Encryption-Friendly Multimedia Coding and Communications: Is it Necessary and Possible?

Shujun Li, Universität Konstanz, Germany

Abstract— This letter discusses some key issues and problems about multimedia encryption, leading to a call for research in an interesting new direction of encryption-friendly multimedia coding and communications.

Keywords—Multimedia security; multimedia coding and communications; encryption-friendliness; selective encryption

I. Introduction

Security is a very important issue in multimedia communication applications. One of the most frequently demanded security functions in multimedia communications is multimedia content protection, i.e., encryption of plain multimedia data at the sender side and decryption of the encrypted data at the receiver side. Typical applications of multimedia encryption include secure video streaming and secure multimedia file sharing over open networks like Internet.

Since the 1990s, a lot of research efforts have been devoted to find good solutions to multimedia encryption [1-5]. While a large number of multimedia encryption schemes have been proposed in the literature and some have been used in real products, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes [6].

Some of the problems and weaknesses are related to the essential conflicts between available multimedia encryption techniques and the underlying multimedia coding standards/specifications. As a consequence, it becomes a really challenging task how to design a multimedia encryption algorithm with all the desired features. In most cases, requirements on some features have to be relaxed to make it possible to find a feasible solution to multimedia encryption. It is actually not a surprise since security was not considered as an essential concern at the design stage of any multimedia coding standard/specification. Security-related multimedia standards like JPSEC and MPEG4-IPMPX do exist, but their main goal is to provide a general framework of adding various security tools into the multimedia coding systems, thus enhancing the interoperability of different components and the renewability of broken security tools.

Then, it becomes a question if multimedia coding and communication systems can be made more encryption-friendly. While the necessity of developing such systems has been justified, it is not clear yet if we will finally be able to find a feasible solution. This calls for more research in this interesting new direction.

In the following sections, I first give a brief survey of research on multimedia encryption and then suggest some open research topics about encryption-friendly multimedia coding and communications.

II. Multimedia Encryption: A Brief Survey

There are a number of features we want to get from a multimedia encryption scheme. The most important ones are listed as follows.

- *A reasonable level of security*: the definition of "reasonable" depends on the target applications.
- *Minimized influence on compression efficiency*: in the ideal case, each syntax element should not be influenced and keep its original size after encryption. This feature is called "size preservation".
- *Format compliance [7]*: encrypted multimedia data can still be decoded by any compatible decoder without the knowledge of the decryption key. This feature serves as a basis of many multimedia communication applications such as post-processing of encrypted multimedia data performed between the sender and the receiver. Some special forms of multimedia encryption, such as *perceptual encryption* [8] and *scalable encryption* [9], also require format compliance.
- *Low computational complexity*: this feature is of particular importance in applications where the computational resource is limited and/or fast encryption speed is demanded. Examples include video encryption on mobile phones and real-time video encryption occurring at a busy VoD server.

Note that size preservation is much more useful than it looks like. Since the encryption process does not change the size of any syntax element, only a small buffer will be enough to support encryption, which help makes the encryption suitable for those portable devices with very limited memory. Furthermore, size preservation also implies that the location of each syntax element in the multimedia bitstream will not change, either, so on-the-fly encryption and simultaneous encryption at different positions will be possible. One interesting application of this feature is a wiki-like distributed video editing service, where multiple editors can access an online video simultaneously, edit selected parts of the video and lock these parts temporarily or permanently via encryption.

According to at which point encryption can be added into the normal multimedia encoding process, there are three possible approaches to realize multimedia content protection: encryption after encoding, joint encryption-encoding, and encryption before encoding.

The first approach is the most natural and simplest way to realize multimedia encryption, and is often called naïve encryption in the literature. The main problem of this approach is its incapability to maintain format compliance.

The third approach was mainly used for encrypting uncompressed multimedia data like BMP images. Since encryption generally leads to a random-like output, unfortunately, it will be very difficult (if not impossible) to further compress the encrypted multimedia data. Recently an innovative idea was proposed to realize compression after encryption at the encoder side by making the encryption key as useful side information available at the decoder side [10]. This proposal can achieve compression after encryption at the encoder side, but decompression and decryption at the decoder side are still inseparable. As a consequence, format compliance cannot be easily fulfilled, either.

