Jonathan Blackledge

Cryptography and Steganography:

New Algorithms and Applications

Prof. Dr. Jonathan Blackledge

Stokes Professor
Science Foundation Ireland

Honorary Professor
Dublin Institute of Technology, Ireland

Distinguished Professor
Center for Advanced Studies
Warsaw University of Technology, Poland

Professor Extraordinaire
Department of Computer Science
University of the Western Cape, South Africa

Technical Director
Lexicon Data Limited, England

http://eleceng.dit.ie/blackledge
http://jmblackledge.web.officelive.com
jonathan.blackledge@dit.ie
jmblackledge@hotmail.co.uk

Editor: **Stanisław Janeczko**

Technical editors: **Małgorzata Zielińska, Anna Żubrowska**

General layout and cover design: **Emilia Bojańczyk / Podpunkt**

For additional information on this series, visit the CAS Publications Website on http://www.csz.pw.edu.pl/index.php/en/publications

ISBN 978-83-61993-05-6
Printed in Poland

Contents

Preface

Developing methods for ensuring the secure exchange of information is one of the oldest occupations in history. With the revolution in Information Technology, the need for securing information and the variety of methods that have been developed to do it has expanded rapidly. Much of the technology that forms the basis for many of the techniques used today was originally conceived for the use in military communications and has since found a place in a wide range of industrial and commercial sectors. This has led to the development of certain industry standards that are compounded in specific data processing algorithms together with the protocols and procedures that are adopted in order to implement them. These standards are of course continually scrutinized for their effectiveness and undergo improvements and/or changes as required. Further, different standards have, for a variety of historical reasons, been developed for particular market sectors. For example, DES (Data Encryption Standard) was originally developed in the early 1970s and in 1976 was selected by the Federal Information Processing Standard for the use in the USA. Since that time, DES has had widespread use internationally and was upgraded to triple DES or DES3 in the 1990s (essentially, but not literally, a triple encryption version of DES in order to compensate for the relatively low key length associated with the original DES).

Information security manifests itself in a variety of ways according to the situation and requirement. However, in general, it deals with such issues relating to confidentiality, data integrity, access control, identification, authentication and authorization. There are a number of practical applications that critically depend on information security measures which include private messaging (encrypting email attachments, for example), financial transactions and a host of online services. All such applications relating to information security require the study of specific mathematical techniques and the design of computational methods which are compounded in the study of cryptography. This includes, not only the design of new approaches, but continual analysis with regard to validating the strengths and weaknesses of a cryptographic algorithm and the way in which it is implemented in practice.

Cryptology is the study of systems that typically originate from a consideration of the ideal circumstances under which secure information exchange is to take place. It involves the study of cryptographic systems, but also the possible processes that might be introduced for breaking the output of such systems—cryptanalysis. This includes the introduction of formal mathematical methods for the design of a cryptosystem and for estimating its theoretical level of security. However, in reality, a cryptosystem often forms just a part of a complex infrastructure involving users that are prone to levels of both stupidity and brilliance that can not be formally classified. Hence the mathematical strength of a cryptographic algorithm is a necessary but not a sufficient requirement for a system to be acceptably secure. In the ideal case, the cryptographic strength of an algorithm and/or implementation method can be checked by means of proving its resistance to various kinds of known attacks. However, in practice, this does not mean that the algorithm and/or its specific application is secure because other unknown attacks may exist. For this reason, the security of a cryptosystem is often based on knowledge of its working legacy and the confidence level that a community has acquired from its continual use over many years, often due to various up-grades, additions and modifications as have been considered necessary. Thus, modern systems for securing information exchange are often based to a large degree on past legacies associated with the performance of relatively well established techniques.

There is a large range of many excellent books, scientific and engineering journals, conferences and a wealth of general information now available with regard to information security. Different commercial products and software packages are available from a diverse range of companies and in such a competitive environment, it is often difficult to evaluate the merits of one system over another. However, the large majority of these systems and methods have a common origin or at least a common theme. This book has been written to introduce the reader to a new theme in information security, namely, the role of chaos in cryptography. Chapter 1 provides an overview of encryption with a focus on the use of Chaos for this purpose. Chapter 2 provides an overview of some basic digital signal processing algorithms which are 'link' between data encryption and its application in communications systems. This chapter also provides details of some algorithms that are used later on in this work. Chapter 3 provides an overview of data encryption algorithms and standards and includes information on example encryption systems and industries. Finally, Chapter 4 provides a detailed discussion on encryption using deterministic chaos, focusing on the design of algorithms that yield high entropy ciphers and utilize many different Iteration Function Systems.

