Secure Arithmetic Coding

Recent generation standards including JPEG2000 and H.264 utilize arithmetic coding, which has led to increased interest in arithmetic coding in the context of image/ video coding

While arithmetic coding (AR) is extremely efficient; however, it was found that as traditionally implemented AR is not particularly secure.

Ref. J.Cleary, et al., “On the insecurity of arithmetic coding,” Comput. Security, Vol. 14, No. 2, pp. 167-180, 1995.

- The Issue of providing both compression and security simultaneously is growing more important given the increasing ubiquity of compressed media files in a host of applications including the Internet, digital cameras, and portable music players, and the common desire to provide security in association with these files.

- When both compression and security are sought, one approach is to simply use a traditional arithmetic coder in combination with a well-known encryption method such as the Advanced Encryption Standard (AES). However, while this will certainly meet both goals, it fails to take advantage of the additional design flexibility and potential computational simplifications that are available if the coding and encryption are performed jointly.

Good References

1. M. Granngetto, et al., “Multimedia Selective Encryption by Means of Randomized Arithmetic Coding,” IEEE T-MM, pp. 905-917, Oct. 2006.
2. H, Kim, et al., “Secure Arithmetic Coding,” IEEE T-SG, pp. 2263-2272, May 2007.
3. M. Sinaie, et al., “Secure Arithmetic Coding with Error Detection Capability,” EURASIP Journal on Information Security, Vol. 2010.

4. Hengjian Li, et al., “A secure and efficient entropy coding based on arithmetic coding,” vol. 14, pp. 4304-4318, 2009.

5. Lili Duan, et al., “A secure arithmetic coding based on Markov model,” Commu Nonlinear Sci Numer Simulat, Vol. 16, pp. 2554-2562, 2011.

- You are encouraged to take this new research topic as one of your final project subjects.

- Both theoretic study and/or real implementation are of great interest.
- This topic is of interest also for Big Data related researches.

Some interesting topics about arithmetic codes

- Code Compression Using Variable-to-Fixed Coding Based on Arithmetic Coding, DCC'03

- Embedded computing systems are space and cost sensitive; memory is one of the most restricted resources, posing serious constraints on program size, Code Compression, which is a special case of data compression where the input source is machine instructions, has been proposed as a solution to this problem.

A Novel Compression and Encryption Scheme Using Variable Model Arithmetic Coding and Coupled Chaotic System

- IEEE T-Circuits and Systems, Aprl 2006

- The focus of this work is to incorporate recent results of Chaos theory, proven to be crypto-graphically secure, into Arithmetic Coding, to devise a convenient method to make the structure of the model unpredictable and variable in nature, and yet to retain, as far as is possible, statistical harmony, so that compression is possible.

Analytical Tools for Optimizing the Error Correction Performance of Arithmetic Codes

- IEEE T-Communications, Sept. 2008

- In Join Source-Channel Arithmetic Coding (JSCAC) schemes, additional redundancy may be introduced into an Arithmetic Source Code in order to be more robust against transmission error.

Distributed Arithmetic Coding for the Slepian-Wolf Problem

- IEEE T-Signal Processing, June 2009

- Distributed source coding schemes are typically based on the use of Channel codes as Source codes. In this paper a new paradigm, named distributed arithmetic coding, which extends AC to the distributed case employing sequential decoding aided by the side information.

Segmentation of Source Symbols for Adaptive Arithmetic Coding

- IEEE T-Broadcasting, June 2012

- Adaptive AC is a general technique for coding source symbols of stochastic process based on an adaptive model, which provides measures of the statistics of source symbols and is updated, along with encoding/decoding processes, when more encoded/decoded symbols are fed as samples to the adaptive model.

- This paper presents segmentation of source symbols to improve the performance of the adaptive arithmetic coder.

- A Highly Efficient Multiplication-Free Binary Arithmetic Coder and Its Application in Video Coding , by Detlev Marpe and Thomas Wiegand