Skema pembagian rahasia menggunakan matriks proyeksi dengan hasil diverifikasi = Verifiable secret sharing scheme using matrix projection

Nurfathiya Faradiena Az Zahra, author

Abstrak

Skema pembagian rahasia adalah teknik untuk membagi data rahasia menjadi n bagian dengan menggunakan threshold k, n, dimana partisipan dapat dengan mudah merekonstruksi rahasia jika diketahui minimum k bagian, tetapi pengetahuan dari k-1 bagian tidak dapat mengurai rahasia. Skema pembagian rahasia ini diperkenalkan oleh Shamir pada tahun 1979. Permasalahan pada skema pembagian rahasia Shamir adalah tidak tersedianya cara untuk melakukan verifikasi bahwa dealer terbukti jujur dalam membagikan rahasia, dan bagian dari rahasia terbukti valid, begitu juga dengan skema pembagian rahasia pada gambar yang diajukan oleh Thien dan Lin, atau metode konstruksi menggunakan matriks proyeksi yang dipublikasikan oleh Li Bai. Di sisi lain, sebuah protokol yang dikembangkan disebut skema pembagian rahasia yang diverifikasi memperbolehkan setiap partisipan melakukan validasi terhadap bagian rahasia yang diterima, untuk memastikan autentikasi dari rahasia. Sebuah gambar watermark berukuran m x m akan digunakan untuk menentukan akurasi dari gambar hasil rekonstruksi. Berdasarkan permasalahan di atas, pada skripsi ini akan dibahas skema pembagian rahasia yang diverifikasi, dimana matriks proyeksi digunakan untuk mengkonstruksi bagian rahasia dan matriks publik dari gambar watermark. Gambar rahasia akan direpresentasikan dalam sebuah matriks persegi, dan gambar watermark digunakan untuk autentikasi, dimana hasil rekonstruksi gambar watermark menjamin akurasi dari hasil rekonstruksi gambar rahasia.
.....Secret sharing scheme is a technique to share secret data into n pieces based on a simple k, n threshold scheme. Participants will easily reconstruct the secret if there are minimum k pieces, while knowledge of any k-1 pieces of shares will not be able to decipher the secret. This scheme is introduced by Shamir in 1979. The problem with Shamirs secret sharing scheme is the scheme do not provide any way to verify that the dealer is honest and the shares are indeed valid. Thien and Lin proposed image secret sharing in 2002, and Bai proposed construction scheme using matrix projection in 2006, but both of the schemes do not solve the existing problem. On the other hand, a developed protocol for secret sharing called verifiable secret sharing allows every participant to validate their received piece to confirm the authenticity of the secret. An m x m watermark image is used to verify the accuracy of the reconstructed image. Based on the explanation above, this thesis discuss a proposed scheme based on verifiable secret sharing, in which the matrix projection is used to create image shares and a public matrix from watermark image. The secret are represented as a square matrix, the watermark image is used for verifiability, where the reconstructed watermark image verifies the accuracy of reconstructed secret image.