IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

A Review on "Hide the data in Encrypted video using Private Key for secure Transmission"

Abhijeet Kotwal[1], Prof.K.N.Shedge[2]

PG Student, Computer Engineering Department, S.V.I.T. Chincholi, Nashik, India [1]

Assistant Professor, Computer Engineering Department, Chincholi, Nashik, India [2]

Abstract: Now Days all people have more concentration about security about data when sending data on the network. Hence new concept is invented, Data hiding in Encrypted video is invented. Data hiding in video preferred encryption algorithm using secrete key because it maintains the originality of the transmitted data at the at the receiver end after decryption. In this way data hide in encrypted video preserve the confidentiality of the content. The data hider may add the additional data in the encrypted video without knowing the original video content. In other hand decryption level the two schemes is available for getting the data first scheme is get the data then decrypt the video and second one is first decrypt the video then get the data.

Keywords: Data Encapsulation, Feature Extraction, Video Coding, Privacy protection, Data Mining.

I. INTRODUCTION

For transmitting any confidential data over the network many issues like hacking, stealing this data may arise. So techniques which prevents this attacks on such confidential data is known as Encryption , In encryption original data is transformed into some secure format so that it will be very hard to understand by third party person. Information adding and data hiding systems play an important role in addressing couple of major challenges that have arisen from the widespread distribution of multimedia content over digital communication networks. In particular, these systems are enabling technologies for enforcing and protecting copyrights, authenticating and detecting tampering of multimedia signals images. This techniques mostly used in medical imaginary, military imaginary or law forensic, in which department distortion of original cover is acceptable.

II. LITERATURE SURVEY

Robust "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. [1]

"Watermarking of compressed and encrypted JPEG2000 images" by A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, Robust watermarking of compressed and encrypted JPEG2000 images, Digital asset management systems (DAMS) generally handle media data in a compressed and encrypted form. It is sometimes necessary to watermark these compressed encrypted media items in the compressed-encrypted domain itself for tamper detection or ownership declaration or copyright management purposes[2].

A.**ARCITECTURE**

"An efficient security system for CABAC bin-strings of H.264/SVC," M. N. Asghar and M. Ghanbari,

An efficient security system for CABAC bin-strings of H.264/SVC, we propose a complete security system for H.264/scalable video coding (SVC) video codec and present a solution for the bit-rate and format compliance problems by careful selection of entropy coder syntax elements (bin-strings) for selective encryption (SE), and the problem of managing multiple layer encryption keys for scalable video distribution. [3]

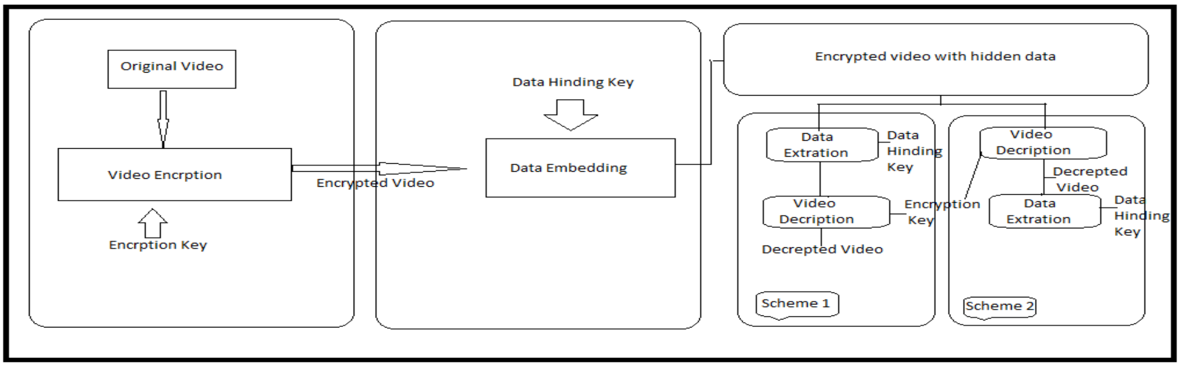
"Prediction mode modulated data-hiding algorithm for H.264/AVC" by D. W. Xu, R. D. Wang, and J. C. Wang, A new real-time watermarking technique based on H.264/AVC video standard is proposed. The algorithm works in the compressed domain by embedding watermark bits into quantized DCT coefficients of 4×4 blocks of the I-frame during the Context-based Adaptive Variable Length Coding (CAVLC) process. [4]
Data hiding in MPEG video files using multivariate regression and flexible macro block ordering T. Shanableh.

