Data Hiding in Video Streaming by Code Word Substitution

Mr. Pinagadi. Venkateswara Rao (Assistant professor)
Annie Ratna Priyanka K [#1], Nivetha R[#2], Priyadharshini P[#3], Seetha M[#4]
[#]Final year, Department of Information Technology
Panimalar Engineering College,
Chennai, India

Abstract- Data hiding techniques can be used to embed a secret message and secret image into a video bit stream for copyright protection, access control and transaction tracking. They are some data hiding techniques to assess the quality of video in the absence of the original reference. To avoid the drawback of existing system such as lossless compression, gray scale mapping and noisy images forces higher bit plane when distortion are easily visible. Data hiding is also used for concealment in applications of video transmission, gray scale mapping and noisy image. Edge quality information and number of bits of a block are hidden in the bit streams processed in an encrypted format to maintain security and privacy.

Index Terms- *Data hiding, video streaming, data encrypted, codeword substitution.*

*****

I.INTRODUCTION

Data Hiding Technique the capacity is not high enough to embed the large video. In previous proposed approach computation and large storage for video data is attracted by more untrustworthy administrators. The direct performing of data hiding in H.264/AVC will avoid leakage of video content which will provide security for technique [1]. Data hiding can be performed by using FFMPEG, Steganography, Visual Cryptographic Scheme, Invisible Watermarking and Base 64 Encoder/Decoder technique the security and video payload can be increased.

FFMPEG Tool is used to split the video into three parts such as audio, video and frames to avoid the video to produce the video without noise. Steganography is a practice of concealing information and then enclose both the image and content in the video. Invisible watermarking technique is used to embed watermark into compressed and encrypted image. This technique is used to transplant data to the encrypted domain. The compression and decompression technique is time consuming process in real time implementation. The speed of compression and decompression is increased by base 64 encoder and decoder technique is used.

In RDH histogram shift, in which space is saved for data embedding and shifting the bins of histogram to the gray valves which help us to convert the image into the binary image [2]. Binary image will help to hide the data into the image easily. The recursive binary code is constructed to achieve rate distortion between the data compression and binary covers.

To avoid the loss and errors while encryption and decryption separate memory is allocated to recover the original image [3]. At the receiver side the data extraction and image recovery is restored with the original key content to restore the image. If the original key content is received, the image will be restored but the extract the exact data. So the image is converting to gray scale and then binary image to get the exact data in decryption.

For example [4] fingerprintsand faces are obtained by outsiders, the biometric templates misuses them for its own purposes. This type of biometric threats exists which had become difficult to prevent unauthorized parties to encrypt the video. To prevent the unauthorized parties to encrypt the video the base 64 encoder and decoder algorithm for codeword substitution is used to prevent the security and transfer through secured system.

Development of computer technology, Internet technology and multimedia data uses images; videos and audios are encrypted using various algorithms such as DES, RSA, IDEA or AES for text or binary data [5]. These algorithms are difficult to use them in video encryption, large volumes and recompression. Data protection or content protection in encrypted scheme is secure when the cost for breaking is no smaller than one paid for its authorization.

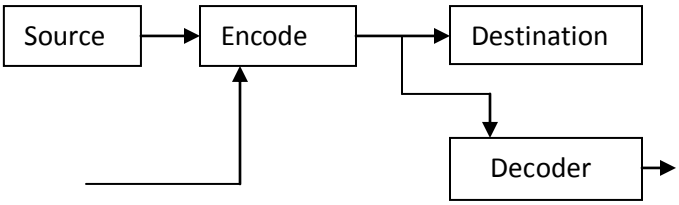
The remainder of the paper is as follows. In Section II, we delineate the proposed scheme, which includes four parts, i.e., Frame selection in encryption, Data hiding using visual cryptography, Frame selection in decryption and Extracting the data. In Section III, we present the experimental results. Discussion is shown in Section IV. Finally in Section V, conclusion is drawn.

II. RELATED WORK

1. Fridich et al constructed general framework for RDH for changing room in encrypted image. By first extracted compressible features of original image and then compressing them looslessly. In this way space can be created for embedding data.

