INNOVATIVE TECHNOLOGY FOR DATA HIDING BY REVERSIBLE VIDEO TRANSFORMATION AND IMAGE PROCESSING

Silpa Rajan[1], Minu Laitha Madhavu[2]

[1]*Silpa Rajan, Mtech Student, Computer Science Engineering, Sree Buddha College, Kerala ,India*
[2]*Minu Lalitha Madhavu, Professor, Computer Science Engineering, Sree Buddha College, Kerala ,India*

---***---

Abstract - *When data is outraced to the cloud, as it contains messy codes it is important to protect the security of data but it should be capable of disbursing the data at the same time. Under such positions, REVERSIBLE VIDEO TRANSFORMATION (RVT) using RDH-EV is tendered. In RVT, the input video is transformed into a target video similar in all parameters. This target video indistinguishable to the input video is outsourced to the server in an encrypted format. The data is then embedded into the encrypted image with the aid of any RDH methods available. This process is extraneous to both sender and receiver ie, both encryption and decryption. Using RDH, RVT increases the embedding capacity as well as the security of data in the cloud is maintained.*

Key Words: **Reversible Data Hiding (RDH), outraced storage in cloud, REVERSIBLE VIDEO TRANSFORMATION (RVT), Prediction –Error Expansion(PEE),Class index Table(CIT)**

1.INTRODUCTION

In RVT [i], [ii], a target video similar in size to that of input video is used. As outsourcing requires affixed space because of large storage space required for inter media files like images, videos, outsourcing has been very favored. But for the large storage space, auxiliary data may be embedded into the data but at the same time no disfigurement to the data is allowed. This proves the requirement of reversible data hiding method (RDH) method where lossless rallying of data occurs after extracting the original message. Medical imaging, military, law forensics all finds applications with this technique. From many RDH methods available, semantic compression and Prediction- Error methods are universally used. In semantic lossless compression, compressed video and target video are homogenous in all respects resulting in good visual quality. But other method has small entropy due to it can be easily compressed and then can be reversibly embedded by modifying the histogram using histogram shifting (HS) or difference expansion(DE).

The two frameworks available are VRAE and RRBE ie Vacating Room After Encryption and Reserving Room Before Encryption. In VRAE, embedding of data occurs after vacating room for encrypted videos by compression. At the decoder side, along with side information, source coding is contrived after compression of encrypted data. Side information defines the interconnection of plain texts capitalized for decompression. Three LSBS (least significant bits) of half of the pixels in each block, for the embedded data room is vacated. Recovery of data and extraction of data is pushed on by finding out which pixel is capsized in one bock. Spatial correlation in decrypted images are used for this purpose. In RRBE, a room is emptied first using any of the RDH method after which it is embedded and outsourced to the cloud.

In this paper, a novel chassis for RDH-EV by reversible video transformation (RVT) is stated. The semantic contents of original image 'I' is converted into another image 'J' such that I can be losslessly recovered from J and hence also known as Semantic Transfer Encryption(STE). Hence the net transformed imaged looks exactly homogenous to the encrypted image J thereby protecting its content. As the encrypted image is in the form of plain text, it avoids the attention of the curious cloud. In RVT based framework, the original input is encrypted into another video on which data embedding using any of the RDH method is employed. It is then to the cloud server after which the data is removed and during decryption part the original video is retrieved back. This process is irrespective of sender and receiver as they are semi- honest, also known as video scrambling, a herculean technique to prevent unwanted interception is used here. A burly Perceptual Video Encryption mode is modulated by selecting one out of multiple unitary transforms in accordance with the encryption key generated from random permutation method at the transformation stage. The phase angle in the DCT based transformation stage of the input residual video frame is gyrated such that a new class of unitary transforms can be engendered. Various rotation angle providing number of Unitary Transforms is plumped on.

2. RELATED WORKS

The first paper[i] talks about high performance coding finding applications in medical imaging, libraries, forensics etc. This talks about predictive appropriate parameters associated with the pwm functions at the encoder is ciphered here so that at the decoder side, the compatible inverse pwm functions can map values back to the same residual values. These are then used to revamp the original signal. Therefore, the mapping is reversible and introduces no losses. The pwm functions on 4×4 residual blocks computed after assessing DPCM-based prediction method for lossless coding of a variety of camera-captured and screen content sequences.

