International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013
ISSN 2229-5518

A Modified Framework For Secure And Robust Blind Data Hiding In Videos Using Chaotic Encryption And Forbidden Zone Concept

Neethu Mathai,Sherly K.K

Abstract— Video data hiding is an important and emerging research area due to the design complexities involved.It has found usage in a great number of applications.. Various aspects are required for a complete system, however most of the works deals with only certain parts of the problem. A complete application should take into account robustness,capacity,security,error correction, human visual system adaptation and similar issues. Hence substantial effort is required inorder to design and develop such systems. Design of a complete video data hiding application constitutes the main motivation of this paper. This paper proposes a new 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 Accumulate codes . Selective embedding is utilized in the proposed 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. Thus this proposed framework helps in 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,chaotic encryption,security

1 INTRODUCTION

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 opting 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 necessiates more complex designs,as a result of the additional temporal dimensions.Therefore, video data hiding continues to constitute an active research area.

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 Accumulate codes.Selective embedding is utilized in the proposed 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.

2. RELATED WORK

Several techniques have been proposed in the literature that hide information in images and video in a robust and transparent fashion([1]–[3]). Authors in [4] and [5] scrambles the pixels of the specific image objects for privacy protection. 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. Sarkar *et al.* [6] proposed a high volume transform domain data hiding in MPEG-2 videos.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 [7], adaptive block selection results in de-synchronization and they utilized RA codes to handle erasures. Insertions and erasures can be also handled by convolutional codes as in [8]. The authors used convolutional codes at embedder. However, the burden is placed on the decoder. In [9], 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.

In the video data hiding method[10],a new robust video data hiding framework using forbidden zone concept and selective embedding is proposed .Selective embedding is utilized in the framework to determine host signal coefficients used for data hiding.The framework also consists of a sequential management scheme in order to withstand frame drop and insert attacks.But the framework does not focuss on security applications.

3. METHODOLOGIES IN PROPOSED SCHEME

A. Fordidden Zone Data Hiding

Forbidden zone data hiding (FZDH) is introduced in [11].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. Let s (bold denoting a vector) be the host signal in R^N and mC{0, 1} be the data to be hidden. Then the marked signal is obtained as given in

$$x = \begin{cases} s, & s \in FZ_m \\ M_m(s), & s \in AZ_m \end{cases} \quad (1)$$

where FZ_m, allowed zone (AZ_m) pair defines the host signal zones where alteration is allowed or not and $M_m(.)$ is a mapping from R^N to a suitable partition of R^N. The requirement on these zones and partitions is simply based on the constraint that they should be mutually exclusive for different m.

The key point of FZDH is the determination of the zones and the partitions. There could be infinite ways to achieve this; however, a practical design can be performed by using quantizers.

B. Selective Embedding

Host signal samples, which will be used in data hiding,can be determined adaptively by the method proposed in [10]. 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 [6].

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.

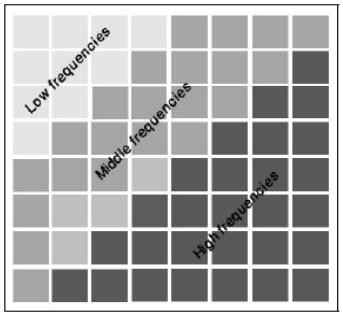

Fig. 1. Low, Middle, and High frequency distribution in a DCT block

C. Chaotic Encryption

Large data size, computational complexity and real 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 [14] 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 unpredictable and random-look nature of chaotic output is the most attractive feature of deterministic chaotic system that may lead to various novel applications.

The three main steps of Triple Key Chaotic Image encryption are:

1. Forming the Binary Image Matrix:
   Input the image.Then the two-dimensional image vector is converted to a one-dimensional vector. Each pixel value is converted to its corresponding binary value.
2. Computing the Initial Parameter:
   The session key K consisting of 20 hexadecimal characters.If less than required amount,then padded with zeroes. Each hexadecimal character in the session key is converted into its binary equivalent of four bits so that session key consists of 80 bits. Then X01 and X02 are computed and initial parameter X(1) is computed when the user enters key X03.
3. Generating a Chaotic Sequence:

The Chaotic sequence X1 X2 X3….XN where N is the number of pixels in the image is generated and are normalized to the image scale.

Decryption procedure is same as the encryption procedure, but takes place only when the session key, initial parameter X(l) and control parameter are correctly entered and generated.

