## Foreword

"Information Hiding" sounds a bit like a bad practice among people who are not always trusted by others. If you are asked by a friend "Are you hiding something from me?" you would instantly deny it, saying "No! No! I have nothing to hide. I'm a very honest man and trusted by all." However, that isn't really true, because you have a lot of information which you don't like to have known, even by your loved ones.

Yes, everyone has several types of confidential information. Therefore, everyone wants to have some good means to hide it securely. Information hiding technology in general came from such a natural desire.

The information age directed people's eyes toward new digital technologies called "watermarking" and "steganography." These two are different in usage, but belong to the same category of information technology, namely, information hiding. They are not evil tricks, but are beneficial solutions for your digital life today.

"Multimedia information hiding" indicates that you are making use of some multimedia data, such as photos, music, videos, and text, to hide your secret data. In most cases, you are replacing parts of a multimedia data file with your confidential data in an imperceptible manner. Such an operation is referred to as "data embedding." If needed, you can easily extract the embedded data by using a special program with a relevant key. Such an operation is termed "data extracting."

This book is neither an easy read on information hiding, nor a collection of survey papers. Instead, it is intended to provide a wide range of hot topics in Multimedia Information Hiding.

The contents of each chapter are summarized in the Preface by the editor, and the respective chapters are written by different authors. All are original writings. Some authors are intending to give a general introduction to the chapter topic, but others are either proposing a new technical scheme for solving difficult problems on the topic, or reporting their new research framework with remarkable outcomes. This book is good for graduate-level students and also very instructive for senior IT engineers now working in industry.

As you read through the chapters, you will often encounter such terms as "hiding," "watermarking," "steganography," "original data," "stego data," "cover," "payload," "robustness," "degradation," and so on. They are all important concepts in information hiding, but they are rather application-oriented terminologies. For example, the idea of "robustness" is necessary for watermarking applications, while "payload" comes in with some steganographic applications. "Degradation" is a concept that should be kept very small in score in order for the embedding operation to not be noticed by third parties.

I myself think "multimedia information hiding" can be rephrased as "multi-layered information data-structure for multimedia contents," because there are some applications where you don't need to hide anything. A typical number of layers in such a structure is just two, consisting of the internal and the external layers.

Let us take an example in a "Content Delivery System over the Internet," where you want to transmit one of your copyrighted photo works only to a designated recipient without it being intercepted when it travels through the transmission line. This type of system can be implemented by using a large-capacity oriented embedding algorithm. An experimental program of such algorithm is already available on the Internet.

The content delivery system here is like the following:

- A. You use some "cover" to carry the copyrighted photo.
- B. You need to make the cover "translucent" in order for anyone to see what is inside by just looking from the outside.
- C. The photo work has no value as long as it stays in the cover.
- D. Opening the cover is only possible by using a special extracting program and a key. The key is handed from you to the recipient in a very safe way.
- E. More specifically, an example photo work is an "artistic portrait file" of a lady, and the cover is its degraded image file, which was created by a noise-adding operation. The noise-added image looks like it is contained in some translucent material. The file format of both images may be BMP.

According to the information hiding terminology, the portrait embedded cover image, originally the degraded portrait, is a "stego image." While, in my rephrased expression, it is a "double layered portrait image" where the original data is in the internal layer and the degraded data is on the external layer. The most important point in this structure is that the external layer is "translucent," in other words, the internal layer is not hidden. I have never heard of any "translucent stego image" in the traditional multimedia information-hiding framework. I feel my terminology is a little better in this type of application.

I suggest all the readers of this book pay attention to realize which data, cover, or payload is more important than the other when they are reading through the chapters. In my wording, you should know which layer is more focused than the other in each topic.

Eiji Kawaguchi Kyushu Institute of Technology, Japan Summer 2012

**Eiji Kawaguchi** received the Dr. Eng. Degree from the Department of Electronics Engineering, Kyushu University, Japan, in 1971. He worked for Kyushu Sangyo University, Kyushu University, Kyushu Institute of Technology, and Keio University from 1969 through 2006. Currently, he is a Professor Emeritus at Kyushu Institute of Technology. His research interests include speech recognition, pattern recognition, image processing, information hiding, content access control, and natural language semantics. He is a co-inventor of BPCS-Steganogrpahy.