Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Enhanced Data Security Transmission of H.264/AVC Video Stream

A.S.Korde[1], Prof. A. P. Hatkar[2]
[1,2]*E & TC department, SVIT Chincholi, Nashik*

Abstract—For the purpose of highly secure data transmission and privacy, sometime there is need of storage and encryption of digital video.During the encryption of video, the data hiding can be performed. In this paper proposed scheme is the secure data transmission with directly hiding data in the encrypted version of H.264/AVC videos is presented, which includes three parts are H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce encrypted video stream and the code word substitution for the data embedding purposes, that it eligible codewords can be substituted. Without knowing the original video content, then, a data hider may embed additional data in the encrypted domain by using codeword substitution technique. Data extraction can be done either in the encrypted domain or in the decrypted domain, in order to adapt to different application. Furthermore, video file size is strictly preserved even after encryption and data embedding.

Keywords— Data hiding, encrypted domain, H.264/AVC, codeword substituting.

I. INTRODUCTION

The most technology trend which provides thehighly efficient computation and large-scale storage solution for video data is cloud computing [1]. The security of data in a cloud networking is critical and it is very important to maintain the security like confidentially, integrity and the availability over the cloud network as well as the other networks. The most popular used standard for video is H.264/AVC (Advanced Video Coding), gives the higher efficiency in video encoding [2]. To address the security and privacy concerns with cloud computing, the capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content. The additional information into an encrypted version of an H.264/AVC video by using data hiding technique, a cloud server can be embedded. The security and privacy can be protected, with the hidden information without knowing the original content which may design for the efficient compression performance and in therate-distortion efficiency in comparison with the existing standards. This technology can be used for many important applications such as the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people.

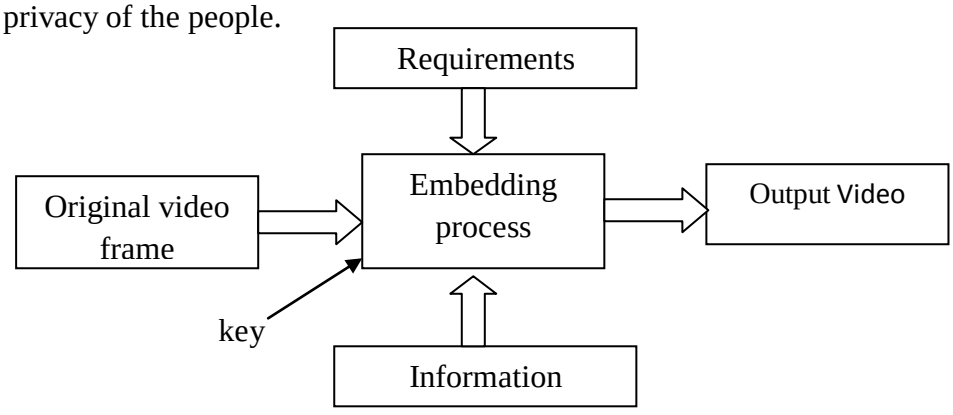

Fig.1 GeneralBlock diagram of data hiding

Fig.1 shows general block diagram of data hiding process which illustrate the process of information insertion in original video to achieve the specific features [2].

There are [2] various needs to manage and/or protect the vast number of videos including:

a. tracking illegal distribution of copyrighted video to secure business revenue;
b. hyperlinking related contents while ensuring the hyperlink information always stays intact with the video to enhance user experiences, and;
c. monitoring video broadcasts and internet distributions to generate reports regarding when, where and how many times a video has been aired/streamed.

However, for the requirement of application, it is necessary to perform data hiding directly in the encrypted domain. This proposes a novel scheme to embed secret data directly in compressed and then encrypted H.264/AVC bit stream. Firstly, by analyzing the property of H.264/AVC codec, the codewords of IPMs, the codewords of MVDs, and the codewords of residual coefficients are encrypted with a stream cipher.

II. RELATED WORK

Title: Overview of the H.264/AVC Video Coding Standard [2]

Description

H.264/AVC is newest video coding standard of the ITU-T Video Coding Experts Group and the ISO/IEC Moving Picture Experts Group. The main goals of the H.264/AVC standardization effort have been enhanced compression performance and provision of a "network-friendly" video representation addressing "conversational" (video telephony) and "nonconversational" (storage, broadcast, or streaming) applications. H.264/AVC has achieved a significant improvement in rate-distortion efficiency relative to existing standards. This article provides an overview of the technical features of H.264/AVC, describes profiles and applications for the standard, and outlines the history of the standardization process.

