International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-7, July 2015

An Efficient Data Hiding Approach For Video Using Twelve Square Substitution Algorithm

Jasmi A, Vishnu Damodaran

Abstract— **Transmission of video over internet is vulnerable to verity attacks from untrustworthy system administrators. So it should be stored and processed in an encrypted format, to maintain security and privacy. It is necessary to perform data hiding in these encrypted video. In this paper, the data hiding is performed by the encryption of a text data using twelve square substitution cipher. It avoids the leakage of video content, which can help address security and privacy. It includes three parts; video encryption, data embedding and data extraction. The efficiency of the proposed scheme is determined by the value of peak signal to noise ratio (PSNR) and structural similarity index measurement (SSIM). Experimental result shows the feasibility and efficiency of the proposed scheme.**

Index Terms— **Data hiding, H.264/AVC, Video encryption, Twelve square substitution cipher.**

I. INTRODUCTION

Most used compression standards for video are MPEG2/H.262, H.263, and MPEG4 Part2[8]. H.264/AVC is a newest compression standard used for video compression, it converts digital video into a format that require less capacity. A significant reduction in file size can achieved without an adverse effect on the visual quality. The main goal of H.264/AVC video standard[8] have been used to enhance the compression performance and provide a provision of a networks friendly video representation addressing conversational (video conferencing, video telephony etc) and non-conversational (storage, broadcast and streaming) applications. H.264/AVC has achieved a significant improvement in rate distortion efficiency[7], image and video quality relative to existing standards. But it provides low bitrates. Encryption techniques provide the basic technology for constructing secure multimedia system, it is the process of encoding message or information in such a way that only authorized party can decode it. In order to provide real time reliable security of digital images and videos, many different encryption algorithms have been developed for secure communications. H.264/AVC is a compression standard, it includes three sensitive parts. Intra prediction mode (IPM), motion vector differences (MVD) and residual data coefficients. To improve the performance including efficiency and security, the codeword of IPM, codeword of MVD, and the codeword of residual data are encrypted with stream ciphers. Digital videos of are sometimes stored and processed in an encrypted format. It is necessary to perform data hiding in encrypted version video to maintain security, privacy and preserves the confidentiality of the content. Data hiding or information hiding or data encapsulation is one of the important techniques for reducing the increasing attacks. It is mainly used for hiding internal details to maintain security and privacy. The compressed video is encrypted using bit XOR operation and a secret data is hidden in the encrypted video by using twelve square substitution algorithm for providing more security. Hidden data is extracted and the original video is reconstructed in the decryption process. This technology can apply to prominent application scenarios. For example, surveillance or medical videos have been encrypted for protecting the privacy of the people or a data base manager may embed the personal information into corresponding encrypted videos to provide data management capabilities in encrypted domain.

Jasmi A, Department of ECE, Younus College of Engineering and Technology, Kollam, Kerala, India.
Vishnu Damodaran, Assistant Professor, Department of ECE, Younus College of Engineering and Technology, Kollam.

II. RELATED WORK

Till now, few successful data hiding scheme in the encrypted domain have been found. A watermarking scheme in the encrypted domain using paillier cryptosystem based on the security requirement [4] and the encrypted image watermarking algorithm based on walsh hadamard transform using paillier cryptosystem[2] is presented. Due to the constraints of paillier cryptosystem, the encryption of an original image results in high overhead in storage and computation. Next reversible data hiding in encrypted images and separable reversible data hiding in encrypted images are proposed. The main disadvantage is that the encryption is performed by using bit-XOR operation. In these methods the host image is in uncompressed format. A robust watermarking algorithm[3] is proposed to embed watermark into compressed and encrypted JPEG 2000 images.

