Implementation of RIDH And FZDH Algorithm to hide data in video over encrypted domain via key modulation :Comparison of RIDH and FZDH Algorithm

Shweta Gangawane[1], Akshata Inamdar[2], Ketaki Kate[3], Madhavi Kunte[4], Mrs.Rohini Pise[5]
[1, 2, 3, 4, 5] Department of Information Technology
[1, 2, 3, 4, 5] Pimpri Chinchwad College Of Engineering

Abstract- *We present a novel reversible image data hiding scheme and FZDH over encrypted domain .Data embedding is achieved through a public key modulation mechanism. At the decoder side, a powerful two-class SVM classifier is designed to distinguish encrypted and non encrypted image patches. [1]Implementation of FZDH and RIDH algorithms on video and compare which algorithm works better*

Keywords- RIDH, FZDH , SVM , Public key modulation

I. INTRODUCTION

RIDH

A method for reversible image data hiding comprising: encrypting an original image by an encryption process to generate an encrypted image, embedding a message into the encrypted image by an embedment process to generate an embedded image, and extracting the message and the original image from the embedded image by a decryption and extraction process. The encryption process including: generating a key stream by using a secret encryption key, and generating an encrypted image by XORing the original image with the key stream.[2] The embedment process including: generating an embedded image by embedding the message via XORing the encrypted image with a predetermined public key set.

A method for reversible image data hiding comprising: encrypting an original image by an encryption process to generate an encrypted image, where in the encryption process including:

Generating a key stream by using a secret encryption key; and generating an encrypted image by XORing the original image with the key stream;embedding a message into the encrypted image by an embedment process to generate an embedded image, wherein the embedment process including: generating an embedded image by embedding the message via XORing the encrypted image with a predetermined public key set; and extracting the message and the original image from the embedded image by a decryption and extraction process, wherein the decryption and extraction process including: generating a decrypted image by XORing the embedded image with the key stream; and generating the message and the original image by XORing the decrypted image with the public key set.

The method of , wherein generating the embedded image by embedding the message via XORing the encrypted image with the predetermined public key further comprises: dividing the encrypted image into encrypted blocks; extracting the message into bits of the message;finding a public key of the public key set associated With each of the bits of the message; and [1]XORing each of the public keys with each of the encrypted blocks to generate embedded blocks.

The method of , wherein generating the embedded image by embedding the message via XORing the encrypted image with the predetermined public key further comprises: Performing XORing each of the public keys with each of the encrypted blocks to generate the embedded blocks until all of the bits of the message are embedded; and assembling the embedded blocks to generate the embedded image.

The method of , wherein generating the message and the original image by XORing the decrypted image with the public key set further comprises: dividing the decrypted image into decrypted blocks; creating decoding candidates by XORing the decrypted blocks with each public key of the public key set; and identifying which of the decoding candidates are original blocks of the original image by determining the bits of the message through a classifier[4].

The method of , wherein generating the message and the original image by XORing the decrypted image with the public key set further comprises: detecting and correcting errors according to property of non-local image similarity; assembling the bits of the message to generate the message; and assembling the original blocks of the original image to generate the original image.

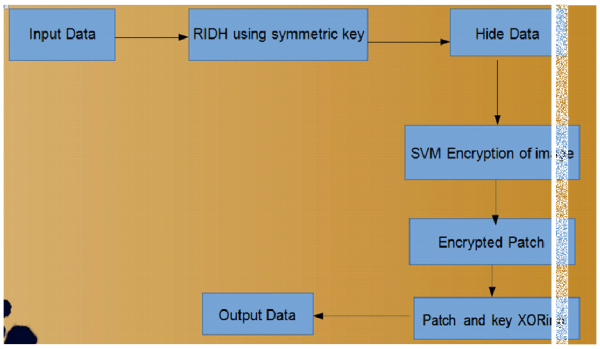

Figure 1. Proposed system architecture

FZDH

Forbidden Zone :

It is defined as the host signal range where no alteration is allowed during data hiding process.

Selective Embedding :

Here host signal samples, which will be used in data hiding,are determined adaptively. The selection is performed at four stages:

1. Frame selection .
2. Frequency band determination.
3. Block selection.
4. Co-efficient selection.

During encryption frame selection is performed and the selected frames are processed blockwise. In this paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH)[2] 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 de synchronization between embedded 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.

Embedding Operation :

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. After obtaining 8 × 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. m is a member of message bits or frame synchronization markers. Message sequence of each group is obtained by using RA codes for T consecutive frames. Each block is assigned to one of these groups at the beginning. After the inverse transform host frame is obtained.

Selective Embedding :

Host signal samples, which will be used in data hiding, are determined adaptively. 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 (T0) the frame is processed. Otherwise, this frame is skipped[3].
2) Frequency band: only certain DCT coefficients are utilized. Middle frequency band of DCT coefficients.
3) Block selection: energy of the coefficients in the mask is computed. If the energy of the block is above a certain value (T1) then the block is processed. Otherwise, it is skipped.
4) Coefficient selection: energy of each coefficient is compared to another threshold T2. If the energy is

above T2, then it is used during data embedding together with other selected coefficients in the same block.

