

# Review on A Robust System For Video And Data Encryption/Decryption Based On Codeword Encoding/Decoding

**Tushar K Shinde**

Department of ETC, PCE  
Nagpur (MH) – 440019, India  
shindetrushar@gmail.com

**Dr. S.S.Shriramwar**

Department of ETC, PCE  
Nagpur (MH) – 440019, India  
ssshriramwar@yahoo.com

**Prof. Vishal Panchbhai**

Department of ETC, PCE  
Nagpur (MH) – 440019, India  
Vishal\_panchbhai@yahoo.com

**Abstract:** Data hiding in encrypted media is a new topic that has started to draw attention because of the privacy-preserving requirements from cloud data management. In this synopsis, an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, 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 code word substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, this method can preserve the confidentiality of the content completely. Confidentiality is a set of rules that prevents the disclosure of any confidential information to unauthorized individuals or systems. Confidentiality of any information can be achieved by data hiding which is a process to hide data into a cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. In this synopsis, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, 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 intra-prediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers. Then a data hider, may embed additional data in the encrypted domain by using code word substitution technique, without knowing the original video content.

**Keywords-** Data hiding encrypted domain, H.264/AVC, code word substituting, privacy-preserving, decompression, data embedding, data extraction.

\*\*\*\*\*

## I. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Steganography's ultimate objectives, which are un-detectability, robustness and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

1. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image.

I. Till now, few successful data hiding schemes in the encrypted domain have been reported in the open literature. In a watermarking scheme in the encrypted domain using Paillier cryptosystem is proposed based on the security

requirements of buyer-seller watermarking protocols. A Walsh-Hadamard transform based image watermarking algorithm in the encrypted domain using Paillier cryptosystem is presented. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image results in a high overhead in storage and computation. Note that, several investigations on reversible data hiding in encrypted images are reported in literature recently. The encryption is performed by using bit-XOR (exclusive-OR) operation. In these methods, however, the host image is in an uncompressed format.

2. In another robust watermarking algorithm it is proposed to embed watermark into compressed and encrypted JPEG2000 images. With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the near future. Obviously, due to the constraint of the underlying encryption, it is very difficult and sometimes impossible to transplant the existing data hiding algorithms to the encrypted domain. To the best of my knowledge, there has been no report on the implementation of data hiding in encrypted H.264/AVC video streams. Only few joint data-hiding and encryption approaches that focus on video have been proposed. The compression/decompression cycle is time-consuming and hampers real-time implementation. Besides, encryption and watermark embedding would lead to increasing the bit-rate of H.264/AVC bitstream. Therefore, it

becomes highly desirable to develop data hiding algorithms that work entirely on encoded bitstream in the encrypted domain. However, there are some significant challenges for data hiding directly in compressed and encrypted bitstream. The first challenge is to determine where and how the bitstream can be modified so that the encrypted bitstream with hidden data is still a compliant compressed bitstream. The second challenge is to insure that decrypted videos containing hidden data can still appear to be of high visual fidelity. The third challenge is to maintain the filesize after encryption and data hiding, which requires that the impact on compression gain is minimal.

3. The fourth challenge is that the hidden data can be extracted either from the encrypted video stream or from the decrypted video stream, which is much more applicable in practical applications.

## II. LITERATURE SURVEY

1. According to D.W. Xu, R.D. Wang the method of Exp-Golomb code words mapping is given for watermarking in H.264/AVC compressed domain.

2. According to X.P. Zhang the method of a novel reversible data hiding algorithm is given for Reversible Data Hiding.

3. According to T. Margaret the method of XOR ciphering technique is given for Reversible Data Hiding in Encrypted Images by XOR Ciphering Technique.

## III. WORKING

A novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which includes three parts, i.e.,

### 1. H.264/AVC video encryption:

#### 1. Intra-Prediction Mode (IPM) Encryption:

According to H.264/AVC standard, the following four types of intra coding are supported, which is denoted as Intra\_4x4, Intra\_16x16, Intra - chroma, and I\_PCM. Here, IPMs in the Intra\_4x4 and Intra\_16x16 blocks are chosen to encrypt.

