ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A New Video Data Hiding Using Forbidden Zone Data Hiding

B.Bhavana
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

B.Poojitha
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

C.Premdas
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

M.Naveen Kumar
Assistant Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

ABSTRACT:

Video data hiding is still an important research topic due to the design complexities involved. We 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. Selective embedding is utilized in the proposed method to determine host signal samples suitable for data hiding. This method also contains a temporal synchronization scheme in order to withstand frame drop and insert attacks. The proposed framework is tested by typical broadcast material against MPEG-2, H.264 compression, frame-rate conversion attacks, as well as other well-known video data hiding methods. The decoding error values are reported for typical system parameters. The simulation results indicate that the framework can be successfully utilized in video data hiding applications.

Index Terms:

Data hiding, digital watermarking, forbidden zone data hiding, quantization index modulation, repeat accumulate codes, selective embedding.

Introduction:

Data hiding is the process of embedding information into a host medium. In general, visual and arual media are preferred due to their wide presence and the tolerance of human perceptual systems involved. Although 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. For instance, image and video data hiding share many common points; however video data hiding necessitates more complex designs as a result of the additional temporal dimension.

Therefore, video data hiding continues to constitute an active research area. Data hiding in video sequences is performed in two major ways: bitstream-level and data-level. In bitstream-level, the redundancies within the current compression standards are exploited. Typically, encoders have various options during encoding and this freedom of selection is suitable for manipulation with the aim of data hiding. However, these methods highly rely on the structure of the bitstream; hence, they are quite fragile, in the sense that in many cases they cannot survive any format conversion or transcoding, even without any significant loss of perceptual quality. As a result, this type of data hiding methods is generally proposed for fragile applications, such as authentication. On the other hand, data-level methods are more robust to attacks.

Therefore, they are suitable for a broader range of applications. Despite their fragility, the bitstream-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. In another approach ,the quantization parameter and DCT (Discrete Cosine Transform) coefficients are altered in the bitstream-level. However, most of the video data hiding methods utilize uncompressed video data. Sarkar et. al. proposes a high volume transform domain data hiding in MPEG-2 videos. They apply QIM to low-frequency DCT coefficients and adapt the quantization parameter based on MPEG-2 parameters. Furthermore, they vary the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes desynchronization. They utilize Repeat Accumulate (RA) codes in order to withstand erasures. Since they adapt the parameters according to type of frame, each frame is processed separately RA codes are already applied in image data hiding.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In [3], adaptive block selection results in de-synchronization and they utilize RA codes to handle erasures. Insertions and erasures can be also handled by convolutional codes as in [4]. The authors use convolutional codes at embedder. However, the burden is placed on the decoder. Multiple parallel Viterbi decoders are used to correct desynchronization errors. However, 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 [5], 3-D DWT domain is used to hide data. They use LL subband coefficients and do not perform any adaptive selection. Therefore, they do not use error correction codes robust to erasures. Instead, 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 as frame drop, insert and repeat. In this paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) [8] and RA codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical data hiding method, which is shown to be superior to the conventional Quantization Index Modulation (QIM) .RA codes are already used in 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 order to incorporate frame synchronization markers, we partition the blocks into two groups. One group is used for frame marker embedding and the other is used for message bits. By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks. We utilize systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. Random interleaving is performed spatio-temporally; hence, dependency to local characteristics is reduced. Host signal coefficients used for data hiding are selected at four stages. First, frame selection is performed. Frames with sufficient number of blocks are selected. Next, only some predetermined low frequency DCT coefficients are permitted to hide data.

Then the average energy of the block is expected to be greater than a predetermined threshold. In the final stage, the energy of each coefficient is compared against another threshold. The unselected blocks are labeled as erasures and they are not processed. For each selected block, there exists variable number of coefficients. These coefficients are used to embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its base quantizer.

EXISTING SYSTEM:

- In special domain, 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. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.

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

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).

- By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks.

ADVANTAGES:

1.User cannot find the original data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.It is not easily cracked.

3.To increase the Security .

4.To increase the size of stored data.

5.We can hide more than one bit.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Main Modules:-
MODULES:

- Input Module :
- ENCRYPTION MODULE
- DECRYPTION MODULE
- DES
- Triple DES
- RSA

Modules Description:
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, such as if the user wishes to hide any image format then it must be compatible with all usual image formats such as jpg, gif, 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 user any formats to hide the secret data.

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. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then 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. Where 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.

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 the 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.

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.

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.

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 was one of the first great advances in public key cryptography.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

Module I/O:
Module Input:

We give original content as input with watermark data embedding. We view flipping an edge pixel in binary images as shifting the edge location one pixel horizontally and vertically.

Module Output:

The output of the project is we reconstruct the pixel horizontally and vertically .we can see the original watermarked data and embedding content.

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. The 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, 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.

The results indicate that the framework can be successfully utilized in video data hiding applications. For instance, Tardos fingerprinting [18], which is a randomized construction of binary fingerprint codes that are optimal against collusion attack, can be employed within the proposed framework with the following settings. The length of the Tardos fingerprint is ln where A is a function of false positive probability false negative probability, and maximum size of colluder coalitionThe 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 these thresholds can be analyzed by using a training set. Then some heuristics can be deduced for proper selection of these threshold values. Additionally, incorporation of Human Visual System based spatio-temporally adaptation of data hiding method parameters as in remains as a future dire.

10. BIBLIOGRAPHY:

Good Teachers are worth more than thousand books, we have them in Our Department.

References Made From:

[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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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,.

[10] E. Esen, Z. Doğan, T. K. Ates, and A. A. Alatan, "Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding,"in IEEE 17th Signal Processing and Communications Applications Conference SIU, 2009.

[11] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for turbolike codes," in Proc. 36th Allerton Conf. Communications, Control, and Computing, 1998, pp. 201—210.

[12] M. M. Mansour, "A Turbo-Decoding Message-Passing Algorithm for Sparse Parity-Check Matrix Codes," IEEE Transactions on Signal Processing, vol. 54, pp. 4376—4392, Nov. 2006.

[13] Z. Wei, K. N. Ngan, "Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19,pp. 337—346, Mar. 2009.

[14] M. Maes, T. Kalker, J. Haitsma, and G. Depovere, "Exploiting Shift Invariance to Obtain a High Payload in Digital Image Watermarking," in IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), vol. 1, 1999.

[15] T. Kalker, G. Depovere, J. Haitsma, and M. J. Maes, "Video watermarking system for broadcast monitoring," in Security and watermarking of multimedia contents Conference, SPIE Proceedings vol. 3657 , 1999, pp. 103—112.

[16] M. Maes, T. Kalker, J. -P. M. G., J. Talstra, F. G. Depovere, and J. Haitsma, "Digital watermarking for DVD video copy protection," IEEE Signal Processing Magazine, vol. 17, pp. 47—57, Sep. 2000.

[17] K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, pp. 1499—1512, Oct. 2009.

[18] G. Tardos, "Optimal probabilistic fingerprint codes," in Proceedings of the thirty fifth annual ACM symposium on Theory of computing (STOC '03), New York, NY, USA, 116—125.

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