Nº: 1	
Título del Artículo	Extended DSA
Revista y/o evento	Journal of Discrete Mathematical Sciences and Cryptography
Año	2019
Autores	Chen-Yu Lee, Wei-Shen Lai
Universidad o institución	Department of Computer Science National Chiao Tung University
Referencia APA	Chen-Yu Lee & Wei-Shen Lai (2008) Extended DSA, Journal of Discrete Mathematical Sciences and ryptography, 11:5, 545-550, DOI: 10.1080/09720529.2008.10698206

Palabras clave

Mesa, pesa, teclado

Resumen

El artículo habla de cómo con la ayuda de encriptación de imágenes a través del código BCH (Bose–Chaudhuri–Hocquenghem) y el algoritmo de firmas digitales podemos tanto encriptar como autenticar una imagen de cualquier resolución sin ningún problema, permitiendo que una imagen se envíe y sea correcto su contenido una vez se ha recibido.

Para la encriptación de la imagen se optó por el código BCH puesto que este algoritmo permite la flexibilidad en cuánto al tamaño de la imagen, es decir, al ser un algoritmo que codifica una imagen, y existen muchos diferentes tamaños de imagen, el código BCH se acopla y encripta la imagen de la mejor manera posible.

Para la generación de la firma digital se hace antes del encriptado y bit a bit, es decir, que al momento de verificar la autenticidad si existe algún tipo de alteración la firma digital fallará. De tal forma que, el proceso general de encriptación sigue los pasos de generar firma digital y encriptar y para desencriptar, desencripta y luego corrobora la firma digital.

Para poder corroborar las firmas digitales se hace por medio de la correlación entre las dos firmas generadas, una al encriptar y otra al desencriptar a través del pico de correlación que es una gráfica que debe tener un pico el cual debe ser exacto en su firma inicial y final, de lo contrario la imagen se alteró.

Los ensayos se hicieron sobre dos tipos de imágenes que tienen diferentes tamaños, de tal forma que, se puede decir que el tamaño no sería un problema.

Herramientas utilizadas

SHA-1 SHA-2 DSA Estándares del NIST para la generación de un DSA.

Comentarios

El artículo es interesante, debido a que en la actualidad podemos encontrar diferentes tipos de herramientas que pueden falsificar la veracidad de una imagen como herramientas de edición de imagen o inteligencias artificiales, lo que podrían alterar la autenticidad de la misma, por medio de este algoritmo podríamos hacerle un poco de contra a estas herramientas y nos aseguraríamos de que la información que envía por medio de imágenes es segura y confiable y no será alterada de ninguna forma y si lo llegase a estar seríamos notificados de ello, por lo que, no importa cuán bien edite una imagen, si su firma no corresponde, la autenticidad de la misma fue alterada, por ende, no debería considerar la imagen como algo válido por más que yo con mi criterio piense que no esté alterado.	
Valoración	3