#### 1. Motion Vector Difference (MVD) Encryption:

In order to protect both texture information and motion information, not only the IPMs but also the motion vectors should be encrypted. In H.264/AVC, motion vector prediction is further performed on the motion vectors, which yields MVD. In H.264/AVC baseline profile, Exp-Golomb entropy coding is used to encode MVD. The code word of Exp-Golomb is constructed as [M zeros], [I NFO], where I NFO is an M-bit field carrying information.

### 2. Data embedding:

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

### 3. Data extraction:

Scheme I: Encrypted Domain Extraction - To protect privacy, a database manager (e.g., cloud server) may only get access to the data hiding key and have to manipulate data in encrypted domain. Data extraction in encrypted domain guarantees the feasibility of our scheme in this case.

Scheme II: Decrypted Domain Extraction - In scheme I, both embedding and extraction of the data are performed in encrypted domain. However, in some cases, users want to decrypt the video first and extract the hidden data from the decrypted video.

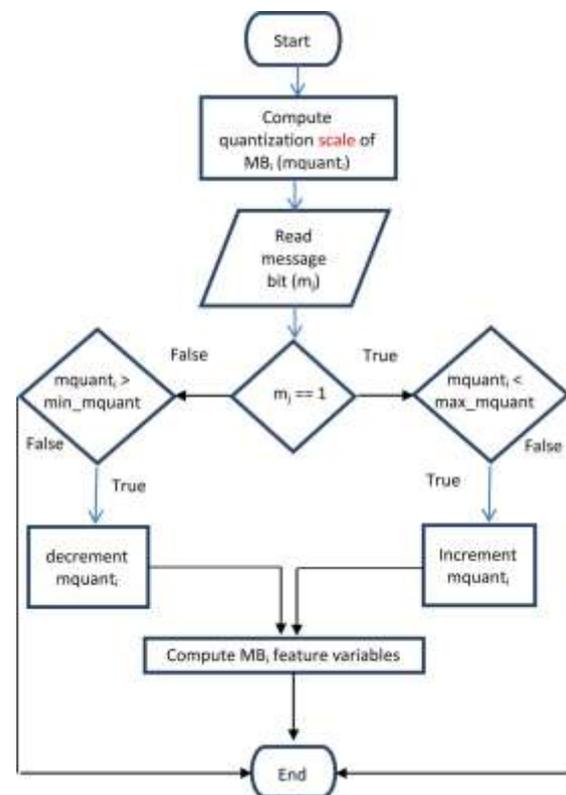
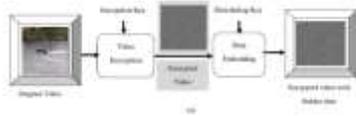


Fig.1. Message insertion flowchart for one macroblock.



a.

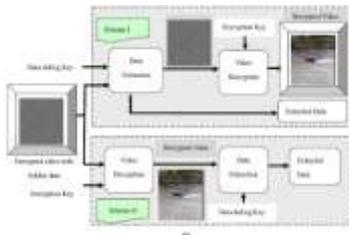


Fig. 1. Diagram of proposed scheme: (a) Data hiding and data extraction in the video and (b) Data hiding and data extraction in the video and data extraction

b.

Fig.2 The sampled signals are separated into segments.



fig.3 Secret color image



Fig.4 Secret gray scale image

#### IV. CONCLUSIONS

The synopsis 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 code words of IPMs, the code words of MVDs, and the code words 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), which keeps the code word length unchanged. Then, data hiding in the encrypted domain is

performed based on a novel code word substituting scheme. In contrast to the existing technologies discussed above, the proposed scheme can achieve excellent performance in the three different prospects.

#### V. REFERENCES

- [1] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
- [2] 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.
- [3] 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.
- [4] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
- [5] 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.
- [6] 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.