Title: Effective watermarking scheme in the encrypted domain for buyer–seller watermarking protocol [3]

Description

In most watermarking schemes for copyright protection, a seller usually embeds a watermark in multimedia content to identify a buyer. When an unauthorized copy is found by the seller, the traitor's identity can be traced by the embedded watermark. However, it incurs both repudiation issue and framing issue. To solve these problems, some buyer–seller watermarking protocols have been proposed based on watermarking scheme in the encrypted domain. In this paper, an enhanced watermarking scheme is presented. Compared with Solanki et al.'s scheme, the enhanced scheme increases effective watermarking capacity, avoids additional overhead and overcomes an inherent flaw that watermarking capacity depends on the probability distribution of input watermark sequence. Based on the security requirements of buyer–seller watermarking protocols, a new watermarking scheme in the encrypted domain with flexible watermarking capacity is proposed. It improves the robustness of watermark sequence against image compressions and enables image tampering detection. Watermark extraction is blind, which employs the same threshold criterion and secret keys as watermark embedding. Experimental results demonstrate that the enhanced watermarking scheme eliminates the drawbacks of Solanki et al.'s scheme and that the proposed watermarking scheme in the encrypted domain outperforms Kuribayashi and Tanaka's scheme.

Title: **Robust Watermarking of Compressed and Encrypted JPEG2000 Images [4]**

Description

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. It is a challenge to watermark these compressed encrypted streams as the compression process would have packed the information of raw media into a low number of bits and encryption would have randomized the compressed bit stream. Attempting to watermark such a randomized bit stream can cause a dramatic degradation of the media quality. Thus it is necessary to choose an encryption scheme that is both secure and will allow watermarking in a predictable manner in the compressed encrypted domain. In this paper, we propose a robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images. The encryption algorithm we propose to use is a stream cipher. While the proposed technique embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the decrypted domain. We investigate in detail the embedding capacity, robustness, perceptual quality and security of the proposed algorithm, using these watermarking schemes: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

Title: **Commutative Encryption and Watermarking in Video Compression [5]**

Description

A scheme is proposed to implement commutative video encryption and watermarking during advanced video coding process. In H.264/AVC compression, the intra-prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' signs are encrypted, while DCT coefficients' amplitudes are watermarked adaptively. To avoid that the watermarking operation affects the decryption operation, a traditional watermarking algorithm is modified. The encryption and watermarking operations are commutative. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked. This scheme embeds the watermark without exposing video content's confidentiality, and provides a solution for signal processing in encrypted domain. Additionally, it increases the operation efficiency, since the encrypted video can be watermarked without decryption. These properties make the scheme a good choice for secure media transmission or distribution

Title: A Reversible Data Hiding Method for Encrypted Images [6]

Description

Since several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results.

Title: Walsh-Hadamard Transform in the Homomorphic Encrypted Domain and Its Application in Image Watermarking [7]

Description

How to embed and/or extract watermarks on encrypted images without being able to decrypt is a challenging problem. In this paper, we firstly discuss the implementation of Walsh-Hadamard transform (WHT) and its fast algorithm in the encrypted domain, which is particularly suitable for the applications in the encrypted domain for its transform matrix consists of only integers. Then by modifying the relations among the adjacent transform coefficients, we propose an WHT-based image watermarking algorithm in the encrypted domain. Due to the constrains of the encryption, extracting a watermark blindly from an encrypted image is not a easy task. However, our proposed algorithm possesses the characteristics of blind watermark extraction both in the decrypted domain and the encrypted domain. This means neither the plain image nor its encrypted version is required for the extraction. The experiments demonstrate the validity and the advantages of our proposed method.

Title: Combined Scheme of Encryption and Watermarking in H.264/Scalable Video Coding (SVC) [8]

Description

This paper presents a combined scheme of encryption and watermarking to provide the access right and the authentication of the video content simultaneously. This scheme protects contents more secure because the encrypted content is decrypted when the watermark is exactly detected. And the scheme is appropriate for real-time applications as it is implemented in the encoding process. In addition, we propose more efficient encryption method and watermarking method in the SVC coding as scrutinizing the structural features. For encryption, we proposed an efficient selective encryption scheme which encrypts the intra prediction modes of 4x4 luma block , the sign bits of texture, and the sign bits of MV difference values in the intra frames and the inter frames. The proposed encryption scheme keeps the format compliance and has time efficiency. For watermarking, we propose the reversible watermarking scheme using intra prediction mode. The proposed watermarking scheme has a little bit-overhead, but the degradation of the visual quality doesn't occur.

