Emerging Cryptographic Challenges in Image and Video Processing

William Puech, Zekeriya Erkin, Mauro Barni, Shantanu Rane, Rinald Lagendijk

EMERGING CRYPTOGRAPHIC CHALLENGES IN IMAGE AND VIDEO PROCESSING

W. Puech[1], *Z. Erkin*[2], *M. Barni*[3], *S. Rane*[4], *and R. L. Lagendijk*[2]

[1] LIRMM, UMR 5506, CNRS, University of Montpellier II, France
[2] Information Security and Privacy Lab, Delft University of Technology, The Netherlands
[3] Department of Information Engineering, University of Siena, Italy
[4] Mitsubishi Electric Research Laboratories, Cambridge, MA, USA

ABSTRACT

In an increasing number of image and video processing problems, cryptographic techniques are used to enforce content access control, identity verification and authentication, and privacy protection. The combination of cryptography and signal processing is an exciting emerging field. This introductory paper gives an overview of approaches and challenges that exist in applying cryptographic primitives to important image and video processing problems, including (partial) content encryption, secure face recognition, and secure biometrics. This paper aims to help the community in appreciating the utility and challenges of cryptographic techniques in image and video processing.

1. INTRODUCTION

Technological advances in digital content processing, production and delivery has given rise to a variety of new signal processing applications in which security risks can no longer be handled in a classical fashion. These applications range from multimedia content production and distribution to advanced biometric signal processing for access control, identity verification and authentication. In many of these cases, security and privacy risks may impede the adoption of new image and video processing services.

For this reason, the use of cryptographic techniques in image and video processing applications is becoming increasingly common. The cryptographic techniques used in these applications can be classified along two dimensions. The first dimension indicates whether the attacker model involves an outsider or one of the parties involved in the processing. For instance, in paid-for video services, the content must be protected against outsiders (non paying viewers) with a cryptographic end-to-end access control solution. But at the same time the content must be protected against the paying customer to avoid them from redistributing the content illegally. Similarly, in biometric systems the threat exists that sensitive biometric information (fingerprints, faces) are obtained by outsiders, or that the party storing and processing the biometric templates misuses them for its own purposes.

The second dimension of classification is the kind of and the way whereby cryptographic techniques are applied. In some image and video processing applications, common cryptographic primitives are used as "add-ons", such that the original (non-secured) image and video processing operations are hardly or not at all affected. In other applications the cryptographic primitives are deeply embedded into the processing algorithms (e.g. the processing algorithms may work directly on the encrypted data), and completely new solutions may emerge.

In this introductory paper, we give an overview of recent and ongoing research and challenges in the exciting field of combining image and video processing and cryptography. The paper also serves as the introduction to the special session on this subject at the *International Conference on Image Procession 2012*, entitled "Recent Advances in Cryptography and Image Processing". Even though the image and video processing applications described rely on cryptographic techniques, no particular background in cryptography is assumed. In Section 2, we overview cryptographic techniques, and in particular selective encryption, in image and video communications. Section 3 describes the research towards face recognition algorithms with privacy protection. Section 4 continues this line of thinking in the context of biometric data. In Section 5, we summarize other emerging applications. We end the paper with a discussion on challenges for future work in Section 6. The paper includes a large number of references for further reading.

2. IMAGE AND VIDEO ENCRYPTION

Multimedia data requires either full encryption or selective encryption (SE) depending on the application requirements. SE is a technique aiming to reduce the required computational time and to enable new system functionalities by encrypting only a portion of the compressed bitstream while still achieving adequate security [1]. SE of images and videos has two main advantages; first, it reduces the computational requirements, since only a part of plaintext is encrypted; second, the encrypted bitstream maintains the essential properties of the

original bitstream. The encrypted bitstream will be compliant and fulfills realtime constraints if the following three conditions are fulfilled:

- To keep the bitrate of encrypted bitstream same as the original bitstream, encrypted codewords must have the same size as the original codewords.
- The encrypted codewords must be valid so that they may be decoded by entropy decoder.
- The decoded value of syntax element from encrypted codewords must stay in the valid range for that syntax element. Any syntax element which is used for prediction of neighboring MBs should not be encrypted.

Several SE methods of image and video based on the Advanced Encryption Standard (AES) has been proposed in literature. For example the encryption of color images in the wavelet transform has been addressed in [2]. In [3], SE was performed on color JPEG images by selectively encrypting only the *luma* component using the AES cipher.

