ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Codeword Substitution Method for Hiding Information in Encrypted Video

Jakhalekar Priyanka R, Prof. Pankaj Agarkar

M.E Student, Dept. of Computer Engineering, Dr.D.Y.Patil School of Engineering, Lohgaon , Pune, India

Assistant Professor, Dept. of Computer Engineering, Dr.D.Y.Patil School of Engineering, Lohgaon, Pune, India

ABSTRACT: To preserving the privacy as well as maintain security of video there is needs to be stored videos in an encrypted format. For copyright protection, access control and transaction tracking we use information hiding techniques, that can be embedded a secret message and secret image into a video bit stream. The quality of video in the absence of the original reference assesses by information hiding techniques. The edge quality information and the no of the bit streams processed in an encrypted format to maintain security as well as privacy. In this paper hiding information directly in the encrypted video stream is proposed. The proposed scheme contains the three main parts, i.e. encryption of video, embedding secret message and extraction of secret message and video.

After analyzing the video codec property, the code words of intra prediction modes (IPM), the code words of motion vector differences (MVD), and the code words of residual coefficients are encrypted. The data hider embeds additional data in the encrypted domain, they use the code word substitution technique. The code word substitution technique gives information without knowing the original video content. After decryption of video secret message remains hidden, it is not visible to a human observer or user. The extraction of data can be done either in the encrypted or in the decrypted domain.

KEYWORDS: Information hiding, encrypted domain, codeword substituting, decrypted domain.

I. Introduction

Today Cloud figuring it is an imperative innovation, which gives an exceptionally effective calculation and give expansive capacity video information. For keeping up the security the cloud administrations are utilized for the concealing that unique video substance or access that video substance is in scrambled structure. There is one data concealing methods can be utilized to insert a mystery data into a video bit stream for copyright assurance, access control and exchange following. The maintaining a strategic distance from the spillage of video substance the data covering up specifically into H.264/AVC scrambled video streams, which can be useful for location the security and protection worries with distributed computing [1].

For instance, a cloud server can implant data into a scrambled adaptation of a video by utilizing the data concealing procedure. By utilizing that concealed data, the cloud server can deal with the video or confirm its uprightness without knowing the first substance, and in this way it protects the security and additionally security. In the reversible information concealing outline for encoded picture after encryption of whole information the extra information can be inserted into the picture and it adjust in a little parts of scrambled information [6].At the season of the installing the information into encoded video the information hider does not realize that the first video substance. After encryption when we decode the video then the data stays shrouded it not saw by human spectator for that we utilized the codeword procedure. Further, giving information security, protection and insurance, data stowing away in scrambled recordings will get to be well known later on. Data covering up in encoded recordings is an extremely troublesome assignment, however in the proposed plan accomplished a superior execution for that.

II. Related work

The secure video processing is an emerging technology used for preserving the privacy. In this paper mainly focus on video data and problem, challenges in securely managing secret video online. There are three aspects for evaluating a secure video processing i.e. security, performance, complexity [1]. In secure video processing the users store their secret videos in encrypted form. There are two parts in the system, the user who owns secret information and server who stores the encrypted videos and performs processing tasks.

In this paper contains processing tasks, video search, classification and summarization. Video summarization is a task of extracting a set of images called as video frames to represent the original video contents. Video classification means that the classify that video into different category.

The reversible data hiding focuses on the data embedding and data extracting on the plain spatial domain [4].There are two keys encryption and data hider key. In this paper it used an improved Zhang's version for reversible data hiding method in encrypted images. The zhang proposed the image encryption and decryption parts. In that the content owner encrypt the original image using the encryption key and passes that encrypted image and embed the data or additional data to encrypted image by using data hider key to the receiver side. In the receiver side first decrypt that image by using encryption key and then extract the data and image recovery using data hider key. Here uses the LSB method. The embedded additional data is not secure it is the disadvantage of that.

The separable reversible information hiding contains content owner encrypts original image using an encryption key. By using the data hiding key data hider compress least significant bits of encrypted image [10]. In that the content owner encrypt the original image using the encryption key and embed the data or additional data to encrypted image by using data hider key. For embedding the data uses the LSB(Least significant bit). Embed the secret data to the each bit pixel of that encrypted image. In the receiver side first decrypt that image by using encryption key and then extract the data and image recovery using data hider key. If the receiver know the encryption key then they only decrypt the image, or if receiver know only data hider key then they only decrypt the secret information. Here uses the lossless compression method that contain additional information can be extracted and also the original content of image is also recovered this is limitation of this paper. So use lossy compression, it is compatible with encrypted image.

