UNIVERSITI PUTRA MALAYSIA

SECURING THE IMAGE THROUGH THE COMBINATION OF ELLIPTIC CURVE CRYPTOSYSTEM AND HILL CIPHER ENCRYPTION

SANIAH BINTI SULAIMAN

FSKTM 2019 23

SECURING THE IMAGE THROUGH THE COMBINATION OF ELLIPTIC CURVE CRYPTOSYSTEM AND HILL CIPHER ENCRYPTION

By

SANIAH BINTI SULAIMAN

Thesis Submitted to the School of Graduate Studies,

Universiti Putra Malaysia,

in Fulfilment of the Requirements for the

Master of Information Security

June 2019

DEDICATIONS

This thesis is dedicated to my husband and my parent. Also thank you to all my family members and friends. Thank you for the support, motivation, advises and continuous love.

ABSTRACT

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

SECURING THE IMAGE THROUGH THE COMBINATION OF ELLIPTIC CURVE CRYPTOSYSTEM AND HILL CIPHER ENCRYPTION

By

SANIAH BINTI SULAIMAN

June 2019

Chair: Associate Professor Dr Zurina Binti Mohd. Hanapi

Faculty: Faculty of Computer Science and Information Technology

The advancement of communication technology helps users sharing the images through internet. However, the sharing through unsecure channels may expose the images to certain attack that will compromise their confidentiality. Image encryption is one of the methods that protect against this threat.

Hill Cipher is being applied in image encryption because of its simple operation and fast computation, but it also possesses a weak security level which requires the sender and receiver to use and share the same private key within an unsecure channel. There is a proposed technique that combines elliptic curve cryptosystem together with Hill

Cipher (ECCHC) to overcome the above mentioned weakness, however, the experiment only performed an analysis on four images which leads to inaccuracy of the results. There were two objectives in this research. The first objective was to redesign and redevelop the image encryption technique, a combination of Elliptic Curve Cryptosystem and Hill Cipher (ECCHC). The second objective was to test the ECCHC technique using 209 images from USC-SIPI database that consisted of 159 grayscale images and 50 colour (RGB) images in order to obtain reliable results.

In ECCHC, the sender and receiver must agree on the elliptic curve function and share the domain parameter to initiate the key generation including private key, public key, and 4 x 4 self-invertible key matrix before sharing image. The image will split into size four (vector of 4 x 1) that later will be encrypted using Hill Cipher with 4 x 4 self-invertible key matrix. The generated 4 x 1 vector image will take modulo 256 to generate the cipher image. Once the receiver receives the cipher image, decryption can be done by using the 4 x 4 self-invertible key matrix, generated on receiver site. Matlab is a simulation environment to conduct the experiments.

There were two experiments of this study. The first experiment was re-implementation of ECCHC technique and run the testing on the same four images that had been used by the based work paper. On the other hand, the second experiment was extensive analysis of ECCHC technique by using 209 images from USC SIPI database. The results from both experiments discussed on Entropy, Peak Signal to Noise Ratio (PSNR) and Unified Average Changing Intensity (UACI). For the second experiment, there were additional results of the analysis on the actual data of the encrypted images to ensure the confidentiality of the encrypted images.. From the obtained results, it has

been proven that several images were not encrypted well. In conclusion, the technique did not guarantee a secure image encryption as it was verified that certain images were not successfully encrypted.

ABSTRAK

Abstrak tesis yang dikemukan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

MELINDUNGI GAMBAR MELALUI PENGGABUNGAN SISTEMKRIPTO LENGKUNG ELIPTIK DAN KOD HILL

Oleh

SANIAH BINTI SULAIMAN

Jun 2019

Pengerusi: Professor Madya Dr Zurina Binti Mohd. Hanapi

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Kemajuan teknologi komunikasi membantu para pengguna untuk berkongsi gambar melalui rangkaian Internet. Walaubagaimanapun, perkongsian melalui saluran yang tidak selamat berkemungkinan besar akan mendedahkan gambar-gambar tersebut kepada serangan-serangan siber tertentu yang mana akan menjejaskan tahap kerahsiaan mereka. Oleh itu, enkripsi gambar adalah salah satu cara untuk mengekang ancaman terhadap gambar.

