Computer Standards & Interfaces 48 (2016) 173–182

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

An optimal modified matrix encoding technique for secret writing in MPEG video using ECC

Ramakrishna Hegde [a,*], S. Jagadeesha [b]

[a] Department of Computer Science & Engineering, SDM Institute of Technology, Ujire, Karnataka, India
[b] Department of Electronics and Communication Engineering, SDM Institute of Technology, Ujire, Karnataka, India

ARTICLE INFO

Article history:
Received 18 February 2016
Received in revised form 1 July 2016
Accepted 1 July 2016
Available online 04 July 2016

Keywords:
Elliptic Curve Cryptography (ECC)
Multi-curve ECC
Artificial Bee Colony Algorithm (ABC)
Modified matrix encoding

ABSTRACT

In recent years, Information Security in the field of digital communication is a relevant part because the advancement hiked the fear of receiving the data snooped at the time of sending it from the sender to the receiver. So, a secure technique is designed by amalgamate both Cryptography and Steganography. Initially, user's confidential details are encrypted using the more secure Multi curve Elliptic Curve Cryptography (ECC) technique. Next, the encrypted cipher is embedded into the H.264 Video using a novel proposed Optimized Modified Matrix Encoding (OMME) steganography technique to embed the secret data. While embedding the encrypted confidential details into the video, pixels from the frames can be selected using an optimization algorithm called Artificial Bee Colony (ABC) in order to reduce distortion of stego video. Finally, the user's secret data embedded in the H.264 Video is extracted and it is de-ciphered. This proposed technique increases the level of security and robustness against attacks in terms of carrier capacity and embedding efficiency when compared to existing methodologies. The proposed work is implemented in the working platform of Matlab and provide data hiding in MPEG video files.

1. Introduction

The rapid development of communication technology due to the global spread of the Internet and the digital information revolution has given rise to a huge increase in the use and transmission of multimedia information, it broadens the scope of right and wrong, as there are privacy violations, information theft and so on. Data hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academia. It contains two main branches: digital watermarking and steganography. The former one is mainly used for copyright protection of electronic products, while steganography is a new way for sealed communication, its main purpose is to convey data secretly by concealing the very existence of communication. It is the process of hiding and transmitting data through carriers in an effort to hide the existence of the data. Steganalysis, on the other hand, is the process of detecting the presence of hidden messages in multimedia. Steganalysis can be applied to digital images and to digital video as reported in [1,2] respectively. Here we are trying to improve steganography techniques by considering different cover Medias to provide high security to the secret data while transmitting it over the networks.

Data hiding is the ability of embedding data into a digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer [3]. Data hiding consists of two sets of data, namely the cover medium and the embedding data, which is called the message. The digital medium or the message can be text, audio, picture or video depending on the size of the message. In general, there are two types of data hiding for video: one that hides the video content itself (video encryption or scrambling) so that nobody understands what is being transmitted; the other that embeds external information into the video, hence utilizing video as the data host.

In common, for data hiding, existing solutions rely on hiding message bits in Discrete Cosine Transformation (DCT) coefficients [4,5], Motion Vectors (MVs) [6,7] and [8], quantization scale [9] or prediction modes. Data hiding can also be applied before compression. For example [10] introduced a method that is robust to heavy JPEG compression. It is also possible to hide data in wavelet domain as reported in [11]. There is a much improved data hiding technique based on $BCH(n,k,t)$ coding which is reported in [12].

Recently as reported in [13] MPEG video files can be used to hide the data using Multivariate regression and flexible macroblock ordering. Wang and Moulin [14] have shown that, risk of detection of data can be reduced to zero level with effective steganography, as long as embedded has a correct knowledge of cover distribution. The main goals for the design of effective steganography algorithms [15] and [16] are,

* Corresponding author.
E-mail address: ramakrishnahegde74@gmail.com (R. Hegde).

http://dx.doi.org/10.1016/j.csi.2016.07.001
0920-5489/

either to modify the cover as little as possible, or to modify the cover data in inconspicuous parts.

Likewise, the work in [17] proposed the use of intra-prediction modes to hide message bits. It was shown that 1 bit can be hidden in each candidate 4 × 4 intra block. Additionally, the work in [18] utilized the block types and modes of intra coded blocks of H.264/AVC to hide message bits. The quantization scale is also used for data hiding, a recent publication in [19] proposed to divide the quantization scale of a macroblock by a certain factor. The factor is multiplied by all ac coefficients in the corresponding macroblock. The procedure is referred to as promoting and exiting a macroblock. If a message bit to hide is equal to zero, then such a procedure is followed, otherwise no action is taken. From a syntax viewpoint, since a relatively large number of prediction modes and block sizes are available in H.264/AVC, it has been proposed to use these variants to hide message bits.

An error resilient video encoding approach is used to help error concealment at the decoder. In [20] two data hiding approaches for data hiding in compressed MPEG video. In the first approach, the quantization scale of a Constant Bit Rate (CBR) video is either incremented or decremented according to the underlying message bit that is to hidden. A second-order multivariate regression is used to associate the macroblock-level features with the hidden message bit. The decoder makes use of this regression model to predict the message bits. However, the message payload is restricted to one bit per macroblock. Macroblocks are assigned to arbitrary slice groups according to the content of the message bits to be hidden.

