International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.1, 2015

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY PAPER ON DATA HIDING TECHNIQUE BASED ON CODEWORD SUBSTITUTION ALGORITHM

K.S.AISWARYA[1], RAMJI D.R[2], Dr. SREEJA MOLE S.S[3],

[1]PG Student, ECE Department, Narayanaguru College of Engineering, Manjalumoodu, K.K.District, Tamilnadu, India, [2]Assistant Professor, ECE Department, Narayanaguru College of Engineering, Manjalumoodu, K.K.District, Tamilnadu, India

[3]Head of the Department ECE, Narayanaguru College of Engineering, Manjalumoodu, K.K.District, Tamilnadu, India, Pin: 629151

Article Received: 22/12/2014 | Article Revised on: 30/12/2014 | Article Accepted on:03/01/2015

ABSTRACT

Digital video needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and 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. In addition, it is more efficient without decryption followed by data hiding and re-encryption. The scheme of data hiding directly in the encrypted version of H.264/AVC video stream which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. By analyzing the property of H.264/AVC codec, the code words of intraprediction modes, the code words of motion vector differences, and the code words of residual co-efficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even after encryption and data embedding. This survey paper take a look into the Code word Substitution based Data Hiding in Image Processing hoping that it will help future innovations and researches in military application, videos in medical field and other applications.

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

INTRODUCTION

Cloud computing has become an important technology trend, which can provide highly efficient computation and large scale storage solution for video data. But cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content is accessible in encrypted form. The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help address the security and privacy concerns with cloud computing [1]. For example, a cloud server can embed the additional information (e.g., video notation, or authentication data) into an encrypted version of an H.264/AVC video by using data hiding technique. With the hidden information, the server can manage the video or verify its integrity without knowing the

original content, and thus the security and privacy can be protected. Similarly when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will become popular in the near future. During H.264/AVC compression [10], the intra-prediction mode (IPM), motion vector difference (MVD) and DCT coefficients sign are encrypted, while DCT coefficients amplitudes are watermarked adaptively. In [11], a combined scheme of encryption and watermarking is presented, which can provide the access right as well as the authentication of video content simultaneously. However, to meet the application requirements, it's 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. The encryption algorithm is combined with the Exp-Golomb entropy coding and Context-adaptive variable-length coding (CAVLC) [12], which keeps the codeword length unchanged. Then, data hiding in the encrypted domain is performed based on a novel codeword substituting scheme. 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.

COMMUTATIVE ENCRYPTION AND WATERMARKING IN VIDEO COMPRESSION

The video encryption and watermarking scheme based on H.264/AVC codec, which gives a solution to the commutation of encryption and watermarking. In this scheme, parameters such as IPM, MVD and residual coefficient's sign are encrypted, while the amplitude of dc or ac is watermarked. To reduce computational cost, the selected parameters are encrypted partially. To keep sign encryption and amplitude watermarking independent, traditional watermark embedding method is modified. To keep robust and imperceptible, the coefficients are selected adaptively according to macro block type. The scheme, shown in Figure 1, is composed of several components: the compression component, encryption component and watermarking component.