This approach hides message bits by modulating the quantization scale of a constant bitrates video. A payload of one message bit per macro block is achieved. A second order multivariate regression is used to find an association between macro block-level feature variables and the values of a hidden message bit. The regression model is then used by the decoder to predict the values of the hidden message bits with very high prediction accuracy. [5]

III.PROPOSED SYSTEM

In this scheme of data hiding in the encrypted version videos is presented, which includes four parts i.e., Frame selection video encryption, data embedding and data

DOI 10.17148/IJARCCE.2015.41289



extraction. By analysing video codec, data hider added data with encrypted video in encryption domain by Using codeword substitution technique or other technology, data extraction can be done in the encrypted and decrypted module. For this arithmetic compression is done efficient transmission of data utilizing minimum bandwidth. Also, the size of file or video is same as the original file after encryption and data hiding.

The purpose of hiding such the information I totally depend upon the user application or requirement.

i. Imperceptibility- The video with data and original data source should be perceptually identical.
ii. Robustness- The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
iii. Capacity-Maximize data embedding payload.
iv. Security- Security is in the key.

Video Encryption:

Video Encryption in a technique H.264/AVC video encryption scheme with good presentation including efficiency, security and performance. By considering the property of H.264/AVC video codes three parts i.e. IPMs, MVDs, and residual coefficient. Are encrypted with cipher stream. The proposed algorithms not work in H.264/AVC encoding techniques but in compressed domain. In this condition bit stream modified directly. Selective encryption in the H.264/AVC compressed domain has been already presented on context-adaptive variable length coding and the CABAC (context-adaptive binary arithmetic coding).

Data Embedding:

There will be more than one techniques available for add data in to H.264/AVC bit stream directly, but this method cannot be used in encryption domain. In encrypted bit stream of h.264/AVC, the proposed data substituting allow to codeword's of level. The sign of level are encrypted data hiding is not affects the sign of levels. The codeword substitution follow the limitation first, after codeword word substitution the bit stream must remain compliance, second is keep bit rate constant, the substituted bit-word size remains constant. Third one is data hiding does cause visual degradation but the impact should be kept to minimum. That's why the data is not visible to normal user after data adding or code word substitution.

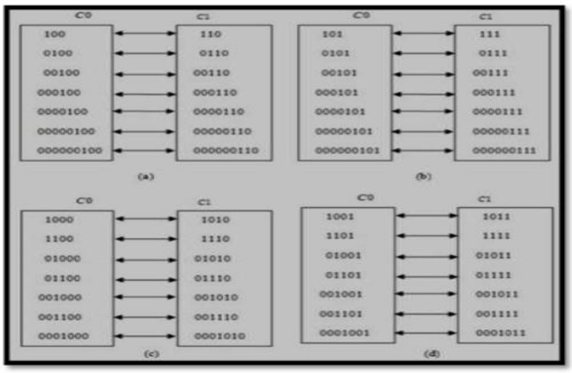


Fig. CAVLC codeword mapping

Data Extraction:

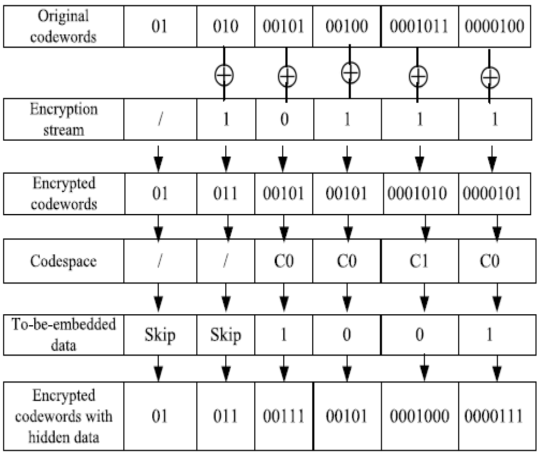
The hide data can be retrieving in encrypted or decrypted domain. The process of extract the data is very fast and simple. The extract the data in two schemes:

Scheme I: Encrypted Domain Extraction. To protect privacy, a database manager have only permission to get data hiding key and work with data hiding key in encryption/decryption domain. Data extraction in encrypted domain guarantees the feasibility of our scheme in this case. In encrypted domain, the encrypted video having hidden data sent directly to extraction module. Data extraction in encrypted domain guarantees the viability of our scheme in this case. In encrypted domain, as shown in below, encrypted video with hidden data is directly sent to the data extraction module,