In this paper it contains the review for H264 AVC/SVC video encryption. In this paper outlines the most recent exploration on video encryption. Here accomplished the adaptability and security, pressure proficiency. In the H264 encryption contains the four sections, encryption before pressure, coordinated encryption, bit stream (arranged encryption), svc encryption. The incorporated encryption contains intra expectation mode, bury forecast mode, movement vector contrast, mystery transform[13].The video encryption plan relies on the application connection. This paper is primarily centered around inter operatability of video encryption. In this paper contains group consistence, packetization, quick forward and extraction of subsequences, vigorous watermarking. For saving the security the video encryption is fundamental errand. Here a safe way to deal with scramble H264, is to encode the whole H 264 piece stream utilizing the AES calculation with the figure square. This paper is organized in taking after parts, quickly synopsis of H264, application situation of video encryption and their comparing diverse documentations. The encryption of video plan safeguards the usefulness of video bit stream. In that paper for the most part centered around video encryption plan for H264 AVC and the interoperability of video encryption with existing procedures for the video information, for example, packetization, (versatile) gushing, rate adjustment, outline extraction, quick forward and watermarking.

III. PROPOSED ALGORITHM

System module having three main parts video encryption, data embedding, data extraction. The Fig1 and Fig 2 shows the video encryption, data embedding, data extraction and video decryption.

1. *Video encryption*

Video encryption requires time efficient scheme to meet the requirement of real time. The scheme proposed security, efficiency and format compliance. After analysing the property of video codec they contains three parts Intra prediction mode (IPM), Motion vector difference (MVD), Residual data encryption. In this encrypted video it is decoded by standard decoder, but encrypted video is completely different compare to the our plaintext video data.

The video encryption first contains the Extraction of video into the no of frames. In that first we extract or divide the video into audio and the number of frames. Then following operations are performed on that selected frames, encrypt that frames and passes it for embedding of data.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

a. Intra prediction mode :

There are four types of intra prediction modes. Intra_4*4, intra_16*16, intra_chroma, I_pcm. Intra_4*4 and intra_16*16 chosen for the encryption purpose. They contains the macro blocks. At the time of the encryption it takes the previously predicted block and the current block can be encrypted. The codeword length remains unchanged means that original codeword and encrypted codeword remains same size.

b. Motion vector difference:

In this type it protected the texture information as well as motion information. It is similar to intra prediction mode. It predict the frames in a video.

c. Residual data encryption:

It keeps the high security there is one type of data called as residual data. That can be encrypted the I frames and P frames.

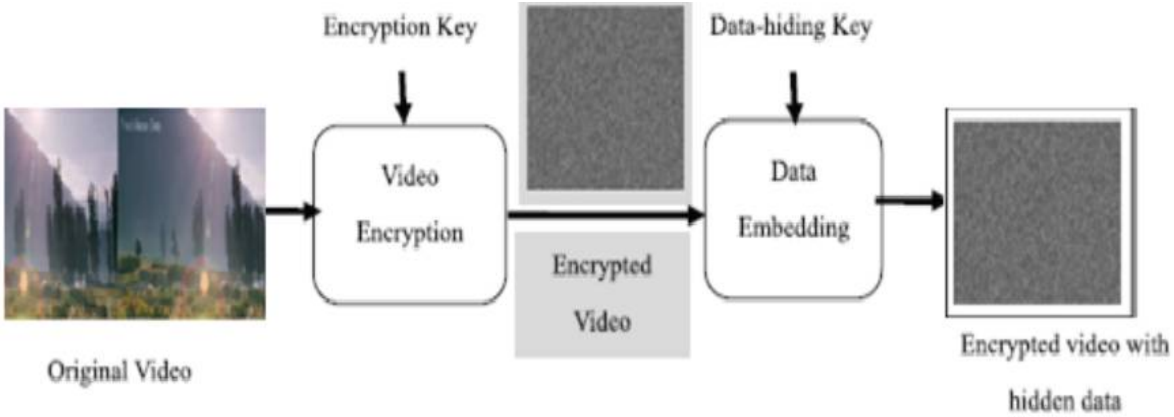

Fig 1.Video Encryption and Data Embedding at sender side

2. Data embedding

In the embedding of data contains embed the additional data into the encrypted video stream. There are few methods for embedding the data into the videos i.e. LSB, codeword method. LSB means that it embeds the bit of message into the each pixel of that image called LSB technique. Here we used codeword for embedding the data. There are three limitations that satisfy codeword method, are as follows:

1. First, the bit stream after codeword substitution decoded by standard decoder.

2. Second, keep that bit rate remains not changed, means that the original codeword and substituted codeword must have same size.

