Chapter 19
Data Hiding Schemes Based on Singular Value Decomposition

Victor Pomponiu
University of Torino, Italy

Davide Cavagnino
University of Torino, Italy

Alessandro Basso
University of Torino, Italy

Annamaria Vernone
University of Torino, Italy

ABSTRACT

Information hiding techniques are acquiring an always increasing importance, due to the widespread diffusion of multimedia contents. Several schemes have been devised in the fields of steganography and digital watermarking, exploiting the properties of different domains. In this chapter, the authors focus on the SVD transform, with the aim of providing an exhaustive overview (more than 100 papers are analyzed) on those steganography and watermarking techniques leveraging on the important properties of such a transform. The large number of algorithms operating in the image, video and audio contexts is first classified by means of a general approach, then analyzed, to highlight the advantages and disadvantages of each method. The authors also give a detailed discussion about the applicability of each reviewed and compared data hiding scheme, in order to identify the most appropriate candidates for practical applications.

INTRODUCTION

Due to the rising dependence on digital media and the unexpected expansion of the distribution opportunities over the Internet, techniques for hiding information into digital contents are achieving significant importance. Such techniques aim to provide the ability to communicate secretly and the capacity to protect copyrighted multimedia content against illegal distribution. Designing such schemes has become a topic of great importance and many researchers have spent much effort in the last years to obtain an effective solution.

DOI: 10.4018/978-1-4666-2136-7.ch019

However, despite many different approaches have been attempted, there is currently no scheme that can preserve imperceptibility of the hidden data while ensuring a high security against malicious attacks.

To help characterizing the differences in capacity, requirements and intended use, data hiding is often divided into two broad subcategories:

- **Steganography:** (from the Greek words στεγανός and γραφειν that mean "cover writing") enables secret communication and is characterized by obscuring the existence of secret messages enclosed into apparently inoffensive cover media (Katezenbeisser & Petitcolas, 1999). Unlike cryptography which aims to scramble the content of the message to keep it secret, the main intention of steganography is to facilitate the existence of a hidden channel that permits transmission of private messages. The model for this secret communication was inspired from a famous example called the "prisoners' problem" (Simmons, 1984). Briefly, two persons, Alice and Bob, are arrested and thrown in prison. During detention, they try to devise an escape plan. However, there is a prison guard, called Eve, which examines the messages exchanged between each other, making the communication extremely difficult. Therefore, Alice and Bob are forced to exchange cover messages, which in reality contain hidden messages linked to the escape plan. In this model, the guardian may have a passive involvement, only observing the messages, or an active implication, trying to modify the private messages without destroying the cover message.
- **Digital watermarking:** is a widespread information hiding technique, aimed to resolve different multimedia security issues (e.g., copyright protection, illegal distribution, broadcast monitoring and authentication) by embedding secret information (i.e., digital watermarks) into media contents. However, differently from steganography, the fact that a content is watermarked is not necessarily a secret. Hence, watermarking techniques require an intrinsic higher robustness if compared to steganography methods, due to the existence of a whole class of attacks aimed to specifically remove the embedded information. Moreover, it should not be possible to remove the inserted watermark without possessing additional information (e.g., a secret key) while maintaining the usability of the digital content. For these reasons, the watermarking context is generally considered more challenging and demanding in terms of security requirements than steganography. Furthermore, while steganographic transmission takes place between two parties, i.e., sender and receiver, watermarking schemes involve one-to-many communication (Katezenbeisser & Petitcolas, 1999).

In the last years, information security requirements have changed from traditional mechanisms to complex and integrated schemes which are able to protect data during transmission. However, each of such hiding schemes cannot provide a complete security solution, since different applications use them to asses a specific goal (i.e., secret communication or copyright protection) in a particular framework. A reliable security solution should wisely combine these primary mechanisms, i.e., cryptography, steganography and watermarking, into a global system (Barni, Bartolini & Furon, 2005; Chandramouli, Kharrazi & Memon, 2004).

It is worthwhile to point out that the secret message can be encrypted before embedding, thus improving the security of the data hiding schemes. The main security primitives, along with their spheres of application, are outlined in Figure 1.