter or temporal prediction, 9 modes for intra or spatial prediction of 4x4 blocks, 4 modes for intra prediction of 16 x 16 macroblocks, and one skip mode. Each 16 x 16 macroblock can be broken down in numerous ways. Thus selecting mode for each macroblock is a critical and time-consuming step that reduces the bitrate at high extent.

By rate distortion optimization algorithm proposed by T Wiegand [11], selection of the optimal mode is achieved, which includes:

1) An exhaustive pre-calculation of all feasible modes to determine the bits and distortion of each.

2) Evaluation of a metric that considers both bitrate and distortion.

3) Selection of the mode that minimizes the metric.

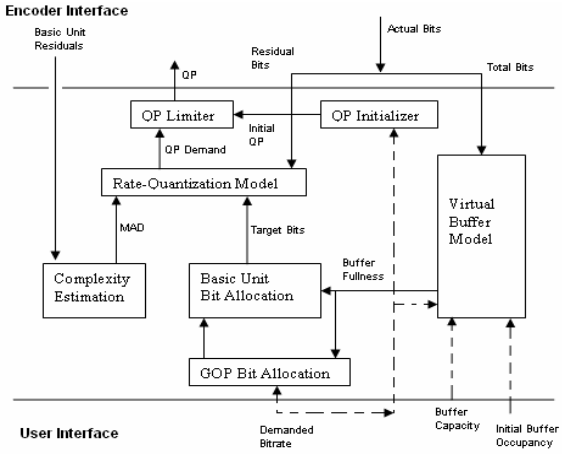


Fig. 4 H.264 Rate Controller

VIII. Actual Hiding Process

After key frame K is generated, the main encryption part is processed. Fig. 5 represents the main encryption process. The main encryption process consists of a XOR operation and watermarking. Original frame is XORed with secrete key and then, the XORed frame is watermarked. The objects for the watermarks are all blocks, and the objects for XOR are all pixels. However, the color value of each pixel can be selectively XORed. From the combination of selective and naive algorithms, we can achieve both security and light-weightness [8, 9, 10]. Signature management is used to manage key information or watermarked information. This component is responsible in providing the information required for relative operations.

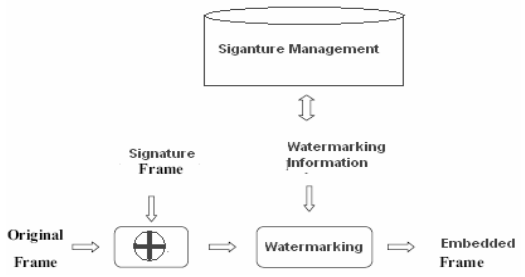


Fig. 5 Embedding steps of Fig. 1

Following are the terms used in embedding algorithm:
S = Seed frame, K = Frame of secrete video
O = The original video frame
X = The XORed frame with O and K
E = Embedded frame.
key1[i] = Keys for First transposition (i = 1,.. S)
key2[j] = Keys for second transposition (j = 1,..X)

Step 1. Transposition

for(i=0; i < block num of S; i++)
begin
Transpos [i] = key1[i] % block [i] of S(Get K)
end

Step 2. XOR

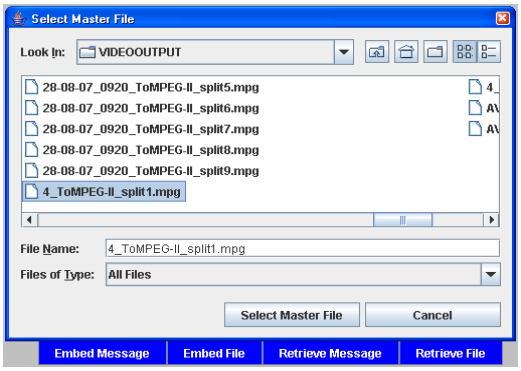
X = O $\oplus$ K; where $\oplus$ is XOR operation

Step 3. Transposition

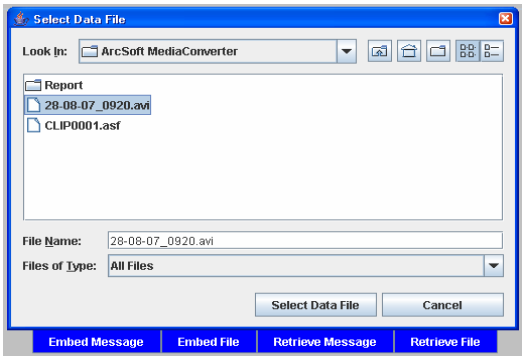
for(j=0; j < block num of X; j++)
begin
E[j] = key2[j] % block [j] of X(Get E)
end

IX. Screen Shots

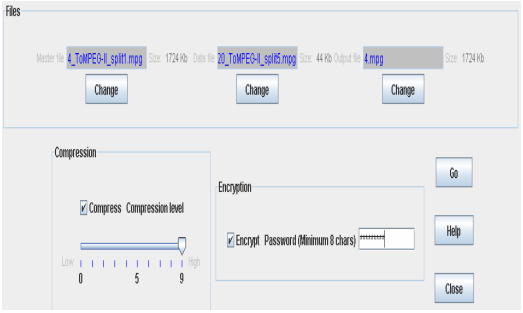
Fig. 6 (a, b, c, d) shows some of the GUI screen designed for selecting carrier video, secrete video, compression and encryption, retrieval of hided RT digital video from carrier video etc.



