# Chapter 14
# Medical Image Encryption:
## Microcontroller and FPGA Perspective

**Sundararaman Rajagopalan**
*Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India*

**Siva Janakiraman**
*Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India*

**Amirtharajan Rengarajan**
*Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India*

## ABSTRACT

*The healthcare industry has been facing a lot of challenges in securing electronic health records (EHR). Medical images have found a noteworthy position for diagnosis leading to therapeutic requirements. Millions of medical images of various modalities are generally safeguarded through software-based encryption. DICOM format is a widely used medical image type. In this chapter, DICOM image encryption implemented on cyclone FPGA and ARM microcontroller platforms is discussed. The methodology includes logistic map, DNA coding, and LFSR towards a balanced confusion – diffusion processes for encrypting 8-bit depth 256 × 256 resolution of DICOM images. For FPGA realization of this algorithm, the concurrency feature has been utilized by simultaneous processing of 128 × 128 pixel blocks which yielded a throughput of 79.4375 Mbps. Noticeably, the ARM controller which replicated this approach through sequential embedded "C" code took 1248 bytes in flash code memory and Cyclone IV FPGA consumed 21,870 logic elements for implementing the proposed encryption scheme with 50 MHz operating clock.*

## INTRODUCTION

Due to the rapid advancements in the field of communication and information technology, various domains have reached tremendous heights in terms of service and performance across the world. One such field is the healthcare which majorly relies upon this advancement, for diagnosis of diseases and telemedicine like treatment mediums. Medical images are widely utilized for the detection of abnormalities which can

DOI: 10.4018/978-1-5225-7952-6.ch014

manifest in various formats such as Magnetic Resonance Imaging (MRI), Computer Tomography (CT) and X- Ray. These images are usually represented in Digital Imaging and Communication in Medicine (DICOM) format. Medical images in this DICOM format are required to be transmitted to other medical practitioners and within the healthcare organization for tele – diagnosis or e – diagnosis. In Hospital Information System (HIS), medical information of the patients is acquired and stored in Picture Archiving Communication Service (PACS) server environment. PACS looks to be a top hierarchy in the HIS in which the medical metadata can be stored for a maximum of 24 to 36 hours and communicated to other hospitals on demand (Qasim, Meziane & Aspin, 2018). However, recent data breaches on healthcare information across the various hospitals have raised serious concerns towards the possible enhancements that can empower secure healthcare information management system. Medical images are more important due to the fact that even a small change in the sections of pixels may lead to wrong diagnosis and shall implicate serious health issues. Hence, encryption is a crucial technique to safeguard these medical details from malicious users (Hu & Han, 2009).

Software as well as hardware platforms can implement image encryption algorithms. However, software based approaches are ubiquitous compared to hardware realizations. Kanso and Ghebleh developed a selective chaos based medical image encryption in which the encryption was implemented in two phases namely shuffling phase and masking phase (Kanso & Ghebleh, 2015). The process can be repeated for several rounds, and in each phase Arnold cat map was used for confusion. The masking process enabled this system to withstand the cryptanalytic attacks. The performance of algorithm was validated by implementing it on different grayscale and color DICOM images and the obtained results evidenced that the encrypted image attained near zero correlation with flat histogram thus providing a strong resistance to statistical attacks. Dhivya *et al.* suggested a medical image encryption approach by employing the combined chaotic map of Logistic – Sine maps (Ravichandran, Praveenkumar, Balaguru Rayappan & Amirtharajan, 2016). The algorithm has been carried out in two stages namely crossover and mutation. In crossover process, the image pixels are shuffled in row wise and column wise in order to obtain the confused image. Mutation is the diffusion process executed using XOR operation. Medical image encryption based on cosine number transform (Lima, Madeiro & Sales, 2015), multiple chaotic mapping (Chen & Hu, 2017), Elgamal encryption technique (Laiphrakpam & Khumanthem, 2017), high speed scrambling and pixel adaptive diffusion with XOR and modulo arithmetic operations (Hua, Yi & Zhou, 2018) and three cryptic techniques namely Latin Square Image Cipher (LSIC), Discrete Gould Transform and Rubik's cube (Praveenkumar, Amirtharajan, Thenmozhi & Balaguru Rayappan, 2015) were all reported in literature which can be implemented on HIS for achieving the confidentiality of the medical images. These algorithms are developed and implemented with the help of software platform. Even though the software-based implementation is inexpensive, they are vulnerable to attacks and time consumable than the hardware-based algorithms (Ravichandran, Rajagopalan, Upadhyay, Rayappan & Amirtharajan, 2018).

Application Specific Integrated Circuit (ASIC) based algorithms provide higher throughput because of its inherent parallelism and customized architecture. However, these ASIC designs are expensive and less adaptable to remodel the algorithms. In order to overcome these limitations of software and ASIC based implementation, Field Programmable Gate Array (FPGA) is an alternate and good candidate due to its advantages such as flexibility, performance, reconfigurability, faster time to market, inbuilt IP core access and parallel computation capabilities (Ramalingam, Amirtharajan & Rayappan, 2016). Microcontrollers are extensively used in IoT applications. Healthcare IoT systems when adopting micro-