2. Another method is based on difference expansion (DE) for vacating room in encrypted image in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus least significance bit(LSBs) of the difference are all-zero and the space created can be used for embedded data.

3. As when data is embedded into the image then the quality of image get disturbed. So it is expected that after the data extraction the image quality should be maintained just like the original image. But the image contain some distortions.



II. PROPOSED SCHEME

Proposed Scheme, which includes four parts, i.e., Frame selection in encryption, Data Hiding using visual cryptography, Frame selection in decryption and extracting the data. By analyzing video codec, data hider may embed data with image in the encrypted domain by using codeword substitution technique, without acquaintance of original data. In order to change to different application, data extraction can be done in the encrypted and decrypted domain. Furthermore, the file size of video is strictly protected even after encryption and data embedding.

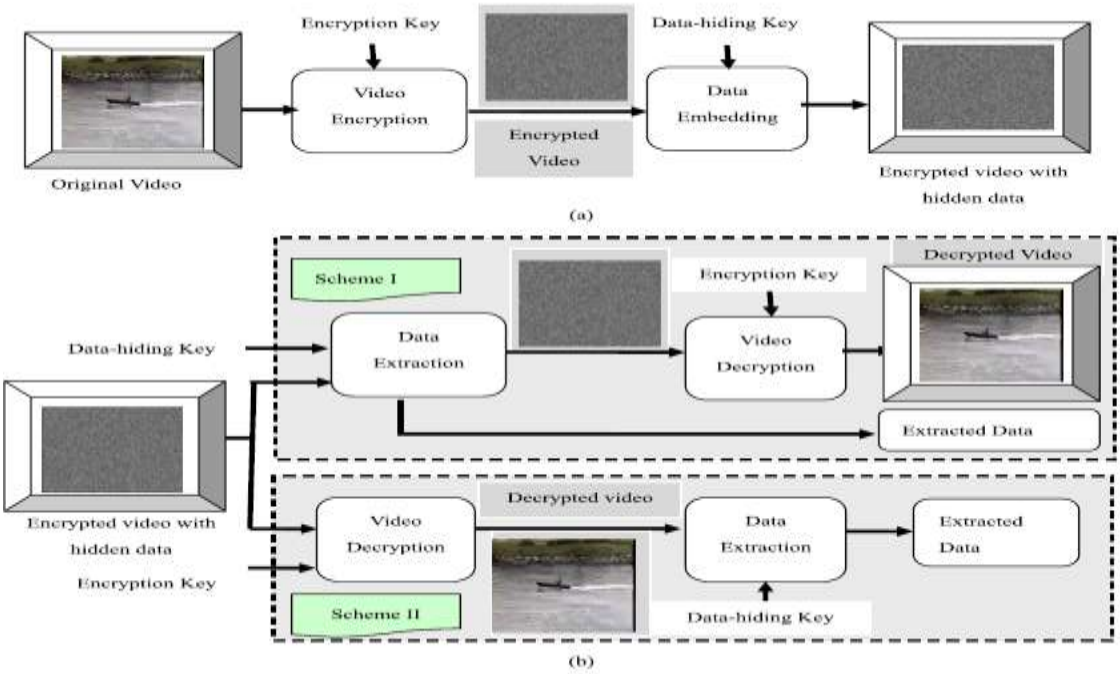


Fig. 1. Diagram of proposed scheme. (a) Video encryption and data embedding at the sender end. (b) Data extraction and video display at the receiver end in two scenarios.

A. Frame Selection in Encryption

In first module, select the video file to hide the Secret image and Data. By using the ffmpeg tool, Video was split up into 3 formats. First the video was split up into audio and video separately. Then the video part will be converting into n number of frames. In future these frames are used to hide the image and the data.

B. Data Hiding Using Visual Cryptography

In second module, we are selecting any two frames from n number of frames. Selecting the Secret image and converting this image into Grey scale image and further converted into Binary image. By using the Visual Cryptography scheme finally the binary image is split up into two shares. To hide data into the share, the data is encrypted using Pailier byptosys and by using the Steganography technique the cipher text is embedded into the two shares. The Invisible Watermarking technique is used to hide two shares into the selected frames and after the image is hided the all frames are converted into video and mix up with audio and finally video was encrypted using the Base 64 Encoder.

