Pengembangan dan analisis metode permutasi chaotic baru berbasis multiputaran mengecil dan membesar untuk enkripsi citra dengan tingkat keamanan tinggi, cepat, dan tahan terhadap gangguan = Development and analysis of a new shrinking and expanding multiple circular based chaotic permutation to enable a fast secure and robust image encryption

Yohan Suryanto, author

Abstrak

ABSTRAK
Perkembangan komputer kuantum, M2M, dan IoT meningkatkan kebutuhan ruang kunci sistem enkripsi. Selain itu, pertukaran citra menggunakan media sosial dalam jaringan non error free menuntut adanya metode enkripsi yang cepat sekaligus tahan terhadap gangguan. Peta chaotic memiliki karakteristik yang sesuai untuk enkrispi citra. Namun, peta chaotic yang ada menghadapi masalah discretization yang membuat ruang kunci dari peta chaotic terbatas dalam domain digital. Dalam disertasi ini, diusulkan sebuah metode permutasi chaotic yang bebas dari masalah discretization sehingga memiliki ruang kunci yang sangat besar yaitu sebesar faktorial dari jumlah elemen yang terlibat dalam permutasi. Metode permutasi chaotic yang diusulkan diuji kesesuaiannya terhadap properti chaotic. Metode yang diusulkan memiliki sifat mixing dan Ergodicity dengan distribusi luaran yang merata dan tidak tergantung dari kunci yang digunakan. Implementasi permutasi chaotic multiputaran mengecil dan membesar PCMPK/B yang diusulkan, ketika diimplementasikan dalam enkripsi citra, menghasilkan enkripsi citra dengan tingkat keamanan yang tinggi, cepat, sekaligus tahan terhadap gangguan. Citra dengan ukuran piksel mxn piksel dienkripsi dalam n set kolom and m set baris menggunakan PCMPK. Metode yang diusulkan memiliki ruang kunci yang sangat besar, yaitu untuk citra berukuran 256x256 piksel ruang kuncinya mencapai 2862208, yang merupakan ruang kunci terbesar yang pernah dicatat untuk enkripsi citra dengan ukuran 256x256 piksel. Metode yang diusulkan sangat sensitif terhadap perubahan kunci sehingga perubahan 1 bit diantara 21684 kemungkinan kunci inisial yang tersedia menyebabkan citra teracak berbeda signifikan untuk citra peppers NPCR 99.65 , UACI 33.35, dan korelasi < 0.008 . Berdasarkan hasil analisis statistik histogram, korelasi, dan entropi dan analisis diferensial, metode yang diusulkan tahan terhadap analisis statistik dan diferensial. Perubahan 1 bit pada citra asli menyebabkan perubahan yang signifikan pada citra teracak untuk citra Lena NPCR 99.60 dan UACI 33.47 . Metode yang diusulkan juga tahan terhadap kompresi jpeg, noise Gaussian noise, Poisson noise, Salt and Pepper noise, dan speckle , data loss, dan brightness contrast adjustment, sehingga citra teracak bisa disimpan dalam format lebih kecil dan ditransmisikan dalam sistem komunikasi non error free. Selain itu, peningkatan metode enkripsi citra yang diusulkan juga memiliki waktu proses yang paling cepat dibandingkan dengan metode enkripsi yang memiliki ruang kunci > 2256 yang disusulkan oleh Hsiao, Wu, dan Parvin. Metode permutasi chaotic yang diusulkan juga diimplementasikan sebagai basis Chaotic Encryption System CES dan dibandingkan performansinya terhadap AES. Hasil uji menunjukkan CES lebih efisien dibandingkan dengan AES. Baik CES maupun AES lolos semua kriteria uji kerandoman NIST Randomness Test, namun CES menunjukkan hasil uji diffusion dan confussion yang lebih baik. Dalam uji diffusion, CES memiliki nilai korelasi lebih rendah dari 0,04 sementara dalam AES lebih besar dari 0,05.

Dalam uji confussion, CES memiliki nilai korelasi lebih rendah dari 0,08 sementara dalam AES lebih besar dari 0,1. Implementasi metode enkripsi CES dalam SoC Xilinx Zynq 7000 juga menunjukkan jumlah cycle per elemen yang lebih efisien dibandingkan dengan AES.
<hr />
ABSTRACT
The advancement of the quantum komputers, M2M and IoT increases the key space requirement of an encryption system. In addition, the exchange of images using social media in a non error free network, requires a relatifly fast encryption methods, as well as robust to the noises. Chaotic map has excellent characteristics for the image encryption. However, existing chaotic maps has dicretization problems that the key space reduce dramatically in the digital domain. In this doctoral thesis, we propose a chaotic permutation method that is free from the discretization problem and hence having the very large key space. The proposed chaotic permutation is tested against the chaotic properties. It complies to the mixing and Ergodicity properties, such that the tranformation result has a uniform distribution, independent to the initial condition or parameter. The proposed image encryption based on the Shrinking and Expanding Multiple Circular Chaotic Permutation has three importance characteristics that are fast, secure, and robust to noise. An image with the mxn pixels size is encrypted in n set column and m set row using the multiple circular chaotic permutation method. The proposed method characterized by a very large key space, such that for an image size of 256x256 pixels, the key space reaches 2862208 which is the largest key space ever recorded in the image encryption. It is sensitive to the changes in key, so that 1 bit change in initial key among 21684 possibilities is likely to produce a significant different ciphered images for image peppers NPCR 99.65 , UACI 33.35, r