Kod Hill sering digunakan dalam proses enkripsi gambar kerana operasinya yang ringkas dan proses pengiraannya yang pantas. Namun, Kod Hill tetap mempunyai tahap keselamatan yang lemah yang mana pengirim dan penerima akan mengguna dan berkongsi kunci rahsia yang sama melalui saluran yang tidak selamat. Justeru, diwujudkan teknik yang diperkenalkan melalui kajian dengan menggabungkan sistemkripto lengkung eliptik dan Kod Hill yang dikenali sebagai teknik ECCHC untuk mengatasi kelemahan yang dinyatakan sebentar tadi. Walaubagaimanapun, eksperimen hanya dilakukan ke atas empat gambar sahaja, maka, ia berkemungkinan menghasilkan keputusan yang tidak tepat. Untuk kajian ini, terdapat dua objektif yang perlu dilaksanakan. Objektif pertama adalah mereka bentuk dan membina semula teknik ECCHC dan menjalankan pengujian yang sama seperti kajian sebelumnya. Objektif yang kedua adalah menjalankan pengujian teknik ECCHC ke atas set data yang baru, diperolehi daripada pangkalan data gambar USC SIPI yang merangkumi 209 gambar; 159 daripada mereka adalah gambar kelabu manakala 50 yang lain adalah gambar berwarna untuk memastikan kebolehpercayaan keputusan eksperimen.

Dalam teknik ECCHC, pengirim dan penerima secara sepakat bersetuju untuk menggunakan satu fungsi lengkung eliptik dan berkongsi parameter domain bagi memulakan penjanaan kunci yang terdiri dari kunci rahsia, kunci umum, dan 4 x 4 kunci matrik pembalikan sendiri sebelum berkongsi gambar. Gambar akan dibahagikan kepada vektor 4 x 1 yang mana ia akan dienkripsi menggunakan Kod Hill bersama dengan 4 x 4 kunci matrik pembalikan sendiri dan penghasilan gambar bersaiz vektor 4 x 1 seterusnya akan menjalani operasi modulo 256 untuk menghasilkan kod gambar. Setelah penerima menerima kod gambar tersebut, dekripsi gambar boleh

dilakukan mengguna 4 x 4 kunci matrik pembalikan sendiri yang dijana di bahagian penerima. Simulasi untuk kajian ini menggunakan Matlab.

Eksperimen pertama melibatkan pembangunan semula teknik ECCHC dan menjalankan pengujian pada empat gambar yang sama seperti yang digunakan oleh kertas penanda aras. Eksperimen kedua pula melanjutkan analisis ke atas teknik ECCHC dengan menggunakan 209 gambar yang diperoleh dari pangkalan data USC SIPI. Keputusan untuk kedua-dua eksperimen membincangkan nilai *entropy*, *Peak Signal to Noise Ratio* (PSNR) dan *Unified Average Changing Intensity* (UACI). Untuk eksperimen yang kedua, terdapat tambahan keputusan daripada analisis yang dilakukan ke atas gambar yang dienkripsi bagi memastikan kesulitan gambar yang dienkripsi tidak dapat dibaca. Keputusan yang diperoleh menunjukkan bahawa terdapat beberapa gambar yang tidak dienkripsi dengan baik. Kesimpulannya, teknik ini tidak menjanjikan tahap keselematan enkripsi gambar yang tinggi kerana eksperimen yang dijalankan telah membuktikan wujudnya gambar yang tidak berjaya dienkripsi dengan baik.

ACKNOWLEDGEMENT

Alhamdulillah praise to Allah S.W.T for the strength and blessing in completing this thesis.

