Data Hiding in RGB Images by Codeword Encryption

VASANTHAPURAM LAKSHMI LAVANYA¹, SRIDEVI², N. V. RAMANAIH³

¹PG Scholar, Dept of DECS, Shree Institute of Technical Education, Mallavaram, Tirupati, India.
²Assistant Professor, Dept of ECE, Shree Institute of Technical Education, Mallavaram, Tirupati, India.
³Assistant Professor, Dept of ECE, Shree Institute of Technical Education, Mallavaram, Tirupati, India.

Abstract: To maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves hiding the data using data hiding algorithm to maintain the images secrecy. We present a new concept for RGB image based data hiding. It introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. It offers very high capacity for cover media compared to other. In secure transformation of data in encrypted image is to provide high network security for data transformation. To protect videos during transmission or cloud storage, encryption of compressed video bit streams and hiding privacy information can be done. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. It is also for the purpose of content notation and tampering detection. Here, data hiding directly in the encrypted version of H.264/AVC video stream. It has following three parts, H.264/AVC video encryption, data embedding, and data extraction. In H.264/AVC codec, the code words of intra prediction modes, motion vector differences, and residual coefficients are encrypted with stream ciphers. A data hider may embed additional data in the encrypted domain by using bits replacement technique, without knowing the original video content. Chaos crypto system is used here to encrypt/decrypt secret text data before/after data embedding/extraction.

Keywords: Bits Replacement Technique, Chaos Crypto System, Encrypted Bit Streams, H.264/AVC.

I. INTRODUCTION

Cloud computing has become an important technology, which provides efficient computation and large-scale storage solution for video data. Cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content can be accessible in encrypted form. The ability of performing data hiding directly in encrypted H.264/AVC video streams avoid the leakage of video data, this protects privacy and security concerns with cloud computing.[1] For example, a cloud server can embed the additional information into an encrypted H.264/AVC video by using data hiding technique. However, higher coding efficiency is likely to increase the difficulty of watermarking. Over the years, several watermarking techniques on H.264/AVC are proposed and realized at various stages in the compression pipeline, i.e., intra-prediction stage, quantized transform coefficients stage, and entropy coding stage. Noorkami and Mersereau [3] employed a human visual model adapted for a 4 × 4 DCT block to increase the payload and robustness.

The algorithm can achieve high robustness, but its computational complexity is relatively high. Zhang et.al [4] proposed a robust video watermarking scheme of H.264/AVC using a grayscale watermark pattern. The pattern insertion process enhanced the robustness, but the computational complexity of the watermark pre-processing makes it a challenge to implement the watermark embedding efficiently. Later, Mansouri et.al [5] exploited the syntactic elements of the video stream for watermark embedding. These algorithms utilize the quantized or un-quantized integer transform coefficients for watermark embedding. Besides DCT coefficients, motion vector (MV) is also used for watermark embedding in many schemes (referred to as MV-based watermarking schemes) [6]. As described in [7], the advanced JND (Just Noticeable Difference) model is hard to be applied to an MV-based watermarking scheme. As a result, it is hard to achieve a satisfied trade-off between the robustness and imperceptibility for most existing MV-based watermarking schemes. In addition to DCT-based and MV-based watermarking schemes, some other algorithms exploit new features of H.264/AVC (such as context-adaptive entropy coding, intra prediction mode and the reference index) for watermarking [8] – [10]. But these algorithms are not robust against some common attacks. Considerable more effort is needed to provide robust watermarking technique for H.264/AVC.

We note that the existing watermarking algorithms prefer to embed the watermark information into DCT coefficients, not only for H.264/AVC, but also for other coding standards such as MPEG-2/4 [11]. The goal of this paper is to provide...
an efficient and robust H.264/AVC compressed domain watermarking. To achieve this goal, we exploited the re-compression architecture of H.264/AVC and characteristics of residual coefficients. The watermark information is embedded in quantized residual coefficients by modifying positive and negative signs. This modification is based on the fact that the coefficients will be changed after re-encoding, while the distribution of positive and negative coefficients remains relatively stable. With this the server can manage the video and crosscheck its integrity without knowing the actual content, thus helps to protect privacy and security. This technology can be used in other application. For example, when surveillance videos or medical videos have been encrypted for protecting the privacy of the people, a database manager can add the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain.

A. Overview of the H.264/AVC

The H.264/AVC [1] video coding standard has been developed and standardized collaboratively by both the ITU-T VCEG and ISO/IEC MPEG organizations. H.264/AVC represents a number of advances in standard video coding technology, in terms of both coding efficiency enhancement and flexibility for effective use over a broad variety of network types and applications. H.264/AVC is a video compression format [2] i.e. standard for high definition digital video. The main goals of the H.264/AVC standard have been used to enhance compression performance and provides a provision of a network-friendly video representation addressing conversational (video telephony) and non-conversational (storage, broadcast, or streaming) applications. H.264/AVC has achieved a significant improvement in rate-distortion efficiency relative to existing standards. H.264/AVC covers all common video applications ranging from mobile to video conferencing and High Definition video storage.

