Chapter 5
Reversible Watermarking Techniques:
Digital Conent Security

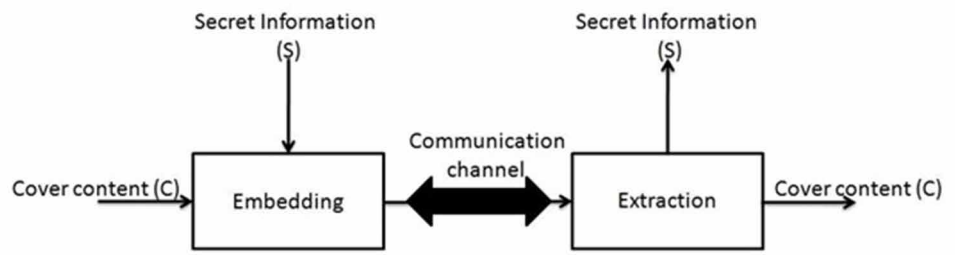
Muni Sekhar Velpuru
Vardhaman College of Engineering, India

ABSTRACT

Digital content security gained immense attention over past two decades due rapid digitization of industries and government sectors, and providing security to digital content became a vital challenge. Digital watermarking is one prominent solution to protect digital content from tamper detection and content authentication. However, digital watermarking can alter sensitive information present on cover-content during embedding, then the recovery of exact cover-content may not be possible during extraction process. Moreover, certain applications may not allow small distortions in cover-content. Hence, reversible watermarking techniques of digital content can extract cover-content and watermark completely. Additionally, reversible watermarking is gaining popularity by an increasing number of applications in military, law enforcement, healthcare. In this chapter, the authors compare and contrast the different reversible watermarking techniques with quality and embedding capacity parameters. This survey is essential due to the rapid evolution of reversible watermarking techniques.

DOI: 10.4018/978-1-7998-2795-5.ch005

Figure 1. Reversible watermarking process



INTRODUCTION

Now-a-days data tampering and copyright violation became a major challenge for digital content security. A watermarking technique is a promising solution for digital content protection. Apart from the watermarking there exists alternate solutions for digital content protection i.e., steganography and cryptography. Here, watermarking and steganography are considered to be data hiding techniques "it hides secret information into cover-content" (A.M. Alattar (2004), M. Barni et. al. (2004), B. Ou et. al. (2012), V MUNI SEKHAR, et. al. (2015). However, both have significant difference in terms of relationship between cover-content and secret information. Steganography is used for secret communication i.e., steganography conceals secret information into cover, if the existence of secret information is revealed, then steganography fails. In the case of watermarking the existence of secret information can be known to anyone, but separating it from cover-content is impossible. Whereas, cryptography does not conceal the secret information, but scrambles the information such that intruder cannot understand without an appropriate key [M. Barni et. al. (2004)].

A watermarking technique ensures protection of the data and ensures whether data is received with or without tempering. However, watermark can include additive noise in cover-content, so it may damage the sensitive information present in the cover. Hence, recovery of exact information at the receiving end may not be possible. In case of military, medical imaging and law-enforcement applications, even slight modification in cover-content may not allowed. Moreover, the need of such application is rapidly increasing every day. Hence, recovery of cover-content after extraction is an essential requirement for many applications. A lossless watermarking or reversible watermarking is a special case in watermarking [M.U. Celik et. al. (2005)]. It can extract exact original cover-content after the extraction process as shown in figure 1.