1) Intra-Prediction Mode (IPM) Encryption:

According to H.264/AVC standard, the following four types of intra coding are supported, which are denoted as Intra_4 ×4, Intra_16×16, Intra_chroma, and I_PCM [1]. Here, IPMs in the Intra_4×4 andIntra_16×16 blocks are chosen to encrypt. It is prominent at the length of the encrypted codeword is the same as the original one. For the format compliance in the decoding process, the blocks in the first row and/or in the first column of encrypted IPMs should have the decodable value, since not all modes are available along the top and the left borders of each frame due to the lack of acquaintance. If the IPM after encryption is not available for an entire block, then the IPM encryption of this block will be skipped. This further indicates that IPM encryption is not secure enough in some specific locations and should be used in combination with other encrypting method. In summary, IPM encryption implies changing the actual mode to another one without violating the semantics and bit stream compliance.

2) *Motion Vector Difference (MVD) Encryption:*

Table II shows the values of MVDsandcorresponding Exp-Golo mb codewords. The last bit of the codeword is encrypted by applying the bitwise XOR operation with a standard stream cipher determined by key. The last bit encryption may change the sign of MVD, but does not affect the length of the codeword and satisfies the format compliance [2]. That corresponding to "2" and "–2" are "00100" and "00101", respectively, which have the same length. It should be verified that when the value of MVD is equal to 0, its corresponding codeword "1" keeps unchanged during the encryption process.

TABLE I
MACROBLOCK TYPES FOR I SLICES AND VARIABLE LENGTH OF CODEWORD IN H.264/AVC [17]

mb_type	Name of mb_type	Intra16x16 PredMode	Chroma CBP	Luma CBP	Codeword
1	I_16x16_0_0_0	0	0	0	010
2	I_16x16_1_0_0	1	0	0	011
3	I_16x16_2_0_0	2	0	0	00100
4	I_16x16_3_0_0	3	0	0	00101
5	I_16x16_0_1_0	0	1	0	00110
6	I_16x16_1_1_0	1	1	0	00111
7	I_16x16_2_1_0	2	1	0	0001000
8	I_16x16_3_1_0	3	1	0	0001001
9	I_16x16_0_2_0	0	2	0	0001010
10	I_16x16_1_2_0	1	2	0	0001011
11	I_16x16_2_2_0	2	2	0	0001100
12	I_16x16_3_2_0	3	2	0	0001101
13	I_16x16_0_0_1	0	0	15	0001110
14	I_16x16_1_0_1	1	0	15	0001111
15	I_16x16_2_0_1	2	0	15	000010000
16	I_16x16_3_0_1	3	0	15	000010001
17	I_16x16_0_1_1	0	1	15	000010010
18	I_16x16_1_1_1	1	1	15	000010011
19	I_16x16_2_1_1	2	1	15	000010100
20	I_16x16_3_1_1	3	1	15	000010101
21	I_16x16_0_2_1	0	2	15	000010110
22	I_16x16_1_2_1	1	2	15	000010111
23	I_16x16_2_2_1	2	2	15	000011000
24	I_16x16_3_2_1	3	2	15	000011001

TABLE II
MVDs AND CORRESPONDING EXP-GOLOMB CODEWORDS

MVD	*code_num*	*codeword*
0	0	1
1	1	010
-1	2	011
2	3	00100
-2	4	00101
3	5	00110
-3	6	00111
4	7	0001000
-4	8	0001001
5	9	0001010
-5	10	0001011
6	11	0001100
-6	12	0001101
7	13	0001110
-7	14	0001111
8	15	000010000
-8	16	000010001
9	17	000010010
-9	18	000010011
...	...	...

3) *Continuing data Encryption:*

In order to keep high security and sensitive data, i.e., the continuing data in both I-frames and P-frames should be encrypted. In this section, a novel method for encrypting the residual data based on the characteristics of codeword substitution is presented in detail.