The main drawback of this algorithm is it may be subjected to some errors on data extraction or image restoration. At this time secure advanced video coding based on selective encryption algorithm[6] is proposed, according to this encryption scheme, both the texture and motion information are encrypted. Which make it difficult to recognize the texture and motion information in the video frames. To hide secret data codeword substitution[1] is used in which different codeword of levels are substitute without changing the length of codeword but the quality of video is less. If the receiver knows the data hiding key, it can find the embedded parameter and easily extract the bit in an encrypted form. Original data is recovered with the help of data hiding key, here the accuracy and security is comparatively inefficient. H.264/AVC is the latest video compression standard, it build on the concept of MPEG 2 and MPEG 4 visual and offers the

potential for better quality compressed video and greater flexibility in compressing, transmitting and storing video. In H.264/AVC compression[8], the intra-prediction mode (IPM), motion vector differences(MVD), and DCT coefficients' signs are encrypted. This encryption scheme offer good performance including security.

III. PROPOSED SYSTEM

In this section, a new technique called twelve square substitution algorithm is used to hide the secret message. The system involves H.264/AVC Coder[7], data hiding and data extraction. The content owner encrypts the original H.264/AVC video stream with encryption key using standard stream cipher to produce an encrypted video stream. Then the data hider can embed additional data into encrypted video stream by using twelve square substitution algorithm without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

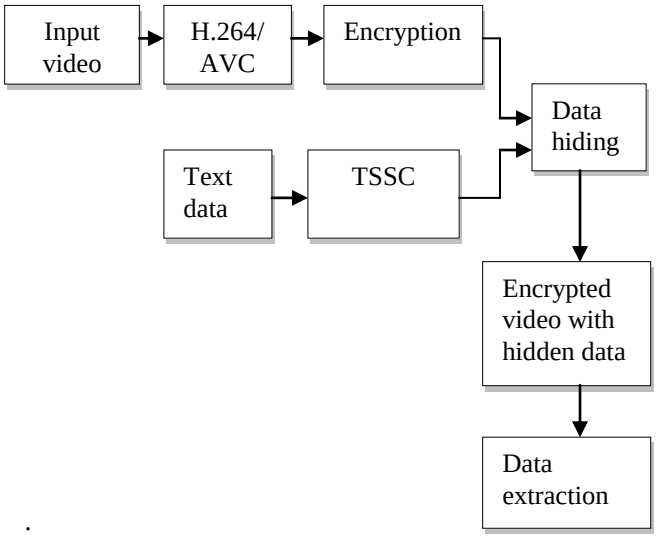

Fig.1.Video Encryption and Data hiding

A. *H.264/AVC Coder*

H.264 is a standard used for video compression, It converts digital video into a format that requires less capacity when it is stored or transmitted, a significant reduction in file size can be achieved with little or no adverse effect on the visual quality.It include encoder and decorder.H.264/AVC encoder carries out the operation such as prediction, transform and encoding process. decoder perform the reverse operations such as video decoding, inverse transform and reconstruction of the video. Video compression (or video coding) is an important technology for applications such as digital television, DVD-Video, videoconferencing, mobile TV and internet video streaming..

B. *Twelve Square Substitution Cipher*

In this paper, an efficient method called twelve square substitution algorithms is used to encrypt the hidden text data. It includes alphabets, numerals and special characters. The twelve-square cipher encrypts alphabets, digits and special characters and thus is less susceptible to frequency analysis attacks. It uses six 5 by 5 matrices each arranged in a square, as shown in table-I. Each of the 5 by 5 matrices contains the letters of the alphabet (usually omitting "Q" to reduce the alphabet to fit into the square) and another six 6 by 7 matrices arranged in squares for digits and special characters, as shown in table-II. All the special characters and digits from your desktop/laptop keyboard.

TABLE I
Plain Text and Cipher Text (Alphabets)

Square-1	Square-2	Squre-3
a b c d e f g h i j k l m n o p r s t u v w x y z	f g h i j k l m n o p r s t u v w x y z a b c d e	k l m n o p r s t u v w x y z a b c d e f g h i j
Squre-4	Squre-5	Squre-6
g m r i t a b c d e f h j k l n o p s u v w x y z	a b c d e f h j k l g m r i t n o p s u v w x y z	a b c d e f h j k l n o p s u v w x y z g m r i t