I would like to express my special thanks of gratitude to my supervisor, Associate Professor Dr Zurina Mohd Hanapi who gave me the best and truthful guidance to complete this thesis. Her guidance helped me in all the time of research and writing of this thesis. Thanks to her for the motivation and patience during this guidance period.

Secondly, I would also like to thank my family, especially to my husband and parent who always believing in me. Thank you for their continuous love, countless of support for all this time. My greatest appreciation to my husband for the financial support and who always by my side throughout this Master year.

My greatest appreciation of friendship goes to all my friends especially to my class mate of Master of Information Security. I would like to thank them for sharing some idea, offering their assistance and giving a motivation that help me to complete my master study.

Last but not least, thank you to all FSKTM lecturers and staffs for their support and care to all FSKTM student. Thank you to them for providing a comfortable, nice, efficient environment and facilities for students like me so that we can focus on our study.

APPROVAL

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Information Security. The members of the Supervisory Committee were as follows:

Signature:_____

Zurina Mohd. Hanapi, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Date:_____

DECLARATION

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustration and citation have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, report, lecturer notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012.

Signature: _____ Date: _____

Name and Matric No.: **Saniah Binti Sulaiman GS51086**

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DMRNRP	Diffusion Mechanism Based on Random Numbers Related to Plaintext
DNA	Deoxyribonucleic Acid
ECCHC	Elliptic Curve Cryptosystem and Hill Cipher image encryption
NPCR	The Number of Changing Pixel Rate
PNSR	Peak Signal to Noise Ratio
PWLCM	Multiple Piece-Wise Linear Chaotic Map
RGB	Red Green Blue
SCPMDP	Simultaneously Intra-Inter-Component Permutation Mechanism Dependent on the Plaintext
UACI	Unified Averaged Changed Intensity

CHAPTER 1

INTRODUCTION

1.1 Introduction

The advancement of communication technology helps the users sharing images through Internet. Most of current communication platforms use images to convey information which include email, social media, text message, and so on. The platform most likely to use digital image is social media. Examples of social media used by the people around the world are Facebook, Instagram, and Tweeter (Jarrahi, 2018). These social media provide a specific feature for sharing images.

The concept of some social media is open and public sharing, on the other hand, some other platforms do not employ this concept such as messaging applications. The messaging applications enable users sharing digital images only to intended receivers. This is completely different from the concept of social media. Same goes for email – it is also one of the platforms used to send the images to other users. To do so, some of these applications utilize an unsecure channel which is Internet. However, the sharing through unsecure channels may expose the image to stalking or stealing activity. Thus, sharing action should be protected from adversary with stalking intention and avoid further cyber attacks (Thein et al., 2017).

The image confidentiality should be only known by the respective sender and receiver. To address the issue, cryptography technique is the most common way to secure the image transmission occurring on the internet (Patel & Belani, 2011). Cryptography is a process of encryption and decryption. Encryption is encrypting the plain message to become cipher that requires some techniques or algorithms to protect the

confidentiality of the message from being read by unauthorized users. On the other hand, decryption is a reverse process of the encryption to convert from cipher to become an original message so that it can be read by the authorized users. There are several image encryption techniques proposed in previous research to ensure the confidentiality of the image. i.e image encryption based on chaotic systems (Zarebnia et al., 2019), image encryption based on secure linear feedback shift register (Saha at al., 2018), image encryption based on finite precision error (Nardo et al., 2019) and so on.

One of algorithms used in image encryption is Hill Cipher. Hill Cipher is encryption that forms messages in matrix and multiply them with the key matrix to produce encrypted messages. This concept can be used not only for textual but also for image because of the matrix concept. Thus, as for this research, a new image encryption proposed by Dawahdeh et al. (2018) entitled "A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher" was employed as a based work paper.