The codeword for each level is made up of aprefix (level_prefix) and a suffix (level_suffix) as *Level codeword* = [*level_ prefix*], [*level_ suffix*]

Table III shows *Levels* with different *suffix Length* and corresponding codeword. The last bit of the codeword is encrypted by applying the bitwise XOR operation with a standard stream cipher, which is determined by an encryption key *E_Key*5. According to Table III, the last bit encryption may change the sign of *Levels*, but does not affect the length of the codeword and satisfies the format flexibility. It should be verified that when *suffix Length* is equal to 0, the code words should keep unchanged during the encryption process.

C. Frame Selection in Decryption

In third module, public key is received by destination and The Encryption was done by using destination public key and video was transmitted. In receiver system, video was Decrypted and split into frames and extracting the shares and data by selecting the frames which was watermarked.

D. Extracting the Data

After extracting the Image and the Data, the Data should be decrypted and the Image received was noisy, so it needs to reconstruct the image to get Binary image. Binary image which is in black and white is then converted into the color image.20% of the black and white is converted the full image cannot be converted into color image.

In this scheme, the hidden data can be extracted either in encrypted or decrypted domain, as shown in Fig. 1(b). Data extraction process is fast and simple. We will first discuss the extraction in encrypted domain followed by decrypted domain.

1) Scheme I: Encryption of Domain Extraction. To protect privacy, a database manager (e.g., cloud server) may only get access to the data hiding key and have to manipulate data in encrypted domain. Data extraction in encrypted domain guarantees the feasibility of our scheme in this case.

2) Scheme II: Decryption of Domain Extraction. In scheme I,both visual cryptographic and extraction of the data are performed in encrypted domain. However, in some cases, users want to decrypt the video first and extract the hidden data from the decrypted video. The received encrypted video with hidden data is first pass through the decryption module.

TABLE III
LEVELS AND CORRESPONDING CODEWORDS

suffixLength	*Level(>0)*	*Codeword*	*Level(<0)*	*Codeword*
0	1	1	-1	01
	2	001	-2	0001
	3	00001	-3	000001
	4	0000001	-4	00000001
1	1	10	-1	11
	2	010	-2	011
	3	0010	-3	0011
	4	00010	-4	00011
	5	000010	-5	000011
	6	0000010	-6	0000011
	7	00000010	-7	00000011
	8	000000010	-8	000000011
2	1	100	-1	101
	2	110	-2	111
	3	0100	-3	0101
	4	0110	-4	0111
	5	00100	-5	00101
	6	00110	-6	00111
	7	000100	-7	000101
	8	000110	-8	000111
	9	0000100	-9	0000101
	10	0000110	-10	0000111
	11	00000100	-11	00000101
	12	00000110	-12	00000111
	13	000000100	-13	000000101
	14	000000110	-14	000000111
3	1	1000	-1	1001
	2	1010	-2	1011
	3	1100	-3	1101
	4	1110	-4	1111
	5	01000	-5	01001
	6	01010	-6	01011
	7	01100	-7	01101
	8	01110	-8	01111
	9	001000	-9	001001
	10	001010	-10	001011
	11	001100	-11	001101
	12	001110	-12	001111
	13	0001000	-13	0001001
	14	0001010	-14	0001011

EXPERIMENTAL RESULTS:

The data hiding system has been planned in the H.264/AVC consulting software version JM-12.2. The standard video sequences in QCIF format (176 ×144) at the 30 frame used for simulating the result. The first 100 frames in each video sequence are used in the experiments. The GOP (Group of Pictures) structure is "IPPPP: one I frame followed four P frames".

A. Security of Encryption Algorithm

In this proposed scheme, the security can be includes cryptographic and perceptual security. The proposed scheme in RC4 is used to encrypt the bitstream, and confusion sequence generated by logistic map is used to encrypt the additional data. They can be proved against cryptographic attacks. Perceptual security indicates to whether the encrypted video is impossible to understand or not. Generally, it determined on the encryption scheme's properties. For example, encrypting only IPM cannot keep protecting necessary, the total encrypted video is intelligible [1]. The proposed scheme encrypts IPM, MVD and remains a coefficient, that's keeps perceptual security of the encrypted video. Due to space limitations, we do not list the results of all frames. If, it can be mentioned every video can be degraded to the same position. The perceptual quality must contain the

high-motion videos with complex textured background get more scrambled after encryption. This is reason for less remains coefficients and MVDs in low-motion videos that are available for encryption.

