Computers and Electrical Engineering 000 (2015) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A data-hiding technique using scene-change detection for video steganography☆

Mritha Ramalingam*, Nor Ashidi Mat Isa

Imaging and Intelligent System Research Team (ISRT), School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, Nibong Tebal 14300 Penang, Malaysia

ARTICLE INFO

Article history:
Received 30 September 2014
Revised 17 October 2015
Accepted 21 October 2015
Available online xxx

Keywords:
Data hiding
Video steganography
Security
Scene change detection
Discrete wavelet transform

ABSTRACT

This paper presents a data-hiding technique using scene-change detection for video steganography. Reducing the distortions in videos and securing the embedded data remain as competing goals in any video steganographic system. In this study, a data-hiding technique using discrete cosine transform (DCT) and discrete wavelet transform (DWT) coefficients is proposed to enhance the security of hidden data and minimize distortions to maintain better video quality. In this work, scene changes are detected using the DCT coefficients of video sequences for hiding data. Then, the cover-video and the payload are fused and normalized using the DWT coefficients to enhance video quality. The MATLAB simulation results indicate that the proposed method outperforms existing state-of-the-art methods. The comparison results reveal that the proposed data-hiding method offers better security and minimizes distortions for better video quality.

1. Introduction

Data hiding in digital multimedia, such as text, image, audio, and video, plays an increasingly vital role in the current trend of secure communication [1]. Secure communication is highly desirable in many cases and has thus given rise to the need to develop new approaches in information hiding [2]. Steganography is one of the most significant techniques for secure communication. Steganography is the art of hiding data within data by concealing the presence of messages [3]. The process of data hiding in basic steganography is shown in Fig. 1. In any basic steganographic technique, the cover-medium serves as the carrier of the secret message, the secret message is the message to be embedded into the cover-medium, and the stego-medium is the medium containing the embedded data [4].

Modern Internet technologies demonstrate that videos are important media for sharing data, medical records, banking information, broadcast information, and military intelligence. Videos are particularly suitable for data hiding for a number of reasons: (1) distortions in videos can be handled faultlessly, (2) hidden data are imperceptible to the human visual system (HVS), and (3) videos provide additional hiding space. The present work is undertaken in consideration of the widespread use of video data. As videos are often stored and transmitted in compressed formats, data hiding should withstand lossy compression [5]. Accordingly, many data-hiding schemes are executed in the transform domain by modifying discrete cosine transform (DCT) coefficients.

A considerable number of steganography studies have been conducted on the spatial and transform domains of cover-media for data hiding [6]. In the spatial-domain approach, data are hidden in the pixels of a cover-medium. The least significant bit

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. E. Cabal-Yepez.
* Corresponding author. Tel.: +60164371457.
E-mail addresses: mritha2011@gmail.com (M. Ramalingam), ashidi@eng.usm.my (N.A.M. Isa).

http://dx.doi.org/10.1016/j.compeleceng.2015.10.005
0045-7906/

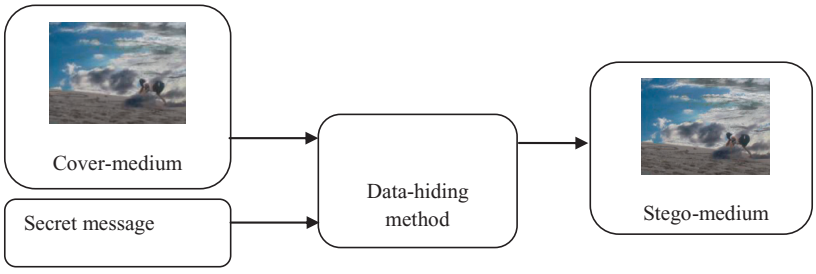

Fig. 1. Data hiding in a basic steganography.

(LSB)-based data-hiding technique is the most widely used spatial-domain-based steganography. In [7], the data were embedded into a compressed video in the transform domain, which is highly vulnerable to steganalysis. The payload was minimal; nevertheless, the method achieved low-video distortion.

In [8], the distortion levels were reduced by employing a method with a dual-convolution code that minimizes the additive distortion in steganography. In recent years, many data-hiding schemes have been developed in the transform domain, in which the data are embedded into the transform coefficients of the cover-medium using polynomial mathematics [9], Fourier transform, DCT, and discrete wavelet transform (DWT). Transform-domain methods are generally more robust than spatial-domain methods [10].

The present work attempts to improve secret-data security by utilizing DCT and DWT coefficients. The key objectives of this study are as follows:

- To enhance the security of hidden data by using scene-change detection and the DCT coefficients of video sequences
- To improve video quality after hiding data using DWT in video sequences

The rest of this paper is organized as follows. Section 2 discusses the methods that are currently used in data hiding, including their advantages and limitations. Section 3 explains the proposed scene-change-detection-based data hiding (SCDH) method for video steganography in the DCT and DWT domains. Section 4 presents the analysis and comparison of the experimental results obtained using the proposed SCDH method, and other existing methods. Section 5 concludes the paper.

1.1. List of abbreviations

HVS - human visual systems; MR-FMO - multivariate regression and flexible macro-block ordering; MPEG - moving picture experts group; LSB - least significant bit; DWT - discrete wavelet transform; DCT - discrete cosine transform; UCI - University of California Irvine; SCDH – scene-change-based data hiding technique; DWTSQ - DWT-based steganography for quality; S-DWT - steganography using DWT; PSNR - peak signal-to-noise ratio; MSE - mean squared error; dB - decibels.

2. Related work

As the present work utilizes the DCT and DWT coefficients, this section presents studies on transform-domain-based techniques. The DCT transforms the cover-image from the spatial domain into the frequency domain. In [11], an adaptive optimization procedure was adopted for the selection of bi-stable parameters to achieve the maximum correlation coefficients under the minimum computational complexity.

In [12], a coherent steganographic technique was presented to improve the security of the secret messages hidden using the DCT coefficients of a cover-image. In the technique, the cover-image was divided into blocks, and the DCT was applied to each block; the number of the most significant bits of the payload was coherently embedded into the DCT coefficients of the cover-image based on the values of the DCT coefficients [12]. The proposed method improved peak signal-to-noise ratio (PSNR), security, and capacity [12]. In [13], data hiding was performed using the DCT and LSB techniques. The DCT-based steganography technique was used to embed the text messages into the LSB of the DCT coefficient of a digital image; the data-hiding capacity of the system is limited, although the method achieved improved quality [13].

Data hiding in the frequency domain, rather than in the spatial domain, was performed in [14]. In the frequency-domain approach proposed in [14], secret messages were embedded into high-frequency DWT coefficients, the DWT coefficients in the low-frequency sub-bands were unmodified to enhance quality, and some basic mathematical operations were performed on the secret message before embedding. The proposed approach achieved improved security [14].

The major advantage of using wavelet transforms in digital-media processing is the significant localization property, which is suitable for many image-processing applications [15]. In [16], text data of considerable size were embedded into selected images using an entropy function and the embedding process was constrained by how much the bit error rate is minimized.

In [17], data were embedded in the frequency domain without compromising image quality; the hidden data were successfully extracted with minimal distortion. However, the capacity and quality of the cover-medium of the steganographic system adopted in [17] needs to be improved.

Please cite this article as: M. Ramalingam, N.A.M. Isa, A data-hiding technique using scene-change detection for video steganography, Computers and Electrical Engineering (2015), http://dx.doi.org/10.1016/j.compeleceng.2015.10.005