3. Third, after decryption of video the information remains hidden, it cannot visible to a human observer.

DOI: 10.15680/IJIRCCE.2016. 0404174

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

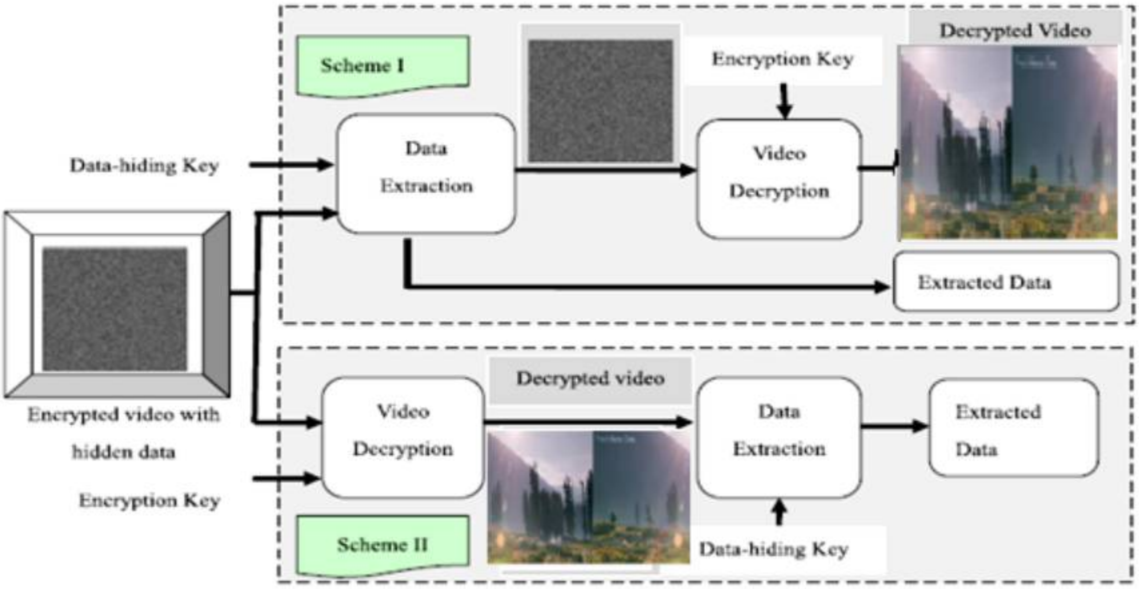

Fig 2.Data Extraction and Video Decryption at receiver side.

3. Data extraction

Data extraction can be done in encrypted domain and decrypted domain. In encrypted domain contains first extraction of hidden data and then decryption of video using encryption key. In decrypted domain contains firstly decryption of video using encryption key and then extract data using data hider key. If the codeword belongs to code space C0 then extracted data bit is 0. If the codeword belongs to code space C1 then extracted data bit is 1.

IV. PSEUDO CODE

Pseudo code for codeword substitution as follows:

```
If (data bit==0)
{
    If(the codeword belongs to C0)
        The codeword is unmodified;
    else if(the codeword belongs to C1)
        The codeword is replaced with the corresponding codeword in C0.
}
else if(data bit==1)
{
    If(the codeword belongs to C1)
        The codeword is unmodified;
    else if(the codeword belongs to C0)
        The codeword is replaced with the corresponding codeword in C1.
}
```

V. Result Analysis

PSNR (Peak Signal to noise ratio), is widely used video quality metrics. PSNR are used to measure the perceptual quality of video, which illustrate the video quality between the original video and video after extraction and encryption process.

Input Data	Non-stego Video PSNR(dB)	Stego Video PSNR(dB)	Proposed Video (dB)
Video 1	39.6	38.33	39.89
Video2	35.84	35.5	36.87
Video 3	31.68	31.62	33.43
Video 4	38.44	37.91	39.32
Video 5	35.15	34.87	36.12
Video 6	32.31	32.17	33.15

Table 1. Comparison of PSNR with non-stego, stego and proposed video.

Therefore, the visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video which is shown in Table 1 that is comparison of PSNR. By modifying the compressed bit stream to embed additional data, the most important challenge is to maintain perceptual transparency, which refers to the modification of bit stream should not degrade the perceived content quality.

