Algoritma baru enkripsi video dengan menggunakan multi chaotic cipher berbasis galois field 256 dan transformasi cosinus diskrit terkuantisasi = A new video encryption algorithm using multi chaotic cipher based on galois field 256 and quantized discrete cosine transform

Suryadi, author

Abstrak

Algoritma baru enkripsi data video yang dikembangkan dalam disertasi ini dinamakan algoritma enkripsi video multi chaos system oleh Suryadi, B. Budiardjo dan K. Ramli (MCS-SBR). Algoritma tersebut ditujukan untuk mereduksi waktu komputasi, rasio kompresi dan untuk meningkatkan daya tahan terhadap known-plaintext attack dan brute-force attack. Usaha yang dilakukan adalah dengan mengintegrasikan dua proses yakni proses kompresi dan dilanjutkan dengan proses enkripsi. Metode proses kompresinya yaitu menggabungkan proses transformasi cosinus diskrit (DCT) dan proses kuantisasi. Hal ini dapat dilakukan karena secara aljabar, DCT terkuantisasi tetap memiliki sifat orthonormal, sama halnya dengan fungsi DCT standar. Sedangkan untuk proses enkripsinya menggunakan metode multi chaos system terdiri dari dua fungsi chaos, yaitu logistic map dan Arnold?s cat map. Masing-masing bertujuan sebagai fungsi pembangkit bilangan acak untuk mendapatkan nilai key stream dan sebagai permutasi acak. Dalam hal ini digunakan 3 buah logistic map dengan satu formula key stream dalam basis galois field (256) sehingga mampu meningkatkan daya tahan terhadap known-plaintext attack dan brute-force attack. Selanjutnya dilakukan pengujian secara praktis dan teoritis.

Hasil analisis pengujian secara praktis menunjukkan bahwa kompleksitas waktunya semakin kecil sehingga ratarata waktu kompresinya semakin cepat, rata-rata prosentase rasio kompresinya 2,35 kali lebih besar, ruang kunci yang dihasilkan mencapai 8,6  1012 kali lebih besar, dan tingkat sensitivitasnya menjadi 2  10−10 lebih kecil, serta bentuk histogramnya mendekati bentuk flat. Hasil pengujian teoritis berstandar internasional dari National Institute of Standards and Technology (NIST), menunjukkan bahwa fungsi pembangkit bilangan acaknya benar-benar menghasilkan bilangan bersifat acak, yang ditunjukkan dengan nilai 𝑃. 𝑣𝑎𝑙𝑢𝑒 = 0,43277 ≥ 0,01. Berdasarkan semua hasil pengujian tersebut, dapat disimpulkan bahwa algoritma enkripsi video MCS-SBR sangat sulit dipecahkan dengan known-plaintext attack dan brute-force attack.

.....

The new video encryption algorithm discussed in this dissertation is called Multi Chaos System developed by Suryadi, B. Budiardjo and K. