Chapter 30
Video Saliency Detection for Visual Cryptography-Based Watermarking

Adrita Barari
Defence Institute of Advanced Technology, India

Sunita V. Dhavale
Defence Institute of Advanced Technology, India

ABSTRACT

The aim of this chapter is to review the application of the technique of Visual cryptography in non-intrusive video watermarking. The power of saliency feature extraction is also highlighted in the context of Visual Cryptography based watermarking systems for videos. All schemes in literature related to Visual cryptography based video watermarking, have been brought together with special attention on the role of saliency feature extraction in each of these schemes. Further a novel approach for VC based video watermarking using motion vectors (MVP Algorithm) as a salient feature is suggested. Experimental results show the robustness of proposed MVP Algorithm against various video processing attacks. Also, compression scale invariance is achieved.

1. INTRODUCTION

The rapid growth in digital video editing technologies has become a threat to the authenticity and integrity of video data. In case of wide range of applications, such as video surveillance, video broadcast, DVDs, video conferencing, and video-on-demand applications, protection of intellectual property rights of transmitted video data is vital. Digital watermarking technology has emerged in last decade as a well-known solution for video copyright protection (Hartung & Kutter, 1999). In digital watermarking technique (Hartung & Kutter, 1999; Petitcolas, F.A.P, 2000), a watermark representing the copyright information (w) is embedded into the cover video (x) to obtain new watermarked signal $\hat{x} = x + w$, practically indistinguishable from x, by people, in such a way that an eavesdropper cannot detect the presence of w in $\hat{x}$. At the

DOI: 10.4018/978-1-7998-1763-5.ch030

time of ownership dispute, the embedded watermark is extracted ($\hat{w}$) from the watermarked video ($\hat{x}$) and used for verification. Almost all digital video data today is distributed and stored in the compressed format. Hence, existing approaches in video watermarking can be categorized as uncompressed domain video watermarking (Sun & Liu, 2005; Chen & Leung, 2008; Blanchi & Piva, 2013) and compressed domain video watermarking (Ardizzone, E., La Cascia, M., Avanzato, A., & Bruna, A., 1999; Lin, Eskicioglu, Reginald, & Edward, 2005; Fang & Lin, 2006; Sejdic, Djurovic & Stankovic 2011; Aly, H., 2011).

A well-designed video watermarking system must offer both perceptual transparency and robustness (Petitcolas, F.A.P, 2000). Perceptual transparency means that the watermarked video should be perceptually equivalent to the original video. Robustness refers to a reliable extraction of the watermark even if the watermarked video is degraded during different intentional and non-intentional attacks. Assuring perceptual transparency is difficult in video compared to that with still images, due to the temporal dimension existing in video. Embedding different watermarks into video frames independently without taking the temporal dimension into account usually yields a flicker effect in video. This is due to the fact that the differences exist between the intensities of pixels at the same position in two successive video frames.

Of late, visual cryptography (VC) has come up as one of the novel solution for image and video watermarking which is capable of providing zero perceptual distortion along with good robustness towards attacks. VC is a cryptographic technique which allows visual information (for example images, text, etc.) to be split into *n* different shares with the help of simple mathematical techniques (Naor & Shamir, 1995). In case of watermarking, a secret watermark image *w* is split into master share *M* and ownership share *O* using VC technique. The master share *M* is generated based on the unique salient features of the host data *h* which needs to be watermarked. The ownership share *O* depends on both binary watermark secret *w* as well as master share *M* and is registered with certified authority *CA*. At the time of dispute over the rightful ownership of the attacked host data $\hat{h}$, ownership is identified by stacking the master share $\hat{M}$ (estimated based on $\hat{h}$) and ownership share *O* kept by the *CA*. Generation of master share *M* affects the robustness and security of VC based watermarking. As *M* is generated based on the unique salient features of the host data *h*, video saliency detection plays an important role in VC based watermarking.

This chapter provides a brief introduction to VC and application of VC in watermarking. The chapter also provides detail overview of existing VC based video watermarking techniques. In case of nonintrusive VC based video watermarking approaches, the importance of video saliency detection stage in generation of master share *M* is analyzed. Finally, a novel approach is suggested for VC based video watermarking techniques using motion vectors.

2. VISUAL CRYPTOGRAPHY IN WATERMARKING

In 1995, a novel visual secret sharing concept called Visual Cryptography (VC) was proposed by Moni Naor and Adi Shamir. VC is a technique which allows visual information (for example images, text, etc.) to be split into *n* different *shares* with the help of simple mathematical techniques. These shares are nothing but pseudo random noise-like structures which reveal no meaningful information if viewed in isolation as seen in Figure 1(a) and 1(b). However, when all the required shares are printed upon transparencies and overlaid one upon the other, they reveal the secret image as illustrated in Figure 1(c). The reconstruction of the secret visual information in this case can be done only with the help of the Human Visual System (HVS). This is the reason why the technique is called *visual* cryptography.