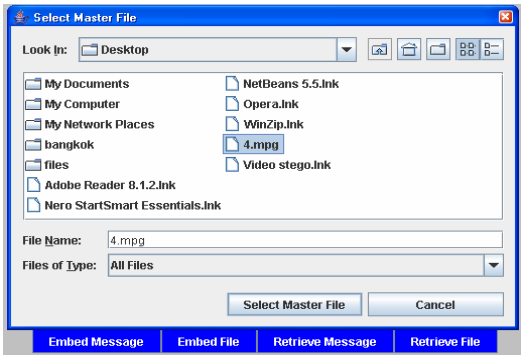
a) GUI for selecting carrier video



b) GUI for selecting secrete (data) video



c) GUI for compression and Encryption (optional)

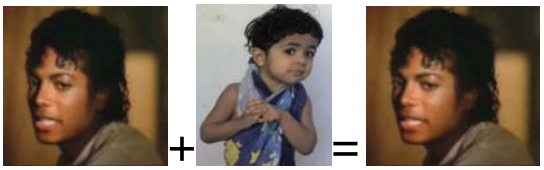


d) GUI for Selecting embedded video for retrieval of RT digital video from carrier video

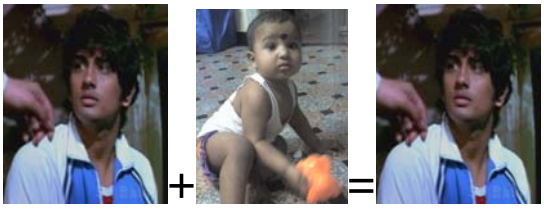
Fig. 6 (a, b, c, d) Some screen shots

X. Results

While applying steganography to RT digital video it has been taken care that the carrier video is not changing in terms of audio and video quality. Fig. 7 shows some of the results obtained.



Carrier video **RT digital video** **Embedded video**



Carrier video **RT digital video** **Embedded video**

Fig. 7 Embedded videos obtained

XI. Conclusion

For the security of real time video data available easily, the approach presented in this paper is definitely going to very effective because after hiding RT digital video; embedded video's quality remain same as of carrier video. The use of latest trends in video coding such as H.264 video coding has given a good strength to our work. If embedding is applied to encoded blocks and not-encoded blocks, the encoder would not be able to find the position of the block that has not been encoded. That is, each block does not have its own motion vector information before encryption. Since B frame has only motion vector information, the compression rate of H.264 is sensitive to the quantity of B frames. Although rate control is not the part of H.264 but by applying the interfacing between H.264 video encoder and rate controller one can dynamically

adjust encoder parameters to achieve a target bitrate. This feature makes H.264 compatible with any kind of bitrate.

REFERENCES

[1] ITU-T Recommendation H.263, "Video coding for low bit rate communication".
[2] Riley and Richardson, "Digital Video Communications", Artech House 1997.
[3] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," Proceedings of the IEEE, Vol. 86, June, 1998.
[4] I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "A secure Robust watermark for Multimedia," IEEE Trans.IP Vol. 6 Dec, 1997.
[5] D. Mukherjee, J. J. Chae and S. K. Mitra, "A Source and Channel Coding Approach to Data Hiding with Application to Hiding Speech in Video," Proceeding of IEEE ICIP '98.
[6] M. D. Swanson, B. Zh and A. H. Tewfik, "Data Hiding for Video-in-Video," Proceedings of IEEE International Conference of Image Processing '97.
[7] B. Tao and B. Dickenson, "Adaptive Watermarking in the DCT Domain," (ICASSP '97), Vol. 4, April 1997.
[8] Marco Cagnazzo, Sara Parrilli "Costs and Advantages of Object-Based Image Coding with Shape-adaptive Wavelet Transform" EURASIP Image Processing Journal Volume, 2007.
[9] A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission Choo, Euijin Lee, Jehyun Lee, Heejo Nam, Giwon Multimedia and Ubiquitous Engineering, 2007.
[10] B. Bhargava, C. Shi, and S. Wang. MPEG video encryption algorithms. Multimedia Tools and Applications, 9 2004.
[11] T. Wiegand, H. Schwarz, A. Joch, F. Kossentini and G. Sullivan, "Rate-Constrained Coder Control and Comparison of Video Coding Standards," IEEE Transactions 7, July 2003.
[12] ITU-T Rec. H.264/ISO/IEC 11496-10, "Advanced Video Coding", Final Committee Draft, Document JVTE022, September 2002.