An Approach Towards Efficient Video Data Hiding Using Prohibited Zone

V.RADHIKA
MCA Student, Dept of MCA,
DRK Institute of Science and Technology,
Hyderabad, Andhra Pradesh, India

Dr.R.V.KRISHNAIAH
PG Coordinator, Dept of CSE,
DRK Group of Institutions,
Hyderabad, Andhra Pradesh, India

Abstract: **The process of embedding information into a host medium is a data hiding. In general, due to their wide presence and the tolerance of human perceptual systems involved visual and arual media are preferred. The methods vary depending on the nature of such media and the general structure of data hiding process does not depend on the host media type. Due to the design complexities involved video data hiding is still an important research topic. A new video data hiding method that makes use of removal correction capabilities of replicate accumulate codes and advantage of prohibited zone data hiding is proposed in this paper. To determine host signal samples suitable for data hiding selective embedding is utilized in the proposed method. In order to withstand frame drop and insert attacks a temporal synchronization scheme is contained in this method. By typical broadcast material against MPEG- 2, H.264 compression, frame-rate renovation attacks, as well as other renowned video data hiding methods the proposed framework is tested here. For typical system parameters the decoding error values are reported. The imitation results specify that the frame can be effectively utilized in video data hiding applications.**

Keywords: Video Data Hiding, Prohibited Zone, Broadcast, Selective Embedding.

I. INTRODUCTION:

In two major ways the data hiding in video sequences is performed: bit stream-level and data-level. The redundancies within the current compression standards are exploited in bit stream level [1] [2] [3]. Typically, for manipulation with the aim of data hiding the encoders have various options during encoding and this freedom of selection is suitable. However, without any significant loss of perceptual quality these methods highly rely on the structure of the bit stream; therefore, they are quite easily broken, and in many cases they cannot survive any format conversion or transcoding. As a result, for fragile applications this type of data hiding methods is generally proposed, such as validation [4] [5]. Data level methods are more robust to attacks and are suitable for a broader range of applications. Despite their fragility, for data hiding applications the bit stream-based methods are still attractive. For hiding data the redundancy in block size selection of H.264 encoding is exploited [6] [7]. The quantization factor and discrete cosine transform (DCT) coefficients are distorted in the bit stream-level is shown in fig 1. However, most of the video data hiding methods utilize uncompressed video data.

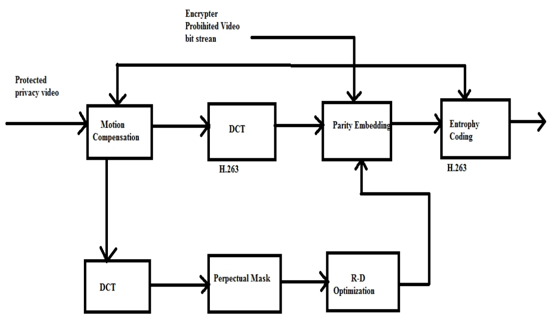


Fig 1: Privacy Preservation using Data Hiding

A high volume transform domain data hiding in MPEG-2 videos is proposed in this paper. Based on MPEG-2 parameters they applied quantization index modulation (QIM) to low frequency DCT coefficients and adapted the quantization parameter [8] [9] [10]. Furthermore, they diverse the embedding rate depending on the kind of the frame. As a result, de-synchronization is caused as insertions and erasures occur at the decoder [11]. To withstand erasures they utilize repeat accumulate (RA) codes in order.

II. FORBIDDEN ZONE DATA HIDING FRAME WORK:

Each frame is processed separately since they adapted the parameters according to type of frame and RA codes are already applied in image data hiding [12] [13]. To handle erasures, the adaptive block selection results in de-synchronization and they utilized RA codes and insertions and erasures can be also handled by convolution codes at embedded. To correct de-synchronization errors multiple parallel Viterbi decoders are used. However, a scheme is successful when the number of selected host signal samples is much less than the total number of host signal samples is observed [14]. To hide data three-dimensional discrete wavelet transform (3-D DWT) domain is used. They do not perform any adaptive selection as they use low-low (LL) sub band coefficients. Therefore, to erasures they do not use error correction codes robust. In order to get rid of local burst of errors the authors performed 3-D interleaving. Additionally, to cope with temporal attacks a temporal synchronization technique is proposed. In this paper, with an additional temporal synchronization mechanism, a new block-based selective embedding type data hiding framework is proposed which encapsulates forbidden zone data hiding (FZDH) and RA codes [14] [15] [16]. To the conventional QIM, a practical data hiding method FZDH is shown to be superior.

III. VIDEO DATA HIDING FRAMEWORK:

The method which incorporates FZDH is a block based adaptive video data hiding is proposed here and shows to be advanced to QIM and aggressive with Distortion-Compensated Quantization Index Modulation (DC-QIM) and removal handling through RA Codes [17] [18]. To determine which host signal coefficients will be used in data hiding are utilized by selective embedding and together we employ block selection and coefficient selection. The de-synchronization due to block selection is handled via RA Codes [19]. By using multi-dimensional form of FZDH in varying dimensions the de-synchronization due to coefficient selection is handled and the frames are processed independently. The intra and inter frames do not yield significant differences is observed here. Therefore, we utilize 3-D interleaving in order to overcome local bursts of error, and use the whole LL sub band of discrete wavelet transform and do not utilize selective embedding. Furthermore, in order to handle frame drop, add, or replicate attacks we provide the method with frame management markers. Hence, to devise a complete video data hiding method that is resistant to de-synchronization due to selective embedding and robust to temporal attacks it can be stated the original contribution of this paper is, while making use of the superiority of FZDH.

