The impact of encryption on compression efficiency of still images

Aparna Gurijala, Syed A. Khayam
Department of Electrical & Computer Engineering, Michigan State University

Summary: This article is concerned with the tradeoff between image compression and security. Contemporary image coding schemes provide image compression by exploiting the spatial and psycho-visual redundancies. Encryption of an uncompressed image removes intelligibility from the original image thereby incurring compression penalties. This results in a trade-off between the competing requirements of encryption and compression.

The global information sharing offered by omnipresent computer networks has caused a multitude of security threats. In particular, secure local-storage and network-transmission of images have emerged as focal research areas. A variety of encryption algorithms can be employed to remove intelligibility from an uncompressed archived image. This “local” encryption is generally performed to preserve data security without any presumption about compression at a later time. However, post-encryption transmission of such locally-stored images stipulates compression in order to improve bandwidth utilization.

This article is concerned with the tradeoff between image compression and security. Contemporary image coding schemes provide image compression by exploiting the spatial and psycho-visual redundancies. Encryption of an uncompressed image removes intelligibility from the original image thereby incurring compression penalties. This results in a trade-off between the competing requirements of encryption and compression.

The performance of image compression standards for encrypted images is largely unexplored. The only work is by Johnson et al. [1] which shows theoretically that through the use of coding with side information principles, the compression of encrypted data can be accomplished without loss of coding efficiency or perfect secrecy in certain scenarios. For example, it is shown that if the original source is Gaussian, the same efficiency can be achieved for lossy compression of an encrypted source, as when encryption is effected after compression. In [1] the decompression and decryption operations are performed jointly at the receiver. On the contrary, most commercial image compression standards perform compression/decompression without any assumption about encryption/decryption at later stages. In this article we evaluate an existing compression standard without making any modifications to it.

To explore the encryption-compression trade-off, we employ JPEG 2000 [2] as an example compression and decryption operations are performed jointly at the receiver. On the contrary, most commercial image compression standards perform compression/decompression without any assumption about encryption/decryption at later stages. In this article we evaluate an existing compression standard without making any modifications to it.

Figure 1: (a) Original and (b) pre/post-filtered (encrypted) images.
Figure 2: PSNR of original and pre/post-filtered images.

Figure 3: Images with partial phase encryption; only (a) 25% and (b) 75% of the phase spectrum of Fig. 1(a) is encrypted.

Figure 4: PSNR of images with different levels of partial encryption.

For security, we use the pre/post-filter based encryption scheme proposed by Kuo et al. [3] as an example. Pre/post-filtering effects encryption by scrambling the phase spectrum of an image. An example of an image encrypted using pre/post-filtering is shown in Fig. 1.

Most image compression encoders, including JPEG 2000, rely on the perceptual details for compression, e.g., frequency weighting, color weighting, visual progressive weighting etc. The pre-filtering process on the other hand removes perceptual details from an image. The encrypted images consequently yield compression inefficiencies. For JPEG 2000, this compression inefficiency is illustrated in Fig. 2, which shows that for the compression rate, an unencrypted image always renders higher peak signal-to-noise ratio (PSNR) than its encrypted counterpart.

We now evaluate a partial phase encryption scheme in a bid to improve compression efficiency. In partial phase encryption, only a fraction of the phase spectrum is subjected to encryption. Fig. 3 illustrates that the pre/post-filter approach renders effective encryption even when a very small fraction (e.g., 25% encryption in Fig. 3 (a)) of the total phase is subjected to encryption. While partial encryption does not considerably reduce complexity in the present FFT-based phase encryption scheme, in other encryption schemes (such as DES, AES etc.) complexity of encryption is generally a linear function of the data length. In such encryption schemes, partial encryption, typically effected in the frequency domain, renders an added advantage of complexity reduction.

The important question here is: Does a partially encrypted image improve the compression efficiency as compared to a fully encrypted image? To address this question, Fig. 4 outlines the compression efficiencies (in terms of PSNR) of images with varying levels of partial encryption. It can be observed that the performance for all encryption levels at low compression rates (0.5 to 4.5 bpp) is satisfactory. Irrespective of the encryption level, the compression performance deteriorates rapidly (with respect to the “no encryption” case) for compression rates greater than 4.5 bpp.
We therefore conclude the following: (i) At low compression rates, encryption can be employed without significant compromise in compression efficiency. Such low bit-rate compression has applications in bandwidth-constrained wireless environments. (ii) Decreasing the level of encryption (using, for example, partial encryption) does not yield much improvement in compression efficiency. Hence, if complexity permits, full encryption should be employed to maximize security of the transmitted images. (iii) In complexity-constrained environments, partial encryption can provide reasonable security.

Aparna Gurijala
Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI, USA
+1-517-290-0643
E-mail: gurijala@egr.msu.edu
www.egr.msu.edu/~gurijala
www.egr.msu.edu/~deller/speechlab_complete_page.html

Aparna Gurijala is a student member of SPIE. She received her M.S. degree in Electrical Engineering from Michigan State University (MSU) in 2001. She will be completing her doctoral studies at MSU in Spring 2006. She has served as a research assistant on the National Gallery of Spoken Word (NGSW) project from 2000 to 2004 and has been involved in the development of speech watermarking algorithms. Her research interests lie in the areas of multimedia security and adaptive signal processing.

Syed Khayam
Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI, 48823, +1-517-290-7299
E-mail: khayamsy@egr.msu.edu
www.syedali.net
www.egr.msu.edu/waves

Syed Ali Khayam received his M.S. in Electrical Engineering from Michigan State University (MSU) in 2003. He is currently a Ph.D. candidate in the Department of Electrical and Computer Engineering at MSU. He has secured the Pakistan Higher Education Commission M.S. and Ph.D. scholarships to pursue post graduate studies at MSU. His research interests include statistical modeling of computer networks, network/multimedia security, cross-layer protocol design and multimedia communications.


Acknowledgements

The authors would like to thank Profs. Hayder Radha and John R. Deller, Jr. for their guidance and very helpful remarks on the initial draft of this paper. The authors would also like to acknowledge the generous financial support extended by the MSU CyberSecurity Initiative to this project.

References