Int. J. Electron. Commun. (AEÜ) 67 (2013) 645–651

Contents lists available at SciVerse ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Video watermarking scheme based on visual cryptography and scene change detection

Th. Rupachandra Singh[a,*], Kh. Manglem Singh[b], Sudipta Roy[a]

[a] Department of Information Technology, Assam University, Silchar 788011, India
[b] Department of Computer Science & Engineering, NIT Manipur, Imphal 795001, India

ARTICLE INFO

Article history:
Received 21 December 2011
Accepted 21 January 2013

Keywords:
Digital watermarking
Visual cryptography
Discrete wavelet transform
Scene change
Video

ABSTRACT

There is wide interest in multimedia security and copyright protection due the explosion of data exchange in the Internet and the extensive use of digital media. We propose a novel video watermarking scheme based on visual cryptography and scene change detection in discrete wavelet transform domain. We start with a complete survey of the current image and video watermarking technologies, and have noticed that majority of the existing schemes are not capable of resisting all attacks. We propose the idea to use different parts of a single watermark into different scenes of a video for generation of the owner's share from the original video based on the frame mean in same scene and the binary watermark, and generation of the identification share based on the frame mean of probably attacked video. These two shares after stacking can reveal the copyright ownership. Experiments are conducted to verify the robustness through a series of experiments. The security requirement of the proposed algorithm is achieved with the visual cryptography.

1. Introduction

The growth of the digital multimedia technology and the successful development of the Internet have not only allowed people to process, deliver and store digital content more easily, but also have gifted the facility of copying it rapidly and perfectly without loss of quality, with no limitation on the number of copies, tempering with and redistributing illegally without authorization. This kind of advantages raises the issue of how to protect copyright ownership. Classical protection such as cryptography is not a solution, because data after decryption can always be distributed in plain form without any restriction, even by the authorized customer. A better solution to this problem is to integrate the security information directly into the content of the digital data in inseparable form during its useful lifespan and digital watermarking is such an effective way to protect copyright of the digital multimedia data even after its transmission. Watermarking is the process that enables data called a watermark, digital signature, tag, or label into a multimedia object such as audio, image or video in perceptually invisible or inaudible manner without degrading the quality of the object, such that watermark can be detected or extracted later to make an assertion about the object [1–4]. The embedded information can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats [5]. Digital watermarking provides value-added protection on the top of data encryption and scrambling for content protection and effective digital rights management [6].

Typically watermark contains information about the origin, ownership, destination, copy control, transaction etc. Watermarking has many different applications such as copyright protection, transaction tracking, copy control, ownership identification, authentication, forensic analysis, playback screening, legacy system enhancement and database linking etc. [7–9]. Copyright protection of digital data is defined as the process of proving the intellectual property rights to a court of law against the unauthorized reproduction, processing, transformation or broadcasting of digital data [7]. It embeds information about the owner of the object and uses for resolving rightful ownership. Each digital object has a unique watermark identifying the buyer of the object, which requires a very high level of robustness for fingerprinting for traitor tracking so that buyers can be traced. For copyright-related applications, the embedded watermark is expected to be robust to various kinds of malicious and non-malicious attacks, provided that the manipulated content is still valuable in terms of perceptual quality [10]. Although some significant progresses have been done recently, one of the major problems in the practical watermarking methods is the insufficient robustness of the existing watermarking algorithms against geometrical attacks such as sharpening, lightening, darkening, cropping, blurring, distorting, scaling, jittering,

* Corresponding author. Tel.: +91 9856508218.
E-mail addresses: rupachandrath@gmail.com (Th.R. Singh), manglem@gmail.com (Kh.M. Singh), sudipta_it@gmail.com (S. Roy).

1434-8411/$ – see front matter © 2013 Published by Elsevier GmbH.
http://dx.doi.org/10.1016/j.aeue.2013.01.008

rotation and, removal attacks such as denoising, quantization, remodulation, filtering, JPEG compression, collusion, print-copy-scanning, cryptographic attacks and protocol attacks. Majority of geometrical and removal attacks come under malicious attacks. Malicious attacks attempt to remove or disable watermark [11].

The present paper proposes a novel video watermarking scheme based on visual cryptography and scene change detection in discrete wavelet transform domain. Different scenes from the video are detected. The frame mean of the all the frames in the same scene is found. The size of the frame mean is equal to the size of a frame in the video. The global mean of the frame mean is also found and its size is one. The watermark to be used in our work is sliced into different parts called sub-watermarks, which are used to generate owner's share based on visual cryptography that checks whether the pixel value of the binary watermark is zero or not, and compares every pixel value of the frame mean in the same scene with the global mean. The algorithm uses an identical sub- watermark for the successive frames in the same scene, but different parts in different scenes. For the generation of identification share, only the frame mean and the global mean of the controversial video are used. The watermark can be revealed by stacking two printed shares on transparency papers.

