Journal of Advanced Research (2016) 7, 193–208

Cairo University

Journal of Advanced Research

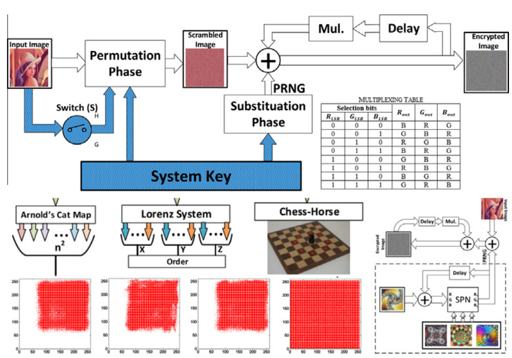
REVIEW

Symmetric encryption algorithms using chaotic and non-chaotic generators: A review

Ahmed G. Radwan [a,b,*], Sherif H. AbdElHaleem [a], Salwa K. Abd-El-Hafiz [a]

[a] *Engineering Mathematics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt*
[b] *Nanoelectronics Integrated Systems Center (NISC), Nile University, Cairo, Egypt*

GRAPHICAL ABSTRACT



ARTICLE INFO

Article history:
Received 27 May 2015
Received in revised form 24 July 2015
Accepted 27 July 2015
Available online 1 August 2015

ABSTRACT

This paper summarizes the symmetric image encryption results of 27 different algorithms, which include substitution-only, permutation-only or both phases. The cores of these algorithms are based on several discrete chaotic maps (Arnold's cat map and a combination of three generalized maps), one continuous chaotic system (Lorenz) and two non-chaotic generators (fractals and chess-based algorithms). Each algorithm has been analyzed by the correlation coefficients

* Corresponding author. Tel.: +20 1224647440; fax: +20 235723486.
E-mail address: agradwan@ieee.org (A.G. Radwan).

Peer review under responsibility of Cairo University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jare.2015.07.002

Keywords:
Permutation matrix
Symmetric encryption
Chess
Chaotic map
Fractals

between pixels (horizontal, vertical and diagonal), differential attack measures, Mean Square Error (MSE), entropy, sensitivity analyses and the 15 standard tests of the National Institute of Standards and Technology (NIST) SP-800-22 statistical suite. The analyzed algorithms include a set of new image encryption algorithms based on non-chaotic generators, either using substitution only (using fractals) and permutation only (chess-based) or both. Moreover, two different permutation scenarios are presented where the permutation-phase has or does not have a relationship with the input image through an ON/OFF switch. Different encryption-key lengths and complexities are provided from short to long key to persist brute-force attacks. In addition, sensitivities of those different techniques to a one bit change in the input parameters of the substitution key as well as the permutation key are assessed. Finally, a comparative discussion of this work versus many recent research with respect to the used generators, type of encryption, and analyses is presented to highlight the strengths and added contribution of this paper.

Ahmed G. Radwan (M'96–SM'12) received the B.Sc. degree in Electronics, and the M.Sc. and Ph.D. degrees in Eng. Mathematics from Cairo University, Egypt, in 1997, 2002, and 2006, respectively. He is an Associate Professor, Faculty of Engineering, Cairo University, and also the Director of Nanoelectronics Integrated Systems Center, Nile University, Egypt. From 2008 to 2009, he was a Visiting Professor in the ECE Dept., McMaster University, Canada. From 2009 to 2012, he was with King Abdullah University of Science and Technology (KAUST), Saudi Arabia. His research interests include chaotic, fractional order, and memristor-based systems. He is the author of more than 140 international papers, six USA patents, three books, two chapters, and h-index = 17.

Dr. Radwan was awarded the Egyptian Government first-class medal for achievements in the field of Mathematical Sciences in 2012, the Cairo University achievements award for research in the Engineering Sciences in 2013, and the Physical Sciences award in the 2013 International Publishing Competition by Misr El-Khair Institution. He won the best paper awards in many international conferences as well as the best thesis award from the Faculty of Engineering, Cairo University. He was selected to be among the first scientific council of Egyptian Young Academy of Sciences (EYAS), and also in first scientific council of the Egyptian Center for the Advancement of Science, Technology and Innovation (ECASTI).

Sherif H. AbdElHaleem received the B.Sc. degree in Electronics and Communication Engineering, a Diploma in Automatic Control and the M.Sc. degree in Engineering Mathematics from the Faculty of Engineering, Cairo University, in 2002, 2004 and 2015, respectively. From 2004 to 2015, he has been working as a professional software developer in ASIE. His research and work interests include software development, database applications, network programming, web developing and cryptography. As part of his M.Sc. work, Eng. AbdElHaleem has published several refereed papers on image encryption.

Salwa K. Abd-El-Hafiz received the B.Sc. degree in Electronics and Communication Engineering from Cairo University, Egypt, in 1986 and the M.Sc. and Ph.D. degrees in Computer Science from the University of Maryland, College Park, Maryland, USA, in 1990 and 1994, respectively. Since 1994, she has been working as a Faculty Member in the Engineering Mathematics and Physics Department, Faculty of Engineering, Cairo University, and has been promoted to a Full Professor in the same department in 2004. Since August 2014, she has also been working as the Director of the Technical Center for Job Creation, Cairo University, Egypt. She co-authored one book, contributed one chapter to another book and published more than 60 refereed papers. Her research interests include software engineering, computational intelligence, numerical analysis, chaos theory and fractal geometry.

Prof. Abd-El-Hafiz is a recipient of the 2001 Egyptian State Encouragement Prize in Engineering Sciences, recipient of the 2012 National Publications Excellence Award from the Egyptian Ministry of Higher Education, recipient of the 2014 African Union Kwame Nkrumah Regional Scientific Award for Women in basic science, technology and innovation, recipient of several international publications awards from Cairo University and an IEEE Senior Member.

Introduction

Symmetric encryption algorithms can be classified into stream ciphers and block ciphers where the image-pixels are encrypted one-by-one in stream ciphers and using blocks of bits in block ciphers. Although block ciphers require more hardware and memory, their performance is generally superior to stream ciphers since they have a permutation phase as well as a substitution phase. As suggested by Shannon, plaintext should be processed by two main substitution and permutation phases to accomplish the confusion and diffusion properties [1,2].

The target of the permutation process is to weaken the correlations of input plaintext by spreading the plaintext bits throughout the cipher text. On the other hand, the substitution