Table I arranged as follows. In Square-1, we have twenty five alphabets excluding the alphabet q, in each row we arranged five alphabets. Square-2 is created from square-1 by taking the first row of square-1 to fifth row place and other rows one position up. Similarly square-3 is created from square-2 by taking the first row of square-2 to fifth row place and other rows one position up. In square-4, we have used a word gmrit in the first row which comprises of the five alphabets and the remaining twenty alphabets are arranged in other four rows continuously excluding the alphabets of the word "gmrit". Square-5 is made from square-4 by taking the first row to third row place. Similarly square-6 is made from square-4 by taking the first row to fifth row place. In table II square-7, the numerals and special characters from a standard laptop are arranged in six rows and seven columns. Square-8 is made from square-7 by taking the first row to sixth row place. Similarly square-9 is created from square-8 by taking the first row of square-8 to sixth row place. Square-10 is created from square-7 by arranging the row elements in columns. Square-11 is created from square-10 by taking the first row of square-10 to third row place. Similarly square-12 is constructed from square-10 by taking the first row into sixth row place.

TABLE II
Plain Text and Cipher Text (Digits And Special Characters)

Square-7	Square-8	Squre-9
0 1 2 3 4 5 6 7 8 9 ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? /	7 8 9 ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? / 0 1 2 3 4 5 6	# $ % ^ & * ( ) _ - + = { [}] ; : " ' \ | < , > . ? / 0 1 2 3 4 5 6 7 8 9 ` ~ ! @
Squre-10	**Squre-11**	**Squre-11**
0 6 ! & + ; < 1 7 @ * = : , 2 8 # ({ " > 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ " > 0 6 ! & + ; < 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ " > 3 9 $) [' . 4 ` % _ } \ ? 5 ~ ^ -] | / 0 6 ! & + ; <

The plain text is read from left to right. If the character is an alphabet it refers to table-I, otherwise if it is a number or a special character it refers to table-II. While scanning the plain text the first alphabet's plain text is in square-1 and its cipher is in same row and column location of square-4. The second alphabet, its plain text is in square-2 and cipher text is in same row and column location of square-5. The third alphabet, its plain text is in square-3 and cipher text is in same row and column location of square-6 and so on. There for, the secret message is the combination of alphabets, number and special characters.
For example, the plain text is: jas3010
Its cipher text is: evj&5~0

IV. Experimental Results

A. *Security of Encryption Algorithm*

The security includes both cryptographic security and perceptual security. Cryptographic security[1] denotes the security against cryptographic attacks. In the proposed scheme, twelve square substitution cipher is used to encrypt the additional data. They have been proved to be secure against cryptographic attacks. Perceptual security refers to whether the encrypted video is unintelligible or not. It depends on the encryption scheme's properties, such as encryption of IPM, MVD, residual coefficients[7]. Which keep perceptual security of encrypted video. The proposed scheme use twelve square substitution algorithm, it shows high security rather than bit XOR operation. The demonstration of original video frame and encrypted video frame with hidden data is shown in Fig.2 and Fig. 3, corresponding decrypted video frame is shown in Fig.4.

Fig.2. Original Video Frame

Fig.3. Encrypted Video with Hidden Data

Fig.4.Decrypted Video Frame with Hidden Data

B. *Visual Quality of Stego Video*

The perceptual quality of the video can be evaluated by the PSNR(peak signal to noise ratio), SSIM(structural similarity index measurement). PSNR is defined as the ratio between the maximum possible power of a signal and the power of occurring noise, it is widely used objective video quality metric. However, it perfectly correlated with a perceived visual quality due to non linear behavior of human visual system. The graphical representation of PSNR value of each frames is shown in Fig. 5. It illustrates the better PSNR giving the twelve square substitution cipher compare with the existing XOR operation.

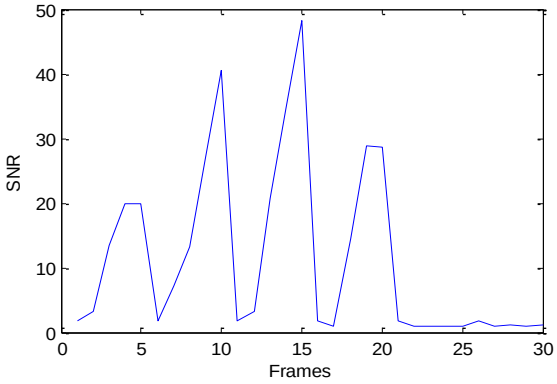

Fig.5. Peak Signal to Noise Ratio

SSIM is a method for measuring the similarity between two images. Measuring the image quality based on initial uncompressed or distortion free image as reference. SSIM is designed to improve peak signal to noise ratio and mean square error. SSIM index lies in the range between 0 and 1, where 1 indicate reference image is identical than the target image. The graphical representation of SSIM value of each frame is shown in Fig.6. Since H.264/AVC is lossy compression, in order to better illustrate the data hiding on the video quality.

