ISSN: 0975-5662, July, 2015 www.ijrct.org

An Adapted Approach for Robust Blind Data Hiding In Forbidden Zone Concept

P.Sridevi[1], M.TechComputer Science &EngineeringE-mail: polishety.sridevi@gmail.com
Dr.Siddharthaghosh[2], Professor, Department of CSE, E-mail: profsiddhartha@gmail.com
Keshav memorial institute of technology, Narayanguda, Hyderabad, Telangana, India.

Abstract

The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. Secure Video Data Hiding is an important research topic due to design complexities involved.Hence substantial effort is required in order to design and develop such systems. Design of a complete video data hiding application constitutes the main motivation of this paper.This paper proposesa new framework for video data hiding that makes use of superiority of Forbidden Zone Data Hiding concept, cryptographic security provided by chaotic encryptionand erasure correction capability of Repeat Accumulate codes. Selective embedding is utilized in the proposed method to determine host signal coefficients used for data hiding. This framework alsocontains a sequential management scheme in order to withstand frame drop and insert attacks.Thus this proposed framework helpsin developing a more secure and robust complete video data hiding system which can be successfully utilized in video data hiding applications.

Index Terms: Video data hiding, Data hiding, secure video data hiding, Forbidden zone data hiding, Selective embedding.

1. INTRODUCTION

Data hiding is essentially a communication system, in which some data is conveyed within a host medium and transmitted to the receiver. There are four main requirements of a typical data hiding system: Imperceptibility, robustness, capacity, and security. The degree of importance of any requirement depends on the type of the application. Some applications may not request some of these basic requirements, except imperceptibility, which is indispensable for most of the data hiding applications.

Data hiding is the process of imperceptibly embedding some information into a host medium. Since the early ages, data hiding is used for mainly secret communication. In the modern age, emergence of the new media types and novel needs resulted in the revival of the data hiding field. As a result of lot of works in the last twenty years, data hiding field has reached to a certain level of maturity and hence, the developed framework can be applied to many different areas. 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. The reason behind the video cover in this approach is due to the huge amount of single frame images per sec. Furthermore, with the development of multimedia and stream media on the Internet, transmitting video on the Internet will not incur any suspicion. Besides, the degradation of video quality cannot be observed by naked eyes, for it may be aroused sometimes by video compression of lower quality 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 dimensions.Therefore, video data hiding continues to constitute an active research area.

2. PROBLEM STATEMENT

Four main requirements are needed for a typical data hiding system: imperceptibility, robustness, capacity, and security. Imperceptibility means there should not be any perceptual degradation due to data hiding. Robustness is the dependability and strength of a data hiding system after certain attacks, in terms of correctly decoding the hidden data. The amount may range from one bit to millions of bits, which depends on the application. Capacity refers to the feasible number of message bits that can be hidden in the host signal.In case of security,for some applications it may be crucial. In that case, algorithms should secure the hidden data so that adversaries can not intrude or interfere by any means. The degree of importance of any requirement depends on the type of the application. The proposed application aims at satisfying these four requirements.This paper proposes a new secure framework for video data hiding that makes use of superiority of Forbidden Zone Data Hiding concept, cryptographic security provided by chaotic encryption and erasure correction capability of Repeat Accumulatecodes.Selective embedding is utilized in the pro-posed method to determine host signal coefficients used for data hiding. This framework also contains a sequential management scheme in order to withstand frame drop and insert attacks.

3. RELATED WORK

With respect to host signal domain, datahiding in video sequences is performed in twomajor ways: bitstream level and data level. InBitstream level, the redundancies within thecurrent compression standards are exploited.Typically, encoders have various optionsduring encoding and this freedom of selectionis suitable for manipulation with the aim of data hiding. However, these methods highlyrely on the structure of the bitstream; hencethey are quite fragile; in the sense that in manycases, they cannot survive any formatconversion or transcoding even without anysignificant loss of perceptual quality. As aresult, this type of data hiding methods isgenerally proposed for fragile applications,such as authentication. On the other hand, datalevel methods are more robust to attacks.Therefore, they are suitable for a broader range of applications. On the other hand, datalevel 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 attractivefor data hiding applications. However, most ofthe video data hiding methods utilizeuncompressed video data. A system proposesa high volume transform domain data hidingin MPEG-2 videos.

They apply QIM to lowfrequencyDCT coefficients and adapt thequantization parameter based on MPEG-2parameters. Furthermore, they vary theembedding rate depending on the type of theframe. As a result, insertions and erasuresoccur at the decoder, which causes desynchronization.They utilize RepeatAccumulate (RA) codes in order to withstanderasures. Since they adapt the parametersaccording to type of frame, each frame isprocessed separately. RA codes are alreadyapplied in image data hiding. In adaptiveblock selection results in de-synchronizationand they utilize RA codes to handle erasures.Insertions and erasures can be also handled byconvolution codes.Multiple parallel decodersare used to correct de-synchronization errors.However, it is observed that such a scheme issuccessful when the number of the selectedhost signal samples is much less than the totalnumbers of host signal samples.

