Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2007, Article ID 19824, 2 pages
doi:10.1155/2007/19824

Editorial

The Interplay between Compression and Security for Image and Video Communication and Adaptation over Networks

Enrico Magli[1] and Qibin Sun[2]

[1] *Dipartimento di Elettronica, Politecnico di Torino, Corso Duca degli Abruzzi 24, Torino 10129, Italy*
[2] *Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613*

Correspondence should be addressed to Enrico Magli, enrico.magli@polito.it

Received 6 December 2007; Accepted 6 December 2007

We are witnessing an unprecedented diffusion of multimedia contents over heterogeneous networks, to desktop and mobile users, with different access bandwidth and quality-of-service requirements and capabilities. Compression is one of the technologies that are making it all possible, by allowing data rate reduction, transcoding, and rate adaptation, which are crucial in the scenario of time-varying communication channels. At the same time, digital rights management is becoming an increasingly important field because of the contents owners' need to protect the data from unauthorized use and verify their origin; hence comes the need to add security features to compressed multimedia contents.

However, the joint provision of compression and security capabilities is not devoid of problems. Although encryption offers a high level of security, it can hinder compression, for example, by altering the statistics of the coefficients to be coded, or the syntax of the compressed file, potentially resulting into a compression loss, or rendering compressed-domain processing difficult or impossible. Other techniques such as data scrambling are more flexible, but also potentially less secure. Recently, there has been a significant amount of research work aimed at finding new ways to integrate data protection techniques into existing and new compression systems, in order to achieve joint compression and security. This integration allows exploiting the hierarchical signal representation in a transform domain, as used by most image and video compression techniques, in order to provide the advanced functionalities required by many modern applications. The forthcoming release of the ISO/IEC JPEG 2000 Part 9 (JPSEC) standard, whose development has witnessed a significant interest from the industry and academia, is an example of how compression and security can coexist and take advantage of each other.

The six selected papers in this special issue provide an up-to-date picture of state-of-the-art research in the field of compression and security, emphasizing the interplay between these two aspects.

The first two papers address the provision of security features within the *JPEG 2000 image compression* framework. Engel et al. in their paper "Format-compliant JPEG2000 encryption in JPSEC: security, applicability, and the impact of compression parameters" consider the new JPSEC standard for secure image communication. They present a packet body encryption scheme that maintains compliance with the syntax, as well as a scheme that encrypts the packet headers in order to improve security. Moreover, they analyze the impact of several parameters on the security and compression performance.

The second paper, by Yang et al., also proposes an encryption algorithm for JPEG 2000. In their manuscript "Efficient and syntax-compliant JPEG 2000 encryption preserving original fine granularity of scalability," the authors describe a new syntax-preserving encryption primitive, and its application to JPEG 2000. The objective is to allow manipulation of the compressed file by, for example, truncating the codestream for transcoding, without compromising security.

The next two papers deal with encryption for *video compression*. In their paper "Digital video encryption algorithms based on correlation-preserving permutations," Socek et al. propose an encryption algorithm that preserves the spatial correlation. In this way, encryption can be performed before compression without disrupting the coding efficiency. This allows to achieve many useful functionalities, such as format-compliance, quality and rate control, and low complexity.

The fourth paper, "Joint encryption and compression with side information of correlated sources," addresses the

problem of security in a distributed video coding framework, where the correlation of adjacent frames is exploited at the decoder, as opposed to the encoder. In their algorithm, Haleem et al. use a structure similar to AES, in which the Slepian-Wolf coder takes the twofold role of compression step and diffusion step for security.

The last two papers are in the field of *secure entropy coding*, and address the design of entropy coders that can achieve both compression and encryption. In their paper "Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream," Xie and Kuo propose a framework that couples randomized entropy coding and bitstream rotation in order to improve the security. They show that their scheme makes known and chosen plaintext attacks extremely difficult.

The last paper by Magli et al., "Joint source, channel coding, and secrecy," deals with the problem where compressed and secured data have to be transmitted over a noisy channel. It is shown that compression, security, and error protection can be implemented into a single tool. They proposed and compare two such schemes, based on arithmetic coding and turbo coding, respectively.

We present this special issue believing that the interplay between compression and encryption is an important research topic, which is highly actual, and will open the way to more research work in the future. We tried our best to embrace the many new research points in this area and combine them into this special issue. Our special thanks go to the reviewers who helped select and shape the papers presented here. We hope these papers will provide a helpful and stimulating reading.

Enrico Magli
Qibin Sun