TRANSFORM BASED DATA HIDING APPROACH IN ENCRYPTED H.264/AVC VIDEO

Vishnu Priya G.S

Abstract-- **Digital video should be stored and processed in an encrypted format in order to provide security and privacy. Due to the higher access of videos by millions of users made its way to use in an authorized manner. In order to prevent tampering detection and for content notation, data hiding is done in the encrypted videos. Because of numerous digital multimedia techniques, data hiding is also important in verification, annotation , recognition and copyright protection of digital media. In this paper, data hiding is done in an encrypted H.264/AVC video streams. The intra prediction mode, motion vector differences and residual data are encrypted. Then codeword substitution technique is used for data hiding. However ,the identical data blocks are encrypted identically. So ,a discrete sine transform based data hiding is used where it has phases namely video encryption ,data embedding and video extraction.This provides better results than the existing system which prevents error propagating to neighbouring blocks.**

Index terms—H.264/AVC , Discrete Sine Transform(DST), Codewords , Quadtree segmentation.

[1]

I. INTRODUCTION

Data hiding becomes one of the important technique for securing the needed data and to provide privacy. For example, there are numerous large number of videos stored in cloud which is an emerging technology accessed by many number of users. But the vulnerability in those services may contribute to loss of important data, its copyright protection of data, validation and identification. The huge development of digital media also has its own vulnerabilities which can be avoided by some measures such as encryption, watermarking and so on. However, video content can be accessible in encryption. So, the required data is hided in the encrypted videos which provides high data security and privacy. H.264/AVC(Advanced video Coding) which is an widely used video compression standards developed by ITU-T video coding experts group and ISO/IEC moving pictures experts group. This H.264/AVC can be used in applications such as broadcasting , storage and also in streaming. This standard can be used in

- Telecasting over satellite , cable ,etc.
- Storage on DVD , magnetic disks.
- Services over ISDN, Ethernet, local area network, Digital subscriber line, wireless and mobile networks, modems, etc.
- In streaming services.
- In Multimedia messaging services.

Here, a sample video is taken as an input and compressed by H.264/AVC coding. Then the video is encrypted by H.264/AVC algorithm.This algorithm include intra prediction mode encryption motion vector difference encryption and residual data encryption.There are some demands for hiding

Vishnu Priya G.S., Department of Computer Science and Engineering ,Avinashilingam University,Coimbatore,TamilNadu,India.

ISSN: 2278 – 1323

data in compressed and encrypted domain. First one is to determine how and when the modification can be done on an bitstream. Next one is the decrypted videos with the hidden data can be a high visual fidelity. The third one is to maintain and preserve file size of the video. The file quality should be same as input video after decryption. Degradation should be small.

II. METHODOLOGIES

Encryption key is used for the original video.Then the video encryption is done which includes intra frame mode encryption ,motion vector difference encryption and residual data encryption which are explained as follows. Initially in the video, the frames are combined which forms a video file.The video can have any number of frames. The first frame is always an I frame and P frames are the remaining frames other than I-frame. The first frame is compared with all other P frames for encryption. The 16*16 block is taken and encrypted.

A. Intra Prediction Mode Ecryption (IPM)

The H.264/AVC standard supports four types of intra coding. They are Intra_4*4,Intra_16*16,Intra_Chroma and I_PCM. Here, Intra_4*4 and Intra_16*16 blocks are taken and used to encrypt. There are four intra prediction modes in Intra_16*16. The IPM for Intra16*16 are specified by the mb type values listed with the codewords. In H.264/AVC, the mb_type is encoded by Exp Golomb code. The codeword length should be same throughout the encryption. The encrypted codeword size should be maintained same as the original codeword .For example, codewords corresponding to ‘1’ and ‘2’ are ‘010’ and ‘011’ with the same length maintained. So, a bitwise XOR operation is applied for performing IPM encryption between the pseudorandom sequence and last bit of codewords. The pseudorandom sequence is generated using standard cipher.

