M.Venkatesh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 127-134 **ISSN: 2321-8363**

Security Analysis of Visual Secret Sharing Scheme

Mr.M.Venkatesh[1], Mr.S.Rajesh[2]

[1] PG Student, [2]Assistant Professor , Department of Computer Science and Engineering,

PRIST University, Trichy District, India

([1] m.venkat.trichy@gmail.com, [2] srajesh37@gmail.com)

Abstract

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be encrypted by the human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information.

It uses the characteristics of human vision to decrypt the encrypted images. For security, it also ensures that hackers cannot perceive any clues about secret image from individual cover images. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Various methods available they are gray level and color images based on studies in black-and-white visual cryptography, the halftone technology, and the color decomposition method. WS-VSS schemes for color images that reproduce clearer images with a smaller pixel expansion compared to US-VSS scheme.

Index Terms — Visual Cryptography, Multi-Secrete Sharing

Full Text: www.ijcsma.com/publications/january2014/V2I119.pdf