Irrespective of the method of encryption that is adopted, all encrypted information raises a 'flag' to the possible importance of the information that it

conveys. For this reason, it is of significant value if encrypted information can be hidden in some way in other data types in order to disguise the fact that it exists. This is known as *Steganography* and the latter half of this book focuses on the mathematical models, algorithms and applications associated with a range of different approaches to hiding information in digital signals and images. After providing an introduction to the principles of Information Hiding and Digital Watermarking given in Chapter 5, the material considers methods for watermarking digital signals based on Chirp Coding and Fractal Modulation as described in Chapter 6.

An overview of digital image watermarking is given in Chapter 7 and in Chapter 8, methods of information hiding and Steganography are addressed in which the image is encrypted by diffusion with a noise field to produce a ciphertext - an encrypted watermark. A cover image (covertext) is then introduced into which the ciphertext is embedded. The watermark image is recovered by removing the covertext and then correlating the output with the original (key dependent) noise source. This approach provides the user with a method of hiding ciphertexts (the scrambled image) in a host image before transmission of the data. In this sense, it provides a steganographic approach to cryptology in which the ciphertext is not apparent during an intercept. Decryption is based on knowledge of the key and access to the host image. In terms of watermarking a digital image, the method provides a way of embedding information in a host image which can be used to authenticate that it has come from a identifiable source, a method that is relatively insensitive to lossy compression, making it well suited to digital image transmission. The methods considered represent a generic solution for undertaking covert cryptology.

With regard to hard copy document authentication, the use of diffusion and confusion using a covertext is not robust. The reason for this is that the registration of pixels associated with a covertext can not be assured when the composite image is printed and scanned. We therefore consider a diffusion only approach to document authentication which is robust to a wide variety of attacks, including geometric attacks, drawing, crumpling, and print/scan attacks. This is because the process of diffusion (i.e. the convolution of information) is compatible with the physical principles of an imaging system and the theory of image formation and thus, with image capture devices (digital cameras and scanners, for example) that, by default, conform to the 'physics' of optical image formation. The diffusion of plaintext (in this case, an image) with a noise field (the cipher) has a synergy with the encryption of plaintext using a cipher and an XOR operation (when both the plaintext and cipher are represented by binary streams). However, decryption of a convolved image (deconvolution) is not as simple as XORing the ciphertext with the appropriate cipher. Here, we consider an approach which is based on pre-conditioning the original cipher in such a way that decryption (de-

diffusion) can be undertaken by correlating the ciphertext with the cipher. If a maximum entropy cipher is used that is uniformly distributed, then the Power Spectral Desnity Function (PSDF) of the output is determined by the PSDF of the plaintext (image). If the image is based on naturally occurring objects which are roughly of a self-affine type, then the PSDF may tend to scale according to a random fractal power law. In other words, the diffusion of self-affine images with white noise will generate output images that are, in effect, random fractal images with fractal-type textures. In this sense, the use of white noise diffusion for document authentication is based on using texture maps which are either fully or partially statistically self-affine. Either way, the outputs considered for document authentication are based on printing textures of a type that are determined by the spectral characteristics of the plaintext which can be applied by using low resolution Commercial-Off-The-Shelf (COTS) printers and scanners. This is the subject of Chapter 9.

The material presented in this book is primarily based on two sources: (i) a series of lecture notes and supplementary teaching and learning materials developed by the author for delivery at post-graduate level and continuous professional development programmes; (ii) research undertaken by the author and associate research students. Much of this research has focused on aspects of information security that has had direct commercial potential and, in most cases, has been sponsored by industry, including companies co-founded established by the author. Thus, although this text concentrates on a range of academic issues concerning the application of chaos to cryptology, for example, it also attempts to illustrate how this application has generated commercially realizable products that are relatively new to the market. This includes the systems such as Crypstic™ and StegoCrypt™ which are registered as 'Technologies to License' at Dublin Institute of Technology - http://www.dit.ie/hothouse/

It is hoped that the information within this work is sufficiently complete and descriptive for both the theoretician who wishes to understand the issues involved, and the practitioner who wishes to apply the techniques. There are certain inevitable limitations, however, imposed on the reader by the conventional static design of textbooks. However, as more and more material is being made available on the Internet it has been possible to collate a series of current links to other relevant resources and applications. This allows potentially easy access to other individuals who are using similar techniques. For this reason, many of the references provided consist of an appropriate conventional citation, a url or both.