MSG Image Encryption Based on AES and RSA Algorithms "MSG Image Security"

Authors : Boukhatem Mohammed Belkaid, Lahdir Mourad

Abstract : In this paper, we propose a new encryption system for security issues meteorological images from Meteosat Second Generation (MSG), which generates 12 images every 15 minutes. 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 15 minutes that will be used to encrypt each frame of the MSG meteorological 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, satellite MSG, encryption, decryption, key, correlation
Conference Title : ICSIE 2014 : International Conference on Signal and Image Engineering
Conference Location : London, United Kingdom
Conference Dates : November 28-29, 2014