D. Erasure Handling

RA codes[11] are serially concatenated codes consisting of a Repetition Code as the outer code and an Accumulator as the inner code with a pseudorandom interleaver 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 convolutional encoder with transfer function 1/(1+D).

Due to adaptive block selection, desynchronization occurs between embedder and decoder. 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 [6] and video [7] data hiding in previous efforts.

RA code is a low complexity turbo-like code. It is composed of repetition code, interleaver, and convolutional encoder. Fig. 2 shows the encoder structure of a RA encoder. The source bits (u) are repeated R times and randomly permuted depending on a key. The interleaved sequence is passed through a convolutional encoder with a transfer function 1/(1 + D), where D represents a first-order delay. Systematic encoding is used in this encoder structure where the message bits are also transmitted across the channel.

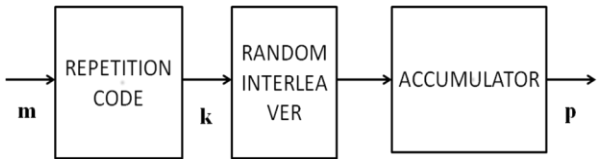

Fig. 2. Encoder of an RA code

E. Frame Synchronization Markers

Each frame within a group of *T* consecutive frames is assigned a local frame index starting from 0 to $T-1$. These markers are used to determine the frame drops, inserts and repeats, as well as the end of the group of frames.

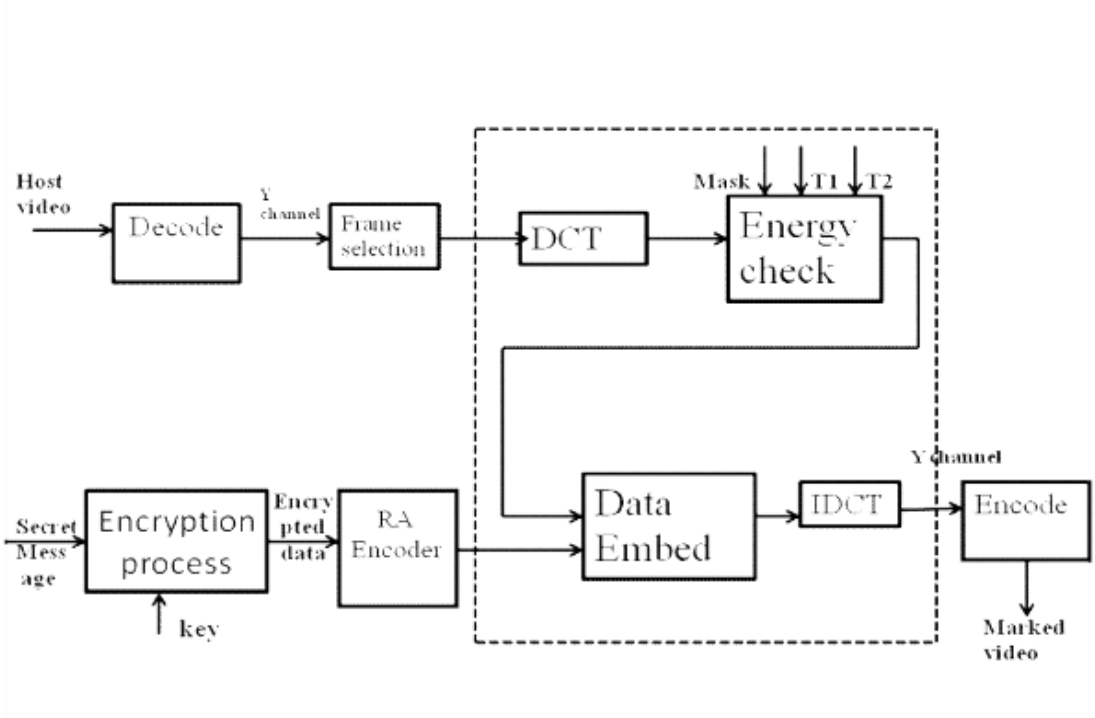

Fig. 3. Embedder flowchart of the proposed video data hiding framework

4. PROPOSED VIDEO DATA HIDING 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 as in [6] and [7].Frame synchronization markers are equiped in order to handle frame drop,insert, or repeat attacks.The framework for embedder is shown in Fig 3.