II. RELATED WORK

Till now, few successful data hiding schemes in the encrypted domain have been found in the open literature.[2] A watermarking scheme using Paillier cryptosystem is proposed based on the security requirements of buyer-seller watermarking protocols[3]. In Walsh-Hadamard transform image watermarking algorithm is used in the encrypted domain using Paillier cryptosystem is presented [4]. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image shows high overhead in storage and computation. Note that, several research on reversible data hiding in encrypted images are found recently. The encryption is performed by using bit-XOR operation. In these methods, the host image is in an uncompressed format. In [5] a robust watermarking algorithm is proposed to embed watermark into compressed and encrypted JPEG2000 images. As development of the multimedia and Internet technology, more information including images, audio and other multimedia, are being transmitted over the Internet. Due to some internal features of images, such as large data capacity and high correlation among pixels, early encryption algorithms are not suitable for practical image encryption.

Recently, the image encryption technologies based on chaos theory have been developed to overcome the disadvantages present in early encryption techniques. In recent years, many video encryption algorithms have been proposed. A Walsh-Hadamard transform based image watermarking algorithm in the encrypted domain using Paillier cryptosystem is presented in [3]. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image results in a high overhead in storage and computation. Here the host image is in an uncompressed format and the encryption is performed by using bit operation. Since this technique does not use any encoder, the uncompressed file require more time for encryption. Tosun and Feng [4] proposed to divide the 64 DCT coefficients after the Discrete Cosine Transform (DCT) into three bands, and then scramble the DCT coefficients in different bands according to user requirements of security levels.

Lian et al. [5] proposed to selectiv intra-prediction modes, DCT coefficients and MVD signs after the quantization. Wu and Kuo [6] proposed to use multi-Huffman trees (MHT) and multi-state indexes (MSI) controlled by keys in the entropy coding process. As these encryption algorithms are all accomplished before the last step of the video compression process, all the encrypted bitstreams could maintain the format-compliance and can be decoded by a standard decoder without decryption, while only obtain the unintelligible video con encrypting or scrambling the DCT coefficients during compression process usually destroys the inherent energy impact capability of the DCT transform, resulted in low compression efficiency. Here full encryption of video is required, which will increase the computational complexity. Furthermore, these algorithms require a computational complexity. Hence, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt. Till now, various encryption algorithms have been proposed and widely used, such as DES, RSA, IDEA or AES, most of which are used for text or binary data. These algorithms are difficult to use directly for video encryption. Thus the Selective encryption scheme works on partial encryption algorithm. During AVC encoding sensitive data as intra-prediction mode, residual data & motion vector difference are partially encrypted. It provides approach for selecting sensitive data to encrypt to make it time efficient, secure & format compliance. The drawback of this paper is that the selective encryption is performed during H.264/AVC encoding & not on compressed domain.
B. Enhanced Selective Encryption Scheme

The author Z. Shahid, M. Chaumont, and W. Puech [6] in the year 2011 proposed Selective Encryption scheme which operates in compressed domain based on context adaptive variable length coding & context adaptive binary arithmetic coding. Thus it overcomes the drawback of previous paper. The selective encryption is performed on the entropy coding stage of H.264/AVC using AES encryption algorithm in CFB mode. Hence it does not affect the bitrates & H.264/AVC bit stream compliance. The proposed method has the advantage of being suitable for streaming over heterogeneous network because of no change in bit rates.

C. Encryption scheme and Codeword Substitution Technique

The previous methods perform encryption and data embedding almost simultaneously during H.264/AVC compression process and not on compressed domain. Hence the compression and decompression cycle is time-consuming and hampers real-time implementation. Besides, encryption and watermark embedding would lead to increasing the bitrate of H.264/AVC bit stream. However, to meet the application requirements, it’s necessary to perform data hiding directly on compressed bit stream in the encrypted domain. To overcome the drawbacks of previous papers, The author D. Xu, R. Wang, & Yun Q Shi [7] in the year 2014 proposed Codeword substitution technique, a data hiding algorithm that work entirely in the encrypted domain, & thus preserves confidentiality of the content. The proposed methodology for video encryption is to use standard stream cipher (RC4) with encryption keys. And after video encryption, codeword substitution technique generates pseudorandom sequence as data hiding key & embed the data into the encrypted video stream without knowing the original content. By making the comparative analysis with the previous papers, this paper [7] achieved a better performance in following aspect:

- Data hiding performed entirely in the encrypted domain, & thus preserves confidentiality of the content.
- The schemes operate directly on the compressed bit stream.
- The schemes can ensure both the format compliance & strict file size preservation.
- In order to adapt to different application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

III. PROPOSED SCHEME

In this section, a novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented; the processing system involves H.264/AVC Coder, Chaos encryption, and Bits replacement to accomplish better compression performance and efficient data hiding. The content owner encrypts the original H.264/AVC video stream with encryption keys using standard stream ciphers 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 Chaos encryption for text, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bit stream like what the traditional ciphers do because of the following two constraints, i.e., format compliance and computational cost as shown in Figs.1 and 2. Alternatively, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt.