B. Visual Quality of Stego Video

The encrypted video must change in hidden data by the server must be decrypted by the user. Therefore, the visual quality of the decrypted video containing hidden data is equal or in expected video. Simulation results have clear that we can firmly to the additional data with a high storage into P-frames while preserving high visual quality. In this process not clear artifacts have been observed in all of the decrypted video frames with hidden data. Then H.264/AVC is lossy compression, in order to better illustrate the data hiding on the video quality, the visual quality of non-stego video stream should be tested. The video sequence obtained by decompressing non-stego video stream is used as the target sequence, while the original uncompressed video sequence is used as the reference video sequence. Similarly, in order to test the visual quality of stego video stream, the video sequence contained by encrypting the data hiding, decrypting, and decompressing process is used as the target sequence. The VQM another approach to measure video quality connects that more within the visual system. In lower VQM value determines higher perceptual video quality, and zero indicates good quality. If a higher QP (quantization parameter) will be shown in lower video quality. It is generally hard to detect the quality that caused by data hiding.

C. Embedding Capacity

Data hiding payload can be considered in kilobits per second. The maximum payload capacity in all the video encoded with different *QP* values is given. In this scheme it depends on the payload on the video content and QP values. This is made by all video and embedding storage can be different qualified codewords. This is be caused by high motion sequence has more qualified *Levels*; the data hiding only operates in P-frames. Specifically, payload decreases with increase in *QP* value. When QP value increases, the number of residual coefficients decreases, and then the qualified *Levels* will be less.

D. Bit Rate Variation

To evaluate the performance in the proposed scheme, bit rate variation *BR_var*caused by encryption and data hiding is also introduced.

BR var = BR em − BR orig /BR orig× 100

Where *BR_em*is the bit rate generated by encryption and data embedding encoder, and *BR_orig*is the bit rate generated by the original encoder. The bit rate of the encrypted and stego video remains unchanged. This is because the encryption and data hiding are all performed by replacing a suitable codeword to another codeword with the same length.

CONCLUSION:

Data hiding is a new technique that had drawn attention because of the privacy- preserving. In this paper, we embed the algorithms to separate the video, audio and frames by using ffmpeg tool. Steganography and visual cryptographic is used for data hiding and extraction of data. The algorithm for bit-rate and converting into gray scale and then to binary is embedded in data hiding using visual cryptography. The speed of compression and decompression is increased by base 64 encoder and decoder technique is used. The data is hider by using codeword substituting. The data hiding is completed by preserving the confidentiality of the content. By using the encrypted video containing the hidden data extracted in encryption or decryption domain. The advantage of this project is by using H.264/AVC Technique. Experimental results can preserve file-size; degradation in video quality is quite small. This project can be applicable for small sized video and for larger sized video.

REFERENCES:

[1] Dawen, Rang and Yun, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution," IEEE trans. Inf. Forensics and security, Vol. 9, No. 4, April 2014.

[2] J.Wag, Man, U. Mur, S. Shi and Prof. Bha, "RDH (Reversible Data Hiding) in Encrypted Images by Reserving Room Before Encryption," in ISO 9001:2008 Certified Journal, Vol. 4, Issue. 4, April 2014.

[3] Anagha and Prof. Pragati, " A Review on Data Hiding Techniques in Encrypted Images," IJCTT, Vol. 4, Issue. 10, Oct 2013.

[4] W. Pue, Z. Erk, M. Bar, S. Ran and R. L. Lag, "Emerging Cryptographic Challenges in Image and Video Processing," IEEE, ICIP 2012.

[5] Shiguo, Zhong, Zhen and Haila, "Secure Advanced Video Coding Based on Selective Encryption Algorithms," Contributed Paper, Manu. rec., March 2006.

[6] Thom, J. Sull, Gisle and Ajay, "Overview of the H.264/AVC Video Coding Standard," IEEE Tran. On Circuits and Sys. For Video Tech. Vol. 13, No. 7, July 2003.