J Real-Time Image Proc (2013) 8:297–306
DOI 10.1007/s11554-011-0219-4

SPECIAL ISSUE

Robust chaotic key stream generator for real-time images encryption

M. S. Azzaz · C. Tanougast · S. Sadoudi · A. Dandache

Received: 17 June 2011 / Accepted: 3 August 2011 / Published online: 24 August 2011

Abstract In this paper, we propose a robust and compact design architecture of hardware chaotic key generator for real-time images encryption. The new proposed approach combines the perturbation technique with a non-linear switching between multiple three-dimensional continuous chaotic systems. The originality of this new scheme is that it allows a low-cost image encryption for embedded systems while still providing a good trade-off between performance and hardware resources. This pipelined architecture is particularly attractive since it provides a high security. Numerical simulations and real-time experimental results using *Xilinx* FPGA Virtex technology have demonstrated the feasibility and the efficiency of our secure solution and can be applied to many secure real-time embedded applications in *System on Chip* (*SoC*). Thorough experimental tests are carried out with detailed analysis, demonstrating the high security and fast encryption speed of the new scheme while still able to resist statistical and key analysis attacks.

Keywords Encryption · Hardware chaotic generator · Image processing · FPGA

1 Introduction

During the last decade, the use of chaos to generate *pseudo-random numbers* (*PRN*) to design digital chaotic stream ciphers has become a very important topic of research. A chaotic dynamical system is a deterministic system, ergodic, sensitive to initial conditions and system's parameters system and has a random-like behavior. These characteristics of chaotic systems are related to the concepts of confusion and diffusion usually used in traditional cryptosystems [1]. As a result of this tight relationship, both analog [2] and digital [3] cryptosystems based chaos have been presented. In fact, many methods have been developed to break the analog secure communication approaches [4, 5]. Most digital chaotic ciphers are claimed to be secure by authors [6], but many of them are actually not [7]. In almost all these cryptosystems, digital chaotic systems are adopted [8]. To design an efficient digital chaotic cipher which is difficult to decrypt against various intentional attacks, many problems must be considered and resolved. According to [9, 10], for a secure cryptosystems, the ciphertext should have a uniform distribution, and the key stream should also have the same property.

Since 1990, a number of *Pseudo-random number generators* (*PNGs*) based on deterministic chaotic phenomena have been proposed [11, 12]. Some of these have only been simulated while others have not been sufficiently optimized for cryptographic applications as they provide certain bias or deviations. Nevertheless, in today's digital communication systems, we must consider another important factor and relate it to the finite precision [13]. When chaotic systems are designed with finite computing precision, dynamic degradations can degrade the performance of the designed cryptosystems including short cycle length, non-ideal distribution and correlation, etc. This issue becomes very important in chaotic cryptosystem design. To solve this problem, some improvement measures have been proposed by researchers; these can be classified into three categories. In the first one, a higher finite precision is used [14]. However, this comes at the expense of additional hardware or software computation. The second one, which is based on cascading multiple

M. S. Azzaz · C. Tanougast (✉) · S. Sadoudi · A. Dandache
Sensors Interfaces and Microelectronic Laboratory of Metz, Paul-Verlaine University, Metz, France
e-mail: Camel.Tanougast@univ-metz.fr