WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AN EFFICIENT AND SECURE DATA HIDING USING ENCODED VIDEO STREAM

Mr.A.Yoganathan[1], Mr.C.A.Kandasamy[2], Ms.A.Bakya[3], Ms.S.Aswini[4], Ms.K.R.Akshaya[5], Mr.P.Ajith[6]

[1,2] Assistant Professor, Department of MCA, K.S.R. College of Engineering, Tiruchengode **yoguayn@gmail.com**, Kandamca86@gmail.com

[3, 4, 5, 6] Student, Department of MCA, K.S.R. College of Engineering, Tiruchengode, bakyabsc09@gmail.com , aswini.saravanan11@gmail.com akshayakr27@gmail.com, ajithaji1999ypw@gmail.com

ABSTRACT

Generally, digital video sometimes are stored and processed in an encrypted format to maintain privacy and security. For the purpose of content notation, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption conserves the confidentiality of the content. In addition, it is more proficient without decryption followed by data trouncing and re-encryption. This study proposes a novel scheme of data hiding directly in the encrypted version of AVI video stream, which includes the following three parts, i.e., AVI video encryption, data embedding, and data extraction.

Keywords – Encryption , Data Embedding, Data Extraction

INTRODUCTION

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to- day life for various applications. Various techniques have been developed in Image Processing during the last four to five decades. Most of the techniques are developed for enhancing images obtained from unmanned spacecrafts, space probes and military reconnaissance flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices and graphics software. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource Bin Zhao [1] et al describe the most watermarking schemes for copyright protection, a seller usually embeds a watermark in multimedia content to identify a buyer.

Rini. J et al [6] describe the secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. Divya h.T et al [3] describe the data hacking is very challenging problem in today's internet world. So Reversible Data Hiding (RDH) in encrypted image is used. With this method original cover can be recovered. In this paper, they proposed a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. This method provides improved PSNR ratio and recovers image with its original quality.

D. Prabhakar et al [4] describe the IMAGE watermarking, which is finding more and more support as a possible solution for the protection of intellectual property rights. Dawen Xu [2] described According to H.264/AVC specific codec architecture, an efficient watermarking scheme for H.264/AVC video is proposed [15]. It is not necessary to fully decode H.264/AVC compressed stream both in the embedding and extracting processes. Experimental results show that the proposed scheme can preserve high imperceptibility while achieving enough robustness against various attacks such as re-quantization, transcoding, AWGN, brightness and contrast adjustment

2.1 Techniques

The Motion Vector Difference (MVD) Encoding is carried out. In order to protect both texture information and motion information, not only the IPMs but also the motion vectors should be encoded. In avi file, motion vector prediction is further performed on the motion vectors, which yields MVD. The values of MVDs are taken. For Data Embedding, in the encrypted bitstream of avi frames, the proposed data embedding is accomplished by substituting eligible codewords of various Levels. Since the sign of Levels are encrypted, data hiding should not affect the sign of Levels. For Data Extraction scheme, the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple.

In addition, the given raw data is perturbed first, then encrypted with 3DES encryption and addition secure key is also embedded in the message. Then the data is embedded in video file. During decryption, the original video file as well as the decrypted data is retrieved. Then the data is decrypted and the perturbed data is found out. Then the original raw message is retrieved.

3. EXPERIMENTS

In the following way the proposed scheme is designed and experimented and the results will be analyzed. The module architecture diagram is shown in Figure 1 which describes the entire process of data hiding techniques

3.1 Add Video File

In this phase, the video file selection is carried out open file dialog control and the path is displayed in text box and the video is displayed in media player control. Then the video file record is saved into 'Videos' table.