Forbidden Zone Data Hiding:

Forbidden zone data hiding (FZDH) is introduced the method depends on the forbidden zone (FZ) concept,which is defined as the host signal range where no alteration is allowed during data hiding process. FZDH makes use of FZ to adjust the robustness-invisibility tradeoff. Several techniques have been proposed in the literature that hides information in images and video in a robust and transparent. With the appropriate private key, the scrambling can be undone to retrieve the original. The drawback of these techniques is that it cannot be used with any other video modification techniques besides scrambling. They applied quantization index modulation (QIM) to low frequency DCT coefficients and adapted the quantization parameter based on MPEG-2 parameters. Furthermore, they varied the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes de-synchronization. They utilized repeat accumulate (RA) codes in order to withstand erasures. RA codes are already applied in image data hiding. In adaptive block selection results in de-synchronization and they utilized RA codes to handle erasures. Insertions and erasures can be also handled by convolution codes. The authors used convolution codes at embedded. However, the burden is placed on the decoder.

4. IMPLEMENTATION

4.1 Selective Embedding:

Host signal samples, which will be used in data hiding, can be determined adaptively by the method proposed. The selection is performed at four stages: frame selection, frequency band determination, block selection, and coefficient selection.

1) Frame selection: selected number of blocks in the whole frame is counted. If the ratio of selected blocks to all blocks is above a certain value,then the frame is processed. Otherwise, the frame is skipped.
2) Frequency band: only certain DCT coefficients are utilized.Middle frequency band of DCT coefficients shown in Fig. 1 is utilized similar to.
3) Block selection: energy of the coefficients in the mask is computed. If the energy of the block is above a certain value then the block is processed. Otherwise, it is skipped.
4) Coefficient selection: energy of each coefficient is compared to another threshold. If the energy is above

the particular threshold, then it is used during data embedding together with other selected coefficients in the same block.

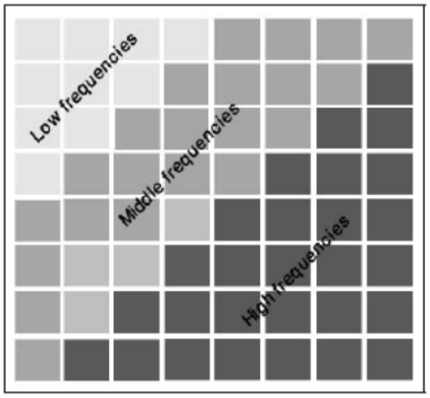

Fig. 1. Low, Middle, and High frequency distribution in a DCT block

4.2 Chaotic Encryption:

Large data size, computational complexity and re-al time constraints make encryption of multimedia data difficult.This makes chaotic scrambling of an image more desirable when compared to conventional encryption algorithms. Many methods have been put forth to perform image encryption using Chaotic Neural Networks. In this paper,chaotic image encryption called the "Triple Key" method is used. In this method, it is required to enter an 80-bit session key in addition to the initial parameter key and the control parameter key. Each of the keys forms just one part of the lock that needs to be opened to obtain the original image.

The position of bits in the 80-bit key determines the scrambling of individual pixels in the encrypted image. Results reveal a very low Correlation coefficient between adjacent pixels in the encrypted image which implies higher security and lower probability of security breach through brute force attacks or statistical analysis. The method is called "Triple-key" because it provides a three-fold protection to the original image and three keys have to be entered in the correct order for decrypting the image. Triple key method of encryption also imparts sufficient amount of confusion and diffusion.The highly un-predictable and random-look nature of chaotic out-put is the most attractive feature of deterministic chaotic system that may lead to various novel applications.

4.3 Erasure Handling:

RA codes are serially concatenated codes consisting of a Repetition Code as the outer code and an Accumulator as the inner code with a pseudorandom interleave in between them. The repetition code is defined as a (n,m) code where each message bit is repeated q times and thus n = q.m. The accumulator can be viewed as a truncated rate-1 recursive convolution encoder with transfer function 1/(1+D).Due to adaptive block selection, de-synchronization occurs between embedded and de-coder. As a result of attacks or even embedding operation decoder may not perfectly determine the selected blocks at the embedder. In order to overcome this problem, error correction codes resilient to erasures, such as RA codes are used in image and video data hiding in previous efforts.

