ISSN 2395-1621

Piracy Control by Data Hiding in Video Sequences

Mrigank Sinha [#1], Romil Rajnish[#2],Namrata Ojha [#3], Avinash Walunj[#4]

[1]gsinhamrigank2@yahoo.com
[2]romililu@gmail.com
[3]ojha.namrata2@gmail.com
[4]avishkarwalunj@gmail.com

[#1234] Computer Engineering Department
GHRCEM Pune, India

ABSTRACT

Video data hiding is still an important research topic due to the design complexities involved. We are propose a new video data hiding method that makes use of erasure correction capability of Repeat Accumulate codes and superiority of Forbidden Zone Data Hiding. The selective embedding is utilized in the proposed method to determine host signal samples suitable for data hiding. In this method also contains a temporal synchronization scheme in order to withstand frame drop and insert attacks. Proposed framework is tested by typical broadcast material against MPEG-2, H.264 compression and frame-rate conversion attacks as-well-as other well-known video data hiding methods. Decoding error values are reported for typical system parameters. In the simulation results indicate that the framework can be successfully utilized in video data hiding applications.

Keywords— **Encryption and decryption, Architecture of propose system**

ARTICLE INFO

Article History

Received : 1st April, 2015

Received in revised form :

3rd April, 2015

Accepted : 6th April, 2015

Published online :

8th April 2015

I. INTRODUCTION

A Data hiding is the process of embedding information into a host medium. General, visual and arual media are preferred due to their wide presence and the tolerance of human perceptual systems involved. The general structure of data hiding process does not depend on the host media type the methods vary depending on the nature of such media. Instance of image and video data hiding share many common points; however video data hiding necessitates more complex designs, as result of the additional temporal dimension. Video data hiding continues to constitute an active research area. The data hiding in video sequences is performed in two major ways: bitstream-level and data-level. The bitstream-level, the redundancies within the current compression standards are exploited. Encoders have various options during encoding and this freedom of selection is suitable for manipulation with the aim of data hiding. These methods highly rely on the structure of the bitstream; They are quite fragile, sense that in many cases they cannot survive any format conversion or transcoding is even without any significant loss of perceptual quality. As a result, In this type of data hiding methods is generally proposed for fragile applications, such as authentication. The other hand data-level methods are more robust to attacks. They are suitable for a broader range of applications. Despite their fragility, Bit stream-based methods are still attractive for data hiding applications. For instance, in, the redundancy in block size selection of H.264 encoding is exploited for hiding data. Another approach, the quantization parameter and DCT (Discrete Cosine Transform) coefficients are altered in the bitstream-level. Most of the video data hiding methods utilize uncompressed video data. Starker et. al. proposes a high volume transform domain data hiding in MPEG-2 videos. They can apply QIM to low-frequency DCT coefficients and adapt the quantization parameter based on MPEG-2 parameters. Furthermore, they vary embedding rate depending on the type of the frame. The result, insertions and erasures occur at the decoder, which causes desynchronization. They are utilize Repeat Accumulate (RA) codes in order to withstand erasures. Since adapt the parameters according to type of frame, Every frame is processed separately RA codes are already applied in image data hiding. Adaptive block selection results in de-synchronization and they utilize RA codes to handle