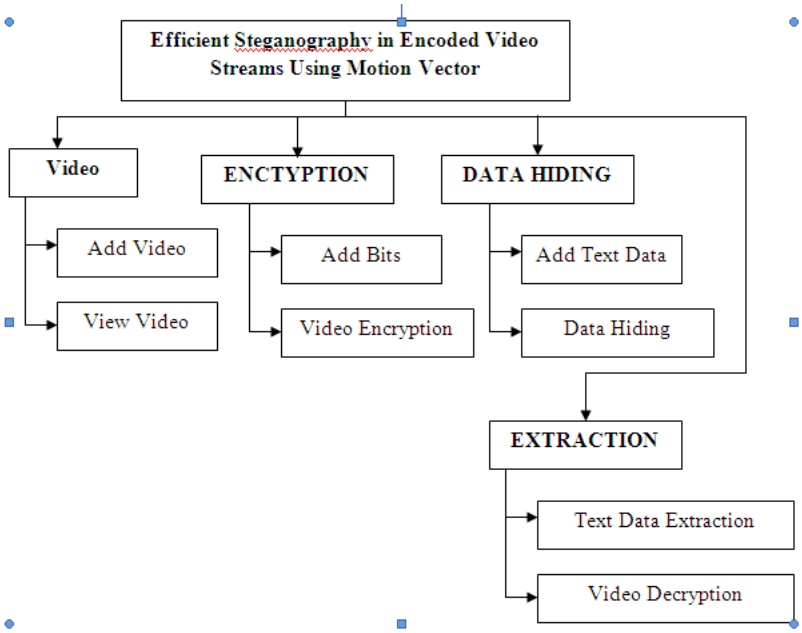

Figure 1: Module Architecture Diagram

3.2 Video File Selection For Enhanced Stagnography

In this phase, the original video file selection is carried out and taken for Video Encryption. Then Encrypted Video is checked for playing in the player

3.3 Text Data Input and Perturbation

In this phase, the text message is given as input. Two random characters are inserted between each two consecutive characters in the text message and the message is perturbated (confused).

3.3 Encrypted Data Embedding

In this phase, the text data is encrypted using 3DES encryption and the bit sequences are taken for hiding. So, using the given data hiding key, the data embedding process is carried out with the given encrypted data. Finally, the encrypted data is made to hide inside the encrypted video.

3.4 Encrypted Data Extracting and Decryption

In this phase, the encrypted video with the hidden data is selected. For data extraction, Data-hiding key is given and the data is first extracted and then decrypted. Then with the video decryption key (same as encryption key), the video is decrypted and original video is obtained. The operation may be carried out in two types.

- First data extraction followed by Video

- Decryption Video decryption followed by data extraction.

4. PROPOSED ALGORITHM

4.1 Video file Parsing

In this process, the video file's number of frames is found out and extracted using AviFil32.dll methods. The frames are saved in a folder.

4.2 Text Data Input and Perturbation

i. Text message selection.
ii. Two random characters are inserted between each two consecutive characters in the text message and the message is perturbated (confused).

4.3 Encrypted Data Embedding

i) Text data is selected.
ii) Key for TripleDES encryption is given
iii) Bit sequences of the perturbated data is taken for hiding.
iv) Frame data of the video is encoded with different pixel values.
v) Using the given data hiding key, the data embedding process is carried out with the given encrypted data.
vi) The encrypted data is made to hide inside the frames in the least significant bits.

4.4 Encrypted Data Extracting and Decryption

i) The encrypted video with the hidden data is selected.
ii) For data extraction, Data-hiding key is given and the data is first extracted and then decrypted.
iii) Then with the video decryption key (same as encryption key), the video is decrypted and original video is obtained.
iv) The operation may be carried out in two types.

- First data extraction followed by Video decryption or
- Video decryption followed by data extraction.

5. Conclusion

The reversible data hiding in encrypted image is examined. Most of the work on reversible data hiding focuses on the data embedding and extracting on the plain spatial domain. But, in some applications substandard subordinate or a channel administrator hopes to tag on some bonus message, such as the foundation information, image notation or validation data, within the encrypted image though user does not know the original image content. And it is also hopeful that the inventive content should be recovered without any blunder after image decryption and message pulling out at receiver side.