5.PROPOSEDVIDEODATAHIDING FRAMEWORK

In the proposed framework,a block based secure video data hiding method is proposed. It incorporates FZDH,provides cryptographic security by chaotic encryption and erasure handling through RA codes. The de-synchronization due to block selection is handled via RA Codes.Frame synchronization markers are equipped in order to handle frame drop,insert, or repeat attacks.The framework for embedder. Y-channel is utilized for data embedding. Steps for achieving a robust framework as proposed by authors are utilized in this framework.In the first step, frame selection is performed and the selected frames are processed block-wise. For each block, only a single bit is hidden. This is for decreasing the embedding distortion.After obtaining 8 by 8 DCT of the block, energy check is performed on the coefficients that are predefined in a mask. Selected coefficients of variable length are used to hide data bit m.

Data Extraction and Decryption

Authenticated users are only allowed to extract the message.Decoder is the dual of the embedder, with the exception that frame selection is not per-formed marked frames are detected by frame synchronization markers.Received video is de-coded to a sequence of frames, from which decoding (of the embedded encrypted data per frame) is performed iteratively.Fig. 2 shows the decoder framework.For message decryption,chaotic decryption process is performed.

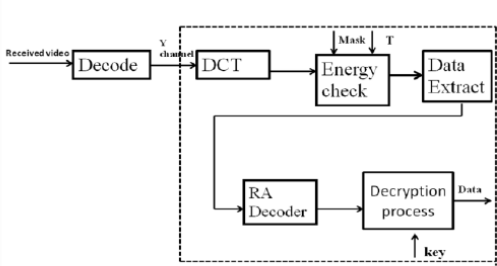

Fig. 2Decoder flowchart of the proposed video data hiding framework

6. CONCLUSION

In the Steganography, DCT method is an efficient steganographic method for embedding the secret message into cover video without producing any changes of quality of video. In this work, this is a new way of hiding the information in a video with more security. The framework incorporates Forbidden Zone Data Hiding,chaotic encryption, selective embedding,erasure handling and temporal synchronization.Incorporation of forbidden zone data hiding and selective embed-ding makes the framework more robust. FZDH is a practical data hiding method, which is shown to be superior to the conventional methods. Host signal samples, which will be used in data hiding, are determined adaptively by selective embedding. Using video as the cover file helps to solve the capacity issue to a big extent.Incorporation of chaotic encryption in the framework helps us to increase security. Error correction coding is implemented in order to obtain an error-free framework for various common attacks. Also the system handles desynchronization between embedder and decoder.Thus the paper proposes a secure video data hiding framework which can be utilized in video data hiding applications.

REFERENCES

[1] M. Suresh Kumar, G. MadhaviLatha, “DCT Based Secret Image Hiding In Video Sequence”, Int. Journal of Engineering Research and Applications, August 2014, Vol. 4, Issue 8(Version 1), ISSN: 2248-9622.

[2] R. Ravi Kumar,V. Kesav Kumar, “Selective Embedding & Forbidden Zone Data Hiding For Strong Video Data Thrashing”, International Journal Of Engineering and Technology,Sep-2013,Volume 4,issue 9,ISSN:2231-5381.

[3] V. Priya, “Reversible Information Hiding In Videos”, International Journal Of Innovative Research in Computer and Communication Engineering, March-2014, vol 2, special issue 1, ISSN: 2320-9801

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

[5] H. Liu, J. Huang, and Y. Q. Shi, “DWT-basedvideo data hiding robust to MPEGcompression and frame loss,” Int. J. ImageGraph., vol. 5, no. 1, pp. 111–134, Jan. 2005.

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

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

[8] E. Esen and A. A. Alatan, “Forbidden zonedata hiding,” in Proc. IEEE Int. Conf. ImageProcess., Oct. 2006, pp. 1393–1396.

[9] E. Esen and A. A. Alatan, “Forbidden zone datahiding,” in Proc. IEEE Int. Conf. Image Process., Oct.2006, pp. 1393–1396.

[10] M. Wu, H. Yu, and B. Liu, “Data hiding in image andvideo: II. Designs and applications,” IEEE Trans. ImageProcess., vol. 12, no. 6, pp. 696– 705, Jun. 2003.

[11] Z. Wei and K. N. Ngan, “Spatio-temporal justnoticeable distortion profile for grey scale image/video inDCT domain,” IEEE Trans. Circuits Syst. Video Technol.,vol. 19, no. 3, pp. 337–346, Mar. 2009.

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

P.Sridevi receivedB.Tech from JNTU University, Hyderabad. She is currently pursuing M.Tech in Computer Science & Engineering Department, Keshav Memorial Institute of Technology, Narayanguda, Hyderabad,Telangana, India-500029

Prof Dr.Siddharthaghosh received Dr. from Osmania University Hyderabad 2011 in artificial intelligence, currently he is working as a Head of the department of computer science&engineering at keshav memorial institute of technology Narayanguda, Hyderabad ,Telangana, India-500029