As [ii] videos are of larger volume, video encryption is done by applying these transforms based on pre-designed secret key, partial encryption is attained. The drawbacks of Huffman coding at the coding stage adaptive arithmetic encoder is pre- owned obtaining the encrypted bit stream. The original video is obtained at the decrypted end.

Video surveillance systems [iii] are widely used in public places. Ubiquitous use of video scrutiny contravene the privacy rights of the people. A novel, on-demand selective protean, privacy preserving mechanism is told in this paper. With complete privacy, the surveillance video can be attuned to or abrogated such that the privacy of set of pedestrians ensuring privacy to the rest of them in a complete manner. A novel Markov chain algorithm with two hidden states, discerning the head contour of the tracked pedestrians and obliterating their faces using an encryption mechanism is used. By encrypting with a unique key derived from a master key is dubious from the detected pedestrian face/head for the privacy preservation purpose.

A lossless data hiding (LDH) scheme [iv] on uncompressed video with a multi-level histogram shifting mechanism in integer wavelet transform (IWT) domain is lodged in this paper. The exact recovery of the original host signal on extricating the embedded information occurs such that the watermarking image is in effected. The approximation sub band image of the luminance component of a video frame is then reckoned in this paper after which it is divided into non- overlapping blocks. A histogram is made on the difference values after calculating the differences between the neighboring elements. On the basis of a multi-level shifting mechanism of the histogram the secret data are embedded.

The exigent[v] areas of study are with the aid of data-hiding key alone an encrypted image/video containing additional data can be extracted easily even though image/video content is unknown to him. But the encryption key helps the receiver to decrypt to obtain only an image/video similar to the original one but the content cannot be redeemed. But both the data hiding key and the encryption key, the additional data as well as the original image/video can be embedded easily. This is done by escaping spatial correlation in natural images

W. Zhang, X. Hu, X. Li, and N. Yu's paper[vi] states that secret messages which restores the original image without distortion can be extracted. It's used in many applications like medical image applications and multimedia archive management. Mostly, histogram applications are used in most of RDH literatures. Difference pair mapping (DPM) is incorporated into two- dimensional histogram and prediction – error expansion. This improves the image quality by 3 db with same quality of images. At the same quality of images, the embedding quality of images can be enhance even to 30, 000 bits.

C. Dragoi and D.Coltuc [vii] , predicts about Prediction – error expansion (PEE) which is composed of two steps:-In the first step, by utilizing pixel prediction strategies, a sharp prediction- error (PE) is generated. In the second step, through expanding and shifting the PE histogram, secret messages are embedded. In the previous PEE methods, two of the above steps are treated independently by focusing on pixel prediction thereby obtaining a sharp PE histogram by aiming at histogram modification focusing on the embedding performance of a given PE histogram. A pixel prediction method based on minimum rate criterion on the basis of minimum rate criterion for reversible data hiding establishing consistency in two steps where a novel histogram modification scheme presented is approximated to get the optimal embedding performance on the generated PE sequence. Through the experiments, it is proposed that the previous state- of- art is outperformed by the proposed method in terms of both prediction accuracy and final embedding performance.

X. Hu, W. Zhang, X. Li, and N. Yu [viii] explains about a two-step clustering thereby clustering thereby optimizing pixel prediction method for Reversible Data

Hiding (RDH) exploiting self –similarities and group structural information of non-local images. Based on RDH schemes, prediction-error expansion (PEE) play an important role. Here based on the structural similarities of patches of image, the authors use a pixel clustering method. For each pixel associated with a pixel an optimized pixel predictor from the group context is predicted. From the experimental results, the proposed method is proven to be better than the state-of- art counterparts like median edge predictor, gradient- adjusted predictor, or simple rhombus neighborhood etc.

W. Zhang, X. Hu, and N. Yu [ix] advances about rate-distortion method for RDH based on recursive code construction (RCC). The optimal transition probability matrix (OTPM) has to be determined for finding out the rate-distortion or for executing RCC. Some methods like square- error- distortion or Li Norm. A unified framework to explore OTPM was used to calculate rate-distortion bound thereby extending it to any distortion metrics

This paper[x] proposes two methods which are discussed below:

1. Vacating Room Before Encryption (VRAE):
This paper proposes that the image I is encrypted into E(I) with the aid of a key by the image owner. The encrypted image E(I) is compressed by embedding data into the cloud server which generates Ew (I) which is stored into the cloud. On a retrieval request, E'w (I) is returned to the receiver by the cloud server which may be an authorized third party generating I through joint decompression and decryption with a key K. Hence E'w (I) may be just E(I) or a modified version obtained by removing the data embedded into it. The compression based RDH method used by cloud server should be specified by the receiver as the cloud server cannot restore E(I) from E'w(I).This in turn proves that RDH method is receiver related.

