Secure Transfer of Medical Images Using Hybrid Encryption Authentication, Confidentiality, Integrity

Authors : Boukhatem Mohammed Belkaid, Lahdir Mourad

Abstract : In this paper, we propose a new encryption system for security issues medical images. The hybrid encryption scheme is based on AES and RSA algorithms to validate the three security services are authentication, integrity, and confidentiality. Privacy is ensured by AES, authenticity is ensured by the RSA algorithm. Integrity is assured by the basic function of the correlation between adjacent pixels. Our system generates a unique password every new session of encryption, that will be used to encrypt each frame of the medical image basis to strengthen and ensure his safety. Several metrics have been used for various tests of our analysis. For the integrity test, we noticed the efficiencies of our system and how the imprint cryptographic changes at reception if a change affects the image in the transmission channel.

Keywords : AES, RSA, integrity, confidentiality, authentication, medical images, encryption, decryption, key, correlation
Conference Title : ICSIPPR 2015 : International Conference on Signal, Image Processing and Pattern Recognition
Conference Location : Paris, France
Conference Dates : February 23-24, 2015

Open Science Index, Electrical and Information Engineering Vol:9, No:02, 2015 publications.waset.org/abstracts/17879.pdf