**Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare**

**ABSTRACT**

There exists a rising concern on security of healthcare data and service. Even small lost, stolen, displaced, hacked, or communicated in personal health data could bring huge damage to patients. Therefore, we propose a novel content-aware deoxyribonucleic acid (DNA) computing system to encrypt medical images, thus guaranteeing privacy and promoting secure healthcare environment. The proposed system consists of sender and receiver to perform tasks of encryption and decryption, respectively, where both contain the same structure design, but perform opposite operations. In either sender or receiver, we design a randomly DNA encoding and a content-aware permutation and diffusion module. Considering introducing random mechanism to increase difficulty of cracking, the former module builds a random encryption rule selector in DNA encoding process by randomly mapping quantity of medical image pixels to outputs. Meanwhile, the latter module constructs a permutation sequence, which not only encodes information of pixel values, but also involves redundant correlation between adjacent pixels located in a patch. Such design brings awareness property of medical image content to greatly increase complexity in cracking by embedding semantically information for encryption. We demonstrate that the proposed system successfully improve cybersecurity of medical images against various attacks in robustness and effectiveness when transmitting data in wireless broadcasting scenarios

**Existing System**

In medical field all patient’s data like text or images (MRI, visual investigations) must be secure and easy to process as physicians are not technicians to apply heavy computation encryption algorithms to secure medical data. So they need more secure and less complicated algorithms for patient data security. In past many security algorithms were introduced such as AES, DES and many more but those algorithms are easy to hack and does not support random permutation or encodings. According to author images encrypted via Random number permutation are more secure as it’s difficult for the hackers to guess Random numbers to properly decode images.

**Disadvantages of Existing System:**

* Less Accuracy

**Proposed System**

In propose paper author generating PWLCM random value by applying SHA algorithm and then encoding images using DNA encoding which will encode each pixel values based on DNA rules. Each pixel will be divided between ACGT DNA encoding as each character has unique binary values like A is represented from 00 to 11 and C represents between 01 to 10 and if image pixel value falls between any DNA rules then that pixel will get replace with either A or C or G or T.After DNA encoding we will apply XOR operations on all DNA encoding with public key to encrypt images. Encrypted image will be send to user with public key and by applying reverse operations Receiver can decrypt the image.

**Advantages of Proposed System:**

* High Accuracy.

**SYSTEM REQUIREMENT:**

**HARDWARE REQUIREMENTS:**

# Processor - Intel i3(min)

* Speed - 1.1 GHz
* RAM - 4GB(min)
* Hard Disk - 500 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* Operating System - Windows10(min)
* Programming Language - Python