South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 64–66

ISSN No: 2454-9614

Efficient Steganography in Encoded Video Streams using Motion Vector Difference

P. Priyanka , C. Selvi*

Department Of Computer Science And Engineering Velalar College Of Engineering And Technology, Erode,Tamilnadu, India.

*Corresponding Author: P. Priyanka

E-mail: ktppriyanka@gmail.com

Received: 10/10/2015, Revised: 13/12/2015 and Accepted: 06/03/2016

Abstract

Digital video sometimes are stored and processed in an encrypted format to maintain privacy and security. For the purpose of content notation, 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. This project proposes a novel scheme of data hiding directly in the encrypted version of AVI video stream, which includes the following three parts, i.e., AVI video encryption, data embedding, and data extraction. By analyzing the property of AVI codec and the code words of motion vector differences 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. Video file size is strictly preserved even after encryption and data embedding. Experimental results have demonstrated the feasibility and efficiency of the proposed scheme.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

1.1 Data Hiding

An effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. The source is first compressed to its entropy rate using a standard source code. The compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. Compression of encrypted data has attracted considerable research interest .The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to

recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator in provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating decompression and decryption functions will be used to reconstruct the original data.

1.2 Data Hiding Process

The reversible data hiding in encrypted image is investigated. Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content and it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side.

A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the data extraction is not separable from the content decryption.

2. Related works

Dawen Xu et al. Digital video sometimes are stored and processed in an encrypted format to maintain privacy and security. For the purpose of content notation, Data hiding in these encrypted videos. Data hiding in encrypted domain without decryption preserves the confidentiality of the content. Proposes a novel 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. 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. Video file size is strictly preserved even after encryption and data embedding.

Ma K.D et al. 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. 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. An enhanced watermarking scheme is presented. 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. Multimedia security is a severe issue in the digital world due to the ease of illegal reproduction and redistribution through the Internet. During the past decade, a large number of watermarking schemes have been proposed.

Rini.J a Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. Content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content. The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data medication. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

References

[1] Dawen Xu et al.,(2014) 'Data Hiding in Encrypted H.264/AVC Video Stream by Codeword Substitution' VOL. 9, NO. 4.
[2] Ma K.D,(2013)'Reversible data hiding in Encrypt images by reserving room before encryption',IEEE Tran.Inf.vol. 8, no. 3, pp. 553–562.
[3] Rini.J (2013)'Study on Separable Reversible Data Hiding in Encrypted Images', Volume 2, Issue 12
[4] Subramanyam A.V et al.,(2012) 'Robust watermarking of compressed and encrypted JPEG2000 images' IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703–716.
[5] Tiziano Bianchi et al., 'on the implementation of the discrete fourier transform in the encrypted domain'vol 4,Issue
[6] Tiziano Bianchi et al.,(2010) 'Composite signal representation and fast and storage-Efficient Processing of Encrypted Signals' Vol 5,no 1.