Elliptic Curve Cryptography is a promising asymmetric cryptographic algorithm with an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [21]. The primary benefit of ECC is that it requires a smaller key size compared to other cryptographic algorithms. This reduces storage and transmission requirements, which leads to faster processing. This is very useful for implementing encryption on small devices with limited resources in terms of power, CPU and memory. It is also very helpful in handling many encrypted sessions for large web servers. The strength of an asymmetric encryption algorithm such as ECC is found in the complexity of computing the inverse of the function used to generate the key. Creating the key is straight forward, but finding the inputs that were used to create the key is computationally infeasible. In ECC, the computationally intense problem is called “Elliptic Curve Discrete Logarithm Problem”, and involves the difficulty in computing the discrete logarithm (exponent) from the result. And there are many hybrid cryptographic algorithms which uses ECC cryptosystem as a base making it an ideal choice. Cryptography for encoding user's secret data converted into encrypted cipher was performed using Elliptic Curve Cryptography (ECC).

The remaining of the paper is manuscript as follows. The works related to data hiding is mentioned in Section 2. The proposed techniques used in hiding of data is mentioned in Section 3. The experimental results and analysis of the research is mentioned in Section 4. Finally, the conclusion of the paper is given in Section 5.

2. Related work

Some of the recent work related to data hiding in MPEG video files is listed below:

With the quick improvement of multimedia and communication advancements, video communication is turning into the fundamental administration in wireless communication networks. Keeping in mind the end goal to enhance the quality of H.264 video transmissions over error-prone wireless networks, Yehet al. [22] displayed a data embedding based content-aware error recovery approach. At the encoder, the vital data of each Macroblock (MB) of the H.264 intra-coded I frame was separated adaptively taking into account scene change data and embedded into the Real-time Transport Protocol (RTP) header of the following frame. At the decoder, if the efficient data for a corrupted MB effectively removed, then the extracted essential data were utilized for error recovery. This methodology could accomplish better error recovery results with comparative or less measure of embedded data.

Dong et al. [23] proposed a Robust FMO (RFMO) algorithm which takes gradient feature of frames into consideration to enhance robustness of video streams, and the Adaptive RS Allocation (ARSA) helps to increase the with only a little increase in bit rate. Flexible Macro-block Ordering (FMO) was a new error resilient tool adopted by H.264/AVC. It had a good performance of error resilience by changing the coding order of macro-blocks in the frame. Redundant slice (RS) was another tool which adds redundant copy of slices into the stream to take precautions against packet loss. However, we shouldn't only care about Peak Signal to Noise Ratio (PSNR) of the video; the robustness of video streams to burst packet loss of wireless channel was also worth considering. In applications, such as real-time video transmission services, degradation of video quality might be tolerable, but collapse of decoder due to burst packet loss would greatly lower user's quality of experience. Thus, the RFMO algorithm could significantly reduce the collapse times of decoder with invisible decrease in visual quality, and the ARSA could still guarantee a high PSNR in the case of high packet loss rate.

To make full use of the correlation between two coefficients, Zhu et al. [24] presented a novel two-dimensional (2D) HM strategy for stereo H.264 video. Firstly, two Quantized Discrete Cosine Transform (QDCT) Alternating Current (AC) coefficients were randomly selected from each embeddable 4 × 4 luminance block. The values of coefficient pairs were classified into non overlapping sets. According to the sets of coefficient pairs, the generated 2D histogram was modified to embed data. When the value of one QDCT AC coefficient was modified by adding or subtracting 1, only one data bit at most could be hidden using the traditional HM, whereas up to three bits of information could be simultaneously embedded by employing this proposed scheme to achieve better capacity-distortion performance.

Zhao et al. [25] presents an inter-embedding error-resilient scheme to reduce the distortion caused by the loss of inter-layer prediction information in SVC. Scalable Video Coding (SVC), an extended version of H.264/AVC, was designed to transmit high-quality video bit streams over heterogeneous networks. However, such video bit streams were sensitive to transmission error, thereby severely degrading its quality. Interlayer prediction in SVC causes errors to be propagated not only to subsequent frames but also to frames in the upper layers, when the errors had occurred in the lower layers. This algorithm exploits the reversible data embedding scheme to hide essential information of the lower layer without damaging the original data. Experimental results demonstrate that the proposed method provides a better PSNR performance than the frame copy by an average of 4.89 dB in a 2-layer SVC decoder, and an average of 4.54 dB in a 3-layer SVC decoder in the case of whole frame loss.

Liu et al. [26] proposed a robust readable reversible data hiding scheme in H.264/AVC. Subsequently, encode the embedded data using BCH syndrome code (BCH) before data hiding to improve robustness, then embed the encoded data into the quantized discrete cosine transform (DCT) coefficients of the 4 × 4blocks of I frames which meet the directions of intra-frame prediction, and the directions of intra-frame prediction were utilized to avert the distortion drift. This new robust reversible data hiding algorithm get more robustness, effectively avert intra-frame distortion drift and get good visual quality.

3. Modelling of ECC and Optimized Modified Matrix Encoding (OMME)

Data hiding approach in which the information is hidden using the motion compensation block sizes of an H.264/AVC video to enable real time scene change detection in compressed video [26]. The schematic representation of the proposed system is given in Fig. 1. In this paper, initial pixel values of H.264/AVC video blocks are rearranged