A Collusion-Resistant Video Watermarking Scheme

Amir Houmansadr[1] and Shahrokh Ghaemmaghami[2]

[1] Electrical Engineering Department, Sharif University of Technology, Tehran, Iran
houmansadr@mehr.sharif.edu
[2] Electronics Research Center, Sharif University of Technology, Tehran, Iran
ghaemmag@sharif.edu

Abstract. A video watermarking scheme is proposed in this paper using the concept of the secret sharing scheme. The owner's mark is split into twin shares, where the shares are inserted into the video frames in the spatial domain in a simple manner. The detection algorithm uses a linear function applied to the twin shares to reconstruct the secret. This makes the watermarked video sequence robust against pirate attacks, such as frame averaging and frame swapping. Due to the compatibility of the exploited secret sharing scheme to geometrical distortions, the watermarking system is also robust to this kind of processing schemes. On account of insertion of various marks into different frames, which are linearly related, the watermarked sequence is robust to collusion attack that is a major concern in the field of video watermarking.

1 Introduction

Illegal copying and distribution of digital media has made the owner's rights to be more and more frequently violated. Traditional solutions for copyright protection, such as encryption, can no longer protect digital contents by themselves. Sooner or later, encrypted media have to be revealed for the aim of consumer's usage that may be the malicious one. At the end of 20^{th} century, digital watermarking was introduced as a complementary solution to protection of digital media ownership.

In copyright protection applications, a digital watermark is an invisible mark that is inserted into a digital media such as audio, image, or video, which is used to identify illegal distributions of copyright protected digital media and also lawbreaking customers. A digital watermark should have certain features to achieve desired functionalities in this case. The embedded mark is to be robust enough against various watermarking attacks, while keeping the perceived quality of the host image unchanged (the imperceptibility requirement). Watermarking attacks consist of deliberate attacks made maliciously to remove or change the mark sequence by lawbreakers and unintentional attacks caused as a result of different kinds of coding and compression made to the digital media prior to transmission and/or storage and also errors occurred during the transmission of the media through networks.

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 343–354, 2007.

Video contents can be mentioned as the most valuable digital media, which are increasingly used illegally, resulting in a huge damage to filmmaking industry. Video watermarking is utilized for different video applications such as copyright protection, fingerprinting, broadcast monitoring, copy protection, and so on [1]. Distinct challenges have arisen in this field, as compared to image watermarking. Because of the more possibilities to perform the collusion attack on video streams, it is a main concern in designing video watermarking systems. Collusion refers to using some watermarked data that is utilized for the aim of watermark removal.

The main goal of this paper is to design a watermarking scheme for video sequences which is robust to collusion attack. In Sect. 2, the main concept of secret sharing is introduced. Sect. 3 describes the proposed insertion and detection watermarking schemes based on the mentioned secret sharing scheme. The collusion attack, in the proposed scheme, is analyzed in Sect. 4 and simulation results are presented in Sect. 5. Finally, the paper is concluded in Sect. 6.

2 Visual Secret Sharing

A secret sharing scheme shares a secret into a number of shares so that the cooperation of a predetermined group of shareholders reveals the secret, while the secret reconstruction is impossible to any unauthorized set of shareholders. *Naor et al.* in [2] proposed a 2-dimentional secret sharing scheme which is known as visual secret sharing (VSS). Since we are using this scheme in the proposed watermarking scheme in this paper, VSS scheme is described in this section.

VSS scheme shares a binary-valued image, which is known as secret image, into two double-sized images so that reconstruction of the secret image from these twin images can be done only if both of them are available. So, a VSS system is composed of the following components:

- Secret image: a digital image composed of $M \times N$ white and black pixels, whose anonymity is the goal of the system;
- VSS sharing scheme: derives two share-images from a secret image in a pseudo-random manner;
- Share-images: digital images composed of $2M \times 2N$ white and black pixels, that are driven from the secret image in a pseudo-random manner. Two share-images are produced in every run of the VSS sharing scheme, known as twin share-images. Different runs of the VSS scheme generates different share-images, and each of these share-images reveals no information about the secret image unless its twin, i.e. the share-image generated in the same run of the VSS sharing scheme, is available;
-VSS reconstruction scheme: retrieves the secret image from every corresponding couple of share-images, i.e. twin share-images. VSS reconstruction scheme is lossless if share-images have not been distorted in any way.

According to the VSS sharing scheme, each pixel in the secret image is split into two 2×2 blocks of pixels, which are chosen form the blocks shown in Fig. 1.