This paper is organized into five sections. Section 2 gives a survey of current image and video watermarking technologies. Section 3 describes the details of the novel video watermarking scheme. Section 4 gives the experimental results, followed by the conclusions in Section 5.

2. Related works

Watermarking system can be characterized by a number of defining properties [12] such as embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, robustness, security, cipher and watermark keys, modification and multiple watermarks, cost, temper resistance, unobtrusiveness, reading detection, unambiguous, sensitivity, scalability etc. Various types of watermarking methods have been proposed for different applications and these can be classified into two categories: either spatial domain or frequency domain using discrete Fourier transform (DFT), discrete wavelet transform (DWT), Fourier Mellin transform (FMT), fractal transform etc. Most of current video watermarking schemes are based on the techniques of image watermarking.

The simplest watermarking in the spatial domain is to flip the least significant bit (LSB) of the chosen pixels in the image. A more robust watermark is to superimpose a watermark over an area of the image. An improvement to the basic LSB substitution is to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given seed or key. The algorithm may survive cropping attack, but is vulnerable to replacing the LSBs with a constant. Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image [13]. Watermarking schemes in the spatial domain are less robust than those in frequency domain [14].

The main strength offered by the transform domain techniques is that they can take advantages of special properties of alternate domains to address the limitations of pixel based methods and/or to support the additional features. Threshold-based correlation watermarking scheme [13] and direct sequence watermark using m-frame [15] are worse than the LSB-based watermarking scheme. Discrete cosine transform based watermarking scheme is more robust to lossy compression [16]. Discrete Fourier transform with template matching [17] watermarking can resist a number of attacks including removal, rotation and shearing. Discrete wavelet transform based watermarking is the most robust to noise addition [18].

Video watermarking introduces some issues not present in image watermarking. In the first issue, video signals are highly susceptible to pirate attacks including frame averaging, frame dropping, frame swapping, statistical analysis, interpolation etc. Such attacks have no counterpart in image watermarking. The second issue is to provide the imperceptibility of the watermark, which is a relatively more difficult problem compared to the image case due to the three-dimensional characteristics of the video. The watermark procedure should take into the variation in the temporal direction into account to provide an imperceptible watermark. Considering large amount of data and inherent redundancy between frames, video watermarking poses many problems. On one hand, the attacker would collude with frames from different scene using the identical watermark from each frame [19]. Using independent watermark for each frame, on the other hand, the attacker would take advantage of motionless regions in successive video frames to remove the watermark by comparing and averaging the frames statistically [20].

Most of the current video watermarking techniques insert watermark directly to uncompressed or compressed video sequences [21,22]. However these methods are not sufficient for copyright protection in video data. Video watermarking has a number of issues, and image based algorithms could not solve these problems. Embedding large amount of data, the redundancy between frames and robustness against temporal attacks are some of the main problems in video applications. The collusion may be either inter-video collusion or intra-video collusion. Neither embedding the same watermark to each frame nor embedding different watermarks in every frame of the video would be robust against all types of common attacks. Embedding identical watermark to each frame of the video leads to the problem of maintaining statistical perceptual invisibility [23]. The collusion can estimate the watermark from each watermarked frame and obtain a refined estimate of the watermark by linear combination. The unwater marked frame can be obtained with subtraction with the watermarked one [21]. On the other hand, applying independent watermarks to each frame also presents problem if regions in each frame remains little or no motion between the consecutive frames [24]. The motionless regions may be averaged to remove the independent watermarks. Averaging independent watermarks converges toward zero. Su et al. have pointed out that collusion can be prevented by embedding identical watermark to the similar frames in the same scene and different watermarks to dissimilar frames [25]. Two types of watermarks (identical and independent) are used for embedding in motionless and motion regions of video respectively.

Embedding watermarks in the detail bands of the discrete wavelet transform increases the robustness of the watermark [13]. Niu and Sun proposed a wavelet based watermarking method that embeds decomposed watermark at different resolution in the corresponding resolution of the decomposed video by means of multire solution signal decomposing [26]. Serdean et al. proposed a blind video watermarking scheme that is invariant to geometrical attacks such as shift, rotation, scaling, and cropping [27]. Their method employed image registration technique to invert the attack and watermark is embedded in the wavelet domain according to a human visual system (HVS) model. Mitchel et al. proposed a multire solution video watermarking using perceptual models and scene change detection [20]. The watermark consisting of static and dynamic temporal components is generated from a temporal wavelet transform of the video scene. The noise-like watermark is statically undetectable to thwart unauthorized removal. Barni et al. proposed a robust watermarking scheme for raw video [28] that alters the discrete Fourier transform coefficients of the brightness components of the to-be-marked frames. Only the first of each group of pictures (GOP) is watermarked. The scheme is robust