Secure System Framework for Secure Visual Cryptography

Abstract

A visual cryptography scheme (VCS) is a secret sharing of secret image shares which involves dividing the secret image into number of shares and a certain number of shares are sent over the network. The decryption process involves stacking of the shares to get the secret image. The main advantage of visual cryptography scheme is that a number of qualified shares are able to recover the secret image without any cryptographic knowledge, calculation and computation devices. Simple Visual Cryptographic technique is not secure. Because simple visual cryptography scheme only deals with creation of secret share and just combined it at receiver side. In the proposed system we apply visual cryptography technique. The image is to be transferred on the network (also known as secret image) is first compressed and then hidden by cover image using LSB technique. To enhance security, additional security measures are applied further to get encrypted image using symmetric key algorithm. The shares are generated from the encrypted image using RNS (Residual Number System) algorithm. Next share stacking procedure is applied using CRT (Chinese Remainder Theorem) algorithm to get final encrypted image at receiver side. Further, decryption of final encrypted image is done by using same algorithm which is used for encryption purpose. By applying this technique security and quality of image is improved and pixel expansion problem will get reduced.
References

- Rajan Kumar, Prasanna Kumar, Sudeepa KB and Ganesh Aithal, "Enhanced security system using symmetric Encryption and visual cryptography", International Journal of Advances in Engineering Technology, July 2013.
- Roberto De Prisco, Alfredo De Santis, "Color visual cryptography schemes for black and white secret images", 2013 Elsevier B. V. All rights reserved.

Index Terms

Computer Science Security

Keywords