Title:Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I and P Frames [9]

Description

This paper presents a novel method for the protection of bitstreams of state-of-the-art video codec H.264/AVC. The problem of selective encryption (SE) is addressed along with the compression in the entropy coding modules. H.264/AVC supports two types of entropy coding modules. Context-adaptive variable length coding (CAVLC) is supported in H.264/AVC baseline profile and context-adaptive binary arithmetic coding (CABAC) is supported in H.264/AVC main profile. SE is performed in both types of entropy coding modules of this video codec. For this purpose, in this paper the encryption step is done simultaneously with the entropy coding CAVLC or CABAC. SE is performed by using the advanced encryption standard (AES) algorithm with the cipher feedback mode on a subset of codewords/binstrings. For CAVLC, SE is performed on equal length codewords from a specific variable length coding table. In case of CABAC, it is done on equal length binstrings. In our scheme, entropy coding module serves the purpose of encryption cipher without affecting the coding efficiency of H.264/AVC by keeping exactly the same bitrate, generating completely compliant bitstream and utilizing negligible computational power. Owing to no escalation in bitrate, our encryption algorithm is better suited for real-time multimedia streaming over heterogeneous networks. It is perfect for playback on handheld devices because of negligible increase in processing power. Nine different benchmark video sequences containing different combinations of motion, texture, and objects are used for experimental evaluation of the proposed algorithm.

III. PROPOSED SCHEME

A] Architecture

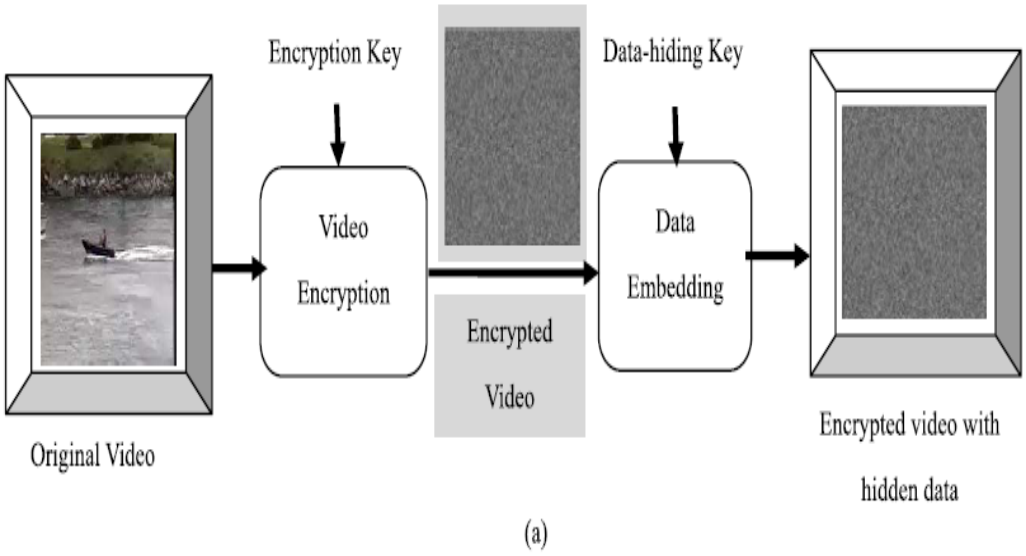

Fig. 2 Diagram of proposed scheme(a) Video encryption and data embedding at the sender end.

