Chapter 1
Reliable Medical Image Communication in Healthcare IoT:
Watermark for Authentication

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

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

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

ABSTRACT

Images have been widely used in the medical field for various diagnostic purposes. In the field of healthcare IoT, secure communication of a medical image concerned with an individual is a crucial task. Embedding patients' personal information as an invisible watermark in their medical images helps to authenticate the ownership identification process. Reliable communication of medical image can be thereby ensured concerning authentication and integrity. Images in DICOM format with a pixel resolution of 8-bit depth are used for medical diagnostics. This chapter deals about the development of a lightweight algorithm to insert patients' identities as an invisible watermark in random edge pixels of DICOM images. This chapter describes the implementation of the proposed lightweight watermarking algorithm on a RISC microcontroller suitable for healthcare IoT applications. Imperceptibility level of the watermarked medical image was analyzed besides its lightweight performance validation on the constrained IoT platform.

DOI: 10.4018/978-1-5225-7952-6.ch001

INTRODUCTION

Internet of Things (IoT) finds its applications in diverse fields such as home automation, pollution monitoring, agriculture, and health care. Images have been predominantly used in medical diagnostic applications. The major aspects of security include confidentiality, integrity, and authentication. Due to the inevitable bondage of IoT devices with internet for data sharing via storage in the cloud, any data communication via IoT device is vulnerable to attacks. In the field of health care IoT, secure communication of a medical image concerned with an individual is a crucial task. Images such as human face can be easily distinguished and identified to authenticate the entry of a person in a restricted area.

In contrast, medical images cannot be distinguished unless it contains unique information about a patient. Information hiding on an image is a process that insets secret information into an image in an undetectable manner with a negligible loss in the original image quality. This work can be accomplished using techniques such as steganography or watermarking. A medical image with a patient's private information embedded as invisible watermark helps to identify the ownership and to authenticate. Thereby, authentication via watermark ensures the reliable communication of medical image.

Digital Imaging and Communications in Medicine (DICOM) is the widely used image format for medical diagnostics. These DICOM images can have a pixel resolution of 8-bit or 16-bit depth. Most of the existing watermarking schemes are designed for implementation on software platform like Matlab. To incorporate reliability on medical images used in healthcare IoT applications, it is necessary to device lightweight watermarking schemes that can be fit into the constrained devices such as microcontrollers used in IoT modules. Using less complex operations that take fewer clock cycles, minimal memory footprint and less power are the major requirements to be addressed while developing lightweight algorithms (Janakiraman, Thenmozhi, Rayappan, & Amirtharajan, 2018). Higher imperceptibility and a good level of randomness in the selection of image pixels for watermark insertion process are the significant parameters to make sure the reliability feature of the watermarking algorithms.

Edges are the pixels in the image that shows a visible disparity in their intensity levels. Identifying the edges of an image helps to locate an object and to know the borderline of a specific entity in an image. There are steganography algorithms that suggest embedding more information on edges to improve the embedding capacity while maintaining a good level of imperceptibility. Sobel mask, Quick mask, and Canny are some of the algorithms that can be used to accomplish edge detection on images. These algorithms decide the edges in an image by processing each pixel value with its surrounding pixels in all direction and by comparing the result with the set threshold values. Setting a threshold too high or too low may have a drastic impact on the ability of an algorithm to detect accurate edges.

This chapter describes the development of a lightweight algorithm in spatial domain that inserts the patient's identity as an invisible watermark in the edge pixels of the DICOM image. Further, this chapter also discusses the implementation aspects of the developed lightweight watermarking algorithm on a constrained microcontroller device suitable for health care IoT applications. Considering the memory constrains on IoT devices, DICOM images with 8-bit depth will be used for the implementation. Watermark information will be embedded in randomly chosen edge pixels of the medical image. Random edge detection will be carried out by applying the quick mask on the medical image with varying threshold values obtained from a Pseudo Random Number Generator (PRNG). Standard metrics such as Mean Average Error (MAE), Mean Square Error (MSE), Laplacian Mean Square Error (LMSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and Normalised Cross Correlation (NCC) are to be analyzed to observe the imperceptibility level of the watermarked medical image.