Cryptology ePrint Archive: Report 2011/631

On the Security of a Cheating Immune Visual Secret Sharing Scheme

Yu-Chi Chen and Du-Shiau Tsai and Gwoboa Horng

Abstract: Visual Secret Sharing (VSS), first invented by Naor and Shamir, is a variant of secret sharing. In the literature, VSS schemes have many applications, including visual authentication and identification, steganography, and image encryption. Moreover, VSS schemes provide the secure services in communications. In 2010, De Prisco and De Santis deeply discussed the problem of cheating in VSS, gave the definition for deterministic cheating, and presented two cheating immune visual secret sharing schemes: 1) the simple scheme 2) the better scheme. However, we discover that the better scheme is not immune as they claimed. In this paper, we analyze this scheme is prone to deterministic cheating in theory and practice.

Category / Keywords: applications / Visual Cryptography, Visual Secret Sharing, Cheating, Cheating Prevention, Cheating Immune Scheme

Date: received 21 Nov 2011

Contact author: s9756034 at cs nchu edu tw