

**ON THE SECURITY OF SOME
MULTIMEDIA ENCRYPTION
SCHEMES**

LI CHENG QING

DOCTOR OF PHILOSOPHY

CITY UNIVERSITY OF HONG KONG

SEPTEMBER 2008

CITY UNIVERSITY OF HONG KONG

香港城市大學

**On the Security of Some Multimedia
Encryption Schemes**

一些多媒體加密算法的安全性分析

**Submitted to
Department of Electronic Engineering
电子工程學系
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
哲學博士學位**

by

**Li Cheng Qing
李澄清**

**September 2008
二零零八年九月**

Abstract

The security of multimedia data becomes more and more important due to the rapid development of the modern computer, networking and information technologies. Notably, the traditional text encryption schemes fail to protect the multimedia data efficiently because of the special properties of multimedia data. To overcome this difficulty, researchers tried to develop special encryption schemes for multimedia data adopting some related nonlinear theories. However, some new schemes have been found to be insecure from the viewpoint of cryptography, and some general recommendations have been drawn to facilitate the design of more secure multimedia encryption schemes.

This thesis is concerned with the security analysis of some multimedia encryption schemes. The security of the schemes against some common attack methods, such as brute-force attack, known/chosen-plaintext attack and differential attack, is investigated in detail with theoretical analyses and experimental verifications. In addition, some special design defects of the schemes are revealed and discussed. The main contributions of the thesis are summarized as follows:

1. The security problems of a symmetric key block cipher using multiple one-dimensional chaotic maps are cryptanalyzed in detail. Some new findings are: 1) a number of weak keys exists; 2) some important intermediate data of the cipher are not sufficiently random; 3) the whole secret key can be broken by a known-plaintext attack with only 120 consecutive known plain-bytes in one known plaintext; 4) an improved version of the chaotic cipher still suffers from all the same security defects.
2. Recently two encryption schemes were proposed by combining circular bit shift and XOR operations, under the control of a pseudorandom bit sequence (PRBS) generated from a chaotic system. These two schemes are cryptanalyzed together, leading to the following findings: 1) there exist some security defects in both schemes; 2) the underlying chaotic PRBS can be reconstructed as an equivalent key by using only two chosen plaintexts; 3) most elements in the underlying chaotic PRBS can be obtained by a differential known-plaintext attack using only two known plaintexts.

Experimental results are given to demonstrate the feasibility of the proposed attack.

3. The security of a recently-proposed chaos-based image encryption scheme is studied in detail. The following problems are found: 1) there exist a number of invalid keys and weak keys, and some keys are partially equivalent for encryption/decryption; 2) given one chosen plain-image, a subkey K_{10} can be guessed with a smaller computational complexity than that of the simple brute-force attack; 3) with at most 128 chosen plain-images, a chosen-plaintext attack can possibly break the following part of the secret key: $\{K_i \bmod 128\}_{i=4}^{10}$, which works very well when K_{10} is not too large; 4) when K_{10} is relatively small, a known-plaintext attack can be carried out with only one known plain-image to recover some visual information of any other plain-images encrypted by the same key.
4. The security of an image encryption scheme based on the Hill cipher is studied and the following problems are found: 1) there is a simple necessary and sufficient condition that makes a number of secret keys invalid; 2) it is insensitive to the change of the secret key; 3) it is insensitive to the change of the plain-image; 4) it can be broken with only one known/chosen-plaintext; 5) it has some other minor defects.
5. Recently, a new image scrambling (i.e., encryption) scheme without bandwidth expansion was proposed based on two-dimensional discrete prolate spheroidal sequences. A comprehensive cryptanalysis is given on this image scrambling scheme, showing that it is not sufficiently secure against various cryptographic attacks including ciphertext-only attack, known/chosen-plaintext attack and chosen-ciphertext attack. Detailed cryptanalytic results suggest that the image scrambling scheme can only be used to realize perceptual encryption, but not to provide content protection for digital images.
6. Based on cryptanalyses of the aforementioned six encryption schemes, some general recommendations for designing secure multimedia encryption scheme are concluded.

Keywords: chaos, cryptanalysis, multimedia encryption, brute-force attack, known-plaintext attack, chosen-plaintext attack, differential attack.

