Función de sustitución para AES en modo ECB para cifrado de imágenes

Marco Tulio Ramírez Torres[1], Luis Felipe De la Rosa García[1], Blanca Jazmín Espíndola Paizano[1], Juan Daniel González Del Rio[1] y Luis Javier Ontañón García Pimentel[1]

1 Coordinación Académica Región Altiplano Oeste, UASLP. tulio.torres@uaslp.mx

En la presente investigación se muestra una función de sustitución especializada en conjuntos de datos altamente redundantes, como pueden ser las imágenes digitales. El algoritmo de cifrado AES (Advanced Encryption Standard) en modo ECB (Electronic Code Book) presenta problemas de seguridad perceptual, debido a la alta correlación adyacente de los pixeles. La función descrita en esta investigación utiliza la sincronización de autómatas celulares en conjunto con un proceso de retroalimentación, esto permite obtener diferentes resultados ante mismos datos de entrada. Una vez procesada la imagen se puede cifrar con el código AES en modo ECB, superando los problemas de seguridad. Una de las ventajas es que en esta modalidad es posible paralelizar el proceso de cifrado.