

Keynote Speech Topic:

Sharing Secrets Using Authenticatable Digital Images

Abstract: Secret sharing is an important technique to ensure well protection of transmitted information by dividing a secret message into several shadows that are held among a set of participants. In this talk, I will introduce a novel secret sharing method using two meaningful digital images with cheating detection. It allows a dealer to share a secret message into two different meaningful images through the guidance of the turtle shell magic matrix. Then, after performing a permutation operation, two meaningful shadow images are generated and distributed to two participants. The secret message can be reconstructed only when both participants cooperate by releasing real shadow images. Honest participant in this method can easily detect whether the other participant is cheating via presenting a faked shadow. Experimental results show that this method ensures high quality of shadow images and good embedding capacity. The cheating detection process is also effective and very easy to implement.