1.2 Problem statement

Hill Cipher is applied in image encryption because of its simple operation and fast computation even though it has a weak security level because it requires the sender and receiver to use and share the same private key within unsecure channels. Due to that reason, image encryption of Elliptic Curve Cryptosystem and Hill Cipher (ECCHC) techniques were proposed by Dawahdeh et al., (2018) to convert Hill Cipher into asymmetric as in asymmetric technique, private key was not shared but generated at receiver side.

However, the proposed technique only performed an analysis on four images which leads to inaccuracy of the results.

1.3 Objective

There are two objectives in this study. The lists of the objectives are:

i. to redevelop the ECCHC technique and testing the same images to obtain the results same as the based work paper by conducting security analysis on entropy, Peak Signal to Noise Ratio (PSNR) analysis and Unified Average Changing Intensity (UACI).

ii. to test the ECCHC technique using 209 images from USC SIPI database that consisted of 159 grayscale images and 50 RGB colour images in order to ensure reliable result.

1.4 Scope

The scope of this study is to redevelop the proposed image encryption by using simulation. This study simulates the ECCHC technique by using Matlab tool, a same simulation conducted by the anchor paper. This Matlab tool run on Windows 10 computer with specification of 8GB RAM and 1.60 GHz processor.

For dataset, the type of image used in this study are grayscale and RGB colour image. For re-implementation purpose, the same four grayscale images from anchor paper are used. These images are Lena, Cameraman, Smandril and Einstein with size 256 x 256 pixels. These images are the original images sent by the author of the anchor paper using email. On the other hand, for the extensive analysis, 159 grayscale images and

50 RGB colour images from USC SIPI database are used as new dataset. These images have the size of 256 x 256, 512 x 512, and 1024 x 1024 pixels.

Overall direction of this study is to determine whether the ECCHC technique able to produce a good result of security analysis and able to preserve the confidentiality of the encrypted image. This study will discuss and conclude whether the ECCHC technique is a secure image encryption technique as claimed by the author of the anchor paper.

1.5 Thesis Structure

The rest of this thesis is organized as follows; Chapter Two presents the literature review explained the background of image encryption, the previous hybrid Hill Cipher and the standard image database used by recent works. Chapter Three elaborates the methodology of this study. It describes the required step, the scenarios of experiments and tool used to complete this study. Chapter Four describes the details on the results obtained from the conducted experiments. The results will be focus on entropy, PSNR and UACI for each image. Finally, Chapter Five conclude the overall of this study and provide some recommendations for future work.

REFERENCES

Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. (2009). Image Encryption Using Advanced Hill Cipher Algorithm from *ACEEE International Journal on Signal and Image Processing* 1: 663–667.

Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S. K. (2007). Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm from *International Journal of Security* 1: 14–21.

Acharya, B., Sharma, M. D., Tiwari, S., & Minz, V. K. (2010). Privacy Protection of Biometric traits using modified Hill Cipher with Involutory Key and Robust Cryptosystem from *Procedia Computer Science* 2: 242–247.

Casas, V. 2006. *An Information Security Risk Assessment Model for Public and University Administrators*, Master Thesis, Texas State University.

Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos from *Signal Processing* 155: 44–62.

Dawahdeh, Z. E., Yaakob, S. N., & Othman, R. R. (2018). A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher from *Journal of King Saud University - Computer and Information Sciences* 30(3): 349–355.

Dinghui, Z., Qiujie, G. U., Yonghua, P., & Xinghua, Z. (2008). Discrete Chaotic Encryption and Decryption of Digital Images from *International Conference on Computer Science and Software Engineering*: 849–852.

Fu, C., Lin, B., Miao Y.S., Liu, X., & Chen J. J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption from *Optic Communications 284*: 5415-5423

Goutham, L., Mahendra, M. S., Manasa, A. P., & Prajwalasimha, S. N. (2017). Modified Hill Cipher Based Image Encryption Technique from *International Journal for Research in Applied Science & Engineering Technology*, *5*(Iv): 342–345.

