ABSTRAK

Ketika penggunaan komunikasi gambar telah meningkat secara dramatis dalam beberapa tahun terakhir, itu diperlukan untuk melindungi transmisi dari penyadap. Mengembangkan komputasi efisien enkripsi gambar dan dekripsi algoritma adalah salah satu tantangan besar dalam keamanan data. Enkripsi gambar berbeda dari enkripsi teks karena beberapa sifat intrinsik dari gambar seperti kapasitas data curah dan redundansi tinggi, yang umumnya sulit untuk menangani dengan menggunakan teknik tradisional. Selain itu, banyak teknik tradisional menggunakan kunci rahasia panjang yang mungkin sulit pengguna untuk mengingat dengan pasti. Dalam tesis ini, skema enkripsi gambar selektif diubah diusulkan dalam rangka meningkatkan waktu enkripsi.

Dalam skema yang diusulkan, itu terdiri dari dua bagian: segmentasi citra dan enkripsi gambar. Segmentasi citra menggunakan teknik potong Grafik iterasi sectional yang menghemat waktu hingga 85% dibandingkan dengan segmentasi citra berulang konvensional. Dalam gambar langkah enkripsi, algoritma menggunakan peta logistik untuk menghasilkan aliran kunci dan Linear Congruential Generator (LCGS) untuk semu nomor acak dalam rangka meningkatkan keamanan gambar terenkripsi.

Tanpa menggunakan kunci eksternal yang panjang, proses enkripsi gambar yang diusulkan dapat menghasilkan gambar berebut benar. Meski menggunakan tiga saluran di enkripsi gambar, konsumsi saat enkripsi dimodifikasi rendah karena tidak ada proses lingkaran.

Selain itu, melakukan kebalikan dari proses enkripsi, dapat memulihkan citra didekripsi identik. Hasil eksperimen skema enkripsi gambar selektif diusulkan menunjukkan bahwa enkripsi hanya wilayah ROI enkripsi gambar parsial lebih efektif dan mengurangi waktu komputasi. Sensitivitas parameter kunci sangat tinggi karena gambar terenkripsi dapat kembali ke gambar asli hanya jika proses dekripsi menggunakan kunci dekripsi yang benar. Meskipun waktu eksekusi dari biaya skema yang diusulkan lebih tinggi dari teknik blowfish dan AES, itu adalah optimal dibandingkan dengan RSA dan ElGamal teknik. Selain itu, bisa melawan serangan diferensial, serangan statistik dan serangan kekerasan.

Kata kunci: sectional segmentasi citra iterasi menggunakan Grafik dipotong, pembangkitan kunci menggunakan peta logistik, metode nomor acak semu menggunakan LCGS, keamanan kinerja yang baik dan waktu proses yang sesuai.

ABSTRACT

When the use of image communication has increased dramatically in recent years, it is needed to protect the transmission from eavesdroppers. Developing a computationally efficient image encryption and decryption algorithms is one of the great challenges in data security. Image encryption is different from text encryption due to some intrinsic properties of images such as bulk data capacity and high redundancy, which is generally difficult to handle by using traditional techniques. Moreover, many traditional techniques used the long secret keys which may be difficult the user to remember with certainty. In the present thesis, the modified selective image encryption scheme is proposed in order to improve the encryption time.

In the proposed scheme, it consists of two parts: image segmentation and image encryption. Image segmentation uses sectional iterated Graph cut technique which saves time up to 85% compared to the conventional iterative image segmentation. In image encryption step, the algorithm uses a logistic map to generate key streams and a Linear Congruential Generator (LCGs) for pseudo random number in order to improve the security of the encrypted image.

Without using the long external key, the proposed image encryption process can generate the scramble image completely. Although using three channels in image encryption, time consumption of the modified encryption is low because of no loop process. Moreover, doing the reverse of the encrypted process, it can recover the identical decrypted image. The experimental results of the proposed selective image encryption scheme indicate that encryption only ROI region as partial image encryption is more effective and reduce the computation time. The sensitivity of key parameter is very high because the encrypted image can return to the original image only if the decryption process use the correct decryption key. Although the execution time of the proposed scheme higher cost than blowfish and AES techniques, it is optimal compared with RSA and ElGamal

techniques. Moreover, it can against the differential attack, statistical attack and brute force attack.

Keywords: sectional iterated image segmentation using Graph cut, key generation using logistic map, the pseudo random number method using LCGs, good performance security and suitable processing time.