International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **7**, July **2009**

 ISSN 1349-4198
pp. 1883–1892

CONTENT-BASED AUDIO AUTHENTICATION WATERMARKING

Michael Gulbis[1], Erika Müller[1] and Martin Steinebach[2]

[1]Institute of Communications Engineering
University of Rostock
Richard-Wagner-Straße 31, 18119 Rostock, Germany
{ michael.gulbis; erika.mueller }@uni-rostock.de

[2]Transaction and Document Security
Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75, 64295 Darmstadt, Germany
martin.steinebach@sit.fraunhofer.de

Received March 2008; revised July 2008

Abstract. *The protection of media data integrity is a challenge addressed by various cryptographic techniques. But none so far only few approaches provide satisfying results with respect to the manipulation detection. Especially distinguishing between allowed audio editing and malicious tampering of the media content or operations with annoying impairment of the perceptual audio data quality is still an open issue. We introduce a content-based authentication watermarking technique. The experimental evaluation of our algorithm shows that the content feature is robust against operation with imperceptible impairment of the audio data content and provides detection of malicious tampering of the perceivable audio data quality and manipulation of the data content. The problem of high watermark payload we solve with a content feature transparent watermark embedding. Our watermark information is embedded in the same domain as used for the content feature extraction without impairment of the content feature. Our method is verified using audio speech data with an overall playback time of about five hours.*

1. **Introduction.** In our modern life multimedia data has become a widely used carrier of information. The rapid development of technology yields to many ways of production, distribution, archiving and editing of multimedia data. This advancements inhere the problem that high quality forgery is be created at a relatively low cost and no sophisticated knowledge. Hence, the integrity of audio data has to be questioned.

Traditional cryptographic mechanisms for integrity and/or authenticity of digital data like checksums, error correction codes or digital signatures include a number of drawbacks in regard to the characteristic of multimedia data. One important difference of multimedia to textual information is the greater degree of freedom with respect to the binary representation of the same information or meaning. While text data usually only allows one binary representation and changes therein immediately lead to errors or modifications of the perceived meaning, multimedia information may keep its meaning even after strong modifications of the binary file representing it. One example is lossy compression: The meaning of stored spoken language does not differ whether it is saved as PCM data or in a lossy compression format like mp3. Therefore, integrity protection of multimedia mostly refers to the preservation of the data content and not its binary representation. Because the content is a subjective perceivable quantity, the definition of integrity varies with the intended use of the data. In general, this means to ensure a requested data quality or to allow only certain types of data manipulations.