Guo, J., Dwi, R., & Heri, P. (2018). Improved Beta Chaotic Image Encryption for

Multiple Secret Sharing from *IEEE Access* 6: 46297–46321.

Gupta, K., & Silakari, S. (2010). Performance Analysis for image Encryption using ECC from *2010 International Conference on Computational Intelligence and Communication Networks* 2: 79–82.

Hamissa, G., Sarhan, A., Abdelkader, H., & Fahmy, M. (2011). Securing JPEG architecture based on enhanced chaotic hill cipher algorithm from *Proceedings - ICCES'2011: 2011 International Conference on Computer Engineering and Systems*: 260–266.

Han, Z., Feng, W. X., Hui, L. Z., Hai, L. Da, & Chou, L. Y. (2003). A New Image Encryption Algorithm Based on Chaos System from *International Conference on Robotics, Intelligent Systems and Signal Processing*, (October): 778–782.

Hassene, S., & Eddine, M. N. (2016). A new hybrid encryption technique permuting text and image based on hyperchaotic system from *2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*: 63–68.

Jarrahi, M. H. (2018). Social Media, Social Capital, and Knowledge Sharing in Enterprise from *IT Professional* 20(4): 37–45.

Jolfaei, A., Wu, X., & Muthukkumarasamy, V. (2016). On the Security of Permutation-Only Image Encryption Schemes from *IEEE Transactions on Information Forensics and Security* 11(2): 235–246.

Kabirirad, S., & Hajiabadi, H. (2015). Cryptanalysis Of An Authenticated Image Encryption Scheme Based On Chaotic Maps And Memory Cellular Automata, (1), 1–11. Retrieved from https://pdfs.semanticscholar.org/b9d3/ec7cd53e30221acdf6890b9bee7da13bcffa.pdf

Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. (2010). A New Modified Version of Advanced Encryption Standard Based Algorithm from *2010 International Conference on Electronics and Information Engineering* 1: 141–145.

Kim, J., & Basavarasu, S. R. (2001). On The Voice and Image Data Encryption using Advanced Encryption Standard (AES) in Counter Mode for Multimedia Broadcasting from *2015 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*: 1–4.

Kumar, N., Kumar, S., & H T, P. (2012). Encryption Approach for Images using Bits Rotation Reversal and Extended Hill Cipher Techniques from *International Journal of Computer Application* 59(16): 10–14.

Lan, R., He, J., Wang, S., Gu, T., & Luo, X. (2018). Integrated chaotic systems for image encryption R from *Signal Processing* 147: 133–145.

Li, P., & Lo, K. T. (2018). A Content-Adaptive Joint Image Compression and Encryption Scheme from *IEEE Transactions on Multimedia*, *20*(8), 1960–1972.

Li, X. M., & Dai, L. (2010). Reality-Preserving Image Encryption Assosiated with the Chaos and the LCT from *2010 3rd International Congress on Image and Signal Processing* 6: 2624–2627.

Mahmoud, A. Y., & Chefranov, A. G. (2014). Hill cipher modification based Pseudo-Random Eigenvalues from *Applied Mathematics and Information Sciences* 8(2): 505–516.

Msolli, A., & Helali, A. (2016). Image encryption with the AES algorithm in wireless sensor network from *2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*: 41–45.

Nardo, L. G., Nepomuceno, E. G., Arias-garcia, J., & Butusov, D. N. (2019). Image Encryption using Finite-Precision Error from *Chaos, Solitons and Fractals: The Interdisciplinary Journal of Nonlinear Science, and Nonequilibrium and Complex Phenomena* 123: 69–78.

Naskar, P. K., & Chaudhuri, A. (2014). A Secure Symmetric Image Encryption based on Bit-wise Operation from *Proceedings - International Conference on 2014 Applications and Innovations in Mobile Computing, AIMoC 2014*, (January): 67–74.