A content owner encrypts the original image using an encryption key, and a data-hider can embed supplementary data into the encrypted image using a data-hiding key while the user does not know the actual content. With encrypted image containing additional data, the receiver may first decrypt it with the encryption key, and then extract the embedded data and recover the original image with the data-hiding key. In this scheme, the data extraction is not distinguishable from the content decryption.

In other words, the supplementary data should be hauling out from the decrypted image, so that the crucial content of original image is uncovered before data pulling out, and if someone has the data-hiding key but not the encryption key, they can't haul out any information from the encrypted image which containing additional data.

6. Future Enhancement

In this study, data hiding is completed entirely in the encrypted domain and the method can preserve the confidentiality of the content completely. With the encrypted video contains the hidden data, the data extraction can be carried out either in encrypted or decrypted domain. In this experimental study video taken in the .avi file only. In future various kinds of file formats can be taken for the entire process. Also, the data hiding process with no degradation in video quality can be carried out.

References

[1] 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

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

[3] 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

[4] 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

[5] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 3, pp. 425–437, Mar. 2013.

[6] Yiqi Tew and Kok Sheik Wong, "An overview of Information Hiding in H.264/AVC Compressed Video", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 24, No. 2, pp. 305-319, 2014.

[7] Dawen Xu, Rangding Wang and Jicheng Wang, "A novel watermarking scheme for H.264/AVC video authentication", Signal Processing: Image Communication, Vol. 26, No. 6, pp. 267-279, 2011

[8] M. Noorkami and R. M. Mersereau, "A framework for robust watermarking of H.264-encoded video with controllable detection performance", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 1, pp. 14-23, 2007.

[9] Jing Zhang, A. T. S. Ho, Gang Qiu and P. Marziliano, "Robust video watermarking of H.264/AVC", IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 54, No. 2, pp. 205-209, 2007.

[10] A. Mansouri, A. M. Aznaveh, Torkamani-Azar F and F. Kurugollu, "A Low Complexity Video Watermarking in H.264 Compressed Domain", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 649-657, 2010

[11] H. A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 1, pp. 14-18, 2011.

[12] Jian Li, Hongmei Liu, Jiwu Huang and Yun Q. Shi, "Reference index-based H.264 video watermarking scheme", ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 8, No. 2S, pp. 1-22, 2012.

[13] Dawen Xu, Rangding Wang and Y. Q. Shi, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 4, pp. 596-606, 2014.

[14] Dawen Xu, Rangding Wang and Jicheng Wang, Prediction mode modulated data-hiding algorithm for H.264/AVC", Journal of Real-Time Image Processing, Vol.7, No.4, pp 205-214, 2012.

[15] Dawen Xu and Rangding Wang, "Watermarking in H.264/AVC Compressed Domain Using Exp-Golomb Code words Mapping", Optical Engineering, Vol. 50, No. 9, pp. 1-11, 2011.

[16] Yulin Wang and A. Pearmain, "Blind MPEG-2 video watermarking robust against geometric attacks: a set of approaches in DCT domain", IEEE Transactions on Image Processing, Vol. 15, No. 6, pp. 1536-1543, 200.

[17] 300 Million UMTS Subscribers. http://www.3gpp.org/300-million-UMTS-subscribers

[18] F. Qian, Z. Wang, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck. Characterizing Radio Resource Allocation for 3G Networks. In IMC, 2010

[19] R. Friedman, A. Kogan, and K. Yevgeny, "On power and throughput tradeoffs of WiFi and bluetooth in smartphones," in Proc.INFOCOM, Shanghai, China, Apr. 2011

[20] T. Pering, Y. Agarwal, R. Gupta, and C. Power, "Coolspots: Reducing the power consumption of wireless mobile devices with multiple radio interfaces," in Proc. ACM MobiSys, 2006, pp. 220–232.