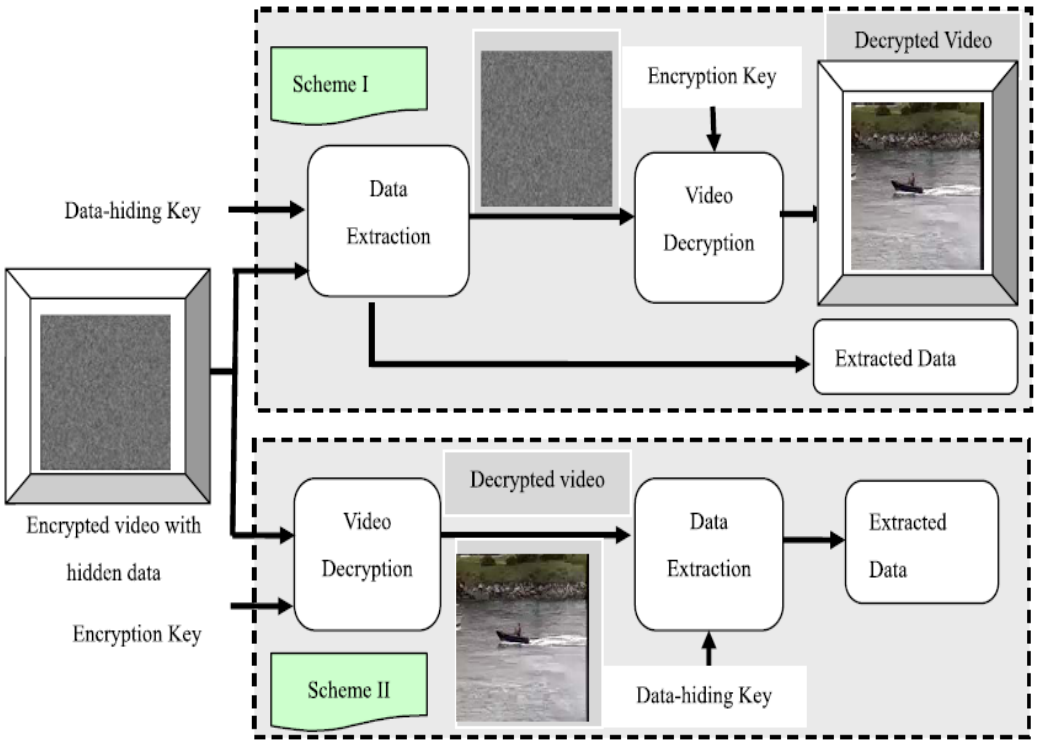

Fig. 2 Diagram of proposed scheme (b) Data extraction and video display at the receiver end in two scenarios.

B] Block Diagram

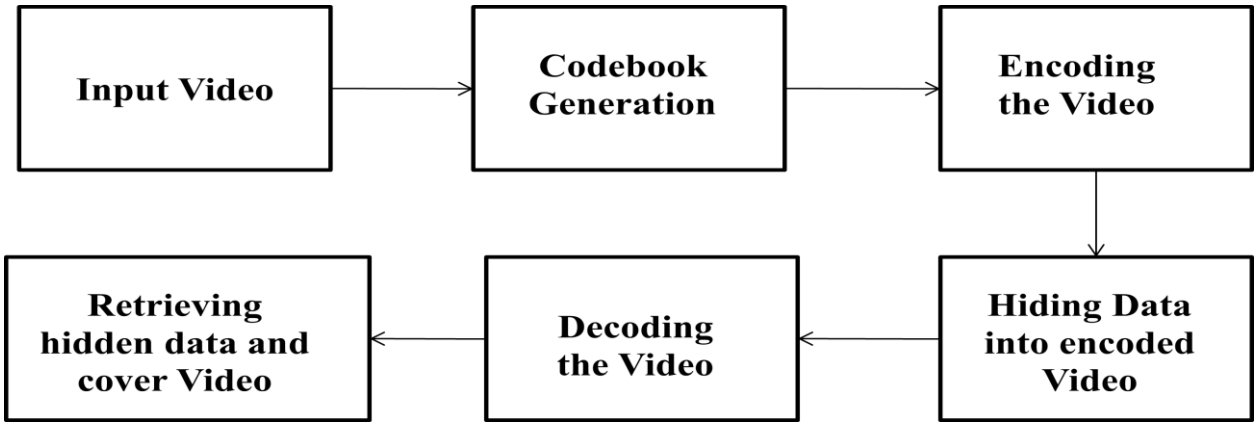

Fig. 3 General Block diagram of Proposed Scheme

In this section, [1] scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which includes three parts, i.e., H.264/AVC video encryption, data embedding and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then, the data-hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using codeword substituting method, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

A scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes three parts :-

i) H.264/AVC video encryption

ii) data embedding and

iii) data extraction

Scope:

- The data hiding is performed directly in encrypted H.264/AVC video bitstream.
- The scheme can ensure both the format compliance and the strict file size preservation.
- The scheme can be applied to two different application scenarios by extracting the hidden data either from the encrypted video stream or from the decrypted video stream.

Objectives:

- The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys using hardware kit to produce an encrypted video stream. Then, the data-hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using codeword substituting method, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version.

Algorithm Used:

- Video Segmentation Algorithm.
- Security of Encryption Algorithm.
- Motion Vector Difference (MVD) Encryption.
- Data Extraction Decoding Algorithm.

