

**CHAOS THEORY BASED CRYPTOGRAPHY IN DIGITAL  
IMAGE DISTRIBUTION**

**Visibility Controlled Image Encryption Scheme (ViCIEn)**



University of Moratuwa, Sri Lanka.  
**MSc IN COMPUTER SCIENCE**  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

**M.H.P. RANMUTHUGALA**

**UNIVERSITY OF MORATUWA  
SRI LANKA**

**DECEMBER 2008**

**CHAOS THEORY BASED CRYPTOGRAPHY IN DIGITAL  
IMAGE DISTRIBUTION**

**Visibility Controlled Image Encryption Scheme (ViCIEn)**



University of Moratuwa, Sri Lanka.  
**M.H.P. RANMUTHUGALA**  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

**This Dissertation was Submitted to the Department of Computer Science and Engineering of the University of Moratuwa in Partial Fulfillment of the requirements for the Degree of M.Sc in Computer Science specializing in Information Systems Security**

**Department of Computer Science and Engineering  
University of Moratuwa  
December 2008**

# Declaration

*“The work included in this report was done by me, and only by me, and the work has not been submitted for any other academic qualification at any institution”*

-----  
Name: M.H.P. Ranmuthugala (078269G)

Date: 2008.12.31



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

*“I certify that the declaration above by the candidate is true to the best of my knowledge and that this dissertation is acceptable for evaluation for the Degree of M.Sc in Computer Science specializing in Information Systems Security”*

-----  
Project Supervisor: Dr. Chandana Gamage

Date: 2008.12.31

# Chaos Theory Based Cryptography in Digital Image Distribution

Visibility Controlled Image Encryption scheme (ViCIEn)



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

## Abstract

The amount of visual information available in digital format has grown exponentially in recent years due to the wide availability of equipments such as digital cameras and camera phones, changes in the way people socially interact by setting up community web pages, wide spread use of the Internet in all types of personal and business activities, and developments in high speed transmission of digital images with high reliability.

However, the wide accessibility of the Internet and its connected hosts and availability of technology to capture network traffic or penetrate hosts have made digital images vulnerable to unauthorized access while in storage and during transmission over a network. Hence users of the Internet and application that use or process digital images need to address security issues to protect commercial value of images and also ensure user privacy and other issues.

Apart from the above security related issues, electronic image trading has become a mainstream trade in cyber space and pay-after-trial services of digital multimedia are in wide practice. For example, thumbnail versions of images are used to provide previews to customers prior to the transaction in order to have a choice of selection. Current practices include showing only a small tile (thumbnail) of the original image, showing a lower-resolution version of the full image, showing the original image overlaid with a visible watermark image, or partial encryption of the images allowing only for a low visibility level than the original image.

Among these schemes, except for the method using partial encryption, other methods can be successfully attacked to obtain the original image by watermark removal, image enhancement, etc. In this context, image encryption becomes important in achieving the security requirements listed earlier to protect commercial interests and ensure privacy.




University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

The objective of the research presented in this thesis is to propose an image encryption technique which is capable of encrypting an image effectively and securely with a predefined visibility level. Unlike a conventional symmetric key encryption scheme, apart from the input plaintext image and the secret encryption key, there will be a third input defining the visibility level of the output ciphertext image. This research studies the use of chaos theory in implementing such an encryption scheme and proposes a concrete image encryption scheme using 2D chaotic maps called Ikeda map and the Kaplan-Yorke map achieving the stipulated objective.

## ACKNOWLEDGMENTS

The author wish to sincerely thank the following people for providing assistance, support, encouragement and inspiration during the writing of this dissertation. First I would like to thank my parents, the project supervisor Dr. Chandana Gamage and the project coordinator Dr. Sanath Jayasena. They provided guidance, encouragement, opportunities and knowledge at a level that few advisors are capable of. Second I would like to thank all the academic staff members at the Department of Computer Science and Engineering, University of Moratuwa. They have provided invaluable academic advises and utmost facilitate in successful completion of the project.

 The process of review gave me the opportunity to correct a number of small errors or omissions that has been observed in the first draft of the thesis. Many of these were first noticed and brought to my attention by alert readers. In particular, I would like to thank Janani for pointing out and correcting such mistakes.

No student or group of students can survive in a university without the help of their fellow students to discuss ideas, share opinions, and to make time spent in the lab and all round enjoyable experience. I would be grateful for all M.Sc 07 colleagues for the corporation given to the successful completion of my project involvements.

Finally I would like to thank all people who provided a great help during my time at the Department of Computer Science & Engineering, University of Moratuwa.