2. Reserving Room Before Encryption (RRBE) :
Here first a room is reserved for the image I by the image owner who embed data into the reserved room and generates E(I) with a key k and then sends it to cloud server which embeds it to the reserved room generating Ew (I) .This is then stored into the cloud from which data can be extracted by the server for further purposes. When the image I is to be retrieved by the receiver (authorized user) , Ew (I) is restored from E(I) by the cloud server which can be send to the user to decrypt the image using the key K. Here the complexity is occurred by the sender who reserves room for RDH by exploiting redundancy within the image ie, RDH used by the cloud should be specified within the sender. Therefore, RDH is sender related.

W. Liu , W. Zeng , L. Dong, and Q. Yao [xi], states that when data is passed through any channel, due to lack of security and limited bandwidth, it has become necessary to compress and encrypt it. Compared to other conventional methods, compression has become an easy and efficient method of encrypting data. The drawback is that many cases demands the reverse procedure too. Here the authors proposes a method whereby the encrypted data is compressed by the aid of Huffman coding and subservient data. The original image is handled by a pseudorandom number sequence by a secret key. The subservient data can also be created by the content owner. Huffman coding is then used to code the quantized values. The principal content of the data is reconstructed at the reconstruction side. This method is superior to other conventional methods which has been proven by experimental results. Also the range of the encrypted image is raised to 10 to 20 %

3. PROPOSED SYSTEM

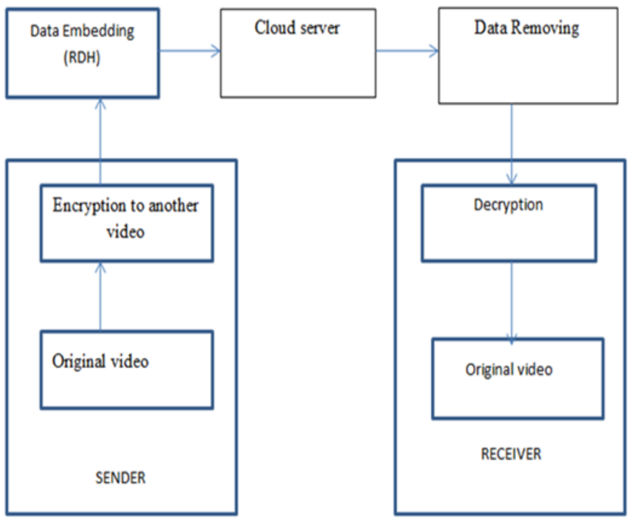

Figure -1: Proposed System Architecture

In RDH-EV, the encrypted video is outsourced to the cloud in the form of a plain text hence avoiding the attention of curious cloud. The encrypted video is embedded into the cloud server using any of the RDH methods. Then the cloud RDH used is client-free which means that the cloud server is irrelevant with both sender and receiver as is semi-honest. RDH-EV is composed of two algorithms, Algorithm 1: Procedure for transformation

A video 'V' along with a key K is used as the input A target video 'J' with the same size as V is chosen from the video database. Both the videos images V, J is divided into several non-overlapping 4x4 blocks. The mean and SD of each block is calculated assuming that the image consists of N blocks. The %α quantile of SDs are classified and CITs for V, J are generated. The blocks of V, J are then paired according to these CITs. The mean difference ▲ui is calculated for each block pair(Bv ,Tv) , where 1<=v<=N.▲uv is added to each pixel of Bv and is then rotated into an optimal direction theta (0 degree,90 degree, 180 degree, 270 degree), yielding a transformed block Tv'. For the target video J, each block is replaced with the corresponding transformed block Tv' for 1<=v<=N and hence the transformed video J' is obtained. ▲uv and theta for each block pairs are collected and are compressed together with the CIT of V. The compressed sequence and the parameter α is compressed by a standard compression technique like AES with a key K. The encrypted sequence is taken as the accessorial information (AV) and its embedded AV is transformed using any of the RDH methods to obtain the encrypted E(V).