![Fig.1. Video Encryption and Data Hiding.](image)

![Fig.2. Data Extraction and Video Decryption.](image)

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. Video compression (or video coding) is an important technology for applications such as digital television, DVD-Video, videoconferencing, mobile TV and internet video streaming. In H.264, encoder converts video into a compressed format and a decoder converts a compressed video back into an uncompressed format [8].

B. Chaos Cryptosystem

Chaotic systems are suitable for data message encryption because they have good properties as follows: 1) chaotic motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain. 2) Flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise. The discrete sequences of the chaotic dynamical system are gained by the following equation.

\[ X_{n+1} = T_n (x_n) \]  \hspace{1cm} (1)

The basic Logistic-map is formulated as, \( f(x)=\mu(1-x) \)

Where, \( x \ (0, 1) \) the parameter \( \mu \) and the initial value \( x_0 \) can be adopted as the system key \( (\mu, x_0) \). The research result shows that the system is in chaos on condition that \( 3.569 < \mu < 4.0 \). [6]
C. Bits Replacement Technique

The frequently used stego graphy method is the technique of LSB substitution. Every pixel of gray-level image consists of 8 bits. One pixel can hence display 28=256 variations. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.[7]

Intra Prediction Mode Encryption: It is used to remove the spatial redundancy from individual frame. Nine intra prediction modes (IPMs) are available in the Intra_4 × 4. These modes are used to generate a prediction macro block for the current macro block. The mode number used in each prediction is encrypted here. A key from RC4 is used for the encryption. The last bit of pseudo random number generated from RC4 is xored with last bit of intra prediction mode number.

Motion Vector Difference Encryption: In order to protect both texture information and motion information, the motion vectors should be encrypted. In H.264/AVC baseline profile, Exp-Golomb entropy coding is used to encode MVD. Here also a key from RC4 is used for the encryption. The last bit of pseudo random number generated from RC4 is Exp-Golomb with last bit of Exp code.

Residual Coefficients Encryption: In order to keep high security, another type of sensitive data, i.e., the residual data in both I-frames and P should be encrypted. In H.264/AVC baseline profile, CAVLC entropy coding is used to encode the quantized coefficients of a residual block [9]. Each CAVLC can be expressed as the following format:

\[\text{Coef f token, Sign of Trailing Ones, Level, Total zeros, Run before}\]

Here, to reduce the complexity, only the Levels of CAVLC are modified. The codeword for each Level is represented as Level codeword = \[\text{[level pref i x], [level suf fix]}\]. The last bit of pseudo random number generated from RC4 is xored with last bit of code words of Level.

IV. CONCLUSION

In this paper, an algorithm to encrypted H.264/AVC bit stream is presented, which consists of video encryption, data embedding and data extraction phases. The data-hider can embed additional data into the encrypted bitstream using codeword substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, our method can preserve the confidentiality of the content completely. Encryption will provide the security and data hiding will provide the authentication of videos from different servers. Since all the process is in compressed domain, the bandwidth required to transmit the data is very less. Instead of encrypting the whole video content, a selective encryption is used, which only encrypt the sensit information like intra prediction mode, motion vector difference and residual coefficients complexity is very less compared to other data hiding techniques.

REFERENCES


Author’s Profile:

Ms. V. Lakshmi Lavanya received B.tech in E.C.E from Srikalahasteeswara Institute of Technology(SKIT), affiliated to J.N.T.U. Anantapur. She is pursuing M.Tech in the stream of DECS in Shree Vidyanikathan institute of Technology(SITE) Her research interests include Digital Image processing, EDC, VLSI, Communication Systems. She participated in Satellite Navigation System workshop held at S.V.University. She participated in Poster presentation on UNWIRED CHARGING the National Level Student Technical Symposium and attended for various presentations at college level.

Miss. Sridevi received B.tech in E.C.E from Padmavathi Mahela university. She received M.Tech in ECE from Vidyanikathan institute of Technology J.N.T.U. Anantapur. Her research interests include Satellite communication, Digital Image Processing, Radar Systems. Now she is working as a Assistant Professor in

International Journal of Scientific Engineering and Technology Research
Volume.04, IssueNo.14, June-2015, Pages: 2557-2561
Mr. N. V. Ramanaiah, He received M.Tech in DECE from SIT, Puttur. His research interests include Digital System Design, Signal Processing and Image Processing. Now he is working as a Assistant Professor in the department of ECE, Shree Institute of Technical Education, Tirupati, AP, India.