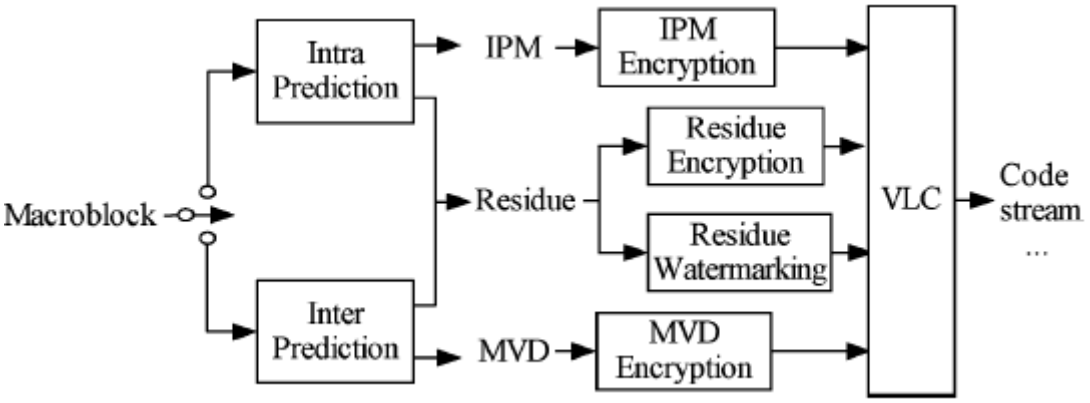

Figure 1: Proposed Watermarking and Encryption scheme based on H.264/AVC

Here, the compression component includes intra-prediction, inter prediction, variable length coding (VLC) etc., the encryption component includes IPM encryption, MVD encryption and residue encryption, and the watermarking component refers to residue watermarking. The encryption process and watermarking process are controlled by independent keys.

OVERVIEW OF THE H.264/AVC VIDEO CODING STANDARD

To address the need for flexibility and customizability, the H.264/AVC design covers a video coding layer [VCL], which is designed to efficiently represent the video content, and a network abstraction layer [NAL], which formats the VCL representation of the video and provides header information in a manner appropriate for conveyance by a variety of transport layers or storage media.

Relative to prior video coding methods, as exemplified by MPEG-2 video, some highlighted features of the design that enable enhanced coding efficiency include the following enhancements of the ability to predict the values of the content of a picture to be encoded.

1. Variable block-size motion compensation with small block sizes
2. Quarter-sample-accurate motion compensation
3. Motion vectors over picture boundaries
4. Multiple reference picture motion compensation
5. Decoupling of reference order from display order
6. Decoupling of picture representation methods from picture referencing capability
7. Weighted prediction
8. Improved "Skipped" and "direct" motion inference
9. Directional spatial prediction for intra coding
10. In-the-loop deblocking filtering

SEPERABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

In separable reversible data hiding, the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

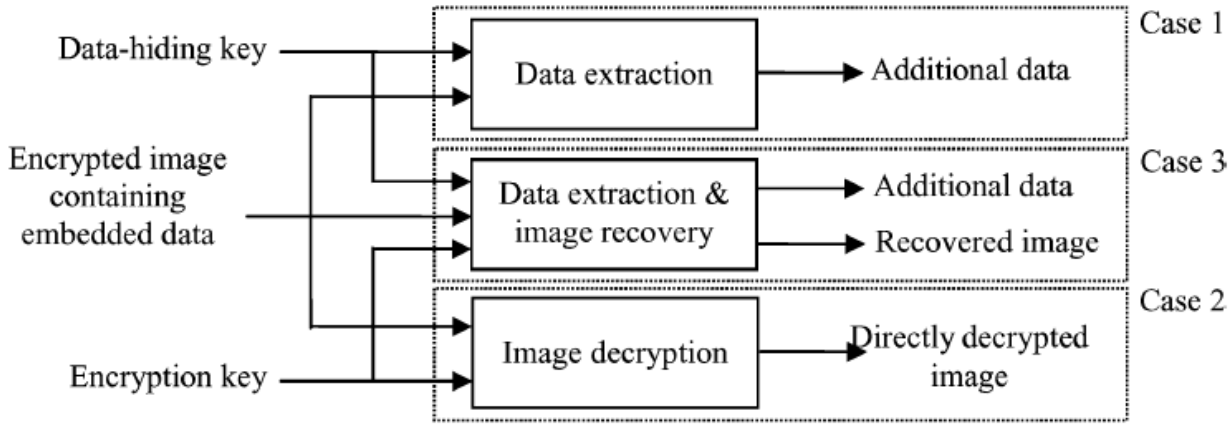

Figure 2: Three cases at receiver side of the separable scheme.

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

SECURE ADVANCED VIDEO CODING BASED ON SELECTIVE ENCRYPTION ALGORITHM

During AVC encoding, such sensitive data as intra-prediction mode, residue data and motion vector are encrypted partially. Among them, the intra-prediction mode is encrypted based on Exp-Golomb entropy coding, the intra-macro blocks, DCs are encrypted based on context adaptive variable length coding (CAVLC) , and intra macro blocks AC's and the inter-macro blocks MVDs are sign-encrypted with a stream cipher followed with variable length

coding. This encryption scheme is secure in perception, keeps format compliance, and obtains high time efficiency though reducing the encrypted data volumes.