Table of Contents

Abstract	i
Acknowledgements	iii
Table of Contents	iii
List of Figures	viii
List of Tables	xi
1 Introduction	1
§1.1 Background and Motivation	1
§1.2 Contributions of this Thesis	2
§1.3 Organization of this Thesis	3
2 Brief Survey on Multimedia Encryption Schemes	5
§2.1 Introduction	5
§2.2 Generic Multimedia Encryption Schemes	6
§2.2.1 Permutation-only Multimedia Encryption Schemes	6
§2.2.2 Image Encryption Schemes	8
§2.2.3 Video Encryption Schemes.	10
§2.2.4 Audio Encryption Schemes	11
§2.3 Chaos-based Multimedia Encryption Schemes	11
§2.3.1 Image Encryption Schemes Based on 1-D Chaotic Maps	11
§2.3.2 Image Encryption Schemes Based on 2-D Chaotic Maps	13
§2.3.3 Chaos-based Video Encryption Schemes	14
§2.3.4 Chaos-based Audio Encryption Schemes	15
§2.4 Conclusion	15

3	Cryptanalysis of a Chaotic Encryption Scheme with External Keys and its Improved Version	16
§3.1	Introduction	16
§3.2	The Original Scheme and its Improved Version.	17
§3.3	Cryptanalysis	19
§3.3.1	Weak Keys.	19
§3.3.2	Weak Randomness of Dynamic Table	21
§3.3.3	Breaking the Secret Key by a Known-plaintext Attack	24
§3.3.4	Security Problem of the Improved Version.	28
§3.4	Conclusion	29
4	Cryptanalysis of two Chaotic Encryption Schemes Based on Circular Bit Shift and XOR Operations	30
§4.1	Introduction	30
§4.2	Two Chaotic Encryption Schemes.	31
§4.2.1	Encryption Scheme Based on the Logistic Map	31
§4.2.2	Encryption Scheme Based on a Delayed Chaotic Neural Network (DCNN).	32
§4.3	Some Security Problems of the Two Schemes	34
§4.3.1	Insufficient Randomness of Chaos-based PRBS	34
§4.3.2	Some Inadequate Sub-keys in the DCNN-based Scheme	38
§4.3.3	Low Sensitivity of Encryption to Plaintexts	39
§4.4	Cryptanalysis	40
§4.4.1	Some Special Properties of Circular Bit Shift Operations	41
§4.4.2	Chosen-plaintext Attack	43
§4.4.3	Differential Known-plaintext Attack	43
§4.5	Conclusion	45
5	Cryptanalysis of a Chaotic Image Encryption Scheme	47
§5.1	Introduction	47
§5.2	The Image Encryption Scheme Under Study	48

§5.3	Cryptanalysis	50
§5.3.1	Two Basic Properties of the Scheme	50
§5.3.2	Analysis of the Key Space	53
§5.3.3	Guessing Sub-keys Separately	62
§5.3.4	Guessing an Important Key with a Chosen Plain-image	62
§5.3.5	Breaking Some Keys with Chosen-plaintext Attack	64
§5.3.6	Known-plaintext Attack Based on a Masking Image	74
§5.4	Conclusion	75
6	Cryptanalysis of an Image Encryption Scheme Based on the Hill Cipher	77
§6.1	Introduction	77
§6.2	The Image Encryption Scheme Under Study	77
§6.3	Cryptanalysis	78
§6.3.1	Some Defects of the Scheme	78
§6.3.2	Known/Chosen-Plaintext Attack	84
§6.4	Conclusion	86
7	Cryptanalysis of an Image Scrambling Scheme without Bandwidth Ex-	
	pansion	87
§7.1	Introduction	87
§7.2	The Image Scrambling Scheme without Bandwidth Expansion	88
§7.3	Cryptanalysis	91
§7.3.1	Ciphertext-only Attack	91
§7.3.2	Known-plaintext Attack.	104
§7.3.3	Chosen-plaintext Attack	107
§7.3.4	Chosen-ciphertext Attack	110
§7.4	Discussion.	111
§7.5	Conclusion	114
8	Conclusion and Remarks on Future Research	116
§8.1	Some Recommendations for Designing Multimedia Encryption Schemes . .	116

§8.2	Summary of this Thesis	119
§8.3	Future Research	120
Bibliography		121
My Publications Related to this Thesis		136