Algorithm II: Procedure for anti- transformation

The encrypted video E(V) and the key K is used as the input to obtain the original video. AV is extracted and the transformed video J' is restored from E(V) using RDH scheme. AV is decrypted using AES scheme using key K and decompressed sequence is used to obtain CIT of V, ▲uv , theta where 1<=v<=N and α. The encrypted sequence is taken as the accessorial information (AV) and its embedded AV is transformed using any of the RDH method to obtain the encrypted video E(V). J' is divided into non-overlapping N blocks with size 4x4.The SDs of these blocks is calculated and CIT of J' is generated in accordance with the %α quantile of SDs. The blocks are rearranged according to the CIT'S OF J'. For each block Tv's of J' (1<=v<=N), Tv' is rotated in the anti-direction of theta and is then subtract ▲uv from each pixel of Tv' to obtain the final output video.

4. EXPERIMENTAL RESULTS

Since in RIT or Reversible Image Transformation, only one image is used for embedding, the embedding rate is less. But in RVT or Reversible Video Transformation, there are a number of video frames used as input and each of these videos frames contain a number of images; each of these images can be used for embedding data. Therefore, the embedding rate of RVT increases to a greater fold. This clearly indicates that RVT is better than RIT.

Embedding Capacity of RVT	Embedding capacity of RIT
765609 bits	68682 bits

Figure -2: Embedding Capacity of RVT and RIT

5.CONCLUSION

In this paper, a contemporary framework for reversible data hiding in encrypted videos (RDH-EV) on the basis of reversible video transformation (RVT). In earlier scheme, a plain text is converted to a enciphered form, RVT –based RDH-EV, the semantics of original image is converted to another target form protecting the privacy of original image. As the encrypted image is in the form of plain text images, it avoids the heed of agog cloud. Also it is free to use any of the RDH methods for watermarking. This above discussed method is also reversible. Using RVT, the original image is losslessly converted into an encrypted format Two methods are espoused for watermarking the image viz, PEE –based method and UES based method. The proposed method further enhances the security of the data when it is fed decrypt the data when it is the form of images. But when data is in the form of video frames, the amount of data that can be embedded increases. That is the data embedding capacity increases by the process.

6.REFERENCES

[1] Silpa Rajan, Minu Lalitha Madhavu, "Reversible Data Hiding by Histogram Modification for Image Contrast Enhancement " , International Research Journal of Engineering and Technology, vol.3 Issue 11 pp.761-76, November 2016

[2] Silpa Rajan, Minu Lalitha Madhavu, "Survey on Reversible Data Hiding in Encrypted Images by Reversible Image Transformation (RIT)", International Journal for Computer science and Engineering System, vol.7 Issue 1,pp: 26-29, March 2017

[3] Piecewise Mapping in HEVC Lossless Intra-Prediction Coding Victor Sanchez, Member, IEEE, Francesc Aulí-Llinàs, Senior Member, IEEE, and Joan Serra-Sagristà, Senior Member, IEEE

[4] Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation, S. Rajagopal, M. Shenbagavalli

[5] Privacy enabled video surveillance using a two state Markov tracking algorithm Peng Zhang, Tony Thomas & Sabu Emmanuel

[6] A reversible data hiding scheme for video robust against H.264/AC compression.

[7] M. A. Alavianmehr, M. Rezaei Dept. of Electrical and Computer Engineering sPasargad University of Shiraz University of Sistan and Baluchestan Shiraz, Zahedan, Iran, M. S. Helfroush, A.Tashk Dept. of

[8] A Electronics and Electrical Engineering Shiraz University of Technology Shiraz, Iran

[9] Novel Method for Data Hiding In Encrypted Image And Video A. Kaja Moideen , K. R. Siva Bharathi

[10] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression,"IEEETrans.ImageProcess.,vol.22,no.7,pp.2775–2785, Jul. 2013. "IEEE Trans. Image Process vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[11] B.ou, X. Li, Y. Zhao, R. Ni, and Y. Shi, "Pairwise prediction-error. Expansion for efficient reversible data hiding,"IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[12] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, 653–664, Mar. 2015.

[13] W. Zhang, X. Hu, and N. Yu," Optimal transition probability of reversible data hiding for general distortion metrics and its applications, "IEEE Trans. Image Process., vol. 24, no. 1, pp. 294–304, Jan. 2015 vol. 24, no. 1, pp. 294–304, Jan. 2015

[14] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[15] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–25