erasures. Insertions and erasures can be handled by convolutional codes as in. The authors use convolutional codes at embedder. The burden is placed on the decoder. Multiple parallel Viterbi decoders are used to correct desynchronization errors. It is observed that such a scheme is successful when the number of selected host signal samples is much less than the total number of host signal samples. In, 3-D DWT domain is used to hide data. They are use to LL subband coefficients and do not perform any adaptive selection. However, they do not use error correction codes robust to erasures. They use BCH code to increase error correction capability. The authors perform 3D interleaving in order to get rid of local burst of errors. Additionally, they propose a temporal synchronization technique to cope with temporal attacks, such like as frame drop, insert and repeat. This paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) and RA codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical video data hiding method, which is shown to superior to the conventional Quantization Index Modulation (QIM). RA codes are already used in the image and video data hiding due to their robustness against erasures. This robustness allows handling desynchronization between embedder and decoder that occurs as a result of the differences in the selected coefficients. In this order to incorporate frame synchronization markers, we are partition into the blocks into two groups. One group is used for frame marker embedding and the other is used for message bits. That means of simple rules applied to the frame markers, Introduce certain level of robustness against frame drop, repeat and insert attacks. We utilize the systematic RA codes to encode message bits and frame marker bits. Each bit is a associated with a block residing in a group of frames. Random interleaving is a performed spatio-temporally; hence, dependency to a local characteristics is reduced. Host signal coefficients used for video data hiding are selected at four stages. The first frame selection is performed. Frames with sufficient number of blocks are selected. Only some predetermined low frequency DCT coefficients are permitted to hide data. The average energy of the block is expected to be greater than a predetermined threshold. In the final stage, energy of each coefficient is compared against another threshold. The unselected blocks is labeled as erasures and they are not processed. For each selected block, there exists variable number of coefficients. These coefficients are used to a embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its base quantizer.

II. DETAILS EXPERIMENTAL

a*1) Literature survey*

Literature survey is the most important step in software development process. Before develop the tool it is necessary to determine the time factor, economy and company strength. These things are satisfied, ten next step is to determine which operating system and language can be used for developing the tool. The programmers start building the tool the programmers need lot of external support. This support can be obtained to senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

Forbidden Zone Data Hiding (FZDH) is introduced. The method depends on the Forbidden Zone (FZ) concept, which is defined to the host signal range where no alteration is allowed during data hiding process. FZDH makes used of FZ to adjust the robustness-invisibility trade-off The mapping function in states that the host signal is modified by adding an additional term, which is scaled version of the quantization difference. In 1-D, this additional term is scalar, whereas in N-D host signal is moved along the quantization difference vector and towards the reconstruction point of the quantizer. Hence, embedding distortion is reduced and became smaller than the quantization error.

In order to fulfil the requirement of mutual exclusion, Reconstruction points of the quantizers that are indexed by different *m* should be non-overlapping, which can be achieved by using a base quantizer and shifting its reconstruction points depending on *m*, similar to Dither Modulation. A typical embedding function that uses a uniform quantizer.

2) Existing System

In special domain is the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods; hide data in another domain such as wavelet domain.

Least significant bit (LSB) is the simplest form of Steganography. The LSB is based on inserting data in the least significant bit of pixels, which lead to slight changes on the cover image that is not noticeable to human eye. This method can be easily cracked, it is the more vulnerable to the attacks.

LSB method has intense affects on the statistical information of image like histogram. Attackers could be aware of a hidden the communication by just checking the Histogram of an image. It is a good solution to eliminate this defect was LSB matching. LSB-Matching is a great step forward in Steganography methods and many others get ideas from it.

3) Proposed System

Data hiding in video sequences is performed in two major ways: bit stream-level and data-level. In this paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH). That means of simple rules applied to the frame markers, Introduce certain level of robustness against frame drop, into repeat and insert attacks.

4) Piracy control

Many video sites are available on internet now a days. To view or download these videos we need to subscribe. But these downloaded videos can be used by others when uploaded on other sites for free. So, to control this piracy, entertainment related companies can use this hiding technique in their web application. The videos on the sites will contain the subscription id of the subscriber which will be known by administrator only if the subscriber is downloading any video. The video will be encrypted by the

subscription id. If the same video is obtained from another site or any other third party we can decrypt the video and find out the subscription id and the subscriber who has done this. So, the accused one will be blocked from that site or some actions can be taken. For example: The tutorials site , channels site can use this application for piracy control.

III. MODULES

1) Input Module

The Input Module is designed as such a way that the proposed system must be capable of handling any type of data formats, If the user wishes to hide any image format then it must be compatible with all usual image formats such as .jpg, .gif and .bmp, it must be also compatible with video formats such as .avi, .flv, .wmf etc.. And also it must be compatible with various document formats, so that the user can be able to the user any formats to hide the secret data.

