TELKOM UNIVERSITY

Abstract

School of Computing The Graduate School

Master of Engineering

Overcoming Alignment Problem on Non-Identical Mathematical Support Visual Cryptography Scheme

by Widhian Bramantya

In visual cryptography, each share needs to be aligned in right position by conducting some geometrical transformation such as translation and rotation so that the secret information appears. This alignment process is relatively hard to be aligned when the shares have small sub-pixel size. Beside that, the shares which have different mathematical support (i.e different shape, size, orientation, or reference coordinate), would take time equal to brute force without knowing position information for revealing secret information. The easiest way for handling the alignment problem in VCS is by adding the frames or special marks outside the shares. Unfortunately, this method weak against cropping or image editing. Another method was introduced by Liu, et al [1]. They modified basis matrices such that it is not necessary to align the shares precisely. The weakness of this method is that the modifying basis matrices makes the shares larger. Then, the time complexity is still high in non-identical mathematical support VCS since they have to search the proper position among the whole pixels. Based on those drawbacks, we propose alignment method without adding additional marks and also maintaining the pixel expansion. In this study, at least 3 points (called 3OP) inside the share are needed for finding the right position easier. In order to camouflaging the 3OP, Chameleon function is necessary by sharing and embedding the needed parameters inside the shares. The result of experiment shows that this method can overcome alignment problem in Non Identical Mathematical Support VCS and takes less time to stack the shares. In addition, the proposed method does not decrease the security of VCS.