In the field of video, SE of H.264 video is proposed by doing frequency domain selective scrambling, DCT block shuffling and rotation [4]. SE of ROI of H.264 has been presented in [5]. It performs SE by pseudo-randomly inverting sign of DCT coefficients in ROI. A scheme for commutative encryption and watermarking of H.264/AVC is presented in [6]. Here SE of some MB header fields is combined with watermarking of magnitude of DCT coefficients but they are not format compliant. SE scheme based on H.264/AVC has been presented on CAVLC and CABAC for I and P frames [7]. This method fulfills real-time constraints by keeping the same bitrate and by generating a completely compliant bitstream. Perceptual encryption has also been presented in [8] where encryption is done with an alternative transform of the DCT coefficients. The robustness of SE videos to attacks which exploit the information from non-encrypted bits together with the availability of side information was studied in [9].

A new challenge in SE of image and video is to decrease the percentage of encrypted bits by keeping the same confidentiality level [10]

3. FACE DETECTION AND RECOGNITION

The image and video data gathered via online photography and video sharing sites, street view, surveillance cameras and institutional databases can easily be used by autonomous systems that use efficient face detection and recognition algorithms to identify and track individuals. This capability raises serious privacy concerns among people. As a result of these concerns, we have witnessed a significant increase in the number of privacy related research in the field of face detection and recognition on image and video data in recent years. In the following, we briefly summarize the state-of-the-art that uses cryptographic techniques to address the privacy issues in the field of face detection and recognition.

Senior and Pankanti [11] provide a description of privacy and give a brief summary on the privacy protection mechanisms for face recognition systems. Lu *et al*. [12] discuss problems and challenges in secure video processing. The solutions based on cryptographic techniques proposed in the literature focus on different techniques like homomorphic encryption (HE), secret sharing and multiparty computation. Avidan and Butman [13] propose a face detection algorithm based on machine learning that is particularly designed for realizing the algorithm efficiently by using secure multiparty computation. Erkin *et al*. [14] propose to encrypt face images using HE and let the Eigenface recognition algorithm work on encrypted data without revealing private information to the holder of the face database as illustrated in Figure 1. Sadeghi *et al*. [15] further improve the efficiency of that approach by replacing the matching mechanism in [14] with a fine-tuned garbled circuit.

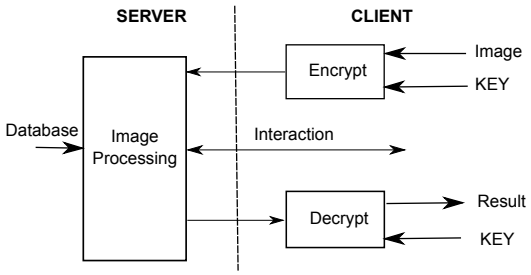

Fig. 1. Protocol actions in the secure face recognition system.

Existing literature on privacy protection in video processing for surveillance also relies on cryptographic primitives. Upmanu *et al*. [16] use secret sharing that requires distributed secure processing and storage. Sohn *et al*. [17] propose watch list screening for video surveillance systems that discriminates groups of identities of interest without revealing face images. For this purpose, the authors use HE to prevent revealing the private information. Osadchy *et al*. [18] propose a new face identification system that is designed for usage in secure computation based on HE and oblivious transfer protocols.

4. MATCHING BIOMETRIC DATA

Encrypted-domain processing also enables privacy-preserving matching of biometrics, which is gaining in importance owing to the hazards of storing human biometrics in the clear. If compromised by an adversary, a biometric can be used to access sensitive information and to illegally impersonate the victim. Unlike traditional security mechanisms like passwords, most biometrics are inherent parts of a person's body, so it is not possible to revoke and replace a compromised biometric an unlimited number of times. A typical application

of privacy preserving matching is when a subject's identity is to be matched against a sensitive database of biometrics owned by a law enforcement agency. In this case, privacy is needed from both sides - the subject's privacy should be preserved if the test fails to find a match against the database, while the biometric database must remain inaccessible to unauthorized parties. Encrypted-domain processing is used to achieve these privacy goals.

While there are many approaches to privacy preserving biometric matching, the recipe usually consists of two stages: (1) Derive discriminable feature vectors from the biometric that achieve desired specifications on the False Reject Rate (FRR), False Accept Rate (FAR), or the Equal Error Rate (EER). (2) Construct a privacy preserving protocol for pairwise matching of the feature vectors, to be executed by the biometric database server and a client possessing the test biometric. It may be desirable to divide the computational and transmission overhead unequally among the two parties, especially when a powerful server containing an encrypted database interacts with a thin client.