Applications

- Content Authentication
- Copyright Protection
- Broadcast monitoring
- Finger printing
- Metadata binding
- Covey communication

IV. EXPECTED RESULTS

PSNR (Peak Signal to Noise Ratio), is widely used objective video quality metric. So the PSNR are used to evaluate the perceptual quality of the video, which illustrate the video quality between the original video and the video after extraction and encryption process.

Table 7.1 Comparison of PSNR with non-stego, stego and proposed video [1]

Input Data	Non-Stego video PSNR (dB)	Stego Video PSNR (dB)	Proposed Video PSNR (dB)
Video Dataset 1	39.60	38.33	39.89
Video Dataset 2	35.84	35.50	36.87
Video Dataset 3	31.68	31.62	33.43
Video Dataset 4	38.44	37.91	39.32
Video Dataset 5	35.15	34.87	36.12
Video Dataset 6	32.31	32.17	33.15

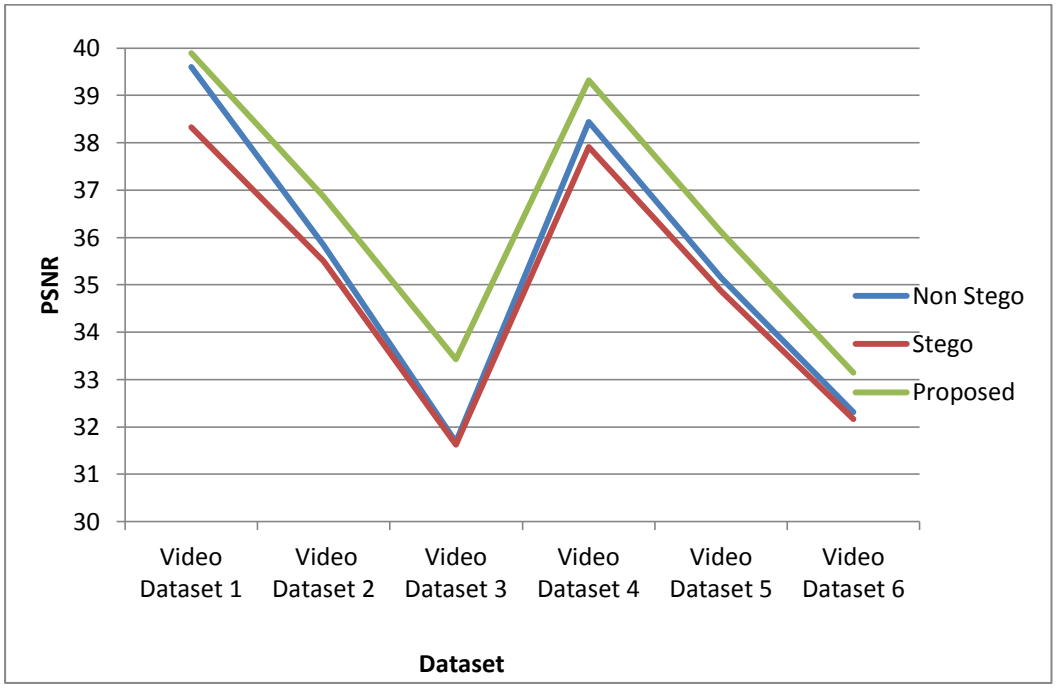

Fig.4 Graph for Comparison of PSNR with non-stego, stego and proposed video

The encrypted video containing hidden data provided by the server should be decrypted by the authorized content owner. Since 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 obtained by encrypting, data hiding, decrypting, and decompressing process is used as the target sequence. That is, in this case, the target video contains hidden data.

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 that is comparison of PSNR. By modifying the compressed bitstream to embed additional data, the most important challenge is to maintain perceptual transparency, which refers to the modification of bitstream should not degrade the perceived content quality.

V. CONCLUSION

Data hiding in encrypted video is a new technology that has started to cause attention dueto the storage and privacy requirements from cloud server network. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bitstream is presented, which includes the video encryption, data embedding and data extraction stages. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e., it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications [1]. The data-hider can embed additional data into the encrypted bitstream using codeword substituting, even though he does not know the original video content. Furthermore the data hiding process is completed entirely in the encrypted domain, so can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides different practical applications. The proposed encryption and data embedding scheme can preserve file-size.

REFERENCES

[1] DawenXu, 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] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[3] 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.

[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] 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.

[6] 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.

[7] 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, pp. 1–15.

[8] 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.

[9] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by 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.

