Review of the book *"Multimedia Content Encryption"*
by Shiguo Lian
CRC Press, Taylor & Francis Group, 2009
ISBN: 1-4200-6527-0, 978-1-4200-6527-5

Jannik Pewny

1 What the book is about

As the title says, the book is about multimedia content encryption. One might think that the combination of AES and a multimedia-file is not that complicated that it is necessary to write a whole book about it. But it is quite interesting to see that the uses of multimedia-content require a different way of using cryptography.

For example, if you want to give a viewer streaming access to a video, you just cannot encrypt the whole file, because you need things like frame-positions to allow fast forward and such.
Since you also want to save computation time, it might be worth to think about encrypting only the most important part of the content, if you do not want unauthorised users to read the content. While you are at it—is it maybe possible to encrypt only format-data, or can an attacker maybe guess these or extract them from the unecrypted content part, making your sceme insecure?
But maybe you just want the opposite—you want to encrypt the "*What makes a HD-Video HD*"-part of a video to allow unauthorized users a low-quality preview and force them to pay if they want the HD-variant.
Or maybe you want to encrypt the video, to make it immune against unauthorised manipulation attempts, but you want to cut and rescale it, without decrypting it. What kind of cipher allows that?

Of course, the resulting sceme would have to be fast, so fast, that you can use it for real-time applications, like video-conferencing.
And video data is big, so that it has to be compressed. And encrypted. But that is slow. Can we do both in one step to save some extra time?

To sum it up, multimedia-content-encrypters do not need really strong ciphers, since they want them weak enough to allow certain actions. And of course they are willing to make a tradeoff between speed and security, cost and security, and "unintelligible for humans" and security.

This book gives you an introduction about these things. The options you have, the tradeoffs you can make or better should not make.

The author starts with an *Introduction* into the work of multimedia content encryption. When it started, where it comes from and what this book has to do with it. It is followed by a chapter about the *Performance requirements* of this special kind of application of cryptography and the *Fundamental techniques* cryptography has to offer for this use.

The next chapters are about the different types of encryption one might want to do in this context:

- *Complete encryption* (encrypting the whole data)
- *Partial encryption* (encrypting only parts of the data)
- *Compression-combined encryption* (encrypting and compressing at the same time)
- *Perceptual encryption* (encrypting in such a way, that it reduces the quality of the content up to a certain adjustable degree)

- *Scalable encryption* (protection againt unauthorised manipulation, but allowing bitrate-conversion and cutting without decryption/decompression)

Commutative watermarking and encryption (making sure that nobody can steal your multimedia-content without you beeing able to prove it) and *Joint fingerpring and decryption* (allowing you to trace somebody who illegally distributed some content you gave him) form the next two chapters.

The author also included some *Typical attacks on multimedia encryption* as well as some *Principles for secure multimedia encryption*, each in an own chapter.

You can also find a list of *Typical applications*, summing up the requirements and possible cryptographic solutions for the particular application and some *Open issues* in this field.

2 What the book is like

In general, the author has a very pleasant style of writing. Compact, but not overshortened, easy to read, but talking about quite complex content.

Each chapter begins with a short introduction of what the chapter is going to be about, so that the reader is up to date with terminology and aims of a certain technique/topic. It follows a highly categorised list of sub-chapters und sub-sub-chapters, leading to a round overview of the whole topic. In the end, there is a pretty short summary, summing up the most important facts of the chapter, to make sure that those did not get lost.

If the author gives formulas or mathematic statements, he usually presents them stepwise, like peak signal-to-noise ratio is defined as

$$PSNR = 10 \log_{10} \left(\frac{L^2}{MSE} \right)$$

where MSE *(mean square error)* satifies

$$MSE = \frac{1}{n} \sum_{i=0}^{n-1} (c_i - p_i)^2.$$

This may seem over simplified when taking examples like the one above into account, but it assures that the reader can understand formulas in their details and buildup.

One also has to mention the very detailed references the author gives at the end of each chapter. They are indexed in the chapters themselves. This terminally anchors the book into scientific literature.

The book is full of nice pictures, graphs and tables, which do really help to present the matter. They are well selected and do underline statements like "Generally, the encrypted image is unintelligible when n is no smaller than 7.".

Apart from that, the author made some awkward categorisations of speed, security, change in compression level and such, judging ciphers for later reference. To me, this meant basically that I had to keep a bookmark in the part of the book where the categorisations where introduced, since e.g. CL0 (meaning "no effect on compression") and FL1 (meaning "Keeping synchronization") are not that self-explanatory.

The chapter named "Some Principles for Secure Multimedia Encryption" is very practical. It gives some examples of do's and dont's and present a "lessons learned". Not only that it is interesting to read and easy to follow, it is also pretty useful. I would recommend you to read the rest of the book, before you try this chapter, since it refers to the previous chapters quite often.

3 Recommendation

This book gives you a good introduction into the different requirements you get to meet, when you are confronted with multimedia content encryption.

Despite that, I can not recommend it to pure cryptographers, since the only interesting statement of this book which is of really cryptographic interest is about the use of partial encryption and its security. I can also not recommend it to pure non-cryptographers (like managers in the multimedia sector or progammers without particular background in cryptography), since they may not understand the uses and implications of primitives like encryption, digital signatures or only the real groundbreaking difference between private-key and public-key cryptography. Not that they cannot learn things like modes of operation of block ciphers or similar things from this book, but there are other books for such general introductions, and I doubt that you can benefit from everything this book has to give, without such knowledge.

On the other hand, this book will fit your needs if you already know something about cryptography and only want to gain casual knowledge about multimedia content encryption or are a future implementer of such systems and want to get an overview of what is done in this field. In the last case, this book will be a great starting point for further study, especially since it gives a lot of references.

Considering the above stated matching readers, the usefulness of this book compared to its price seems somewhat questionable.

The reviewer is a student of IT-Security at the Ruhr-University of Bochum (Horst Görtz Institute)