UNIVERSITAS TELKOM

Abstrak

Fakultas Informatika
Sekolah Pascasarjana Teknik Informatika

Master Teknik Informatika

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

by Widhian Bramantya

Di dalam visual visual cryptography, share perlu ditumpuk dan disejajarkan pada posisi yang tepat dengan melakukan transformasi geometris seperti translasi dan rotasi untuk memunculkan suatu informasi rahasia. Proses penjajaran ini relatif sulit dilakukan ketika share mempunyai ukuran sub-pixel yang kecil. Disamping itu, share yang tidak identik secara matematis (i.e bentuk, ukuran, orientasi, arau koordinat acuan yang berbeda), akan memakan waktu yang lama (berdasarkan metode brute force) tanpa mengetahui informasi tentang posisi yang tepat. Cara yang paling mudah untuk menangani permasalahan penjajaran pada VCS adalah dengan menambahkan frame atau penanda khusus diluar share. Namun, metode ini rawan dengan pemotongan atau perubahan gambar. Metode lainnya telah diperkenalkan oleh Liu, dkk [1]. Mereka memodifikasi matriks dasar sedemikian rupa sehingga share tidak perlu disejajarkan dengan akurat. Kelemahan dari metode ini yaitu, perubahan matriks dasar yang semakin besar akan membuat share menjadi besar. Kemudian, kompleksitas waktunya masih tinggi jika diterapkan di share yang tidak identik, dikarenakan mereka harus mencari posisi yang benar satu per satu piksel dalam share. Berdasarkan kelemahan ini, kami membuat metode penjajaran tanpa menambah penanda khusus dan juga meminimalisir perbesaran matriks dasar. Pada penelitian ini, dibutuhkan setidaknya 3 titik (dinamakan 3-Orthogonal-Points atau 3OP) di dalam share untuk menemukan posisi yang tepat dengan mudah. Untuk menyembunyikan 3OP, kami menggunakan fungsi Chameleon untuk membagi parameter dan kemudian menanamkan parameter tersebut di setiap share. Hasil eksperimen menunjukkan bahwa metode ini dapat menyelesaikan permasalahan penjajaran di Non Identical Mathematical Support VCS dan memakan waktu yang lebih singkat untuk mendekode share tersebut. Selain itu, metode yang kami usulkan juga tidak mengurangi keamanan dari VCS itu sendiri.