

Reversible Data Hiding with Multiple Secret Sharing Using Cryptography Approach

Mr. K. Jeeva¹, G. Dhanavarsha², K. Nanthini³

Assistant Professor, Department of Internet of Things¹

Students, Department of Information Technology^{2,3}

Dhanalakshmi Srinivasan University, Samayapuram, Thiruchirapalli, Tamilnadu, India

Abstract: Visual Cryptography (VC) is used to break an image into two random shares which when separately viewed reveals no information about the secret image. The secret image can be obtained by super imposing the two shares. Conventional visual cryptography scheme is used to encrypt a single image into n shares. The image can be decoded by using only shares. Many visual cryptographic methods use binary images only for this process. A sufficient condition to be satisfied by the encryption of MSS (Multiple Secret Sharing) schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of MSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate MSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation. The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an ECC based multi secret sharing is proposed to send secret information from the source to the destination in a secured way. The secret text was hidden within the image. The image is hidden inside an image using Modified LSB methodology. Then image is splitted into shares and encrypted using ECC method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. At the receiver end, the hidden data is extracted from the recovered image. Experimental results show that the dimensions of the original image and the recovered image are same.

Keywords: Visual Cryptography, Multi-Secret Sharing (MSS), Elliptic Curve Cryptography (ECC), Image Encryption, Secure Communication, Data Hiding, Cryptographic Security