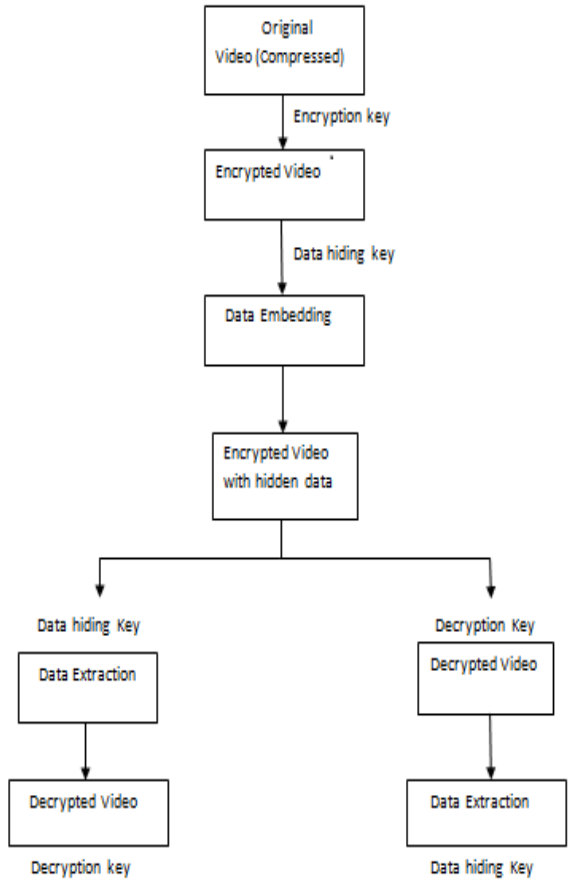

Fig 1. Flowchart of video encryption and data extraction

B. Motion Vector Difference Encryption

The video also has its texture information and motion information which should be encrypted to protect it. The motion vector prediction is performed on motion vectors and Exp Golomb entropy coding is used to encode motion vector difference.The last bit of the codeword is encrypted

with cipher by applying bitwise XOR operation.The codewords corresponding to ‘1’ and ‘-1’ are ‘010’ and ‘011’ which has the same codeword length.The codeword will be ‘1’ when the value of MVD is ‘0’ and it remains during the encryption process.

ISSN: 2278 – 1323

C. Residual Data Encryption

The I frames and P frames both have a residual data which is a sensitive type of data has to be encrypted to provide better security.In H.264/AVC,the coefficients of residual block are encoded by CAVLC entropy coding. Each CAVLC codeword can be defined as

{ Coeff_Token , Sign of_Trailing_Ones, Level, Total_Zeros,Run_before } (1)

The Coeff_Token, Total_zeros and Run_before remains constant while the sign_of_Trailing_ Ones and Level codewords are changed.Bit '0' is assigned as bit '1' and bit '1' is assigned as '-1'. The codewords are encrypted by bitwise XOR operation.The codeword for each level defined as

Level codeword =[level_prefix],[level_suffix]

Fig 2.a Original video frame

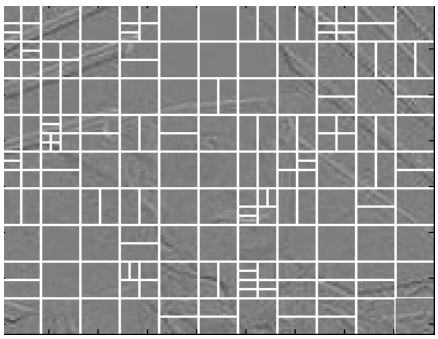

Fig 2.b Encrypted video frame

III DATA EMBEDDING

The data is embedded into the video after compression and encryption. The data should be secured safely to prevent from hackers who can hack even after encryption.Data to be embedded is converted to ASCII standard values.Then the ASCII values are converted to binary and the data is hided. All the values should be of same size to keep the length consistent.