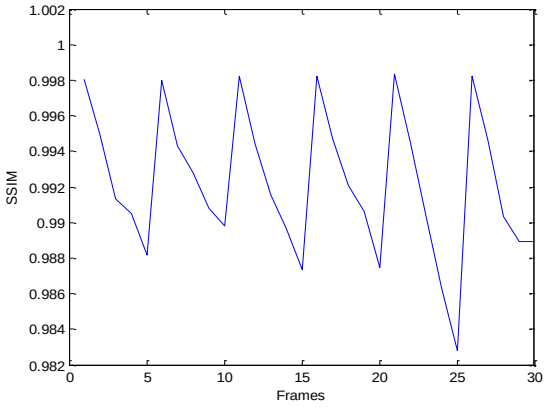

Fig.6.Structural Similarity Index Measurement

The comparison between existing system and proposed system is shown in Table.III. It illustrate the comparison between the PSNR and SSIM value of existing system, that is the data hiding key is encrypted with XOR operation and proposed system using twelve square substitution cipher.

TABLE III

Comparison Between PSNR And SSIM Value Of Existing And Proposed Systems

Frames	PSNR		SSIM	
	Existing system	Proposed system	Existing system	Proposed system
1	3.150	9.039	0.9970	0.9981
2	11.90	24.49	0.9932	0.9940
3	20.27	30.66	0.9913	0.9933
4	21.24	30.29	0.9905	0.9920
5	20.29	35.44	0.9980	0.9980
6	3.201	9.054	0.9940	0.9943
7	11.46	30.51	0.9920	0.9928
8	11.21	28.54	0.9908	0.9925
9	15.25	30.50	0.9908	0.9909
10	20.04	28.20	0.9953	0.9980

V. Conclusion

Data hiding is the one of the important technique is to improve the security and privacy of the systems. This paper presents an algorithm to embed additional data in encrypted H.264/AVC bit streams. A text is hidden by using twelve square substitution cipher algorithm without knowing the original video content. Since data hiding completely entirely in the encrypted domain, this method can preserve the confidentiality of the content. It provides two level of security, one is the cryptographic level and other is the steganography level. Multiple substitution is the one of the advantage of twelve square substitution algorithm. Encrypted video contain hidden data, data extraction can be carried out either in encrypted or decrypted domain.

Acknowledgment

The authors would like to thank anonymous reviewers for their constructive comments and valuable suggestions that helped in the improvement of this paper.

References

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, "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

[2] P. J. Zheng and J. W. Huang, "Walsh-Hadamard Transform In The Homomorphic Encrypted Domain And Its Application In Image Watermarking," in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012

[3] 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

[4] 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

[5] 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.

[6] S. G. Lian, Z. X. Liu, "Secure advanced video coding based on selective encryption algorithm" IEEE Transaction on consumer electronics, Vol. 52, no.2 , pp. 621-629, May 2006

[7] Wen Gao, M. Siwei, "Rate distortion analysis for H.264/AVC video coding and its application to rate control", IEEE Transaction on video technology, Vol 15, No. 12,pp.1533-1544,2005.

[8] Wiegand T, Sullivan G. J, Bjontegaard G, and Luthra A, "Overview of the H.264/AVC video coding standard," IEEE Transaction Circuits System Video Technology, Vol. 13, No. 7, pp. 560–576, 2003

Jasmi A, M. Tech. Student, Applied Electronics and Instrumentation Engineerig, Department of ECE, Younus College of Engineering and Technology, Kollam, Kerala, India.

Vishnu Damodaran, Assistant Professor, Department of ECE, Younus College of Engineering and Technology, Kollam, Kerala, India.