The Exp-Golomb Encryption Algorithm (EGEA):

In AVC, the intraprediction modes are encoded with Exp-Golomb codes. This kind of codeword is composed of R zeros, one '1' – bit and R bits of information (Y). Here, the intra-prediction mode is X=2R+Y-1, and R = [log2 (X+1)]. Thus, the encryption process is shown in Figure 3. That is, X is firstly encoded into a variable-length code with Exp - Golomb coding, and then only the information part Y is encrypted into Z with a stream cipher. As can be seen, this process is similar to table permutation. The main difference is that the permutation operation happens only in the codeword with the same length, and the key changes with the intra/inter-prediction mode. The decryption process is symmetric to the encryption one.

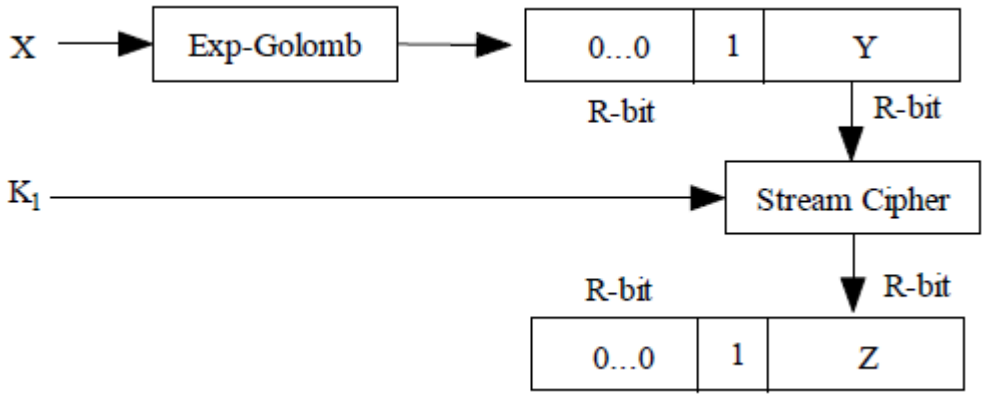

Figure 3: The Exp-Golomb encryption algorithm.

The CAVLC Encryption Algorithm (CEA):

During CAVLC encoding, parameters such as the number of coefficients, trailing ones (coeff_token), the sign of each T1, the levels of the remaining non-zero coefficients, the total number of zeros before the last coefficient and each run of zeros are encoded respectively. In order to keep low cost and keep the code format unchanged, it is preferred to encrypt only few of the parameters. Thus, we propose to encrypt only the signs of T1 and the levels of the remaining non-zero coefficients while keep other parameters unchanged. Considered that these parameters are often of variable length, the stream cipher is more suitable for length-kept encryption. So the stream cipher is used here to encrypt the selected parameters. The encryption process is realized during encoding process, thus the code format keeps unchanged, which makes it practical to decode or decrypt the videos correctly.

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE BY RESERVING ROOM BEFORE ENCRYPTION

In this method, we first empty out room embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSB's in the encrypted image can be used to embed data. Not only does this method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- Real reversibility is realized, that is data extraction and image recovery is free of any error.
- For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

As shown in Figure 4, the content owner first reserves enough space on original image and then convert the image into its encrypted version with the encryption key. Now the data embedding process in encrypted images in inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE (Reserving Room Before Encryption) to achieve better

performance compared with techniques from Frame work VRAE (Vacating Room After Encryption). This is because in this new frame work, which follows the customary idea that first losslessly, compresses the redundant image content (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