IV. RESULTS

Forbidden zone data hiding is observed better than quantization index modulation, in particular at low compression bitrates and minute embedding distortion standards. In common video processing attacks the number of the selected blocks depends on the content and varies slowly with time. The abrupt changes communicate to shot limitations. We detect that embedder and decoder choose different number of blocks.

Interestingly, for small rates the decoder can choose higher number of blocks. In the frame-rate conversion then we examine that different rates have similar results. Frame insertions and drops do not differ as long as they can be detected correctly by synchronization markers. On the other hand, error-free decoding is not possible with the utilized system parameters. One should increase the repetition rate, embedding distortion, or number of frames in order to achieve error-free decoding.

V. CONCLUSION:

A new video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH is proposed in this paper. To frame manipulation attacks via frame synchronization markers this method is also robust. The data hiding method of the proposed framework first we compared FZDH and QIM. Especially for low embedding distortion levels we observed that FZDH is superior to QIM. The framework was tested with MPEG-2, H.264 density, scaling and frame-rate conversion attacks. For error-free decoding typical system parameters are reported. The results indicate that in video data hiding applications the framework can be successfully utilized. A more recent quantization based method is also compared with the proposed framework against the canonical watermarking method JAWS. The results indicate an important advantage over JAWS and an equivalent performance. On the proposed method the experiments also shed light on possible improvements. By using a training set the range of these thresholds can be analyzed. For proper selection of these threshold values some heuristics can be deduced.

REFERENCES

[1] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, “Data hiding in H-v264 encoded video sequences,” in Proc. IEEE 9th Workshop Multimedia Signal Process., Oct. 2007, pp. 373–376.

[2] A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, “Adaptive MPEG-2 video data hiding scheme,” in Proc. 9th SPIE

Security Steganography Watermarking Multimedia Contents, 2007, pp. 373–376.

[3] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding using erasure and error correction," IEEE Trans. Image Process., vol. 13, no. 12, pp. 1627–1639, Dec. 2004.

[4] M. Schlauweg, D. Profrock, and E. Muller, "Correction of insertions and deletions in selective watermarking," in Proc. IEEE Int. Conf. SITIS, Nov.–Dec. 2008, pp. 277–284.

[5] H. Liu, J. Huang, and Y. Q. Shi, "DWT-based video data hiding robust to MPEG compression and frame loss," Int. J. Image Graph., vol. 5, no. 1, pp. 111–134, Jan. 2005.

[6] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: I. Fundamental issues and solutions," IEEE Trans. Image Process., vol. 12, no. 6, pp. 685–695, Jun. 2003.

[7] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: II. Designs and applications," IEEE Trans. Image Process., vol. 12, no. 6, pp. 696– 705, Jun. 2003.

[8] E. Esen and A. A. Alatan, "Forbidden zone data hiding," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 1393–1396.

[9] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. Inform. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.

[10] E. Esen, Z. Do˘gan, T. K. Ates, and A. A. Alatan, "Comparison of quantization index modulation and forbidden zone data hiding for compressed domain video data hiding," in Proc. IEEE 17th Signal Process. Commun. Applicat. Conf., Apr. 2009, pp. 404–407.

[11] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for turbo-like codes," in Proc. 36th Allerton Conf. Commun. Control Comput., 1998, pp. 201–210.

[12] Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding Ersin Esen and A. Aydin Alatan, Member, IEEE.

[13] M. M. Mansour, "A turbo-decoding message-passing algorithm for sparse parity-check matrix codes," IEEE Trans. Signal Process., vol. 54, no. 11, pp. 4376–4392, Nov. 2006.

[14] M. Maes, T. Kalker, J. Haitsma, and G. Depovere, "Exploiting shift invariance to obtain a high payload in digital image watermarking," in Proc. IEEE ICMCS, vol. 1. Jul. 1999, pp. 7–12.

[15] T. Kalker, G. Depovere, J. Haitsma, and M. J. Maes, "Video wa- termarking system for broadcast monitoring," in Proc. SPIE Security Watermarking Multimedia Contents Conf., vol. 3657. 1999, pp. 103– 112.

[16] M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, F. G. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protec- tion," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 47–57, Sep. 2000.

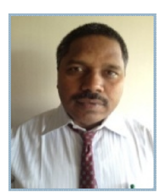
[17] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," IEEE Trans. Circuits Syst. Video Tech- nol., vol. 19, no. 10, pp. 1499–1512, Oct. 2009.

[18] G. Tardos, "Optimal probabilistic fingerprint codes," in Proc. 35th Annu. ACM STOC, 2003, pp. 116–125.

[19] B. Skoric, T. U. Vladimirova, M. Celik, and J. C. Talstra, "Tardos fingerprinting is better than we thought," IEEE Trans. Inform. Theory, vol. 54, no. 8, pp. 3663–3676, Aug. 2008.

BIOGRAPHY

V Radhika has completed B.Sc (Computers) from Sri Venkateswara Degree College, Kodad, Nalgonda, and pursuing MCA in DRK Institute of Science and Technology, JNTU, Hyderabad. Her main research interest includes Data Mining, Information Security & Computer Networks.



Dr.R.V.Krishnaiah, did M.Tech (EIE) from NIT Warangal, MTech (CSE) form JNTU, Ph.D, from JNTU Anantapur, He has memberships in professional bodies MIE, MIETE, MISTE. He is working as Principal in DRK Institute of Science and Technology, Hyderabad. His main research interests include Image Processing, Security systems, Sensors, Intelligent Systems, Computer networks, Data mining, Software Engineering, network protection and security control. He has various publications and presentations in various national and international journals.