Naveenkumar, S. K., Panduranga, H. T., & Kiran. (2015). Chaos and Hill Cipher Based Image Encryption for Mammography Images from *ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems*: 1–4.

Panduranga, H. T., & Kumar, N. (2012). Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique from *International Journal of Computer Applications* 60(16): 975–8887.

Panduranga, H. T., S, S. K. H., & K, N. K. S. (2012). Hybrid approach for Dual Image Encryption Using Nibble Exchange and Hill-Cipher from *2012 International Conference on Machine Vision and Image Processing (MVIP)*: 101–104.

Parvaz, R., & Zarebnia, M. (2018). A combination chaotic system and application in color image encryption from *Optics and Laser Technology* 101: 30–41.

Patel, K. D., & Belani, S. (2011). Image Encryption using Different Techniques: A review from *International Journal of Emerging Technology and Advanced Engineering* 1(1): 30–34.

Patro, K. A. K., & Acharya, B. (2019). An efficient colour image encryption scheme based on 1-D chaotic maps from *Journal of Information Security and Applications* 46: 23–41.

Ponuma, R., Amutha, R., & Haritha, B. (2018). Compressive Sensing and Hyper-Chaos Based Image Compression-Encryption from *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*: 1–5.

Rajput, Y., & Gulve, A. K. (2014). A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher from *International Journal of Computer Application 95*(4): 435–444.

Saha, S., Karsh, R. K., & Amrohi, M. (2018). Encryption and Decryption of Images using Secure Linear Feedback Shift Registers from *2018 International Conference on Communication and Signal Processing (ICCSP)*: 295–298.

Sazaki, Y., & Putra, R. S. (2016). Implementation of Affine Transform Method and Advanced Hill Cipher for Securing Digital Images from *Proceeding of 2016 10th International Conference on Telecommunication Systems Services and Applications, TSSA 2016: Special Issue in Radar Technology*: 1–5.

Sethi, N., & Vijay, S. (2013). Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique from *Conference on Advances in Communication and Control Systems*: 46–50.

Sun, S., & Guo, Y. (2015). A Novel Image Steganography based on Contourlet Transform and Hill Cipher from *Journal of Information Hiding and Multimedia Signal Processing* 6(5): 889–897.

Taneja, N., Raman, B., & Gupta, I. (2012). Combinational domain encryption for still visual data from *Multimedia Tools and Applications* 59(3): 775–793.

Thein, N., Nugroho, H. A., Bharata, T., & Mustika, I. W. (2017). Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes from *2017 International Conference on Advanced Computing and Applications (ACOMP)*: 122–126.

Wang, X., & Li, Z. (2019). A color image encryption algorithm based on Hopfield chaotic neural network from *Optics and Lasers in Engineering* 115(July 2018): 107–118.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI Randomness Tests for Image Encryption from *Cyber Journals: Multidisclinary Journals in Science Technology, Journal of Selected Areas in Telecommunications (JSAT)*: 31–38.

Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map from *Pattern Recognition Letter* 31: 347-354.

Zarebnia, M., Pakmanesh, H., & Parvaz, R. (2019). A Fast Multiple-Image Encryption Algorithm based on Hybrid Chaotic Systems for Grayscale Images from *Optik - International Journal for Light and Electron Optics*, *179*(October 2018): 761–773.

Zhao, L., Adhikari, A., Xiao, D., & Sakurai, K. (2012). On the security analysis of an image scrambling encryption of pixel bits and its improved scheme based on self-correlation encryption from *Communication in Nonlinear Science and Numerical Simulation* 17: 3303-3327

Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with Chaotic Maps from *Mathematical and Computer Modelling* 52: 2028–2035.

Zhao, X. Y., Cheng, G., Zhang, D., Wang, X. H., & Dong, G. C. (2004). Decryption of pure position permutation algorithms from *Journal of Zhejiang University-SCIENCE A* 5: 803-809

Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation from *Information Sciences* 181(6): 1171–1186.