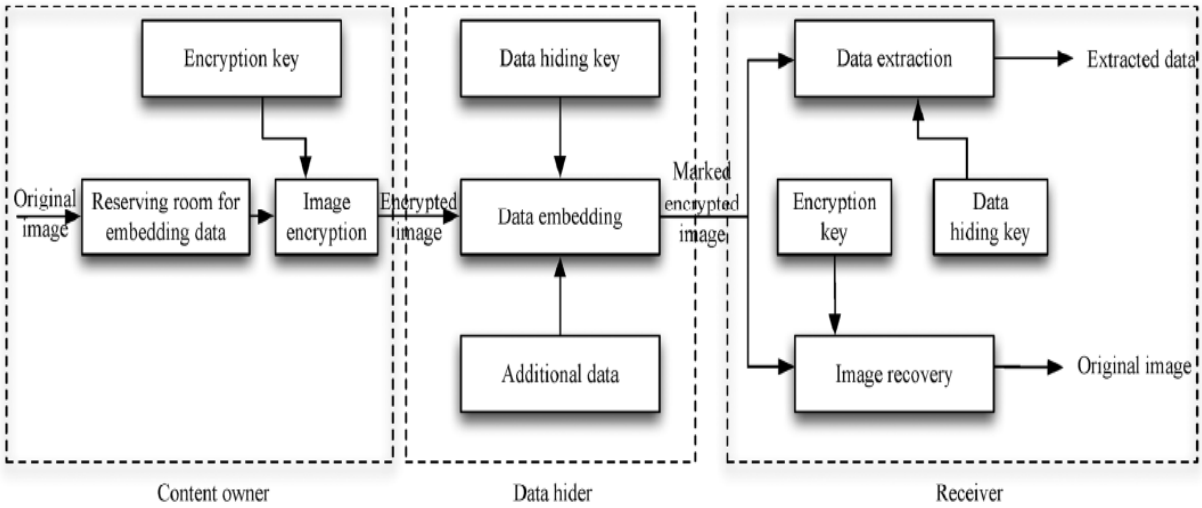

Figure 4: Framework: Reserving Room Before Encryption (RRBE)

The framework "RRBE" which primarily consists of four stages: generation of encrypted image, data hiding in encrypted image, data extraction and image recovery.

PROPOSED METHOD

In the proposed method, a 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. In the encrypted bit stream of H.264/AVC, the proposed data embedding is accomplished by substituting eligible codewords of Levels. Since the sign of Levels are encrypted, data hiding should not affect the sign of Levels. Besides the codewords substitution should satisfy the following three limitations. First, the bit stream after codeword substituting must remain syntax compliance so that it can be decoded by standard decoder. Second, to keep the bit-rate unchanged, the substituted codeword should have the same size as the original codeword. Third, data hiding does cause visual degradation but the impact should be kept to minimum.

CONCLUSION

In this paper different encryption algorithms and data hiding approaches are discussed. Data hiding in encrypted media has started to draw attention because of the privacy-preserving requirements from cloud data management. In codeword substitution based hiding, an algorithm is used to embed additional data in encrypted H.264/AVC bit stream, which consists of video encryption, data embedding and data extraction phases. 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. The data hider can embed additional data into the encrypted bit stream using codeword substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain which 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 two different practical applications.

Another advantage is that it is fully compliant with the H.264/AVC syntax. Experimental results have shown that selective encryption and data embedding scheme can preserve file size, whereas the degradation in video quality caused by data hiding is quite small.

REFERENCE

[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, May 2011, pp.5856 – 5859.

[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]. 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.

[4]. 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.

[5]. X.P.Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol.18, no.4, pp.255-258, Apr.2011.

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

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

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. S.G.Lian, Z.X.Liu, Z. Ren, and H.L.Wang," Secure advanced video coding based on selective encryption algorithms, "IEEE Trans. Consumer Electron., vol.52, no.2, pp.621-629, May 2006.

[14]. 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.

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

[16]. 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.

[17]. Advanced Video Coding for Generic Audio Visual Services, ITU, Geneva, switcherland, Mar.2005.

[18]. 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.

[19]. [19] I.E.G.Richardson, H.264 and MPEG-4 Video Compression: Video Coding for next Generation Multimedia. Hoboken, NJ, USA: Wiley, 2003.

[20]. 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.

[21]. D.W.Xu and R.D.Wang, " Watermarking in H.264/AVC Compressed domain using Exp-Golomb code words mapping," Opt. Eng., vol.50,no.9, p.097402, 2011.

[22]. 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.

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