Scheme II: Decrypted Domain Extraction. In scheme 1 data adding and extraction of hide data both performed in decryption domain. Some condition user decrypts the video first and after that extracts the data. For example, an authorized user, which needs the encryption key, received the encrypted video with hidden data. The received video can be decrypted using the encryption key. That is, the decrypted video still includes the hidden data, which can be used to trace the source of the data. In some cases, users want to decrypt the video first and extract the hidden data from the decrypted video. For example, a legal user, which owned the encryption key, received the encrypted video with hidden data. The received video can be decrypted using the encryption key. That is, the decrypted video still includes the hidden data, which can be used to trace the source of the data. Since the encryption streams depend on the encryption keys, the decryption is possible

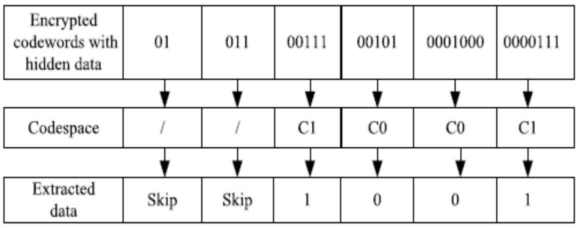
DOI 10.17148/IJARCCE.2015.41289

only for the authorized users. After create the decrypted codeword with data (hidden), the content owner can further extract the hidden information.



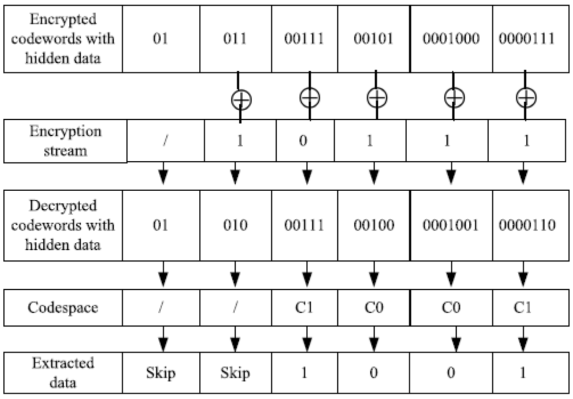
Original codewords	01	010	00101	00100	0001011	0000100
Encryption stream	/	1	0	1	1	1
Encrypted codewords	01	011	00101	00101	0001010	0000101
Codespace	/	/	C0	C0	C1	C0
To-be-embedded data	Skip	Skip	1	0	0	1
Encrypted codewords with hidden data	01	011	00111	00101	0001000	0000111

Fig Data embedding.



Encrypted codewords with hidden data	01	011	00111	00101	0001000	0000111
Codespace	/	/	C1	C0	C0	C1
Extracted data	Skip	Skip	1	0	0	1

Fig Data extraction in encrypted domain.



Encrypted codewords with hidden data	01	011	00111	00101	0001000	0000111
Encryption stream	/	1	0	1	1	1
Decrypted codewords with hidden data	01	010	00111	00100	0001001	0000110
Codespace	/	/	C1	C0	C0	C1
Extracted data	Skip	Skip	1	0	0	1

Fig Data extraction in decrypted domain.

B.**ALGORITHM**

1. Generate encryption streams with the encryption keys as given in Architecture.
2. The codeword of IPMs, MVDs, Signoff Trailing Ones and Levels are identified by parsing the encrypted bit stream.
3. The decryption process is identical to the encryption Process. The encrypted codeword's can be decrypted by performing XOR operation with generated encryption streams, and then two XOR operations cancel each other out, which renders the original plaintext. Since the encryption streams depend on the encryption keys, the decryption is possible only for the authorized users. After generating the decrypted codeword with hidden data, the content owner can further extract the hidden information.
4. The last bit encryption may change the sign of Level. However, the encrypted codeword and the original codeword are still in the same code spaces. If the decrypted codeword of Level belongs to code space C0, the extracted data bit is "0". If the decrypted codeword of Level belongs to code space C1, the extracted data bit is "1".

Generate the same pseudo-random sequence P that was used in embedding process according to the data hiding key. The extracted bit sequence should be decrypted to get the original additional information.

IV. CONCLUSION

At the end we conclude that, we have partially created the basics of our project. I studied the existing system some pros and cons of existing system because of this Cons we proposed a new approach which overcomes the cons. In proposed system, data is hiding in video using encryption key and recover the original image / video after decryption process and also get message.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014

[2] 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.

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

[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] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 455–464, Apr. 2012.

[6] 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.

[7] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Let. vol. 19, no. 4, pp. 199–202, Apr. 2012.

[8] D. K. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in Proc. IEEE ICME, Singapore, Jul. 2010,pp. 117–121.

[9] S. W. Park and S. U. Shin, "Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC)," New Directions Intel. Interact. Multimedia, vol. 142, no. 1, pp. 351–361, 2008.

[10] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

DOI 10.17148/IJARCCE.2015.41289