Secure matching of biometrics involves privately computing a distance function between pairs of biometric feature vectors. This is accomplished in the encrypted domain using public key homomorphic cryptosystems. Additive homomorphisms such as the Paillier [19] and Damgård-Jurik [20] methods have been overwhelmingly preferred for this task. Barni *et al.* [21] have used the Paillier cryptosystem to determine the Euclidean distance between fingerprint feature vectors. Bringer *et al.* [22] propose matching of binary biometric feature vectors via the Hamming distance metric. Barbosa *et al.* [23] proposed to improve the authentication accuracy using a Support Vector Machine (SVM) classifier within a protocol based on the Paillier cryptosystem. Recently, Blanton and Gasti [24] demonstrated a significant speedup in biometric matching with homomorphic cryptosystems, achieving pairwise Hamming distance computation between 2048-bit encrypted biometrics in less than 150 milliseconds.

5. OTHER EMERGING APPLICATIONS

The use of cryptographic techniques is also emerging in other signal processing domains, often driven by the need to protect the privacy of user-related information. In smart electricity grids, for instance, the energy demand of individual users is monitored by smart meters for the purpose of load balancing in the energy network and real-time energy price negotiations. Unfortunately, it is easy to infer users' behavior from the observed energy demand. Signal processing solutions are emerging that bring cryptographic techniques to smart meters such that load balancing and price negotiations can be performed by the energy distributor, but in such a way that, at the same time, the privacy of the user is protected [25].

A common service provided in social networks is to generate recommendations for finding new friends, groups and events using collaborative filtering techniques. The data required for the collaborative filtering algorithm is collected from sources such as the user's profile, friendships, clicklogs, and other actions. The service providers often also have the right to distribute (processed) data to third parties for completely unrelated commercial or other usage. In [26] a solution is described in which recommendations can be made without the service provider learning the privacy-sensitive information of the user.

Medical data forms another type of privacy sensitive information. In [27] the focus is on the analysis of ECG data by a remote server. The security set-up considers a situation in which the server is asked to elaborate a diagnosis by relying on the ECG profile, without learning anything about the profile and even the output of diagnosis. The solution proposed in [27] achieves such a goal by relying on garbled circuits theory. Interestingly the implementation provided in [27] permits to process a single heart beat in 3-4 seconds of CPU time, almost approaching real time processing of ECG's.

In other situations, protecting the details of the processing algorithm is also important (private function evaluation). This is the case, for instance, when the service provider's rather than the user's data must be protected. In [28], a solution is described that protects the weights of a trained neural network. The rationale for doing that is that these weights may be the result of an (expensive) training process with unique data and hence are valuable information that needs to be protected. Another example of such a situation is described in [29], where a linear decision tree is applied to encrypted data without that the exact shape of the tree is revealed.

6. CONCLUSION AND CHALLENGES

Despite being computationally demanding, cryptographic techniques have facilitated solutions to a variety of security issues in image and video processing. Even though the different applications come with different challenges, it is clear that the signal processing community will have to face three main challenges in future work. First, the utility and limitations of cryptography are not very well known to the community, which hampers the widespread consideration of cryptographic solutions for security problems in image and video processing. Second, cryptographic operations are often computationally expensive. *Efficient* usage of cryptographic protocols is therefore imperative. And third, certain cryptographic techniques cause ciphertext expansion of two orders of magnitude, such as public-key encryption of image pixels. Efficient data packing strategies and operations are then needed.

7. REFERENCES

[1] A. Uhl and A. Pommer, *Image and Video Encryption. From digital Rights Management to Secured Personal Communica-*

tion, Springer-Verlag, 2005.

[2] K. Martin, R. Lukac, and K.N. Plataniotis, "Efficient Encryption of Wavelet-Based Coded Color Images," *Pattern Recognition*, vol. 38, no. 7, pp. 1111–1115, Jul. 2005.

[3] J.-M. Rodrigues, W. Puech, and A.G. Bors, "Selective Encryption of Human Skin in JPEG Images," in *IEEE Int. Conf. on Image Processing, Atlanta, USA*, Oct. 2006, pp. 1981–1984.

[4] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," *IEEE Trans. on Multimedia*, vol. 5, pp. 118–129, 2003.

[5] F. Dufaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 18, no. 8, pp. 1168 –1174, aug. 2008.

[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 17, no. 6, pp. 774–778, June 2007.