2) Encryption Module

In Encryption module, it consists of Key file part, where key file can be specified with the password as a special security in it. The user can type the data or else can upload the data also though the browse button, when it is click on the open file dialog box is opened and where the user can select the secret message. After the user can select the image or video file through another open file dialog box which is opened when the cover file button is clicked. The user can select the cover file and then the Hide button is clicked so that the secret data or message is hidden in cover file using Forbidden Zone Data Hiding Technique.

3) Decryption Module

This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then user should select the encrypted cover file and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

4) Des

This module consists of same as Encryption and Decryption part using DES algorithm. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.

5) Triple Des

This module consists of same as Encryption and Decryption part using Triple DES algorithm. Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

6) Rsa

This module consists of same as Encryption and Decryption part using RSA algorithm. RSA is the first algorithm known to be suitable for signing as well as encryption, and it was one of the first great advances in public key cryptography. RSA is widely use in electronic commerce protocols, and it is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

IV. FIGURE

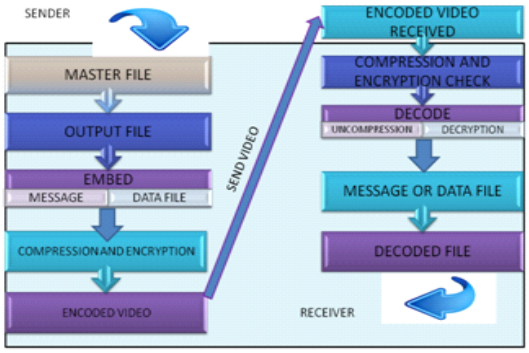

FIG.1 ARCHITECTURE OF PROPOSE SYSTEM

V. CONCLUSION

In this paper, we propose a new video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH. Method is also robust to frame manipulation attacks via frame synchronization markers. First, we compare FZDH and QIM as the data hiding method of the proposed framework. We observe that FZDH is superior to QIM, is a especially for low embedding distortion levels. The framework is tested with MPEG-2, H.264 compression, scaling and frame-rate conversion attacks. Typical system parameters are reported for error-free decoding. Results indicate that the framework can be successfully utilized in video data hiding applications. For instance, Tardos fingerprinting, which is the randomized construction of binary fingerprint codes that are optimal against collusion attack, they can be employed within the proposed framework with the following settings. The minimum segment duration required for Tardos fingerprinting at different operating conditions are given in Table VI. We also compared the proposed framework against the canonical watermarking method, JAWS, and a more recent quantization based method. The results indicate a significant superiority over JAWS and a comparable performance with. The experiments also shed light on possible improvements on the proposed method. Firstly, the framework involves a number of thresholds (*T0*, *T1*, and *T2*), which are determined manually. The range of thresholds can be analyzed by using a training set. Some heuristics can be deduced for proper selection of these threshold values. In additionally, incorporation of Human Visual System based spatio-temporally adaptation of data hiding method parameters as in remains as a future direction.

VI. ACKNOWLEDGEMENT

I wish to express my sincere gratitude to the administration of Department of Computer Engineering of G.H.R.C.E.M, Pune, India. In particular I would like to thank Prof. Sandeep.Gore (G.H.R.C.E.M, Pune) for his invaluable guidance.

REFRENCES

[1] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data Hiding in H- 264 Encoded Video Sequences," in IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007, pp. 373—376.

[2] A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Adaptive MPEG-2 Video Data Hiding Scheme," in Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX, 2007.

[3] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, , and S. Chandrasekaran, "Robust image-adaptive data hiding using erasure and error correction," IEEE Transactions on Image Processing, vol. 13, Dec. 2004, pp. 1627—1639.

[4] M. Schlauweg, D. Profrock, and E. Muller, "Correction of Insertions and Deletions in Selective Watermarking," in IEEE International Conference on Signal Image Technology and Internet Based Systems, SITIS '08, 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. Journal of Image and Graphics, vol. 5, 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 Transactions on Image Processing, vol. 12, pp. 685—695, June 2003.

[7] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video II: Designs and applications," IEEE Transactions on Image Processing, vol. 12, pp. 696—705, June 2003.

[8] E. Esen and A. A. Alatan, "Forbidden zone data hiding," in IEEE International Conference on Image Processing, 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 Transactions on Information Theory, vol. 47, May 2001, pp. 1423-1443, May 2001.

