Medical Image Encryption using Two Dimensional Scan Approach

Rinkee Gupta, Jaipal Bisht, Amit Gupta

Abstract: This is Medical image encryption method where Medical image is encrypted by specific rule that is rearrangement of image pixels. In this paper, we present Medical Image encryption and decryption by two dimensional scan Approach. Scan language is based on spatial accessing methodology that can generate a wide range of scanning paths. This paper presents a overview of encryption and decryption algorithm, implemented in MATLAB environment and tested on various images.

Index Terms- Encryption, Decryption, Two Dimensional Scanning, Medical Image.

I. INTRODUCTION

Image Security is an important issue in communication and storage, and encryption is one the ways to ensure security. Image encryption has a wide range of applications in inter-net communication, multimedia systems, medical imaging, telemedicine, and military communication. There already exist several image encryption methods like SCAN-based methods, chaos-based methods, tree structure-based methods, and other miscellaneous methods. However, each of them has got their own strengths and weakness in terms of security level, speed, and stream size metrics. Hence, we now propose a new encryption method that would make an attempt to address the above mentioned problems.

The proposed image encryption method is based on rearrangement of the pixels of the image. The rearrangement is done by scan patterns that generated by the SCAN methodology. The scanning path of the image is a random code form, and by specifying the pixels sequence along the scanning path. Note that scanning path of an image is simply an order in which each pixel of the image is accessed exactly once. Such an encryption also involves the specification of set secret scanning paths. Therefore, the encryption needs a methodology to specify and generate a larger number of wide varieties of scanning paths effectively.

II. TWO DIMENSIONAL SCAN

The Scan is a formal language which is -based on two dimensional spatial accessing methodologies which can represent and generate a large number of wide varieties of scanning paths. The SCAN is a family of formal languages such as Simple Scan, Extended Scan, and Generalized Scan, each of which can represent and generate a specific set of scanning paths. Each Scan language is defined by a set of basic scan patterns; a set of partition patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns and transformations with scanning or partitioning.

A scanning of a two dimensional array \( P = \{p(i, j): 1 \leq i \leq x, 1 \leq j \leq y\} \) is a bijective function from \( P \) to the set \( \{1, 2, \ldots, pq\} \). In other world, a scanning of a two dimensional array is an order in which each element of the array is accessed exactly once. In this paper the terms scanning, scanning paths, scan pattern, and scan words are used interchangeably. Note that an \( pxq \) array has \( (pxq)! \) Scanning.

A. About Partition

There are three basic partition patterns that include

- B type partition patterns
- Z type partition patterns
- X type partition patterns
Each basic partition pattern has eight different transformations which depend on initial point and the final point.

**B. Scanning Pattern**

We have four basic scanning patterns namely,

- Continuous Raster C
- Continuous Diagonal D
- Continuous Orthogonal O
- Spiral S

All the above mentioned scanning patterns are clearly shown in figure 2.2.1.

---

**III. METHODOLOGY**

Since most images require different scanning in different subregions, the encryption specific SCAN language allows an image region to be recursively partitioned into four subregions, and each subregion to be scanned independently. When an image region is partitioned, the order in which the four subregions are scanned is specified by a partition pattern. The partition patterns are represented by letter B, letter Z, and letter X, each of which has eight transformations as previously mentioned.

Following by basic scan patterns and partition patterns to produce concept, we use a random code generating produce the SCAN word and to define encryption key. The SCAN word contain scan and partition patterns. The scan partition word has C0~C7, D0~D7, O0~O7 and S0~S7. The partition word has B0~B7, Z0~Z7 and X0~X7. This word separately has been done using special scanning paths and partition. Because the SCAN word has large variation, so we can attain encryption technology. A given image is encrypted by rearranging the pixel of the image using a set of scanning paths.
This paper proposed encryption key rules assume that maximum image size is 512×512. The partition institution least is 4×4 image size, then the least size done scan patterns. However, the scan patterns institution when the image not done partition. Late the 16×16 size image and the scanning path shown in Figure 1. The scanning path is corresponding to the SCAN word constructed as follows. The SCAN word defines encryption key can achieve encryption objective.

![Diagram of the scanning path](image-url)
IV. RESULT

The proposed encryption methodology was implemented in software using MATLAB 7.1 Figure 5.1 shows the 512 × 512 colour-scale Medical image. The process encryption image is compliance the encryption key. It is clear that the SCAN methodology image encryption and decryption achieves an excellent encryption. When execute

Fig 4.1 Encryption Image diagram

V. CONCLUSION

This method gives a lossless encryption of image. This also gives majority of variable lengths of the encryption keys. It has high execution speed. Another main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible. This Encryption uses only integer arithmetic and it can be easily implemented in the hardware.

REFERENCES