[7] Z. Shahid, M. Chaumont, and W. Puech, "Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I and P frames," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 21, no. 5, pp. 565–576, 2011.

[8] S.K. Au Yeung, S. Zhu, and B. Zeng, "Perceptual Video Encryption using multiple 8x8 transforms in H.264 and MPEG-4," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, pp. 2436–2439, May 2011.

[9] A. Said, "Measuring the Strength of Partial Encryption Scheme," in *IEEE Int. Conf. on Image Processing*, 2005, vol. 2, pp. 1126–1129.

[10] L. Dubois, W. Puech, and J. Blanc-Talon, "Smart selective encryption of cavlc for h.264/avc video," in *IEEE Intl. Workshop on Information Forensics and Security - WIFS'11*, 2011.

[11] A. W. Senior and S. Pankanti, "Privacy protection and face recognition," in *Handbook of Face Recognition*, Stan Z. Li and Anil K. Jain, Eds., pp. 671–691. Springer London, 2011.

[12] W. Lu, A. L. Varna, and M. Wu, "Secure video processing: Problems and challenges," in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, 2011, pp. 5856–5859.

[13] S. Avidan and M. Butman, "Efficient methods for privacy preserving face detection," in *Advances in Neural Information Processing Systems*, B. Schölkopf, J. Platt, and T. Hoffman, Eds., pp. 57–64. MIT Press, Cambridge, MA, 2007.

[14] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, R. L. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Privacy Enhancing Technologies Symposium*, Seattle, USA, 2009, pp. 235–253.

[15] A-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *Int. Conf. on Information security and cryptology*, Berlin, Heidelberg, 2010, pp. 229–244, Springer-Verlag.

[16] M. Upmanyu, A.M. Namboodiri, K. Srinathan, and C.V. Jawahar, "Efficient privacy preserving video surveillance," in *Computer Vision, IEEE International Conference on*, 29 2009-oct. 2 2009, pp. 1639 –1646.

[17] H. Sohn, K. N. Plataniotis, and Y. M. Ro, "Privacy-preserving watch list screening in video surveillance system," in *Pacific Rim conference on Advances in multimedia information processing: Part I*, Berlin, Heidelberg, 2010, PCM'10, pp. 622–632, Springer-Verlag.

[18] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "Scifi - a system for secure face identification," in *Security and Privacy, IEEE Symposium on*, may 2010, pp. 239 –254.

[19] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology, EUROCRYPT*. 1999, vol. 1592, pp. 233–238, Springer-Verlag, LNCS.

[20] I. Damgård and M. Jurik, "A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System," in *International Workshop on Practice and Theory in Public Key Cryptosystems*, Cheju Island, Korea, Feb. 2001, pp. 119–136.

[21] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, et al., "Privacy-preserving fingercode authentication," in *ACM workshop on Multimedia and Security*, Rome, Italy, 2010, pp. 231–240.

[22] J. Bringer, H. Chabanne, M. Izabachene, D. Pointcheval, Q. Tang, and S. Zimmer, "An application of the goldwasser-micali cryptosystem to biometric authentication," in *Australasian Conf. on Information Security and Privacy*, Queensland, Australia, 2007, pp. 96–106.

[23] M. Barbosa, T. Brouard, S. Cauchie, and S. de Sousa, "Secure biometric authentication with improved accuracy," in *Australasian Conf. on Information Security and Privacy*, Wollongong, Australia, 2008, pp. 21–36.

[24] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in *European Symposium on Research in Computer Security*, Leuven, Belgium, September 2011.

[25] C. Castelluccia, A. C-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 5, pp. 20:1–20:36, June 2009.

[26] Z. Erkin, M. Beye, T. Veugen, and R.L̃. Lagendijk, "Efficiently computing private recommendations," in *IEEE Int. Conf. on Acoustic, Speech and Signal Processing*, Prag, Czech Republic, May/2011 2011, pp. 5864–5867.

[27] M. Barni, P. Failla, R. Lazzeretti, A-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," *Information Forensics and Security, IEEE Trans. on*, vol. 6, no. 2, pp. 452–468, June 2011.

[28] C. Orlandi, A. Piva, and M. Barni, "Oblivious neural network computing via homomorphic encryption," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–11, 207.

[29] M. Barni, P. Failla, V. Kolesnikov, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Secure evaluation of private linear branching programs with medical applications," in *European Symposium on Research in Computer Security*. 2009, vol. 5789, Springer-Verlag, LNCS.