Chapter 12
Feature Based Watermarking

Hedley Morris
Claremont Graduate University, USA

Mohammad Eyadat
California State University, USA

Imad Muhi
New York Institute of Technology, Jordan

ABSTRACT
A digital media product must be protected with a watermark. This mark must be resilient yet transparent to legitimate users of the media. There are those who seek to cloud the ownership of digital media by tampering with the embedded marks. For example, a small rotation, scale change or cropping of an image can make it difficult, or impossible, for the legitimate owner to recover the watermark. This is called a geometric attack. The authors present a new paradigm for rendering any watermarking scheme resistant to such geometric attacks. This is done by means of a new image transform to a Rotation, Scaling, and Translation (RST) invariant domain based on ideas from shape theory. They also propose extensions of this technique to video watermarking. Finally, the authors provide an example of how these ‘shape based’ concepts can be extended to more general relational databases provided an abstract notion of shape is employed.

INTRODUCTION
The growth of the Internet has led to a massive distribution of digital multimedia data. This has spawned major concerns over intellectual property and ownership rights. By its nature digital data offers the possibility of mass duplication and the unfettered distribution of copyrighted materials. These concerns led to the Digital Millennium Copyright Act in 1998. Watermarking involves embedding a hidden signal, a watermark, directly into digital data in an irreversible fashion. Such a watermark can be used for standard tasks such as the copyright protection of intellectual property, the tracking of illegal copies and copy protection, the direct control of duplication devices. Watermarks can also be used to test for data tampering, say of medical data. In this chapter we will consider mainly the watermarking of images and videos with a brief description of the watermarking of relational databases. This chapter
demonstrates how an approach to watermarking based on ideas from shape theory provides a new set of methods that allow conventional watermarking methods for images to be extended to more general digital objects such as video streams and relational databases. The approach is to mark not individual elements such as pixels but identifiable subsets of the data. Shape theory (Kendall, 1999) is concerned with algorithms for the recognition of similar objects. Watermarking is concerned with the hiding of data in digital objects. Attacks distort such objects and so, to recover the watermark, it is necessary to be able to recognize deformations of objects as similar. Shape theory is all about algorithms for similarity testing (Goodall, 1999).

Hiding information in a multimedia data is easy. Doing so in a way that allows its retrieval or to proves its existence is a different matter. This is especially so when outside agents are trying their best to remove or replace your mark.

Geometric attacks alter the image in such a way that it is difficult to find where the mark is hidden. Watermarks that are invariant to geometric distortions can be designed, see for example (Bas et al., 2002) for the basic watermarking method.

Based on the well known algorithms and approaches we may summarize these approaches into 3 categories:

1. Using the Fourier-Mellin-Transform for the required invariance. An invariant vector is constructed from the slices of the log-polar mapped Fourier magnitude spectrum. A watermark is embedded by modifying this vector. Algorithms using the Fourier-Mellin transform suffer serious implementation difficulties. The log-polar and inverse log-polar mapping introduces errors during insertion. As they use the Fourier magnitude spectrum, interpolation performance is poor because interpolation only performs well with the sample values with the same scale.

2. There are many other implementation problems to consider. Watermarking algorithms using a feature of an image were proposed as the second generation watermark. As features of the image have high invariance to distortions, they can be used as a key to find the insertion location. The features of the image have high invariance to distortions, and consequently determine where a mark has been inserted, see (Cox, et al., 2002).

3. In this chapter we propose a new feature-frame based image watermarking method that is resistant to geometrical attacks. Our approach is based on regions rather than points. A set of k-sided polygons in the plane is called a frame of k-ads. In order that our k-ads should be identifiable we use polygons whose vertices are image features. To give us the robustness required, the features chosen must be stable feature points. We must be able to identify and locate the equivalent k-ads in geometrically attacked images. Our methods do not depend on the feature point locator but we do require that the method not produce too many feature points. A regular Harris corner detector produces a huge number of features which change under rotations. A feature detector that is able to select mostly robust points that are preserved under geometric attack is needed. For our work we have selected the SIFT method, see (Ettinger, 2002)

We present a new watermarking scheme in which the watermarking is carried out in the spatial domain using robust feature points to aid in its embedding and extraction. These specific feature points are not only used to embed information, but also act as a geometrical reference. Our new method is based on embedding multiple copies of watermarks in regions around robust feature points and using shape theory to remediate the effects of affine attacks. In this chapter we show that:

• This new approach to watermarking that is based on a feature-frame in an image