# TABLE OF CONTENTS

Declaration .....	i
Abstract .....	ii
Acknowledgements .....	iv
Table of Contents .....	v
List of Figures .....	vii
List of Tables .....	ix
<b>Chapter 1 – Introduction .....</b>	<b>1</b>
<b>Chapter 2 - Chaos based Image Encryption .....</b>	<b>5</b>
2.1 Chaos based Cryptography .....	5
2.2 Specific properties of chaotic systems .....	6
2.3 Chaos and Cryptography – Illustration of basic principles .....	9
2.3.1 Logistic map and analysis .....	9
2.3.2 Lorenz System .....	11
2.3.3 Baptista method and Logistic map .....	14
2.4 Analog and Digital chaos systems .....	16
2.4.1 Chaos Synchronization .....	17
2.4.2 Analog Chaos based Secure Communications .....	17
2.4.3 Digital Chaos-based cryptosystems .....	20
2.5 Image Encryption, Why? .....	21
2.5.1 Some Special Features of Image Encryption Schemes ....	21
2.6 Image Encryption design Architectures .....	22
2.7 Chaos based Crypto System Design rules .....	27
2.7.1 Crypto Analysis .....	34
2.7.2 Chaos specific attacks .....	38
2.8 Characteristics of an Image Cryptosystem .....	38
2.9 Image Encryption Algorithms .....	39
2.10 Research Issues of an Image Cryptosystems .....	43

2.10.1 Experiences and Lessons .....	44
2.11 Other Mechanisms used for Image Protection .....	46
<b>Chapter 3 -The Design of ViCIEn Scheme .....</b>	<b>48</b>
3.1 Proposed Image Encryption Architecture .....	49
3.1.1 The Encryption Process .....	49
3.1.2 The Decryption Process .....	68
<b>Chapter 4 - Security Analysis of ViCIEn .....</b>	<b>71</b>
4.1 Statistical Analysis .....	71
4.1.1 Histogram Analysis. ....	72
4.1.2 Correlation Coefficient Analysis .....	72
4.2 Sensitivity/ Differential Analysis .....	76
4.2.1 Number of Pixels Change Rate. ....	77
4.2.2 Unified Average Changing Intensity .....	77
4.3 Information Entropy Analysis .....	79
4.4 Key Space Analysis .....	81
4.4.1 Exhaustive Key Search.....	81
4.4.2 Key Sensitivity Analysis .....	81
<b>Chapter 5 - Conclusion .....</b>	<b>85</b>
<b>References .....</b>	<b>91</b>



## LIST OF FIGURES

1.0	Image Encryption Illustrated .....	3
2.1	Bifurcation Diagram .....	10
2.2	Sensitivity to initial conditions .....	10
2.3	Invariant distribution of the iterates .....	11
2.4	Time series $x(t)$ for chaotic Lorenz parameters .....	12
2.5	Phase space plot of the Lorenz Attractor .....	13
2.6	Frequency Distribution of iterates of Logistic map.....	15
2.7	Basic structure of a typical chaotic masking system .....	18
2.8	Basic structure of a typical chaotic switching system .....	19
2.9	Basic structure of a typical chaotic modulation system .....	19
2.10	Typical architecture of a chaos-based image cryptosystem .....	23
2.11	Secret Key Encryption .....	29
2.12	Public key ciphers .....	30
2.13	Bifurcation diagram of the Rossler attractor .....	32
2.14	Cryptographic elements in a symmetric cryptosystem .....	36
3.1	The Image Encryption Process .....	49
3.2	Point Trajectories of Ikeda map for various $u$ values .....	53
3.3	The bifurcation diagram of Ikeda map .....	54
3.4	The Ikeda attractor .....	55
3.5	The Kaplan Yorke map Chaotic Attractor .....	56
3.6	2D Image Convolution .....	59
3.7	Kaplan Yorke Visibility Level control parameter variation .....	63
3.8	The Decryption Process .....	68
4.1	Distribution of two vertically adj. pixels in the plain image .....	74
4.2	Distribution of two vertically adj. pixels in the encrypted image .....	75

4.3	Distribution of two horizontally adjacent pixels in the plain image	75
4.4	Distribution of two horizontally adj. pixels in the encrypted image	75
4.5	Distribution of two diagonally adj. pixels in the plain image .....	76
4.6	Distribution of two diagonally adj. pixels in the encrypted image	76
4.7	Information Entropy Vs. $\alpha$ – Value (Image: Lena) .....	80
4.8	Information Entropy Vs. $\alpha$ – Value (Image: Cman) .....	80
4.9	Cman Image – Decrypted Image and the histogram .....	82
4.10	Cman Image – Decrypted image and the Histogram .....	82
5.1	Correlation Coefficient & Entropy value Variation (Image: Cman)	90



University of Moratuwa, Sri Lanka.  
 Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

## LIST OF TABLES

2.1	Chaotic Properties and cryptographic relationship .....	7
2.2	Division of Logistic Attractor into S sites .....	14
3.1	Image Encryption results – Ikeda Map .....	61
3.2 (A)	Image Encryption results (Lena) – Kaplan-Yorke Map .....	64
3.2 (B)	Image Encryption results (Cman) – Kaplan-Yorke Map .....	65
3.3	Image Encryption Quality Analysis.....	67
4.1	Correlation Coefficient Analysis .....	74
4.2	NPCR Analysis Results. ....	78
4.3	UACI Analysis Results .....	78
4.4	Information Entropy Analysis for Lena and Cman Images.....	79
4.5	Key Sensitivity Analysis – Cman Image .....	83
4.6	$P_{(interim)}$ value variation and Decrypted Images .....	84