Now it becomes clear that joint encryption-encoding is the most appropriate approach to multimedia encryption. To ensure format compliance, some syntax elements should be left unencrypted. That is, the idea of *selective encryption* (also called *partial encryption*) [11-13] should be used. Note that selective encryption can help get a better balance between requirements on security and complexity. According to which syntax elements are selected for encryption with what encryption technique(s), the following basic encryption methods have been reported in the literature: secret permutations of various syntax elements, FLC (fixed-length codeword) encryption, VLC (variable-length codeword) index encryption, secure entropy coding, "virtual full encryption" working with arithmetic coding or adaptive entropy coding, header encryption, and so forth. Although most of the basic encryption methods can provide acceptable solutions to some applications, there always exist tradeoffs between different aspects of the overall performance of the joint encryption-encoding systems. Some known tradeoffs are shown in the following list.

- Secret permutations can easily ensure format compliance and size preservation, but it is not secure against plaintext attack when being used alone.
- FLC encryption can absolutely maintain format compliance and size preservation, but it is unable to provide a very high security level.
- VLC index encryption can be configured to ensure format compliance and security, but it always influences the compression efficiency (though slightly in most cases) and cannot maintain size preservation.
- Most secure entropy coders are either insecure against chosen plaintext attack or unable to offer a better performance than naïve encryption (see Sec. IV.B of [19] for an example of the second case). Secure entropy coding is often unable to keep format compliance.
- "Virtual full encryption" and header encryption cannot ensure format compliance sometimes.

It has been found that most of the tradeoffs are related to essential conflicts between the encryption techniques involved and the underlying multimedia coding standards/specifications. In fact, plenty of cryptanalysis work on error concealment attacks [8, 14-17] has clearly shown that selective encryption cannot conceal all perceptual information effectively, because some perceptual information is coded in such a way that it cannot be encrypted effectively as long as format compliance and/or low computational complexity has to be maintained. This justifies the necessity of the quest for encryption-friendly multimedia coding and communication systems.

Another interesting observation about selective encryption is the impossibility to offer 100% security. Assuming we choose to encrypt ALL sign bits of ALL DCT coefficients in an MPEG video, then only 50% sign bits will be flipped in an average sense. A similar phenomenon was demonstrated with a uniform quantizer in [12]. This problem is obviously related to the relatively short sizes of some independently coded syntax elements (such as sign bits) in coded multimedia data.

III. Open Research Topics

According to our discussion given in the last section, I feel the following research topics will be of particular importance for the research on encryption-friendly multimedia coding and communications, and for multimedia encryption as a whole.

A. New objective performance metrics tailored for the specific needs of multimedia encryption like ESS proposed in [18].

A number of metrics are needed to answer at least the following four research questions:

- How to better measure the visual quality degradation of selectively encrypted multimedia data?
- How to better evaluate the performance of error-concealment attack?
- How to define multimedia-friendliness for different multimedia coding and communications systems?
- How to better evaluate the overall performance of a multimedia encryption solution to a specific application?

B. Measurable technical limits of current multimedia encryption techniques.

Based on the objective metrics developed for the last suggested research topic, we can quantitatively study how far different multimedia encryption techniques can go on a given multimedia coding and communication system.

C. Development of a general-purpose benchmarking system for evaluating the overall performance of different multimedia encryption algorithms.

An interface between various multimedia encryption algorithms and multimedia coding/communication platforms should be designed to ease the usability of such a benchmarking system.

D. Possible amendments to existing multimedia coding/communications systems or new paradigms of multimedia coding/communications, for the benefit of enhancing encryption-friendliness.

One possible direction is to further improve the compression-after-encryption scheme proposed in [10].

E. Joint watermarking-encryption and joint fingerprinting-decryption.

By combining watermarking with encryption, we will be able to not only enhance encryption-friendliness of a multimedia coding/communication system, but also its friendliness to other security factors as a whole. In addition, it is also possible to use the embedded side information to enhance the security of the multimedia encryption algorithms.

F. Information retrieval and other signal processing operations performed on encrypted multimedia data.

It certainly makes sense to do information retrieval and signal processing operations on selectively encrypted multimedia data. Furthermore, it is also possible to do the same task on fully encrypted multimedia data, according to some recent research in cryptography. Embedding watermarks in encrypted data might also be yet another way to achieve the same goal.

