An Efficient Encryption Algorithm for 3D Medical Images

T.K. Senanayake*
Department of Physical Science, Faculty of Applied Science, University of Vavuniya, Sri Lanka

Abstract: With the rapid advancement of digital medical imaging technologies, the need to safeguard sensitive patient data has never been more critical. This thesis presents a robust software solution for the encryption of 3D medical images, focusing on two widely used formats: DICOM and NIfTI. The encryption algorithm developed in this research employs a multi-layered approach to ensure maximum data protection. The process begins with a permutation of the pixel values, disrupting the inherent spatial relationships within the image. This is followed by a scrambling technique, which further obscures the pixel arrangement. To add an additional layer of complexity, an XOR operation is applied, where pixel data is combined with a binary key. The final stage of encryption utilizes the Advanced Encryption Standard (AES), a globally trusted cryptographic method. This encryption framework has been rigorously tested to validate its effectiveness in maintaining the confidentiality and integrity of 3D medical images. Entropy analysis, NPCR, UACI, histogram analysis, and correlation analysis were employed to confirm the randomness, sensitivity, and security of the encrypted images. The results demonstrate that the software provides a high level of protection against unauthorized access and potential attacks. This solution is not only practical but also offers a significant enhancement to current security protocols used in healthcare systems for the transmission and storage of medical images.

Keywords: Medical image encryption, DICOM, NIfTI, 3D medical images, AES encryption

**Corresponding author's email: theshankavishka828@gmail.com*