Y-channel is utilized for data embedding. Steps for achieving a robust framework as proposed by authors in [10] is 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.For increasing the security,encrypted message file obtained is given for embedding. After the inverse transform host frame is obtained.

Decoder is the dual of the embedder, with the exception that frame selection is not performed. Fig. 3 shows the flowchart for a single frame. Marked frames are detected by using frame synchronization markers. After selecting the marked frames,encrypted data is retrieved.This encrypted data when fed to the chaotic decryption process, the original secret file is obtained.Decoder employs the same system parameters and determines the marked signal values that will be fed to data extraction step.

Various stages in the framework can be divided into:
1.Video Acquisition
2.Data Encryption
3.Hiding of Encrypted data
4. Data Decrypting &Extracting phase

An authentication for login and logout the system makes system more secure and robust. So authentication is included.The only authorized user can hide and disclose the message which makes the system more secure and robust.

Video Acquisition

A video file consist of several image sequences, so considering the data hiding technique of image will also apply for video data hiding. Generally we consider a larger clip for the embedding purpose. Video segmentation is a very important step for the efficient secret data embedding. This is due to the fact that a digitized movie video data can be several gigabytes in size.Input video is decompressed at first into a sequence of frames.Then particular frames are selected from the sequence of frames in two stages.First,blocks with high energy are selected and such selected blocks in the whole frame is counted.If the ratio of such selected blocks to whole blocks is above a certain value(T0),then frame is processed.Data is embedded in the luminance (Y) component only.Y component is selected because it undergoes less compression and least likely to be damaged. Here the Selective Embedding in Coefficients" (SEC) scheme for hiding is employed.

The system parameters are tuned manually.The proposed framework utilize the following experimentally proven values[10] during the experiments: T0 = 0.05, T1 = 1000, T2 = 500, T = 3. One should note that threshold values are selected for the test video at 9 Mbps with resolution 720 by 576 and block size 8 by8. Different dimensions might require some other threshold values.

Data Encryption

After completion of login process, the User Selects the Carrier (Cover) File in which the message is to be hide. Then user selects the message file and enters a password to the message file. This password is used as the secret key for encryption Steganography by itself does not ensure secrecy, but neither does simple encryption. If these methods are combined, however, stronger encryption methods result. If a message is encrypted and then embedded in an image , video, or voice, it becomes even more secure. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message..But with steganography, the interceptor may not know that a hidden message even exists.

Data Embedding

The selected frames are then converted from spatial domain to frequency domain. Hiding data in DCT makes the data more secure by minimizing perceptual distortion. DCT seperates images into parts according to its visual importance. 8 by 8 DCT of blocks in the selected frames are obtained In the next step,we are performing energy check inorder to select some particular blocks and coefficients for data embedding purpose.By energy check,we get certain blocks.The middle frequency components in the selected blocks are then chosen for data embedding.It is because they avoid most visual important parts of the image(low frequencies).Also does not overexpose themselves to removal through compression(high frequencies).

Block selection and Coefficient selection are done by energy checks. In Block selection ,energy of the coefficients in the mask(middle frequency band) is computed. If the energy of the block is above a certainvalue (T1) then the block is processed.In Coefficient selection, energy of each coefficient is compared to another threshold T2. If energy is above T2, then it is used during data embedding. Selected coefficients in the block of variable length are used to hide encrypted data bit *m.*

Each selected frame is assigned a local frame index starting from 0 to $T-1$.Markers are used to determine the frame drops, inserts and repeats, as well as the end of the group of frames. Markers thus prevents temporal attacks and thus increases robustness of system.

Channel noise may cause desynchronization at the decoder. Error resilence is added by Repeat Accumulate Codes codes and modified frames are then converted into MPEG-2 videos.Systematic RA encoding is used here.In systematic encoding message bits form part of the codeword and are then transmitted.In non-systematic encoding,message bits do not form part of the codeword and hence are not transmitted.

Algorithm of RA Encoder:

1. Take K source bits.
   s1s2s3 ……sK
2. Repeat each bit three times, giving N = 3K bits.
   s1s1s1s2s2s2s3s3s3……sKsKsK
3. Permute these N bits using a random permutation (same for every codeword). Call the permuted string as u.
   u1u2u3u4u5u6u7u8u9…..uN
4. Transmit the accumulated sum.
   t1 = u1
   t2 = t1 + u2 (mod 2)…

. **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 performed Marked frames are detected by frame synchronization markers. Received video is decoded to a sequence of frames, from which decoding (of the embedded encrypted data per frame) is performed iteratively. Fig. 4 shows the decoder framework.