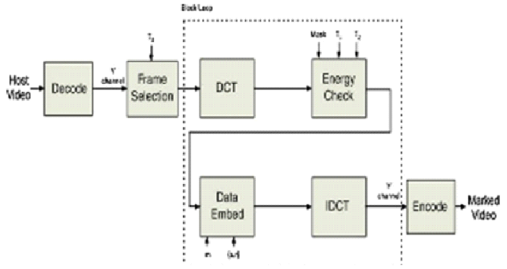

Figure 2. Embedded Flowchart Of The Proposed Video Data Hiding Framework For A Single Frame.

Processing :

- Frame broken into blocks.
- DCT is applied to each frame.
- Frame is compressed using quantization .
- Data stored in reduced space.

2. Embedding : It has following stages

- Frame selection.
- DCT.
- Energy Check.
- Embedding of data.

Decoder Information :

Decoder is the dual of the embedded, with the exception that frame selection is not performed. Marked frames are detected by using frame synchronization markers. Decoder employs the same system parameters and determines the marked signal values that will be fed to data extraction step. Non-selected blocks are handled as erasures. Erasures and decoded message data probabilities (om) are passed to RA decoder for T consecutive frames as a whole and then the hidden data is decoded.

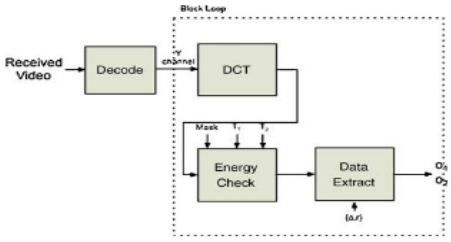

Figure 3. Embedded Flowchart Of The Proposed Video Data Hiding Framework For A Single Frame.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Secure video steganography with encryption based on LSB Technique:

In this paper the LSB technique is used to hide data image within video file, evidently safe images or files may quiet hide information using steganography, so when the encrypted file is decoded ,the hidden message is not seen. The LSB approach is used in conjunction with the transformation techniques.

Hiding Text In Video Using Steganography Technique: KTL Tracking Algorithm:

The proposed algorithm encompasses four distinct steps.

First in the encryption process the secret message is pre processed, and secret message is encoded by applying BCH codes.

Second to identify the facial regions of interest.

Third the embedding process it embeds the encoded secret message into the high and middle frequency wavelet coefficients.

In Fourth the extraction process extracting the secret message from high and middle frequency wavelet coefficients for each RGB components of all facial regions is accomplished.

Secure Data Hiding Technique Using Video Steganography and watermarking

In this paper they have proposed a new system for the combination of Steganography with watermarking which could be proven as a highly secured method for data communication .

A Survey: Video Steganography and Security Forbidden Zone and Selective Embedding

This system makes use of correction ability of copying store codes and advantage of forbidden zone data hiding is used. This system is tested by all types of videos that type of video which help to data hiding like avi , mp4 etc. In this study the encryption and decryption techniques used to security key. Without that key no one can see the unique data. This technique is used to secure the database from illegal and the destructive forces. It has large erasure capability of data hiding.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

A. COMPARISION OF RIDH AND FZDH

We compared our result with FZDH, data capacity of FZDH is 2/3 of our proposed algorithm. in FZDH if hidden data byte increases video quality decreases.

FZDH take less time as compare to RIDH.Security of RIDH increases as client side key is not required.

Table 1.

Time Complexity		
Algorithm	Embed	Extract
FZDH	1 sec	1.5 sec
RIDH	3 sec	4.2 sec

Table 2.

Data Capacity	
Algorithm	In MB
FZDH	$1/15^{th}$ of video file
RIDH	$1/10^{th}$ of video file

B. Use of Simulation software

The extent to which the existing application can be reused for further version is reusability .Our application can be reused a number of times without any technical difficulties.
Software requirements

- JDK 1.7
- Netbeans IDE 7.0.1
- Windows 7

C. RESULTS

PSNR:56
PSNR:54
PSNR:57

IV. CONCLUSION

In our work we implemented RIDH algorithm on video file frames, which not increase performance but also increase the data hidden capacity. as we use svm accuracy is increased but at the same time time complexity too in future we think about to reduce feature vector of svm to reduce time complexity. A new technique of video data hiding framework proposed which is robust to frame manipulation attacks. It incorporates erasure correction capability of FZDH and RIDH. When compared with FZDH, this method is better than FZDH especially in terms of low distortion levels. The experimental results show that, this method is robust to numerous frame rate conversion attacks.

V. ACKNOWLEDGMENT

We thank our Professor Mrs.Rohini Pise and HOD Dr. Sudeep Thepade for guiding and supporting us in this topic

REFERENCES

[1] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[2] X. Li, W. Zhang, X. Gui, and B. Yang, “A novel reversible data hiding scheme based on two dimensional difference-histogram modification,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091–1100, Jul. 2013.

[3] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[4] X. Zhang, “Reversible data hiding with optimal value transfer,” IEEE Trans. Multimedia, vol. 15, no. 2, pp. 316–325, Feb. 2013.

[5] T. Bianchi, A. Piva, and M. Barni, “On the implementation of the discrete Fourier transform in the encrypted domain,” IEEE Trans. Inf.Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[6] T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage-efficient processing of encrypted signals,” IEEE Trans.Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[7] M. Barni, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider, “Privacy-preserving ECG classification with branching programs and neural networks,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.

[8] Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk, “Generating private recommendations efficiently using homomorphic encryption and data packing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.

[9] M. Chandramouli, R. Iorga, and S. Chokhani, "Publication citation: Cryptographic key management issues & challenges in cloud services," US Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 7956, 2013, pp. 1–31.

[10] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.