Reference

[1] A. Uhl, A. Pommer, *Image and Video Encryption: From Digital Rights Management to Secured Personal Communication*. Springer, 2005.

[2] B. Furht, E. Muharemagic, and D. Socek, *Multimedia Encryption and Watermarking*. Springer, 2005.

[3] S. Lian, *Multimedia Content Encryption: Techniques and Applications*. CRC, 2008.

[4] B. Furht, D. Kirovski (Eds.), *Multimedia Security Handbook*. CRC, 2004.

[5] W. Zeng, H. Yu, C.-Y. Lin (Eds.), *Multimedia Security Technologies for Digital Rights Management*. Academic Press, 2006.

[6] S. Li, Z. Li, W. A. Halang, "Multimedia Encryption," in *Encyclopedia of Multimedia Technology and Networking*, 2nd Edition, edited by Margherita Pagani, Volume II, pp. 972-977, IGI Global, 2008.

[7] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, W. Jin, "A format compliant configurable encryption framework for access control of video," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 12, no. 6, pp. 545-557, 2002.

[8] S. Li, G. Chen, A. Cheung, B. Bhargava, K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 17, no. 2, pp. 214-223, 2007.

[9] Bin B. Zhu, Chun Yuan, Yidong Wang, Shipeng Li, "Scalable Protection for MPEG-4 Fine Granularity Scalability," *IEEE Trans. Multimedia*, vol. 7, no. 2, pp. 222-233, 2005.

[10] Mark Johnson, Prakash Ishwar, Vinod Prabhakaran, Daniel Schonberg, Kannan Ramchandran, "On Compressing Encrypted Data," *IEEE Trans. Signal Processing*, vol. 52, no. 10, pp. 2992-3006, 2004.

[11] X. Liu, A. M. Eskicioglu, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions," in *Proc. IASTED CIIT'2003*, 2003.

[12] T. Lookabaugh, D. C. Sicker, Selective Encryption for Consumer Applications, *IEEE Communications Magazine*, vol. 42, no. 5, pp. 124-129, 2004.

[13] T. Lookabaugh, D. C. Sicker, D. M. Keaton, W. Y. Guo, I. Vedula, "Security Analysis of Selectively Encrypted MPEG-2 Streams," in *Multimedia Systems and Applications VI,* Proc. SPIE, vol. 5241, pp. 10-21, 2003.

[14] C.-P. Wu, C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Trans. Multimedia*, vol. 7, no. 5, pp. 828-839, 2005.

[15] A. Said, "Measuring the strength of partial encryption schemes," in *Proc. ICIP 2005*, vol. 2, pp. II-1126-9, 2005.

[16] T. Uehara, R. Safavi-Naini, P. Ogunbona, "Recovering DC coefficients in block-based DCT," *IEEE Trans. Image Processing*, vol. 15, no. 11, pp.3592-3596, 2006.

[17] Dominik Engel, Thomas Stütz, and Andreas Uhl, "Format-Compliant JPEG2000 Encryption in JPSEC: Security, Applicability, and the Impact of Compression Parameters," *EURASIP J. Information Security*, vol. 2007, Article ID 94565, 2007.

[18] Y. Mao, M. Wu, "Security evaluation for communication-friendly encryption of multimedia," in *Proc. ICIP 2004*, vol. 1, 569- 572, 2004.

[19] Goce Jakimoski, K. P. Subbalakshmi, "Cryptanalysis of Some Multimedia Encryption Schemes," IEEE Trans. Multimedia, vol. 10, no. 3, pp. 330-338, 2008

Shujun Li received his B.S. degree in Information Science and Engineering, and his Ph.D. degree in Information and Communication Engineering, both from the Xi'an Jiaotong University, China, in 1997 and 2003, respectively. After getting his Ph.D. degree, he was doing postdoctoral research in the City University of Hong Kong and in The Hong Kong Polytechnic University from September 2003 to January 2007. From January 2007 to June 2008, he was a Humboldt Research Fellow with the FernUniversität in Hagen, Germany. Currently, he is a Zukunftskolleg Fellow with the Universität Konstanz, Germany. His current research interests include multimedia security, chaotic cryptography and human iterative proofs.