Abstract

In cryptography, the art of secret sharing, is to share among a group of selected few an individual share of the secret. Individual shares are of no use on their own. The multifaceted implementation of this scheme in literature including Shamir, Blakley and Asmuth-Bloom to name a few, has led to the emergence of higher computational complexity during both sharing and reconstruction and generates noise like shares. In order to come up with a meaningful sharing scheme, Lin and Tsai proposed a method that uses Steganography using Shamir’s secret sharing scheme; again which led to high computational complexity. Therefore, in order to overcome the above problem, a new scheme is suggested which deploys simple graphical masking, done by simply ANDing, value substitution for share generation and reconstruction can be done by value re-substitution and then ORing the qualified set of shares. Also, this proposed method finally creates, meaningful shares by using Steganography; instead of noise like shares.

References
5. Resch, Jason; Plank, James (February 15, 2011).
8. "Unvanish: Reconstructing Self-Destructing Data'

Index Terms

Computer Science

Security

Keywords
Secret Sharing, Steganography, Low computational complexity, High level encryption