For message decryption, chaotic decryption process is performed .

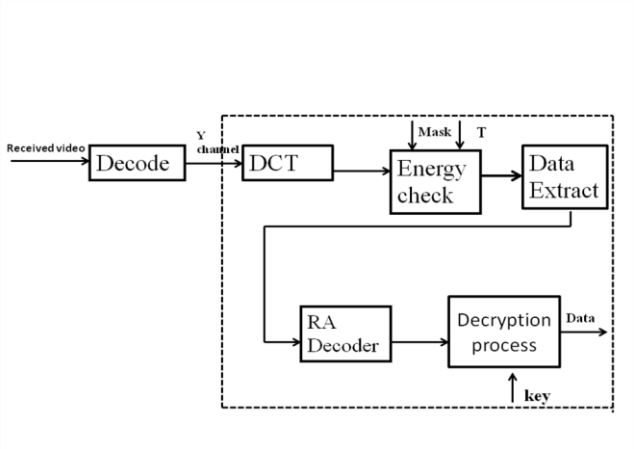

Fig. 4. Decoder flowchart of the proposed video data hiding framework

5. RESULTS AND ANALYSIS

An optimal test for the proposed technique is done .The full framework was successfully implemented in Matlab.The proposed embedding scheme is tested on video clips. Experimental results show that: 1) The proposed technique improves the robustness of the video. (2) The video is visually similar in quality to the original 3) Method also provides security against certain cryptographic attacks. Figure 5(a) and 5(b) shows the image frames from the video before and after embedding the required data.A database of small size video clips was used to conduct the experiments.. In all the experiments peak-to-signal noise ratio (PSNR) was used as a comparison metric. It is found that there was no human eye perceptible difference in the resulting image frames. The stego-video was passed through internet to a specified user. The file was completely recovered with no errors.

6. CONCLUSION

Video Steganography deals with hiding secret data or information within a video.Four main requirements are needed for a typical data hiding system: imperceptibility, robustness, capacity, and security.The proposed application aims at maximizing these four requirements. The framework incorporates Forbidden Zone Data Hiding,chaotic encryption, selective embedding,erasure handling and temporal synchronization.Incorporation of forbidden zone data hiding and selective embedding 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.

Fig. 5(a) Four consecutive video frames before embedding

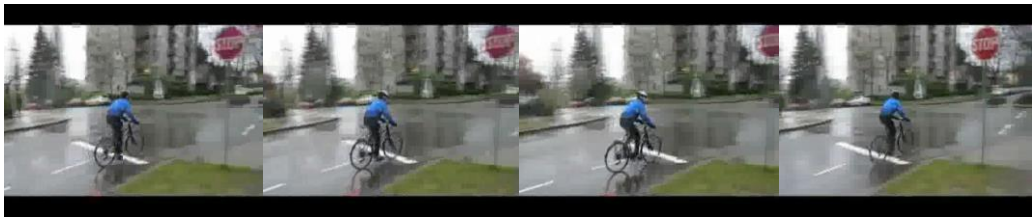

Fig. 5(b) Four consecutive video frames after embedding data

REFERENCES

[1]M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," Proc. IEEE, vol. 86, pp. 1064–1087, Oct. 1998.

[2]F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Oct. 1999.

[3]R. B.Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," Proc. IEEE, vol. 87, pp. 1108–1126, Oct.1999.

[4]T. E. Boult, "Pico: Privacy through invertible cryptographic obscuration,"in Computer Vision for Interactive and Intelligent Environments - the Dr.Bradley D. Carter Workshop Series, 2005.

[5]F. Dufaux and T. Ebrahimi, "Scrambling for video surveillance witprivacy," 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), p. 160, 2006.

[6]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.

[7]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

[8]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.

[9]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.

[10]E. Esen and A. A. Alatan,"Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding",Ieee Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 8, August 2011

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

[12]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.

[13]Wang Shou-Dao, Xiao Chuang-Bai, Lin Yu,"A High Bitrate Information Hiding Algorithm for Video in Video",World Academy of Science, Engineering and Technology 35 2009

[14]Srividya.G, Nandakumar.P, "A Triple-Key Chaotic Image Encryption Method", in Proc. IEEE Int. Conf. ICCSP, Feb.2011