Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2009, Article ID 710919, 2 pages
doi:10.1155/2009/710919

*Editorial*

# Enhancing Privacy Protection in Multimedia Systems

**Sen-ching Samson Cheung,[1] Deepa Kundur,[2] and Andrew Senior[3]**

[1] *Department of Electrical and Computer Engineering, University of Kentucky, 453 F. Paul Anderson Tower, Lexington, KY 40506, USA*
[2] *Department of Electrical and Computer Engineering, Texas A&M University, 111D Zachry Engineering Center, College Station, TX 77843-3128, USA*
[3] *Google Research, 76 Ninth Avenue, New york, NY 10011, USA*

Correspondence should be addressed to Sen-ching Samson Cheung, cheung@engr.uky.edu

Received 31 December 2009; Accepted 31 December 2009



The right to privacy has long been regarded as one of the basic universal human rights. In the last thirty years, advances in computing technologies have brought dramatic improvements in collecting, storing, and sharing personal information between government agencies and the private sector. The combination of ubiquitous sensors, wireless connectivity, and powerful recognition algorithms makes it easier than ever to monitor every aspect of our daily activities. From the use of sophisticated pattern recognition in surveillance video to the theft of biometric signals and personal multimedia contents, people have become increasingly wary about the privacy of their multimedia data. To mitigate public concern about privacy violation, it is imperative to make privacy protection a priority in current and future multimedia systems.

Even though research on privacy enhancing technologies (PET) began more twenty years ago, most of the existing schemes focus on textual or categorical data and are inadequate to protect multimedia. The particular challenges include but are not limited to the difficulties in extracting semantic information for protection, the ability to apply cryptographic primitives to high data-rate multimedia streams, basic signal processing algorithms for protecting privacy without destroying the perceptual quality of the signal, and privacy models for governing and handling privacy rights in multimedia systems. Within the signal processing and multimedia communities, many obfuscation techniques have been proposed for protecting sensitive information while allowing certain legitimate operations to be performed. These schemes typically lack a rigorous model of privacy, and their protection become questionable when scaled to large datasets. The cryptography community has long developed rigorous privacy models and provably secure procedures for data manipulations. These procedures are primarily developed for fundamental computational models like the Boolean circuits. As a result, they usually lead to a blowup in complexity when applied to realistic multimedia applications.

In the past few years, interdisciplinary collaborations among experts in cryptography, multimedia, pattern recognition, and data mining have produced important theoretical results and practical protocols that began to find their usage in practical applications. These collaborations have the potential of not only providing enhanced level of privacy but also revolutionizing the research frontier in the fundamental studies of multimedia and security. The goal of this special issue on enhancing privacy protection in multimedia systems is to bring to the readers some of the latest developments in this exciting area. Six papers are selected for this special issue, covering topics ranging from encrypted-domain signal processing, privacy data preservation to matching of scrambled images.

The first two papers of this issue focus on the development of signal processing algorithms on data encrypted with a special type of crypto-system-Homomorphic Encryption (HE). HE provides provably secure public-key encryption. At the same time, HE allows many mathematical operations to be performed on the encrypted data. Its popularity among researchers in signal processing and data mining is not accidental, though its high computational complexity still poses

a significant hurdle to overcome. In "Encrypted domain DCT based on homomorphic cryptosystems," Bianchi et al. demonstrate how the 1-dimensional and 2-dimensional Discrete Cosine Transform, among the most commonly used signal processing operations, can be realized in the HE domain. They propose a signal model that allows multiple stages of noninteractive computations in the encrypted domain, and a packing approach to group a number of pixels together in a single encrypted word for faster computation. Detailed bounds on accuracy and packing efficiency are also derived.

In the second paper, "Anonymous biometric access control", Ye et al. use HE to realize an iris-based Anonymous Biometric Access Control (ABAC) system. An ABAC system uses biometrics to confirm the membership of an incomer but is oblivious to which entry the incomer's biometric matches. The authors describe an interactive protocol for iris matching in the encrypted domain. They also propose k-Anonymous Quantization (kAQ) to reduce the search complexity. kAQ partitions the database into groups of maximally diverse iris patterns before narrowing the complicated encrypted domain search to within a single group.

Privacy-aware systems based on HE require all parties involved in the distributed computation to agree upon a specific computational protocol. In many practical situations such as video surveillance and web content distribution, the types of possible computations on the data are practically unbounded and uncontrollable by the owner. Thus, sensitive information within the data must first be redacted before being released to others. An important consideration for many applications is that the redaction process needs to be reversible. For example, the redaction may be carried out at an intermediate processor which does not have the ownership of the data. The heterogeneity in access privileges among receivers may also require selective revealing of redacted objects. In addition, the reversibility of the redaction process can fulfill the liability of faithfully preserving contents such as surveillance videos which might be used in legal proceedings. Three papers in this special issue consider different aspects of this reversibility problem.

In "Compression independent reversible encryption for privacy in video surveillance," Carrillo et al. propose a permutation-based encryption scheme to be applied on selected regions in surveillance videos such as faces of individuals that reveal identity information. The encryption permutes pixel values using a logarithmic signature-based pseudorandom sequence. The proposed encryption is shown to have robust performance—the encrypted regions can still be decrypted after the redacted video is compressed at different quality levels or transcoded between different compression standards. Automatic methods to detect encrypted regions are also proposed.

Instead of spatial-domain encryption, Li et al. tackle the problem of preserving privacy data in the frequency domain in their paper "Recoverable privacy protection for video content distribution." Sensitive regions are first transformed into the Discrete Wavelet Transform (DWT) domain in which the low-frequency contents are kept as the redacted output. The high frequency details are treated as privacy data and preserved as hidden data. They are hidden in various frequency components, depending on whether JPEG (DCT) or JPEG2000 (DWT) is used, and the selection of the components for embedding is based on a secret key.

Both of these papers combine the specific redaction methods with the preservation of the privacy data. Paruchuri et al. in "Video data hiding for managing privacy information in surveillance systems" decouple these problems and propose a high-capacity frequency-domain data hiding scheme to preserve the privacy data regardless of the redaction methods. Their contribution is an optimization strategy to select the appropriate frequency coefficients for data embedding that simultaneously minimize the perceptual distortion and maximize the compression efficiency for a target amount of hidden data. Both reversible and irreversible data hiding schemes are considered.

In the last paper "One-time key based phase scrambling for phase-only correlation between visually protected images," Ito and Kiya proposed a new phase-only image matching scheme on Discrete Fourier Transform (DFT) coefficients whose phases are scrambled for visual privacy protection. Unlike previously proposed schemes, the matching process does not require the secret key for scrambling and theoretical justification is provided for the case when the pseudorandom phases are restricted to two possible values. Visual protection is measured based on error energy between the original and phase-scrambled images, and various attack models are also considered.

## Acknowledgment

We appreciate the contributing authors for their interesting and stimulating work. Our special thanks go to the reviewers who helped selecting and shaping the papers presented here. Besides choosing the highest quality papers for this special issue, our selections of papers are also geared towards striking a balance between inclusion of new research points and providing different viewpoints and designs on topical problems. We hope that this special issue can open the way to newcomers and experts alike into innovative privacy-enhancing designs of multimedia systems.

*Sen-ching Samson Cheung*
*Deepa Kundur*
*Andrew Senior*