IV PROPOSED SYSTEM

The Discrete Sine Transform(DST) is used for hiding important data in encrypted H.264/AVC video. This DST uses quadtree segmentation method which provides better quality and preserves the size of the file. The video which is encrypted is taken and data is embedded into it by the quadtree method. The quadtree method segments the square image into four equal sized square blocks. Then each block is tested to know the similarity between them. If the blocks are similar, the blocks are not divided further. If the blocks are not similar and does not meet the constraints, then the blocks are subdivided again into another four blocks.

This method of Discrete sine transform shows the structure of the image.The quadtree method of this transform identifies the object in the frame and take it as a line. Then divides the image into blocks. The object with empty space block is subdivided again into blocks. The block with only object is not divided and also the block with no object are not divided. Then the alphabets which is to be hided are saved. Then the alphabets are converted into ASCII(American Standard code for Information Interchange) standard. Again the ASCII values are converted to binary and hided. The key size is also shown when the data is extracted. In the data extraction, binary value is converted to ASCII and the ASCII value is converted to alphabets to get the required data.

ISSN: 2278 – 1323

V DATA EXTRACTION

Decryption key is used to decrypt the encrypted video. The data which is embedded could be extracted in both encrypted domain and also on decrypted domain.

Encrypted domain:

- User encrypt the video stream by encryption key.
- Required data is embedded into the video by codewords.
- Data is extracted before encrypting the video.
- Video is decrypted by decryption key.

Decrypted domain:

Sometimes, user needs the video first. So, the video is decrypted and then the data.

- User encrypt the video stream
- Required data is embedded into the video by codewords
- Video is decrypted by decryption key
- Then the data is extracted from the decrypted video

VI. CONCLUSION AND FUTURE WORK

The data is hided in an encrypted domain to provide both security and privacy. Video encryption, data embedding and data extraction are used here. The algorithm used may preserve the bit rate and also the file size which is important for high quality video. Experimental results shows that the proposed system can achieve better quality and performance. Future work may be competed with developing data hiding algorithms by preventing degradation.

REFERENCES

[1]. M. Schuster and Aggelos K. Katsaggelos, "An Optimal Quadtree-Based Motion Estimation and Motion-Compensated Interpolation Scheme for Video Compression" IEEE, 1998.

[2]. Gerardo, Hugo Jair, Luis Enrique, "Simplified Quadtree Image Segmentation for Image Annotation" 2011.

[3]. Kaladharan N**,** "Unique Key Using Encryption and Decryption of Image", 2014.

[4]. Hsiang-Cheh Huang and Wai-Chi Fang, "Authenticity Preservation with Histogram-Based Reversible Data Hiding and Quadtree Concepts", 2011.

[5]. Samira Bouchama, Latifa Hamami, and Hassina Aliane, "H.264/AVC Data Hiding Based on Intra Prediction Modes for Real-time Applications", 2012.

[6]. Po-Chun Chang , Kuo-Liang Chung , Jiann-Jone Chen , Chien-Hsiung Lin and Tseng-Jung Lin, "A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames", 2014.

[7]. ThomasWiegand, Gary J. Sullivan, Gisle Bjøntegaard, and Ajay Luthra, "Overview of the H.264/AVC Video Coding Standard" IEEE, 2003.

[8]. Alekhya Orugonda and S.Rajan, "Hiding the Military Secret Message by Reversible Data Hiding", 2013.

[9]. A. Kaja Moideen1 and K. R. Siva Bharathi, "A Novel Method for Data Hiding In Encrypted Image And Video", 2014.

[10]. Deepthi Barbara Nickolasa, Sindhuja.Ba and A.Sivasankar, " Enhancement of Data Hiding Process in Encrypted Image Using Advanced Encryption Standard" , 2013.

ISSN: 2278 – 1323

Vishnu Priya G.S completed Bachelor of Engineering in Information Technology and Master of Engineering in Computer Science and Engineering from Avinashilingam University, Coimbatore.

ISSN: 2278 – 1323