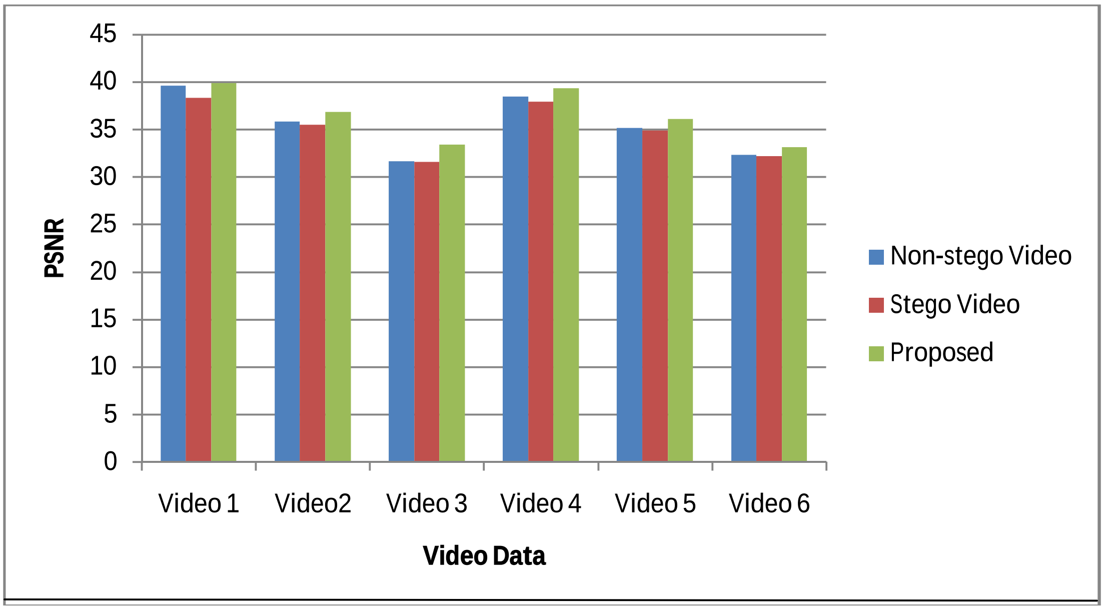

Fig 3. Graph for the comparison of non stego, stego and proposed videos

DOI: 10.15680/IJIRCCE.2016. 0404174

VI. Conclusion and Future Work

Information hiding in encrypted video is new topic for preserving the privacy and requirement into the cloud computing. The proposed scheme contains the three main parts, video encryption, data embedding, data extraction. This technique follows without decryption the re-encryption takes place. For the embedding the data into the video stream uses the codeword substitution method. At the time of data embedding the data hider does not know the original video contents. When we can decrypt the video the hidden information remains invisible to human. Data extraction is done in the encrypted domain and in decrypted domain. Here we preserve the confidentiality of video content and also preserve the privacy and the quality of video. It can be further enhanced by hide the information inside the audio file of videos instead of frames. It will help to retain picture quality of video.

References

1. W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, pp. 5856–5859 May 2011.
2. B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.
3. W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” Proc.SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.
4. D. W. Xu, R. D. Wang, and J. C. Wang, “Prediction mode modulated data-hiding algorithm for H.264/AVC,” J. Real-Time Image Process., vol. 7, no. 4, pp. 205–214, 2012.
5. X. P. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp.255–258, Apr. 2011.
6. A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” IEEE Trans. Multimedia , vol. 14, no. 3, pp. 703–716, Jun. 2012.
7. S. W. Park and S. U. Shin, “Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC),”New Directions Intell. Interact. Multimedia, vol. 142, no. 1, pp. 351–361, 2008.
8. W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using sidematch,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012
9. X. P. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol.7, no. 2,pp. 826–832, Apr. 2012D.
10. Z. Shahid, M. Chaumont, and W. Puech, “Fast protection of H.264/AVCby selective encryption of CAVLC and CABAC for I and P frames,”IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 5, pp. 565–576, May 2011.
11. K. D. Ma, W. M. Zhang, X. F. 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.
12. T. Stutz and A. Uhl, “A survey of H.264 AVC/SVC encryption,”*IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3,pp. 325–339, Mar. 2012.
13. S. G. Lian, Z. X. Liu, and Z. Ren, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol. , vol. 17, no. 6, pp. 774–778, Jun. 2007.
14. D. W. Xu, R. D. Wang, and J. C. Wang, “Prediction mode modulated data-hiding algorithm for H.264/AVC,” *J. Real-Time Image Process.*,vol. 7, no. 4, pp. 205–214, 2012.
15. J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, “An improved selective encryption for H.264 video based on intra prediction mode scrambling,” *J. Multimedia*, vol. 5, no. 5, pp. 464–472, 2010.

BIOGRAPHY

Priyanka R Jakhalekar is a M.E Student in the Computer Engineering Department, Dr. D.Y. Patil School of Engineering, Lohgaon, Pune, India. Her research interests are Data Mining and Network Security.

Prof.Pankaj Agarkar is a Assistant Professor and PG-Coordinator in Dr. D.Y.Patil School of Engineering, Lohgaon, Pune, India. He has 20 years of experience in teaching.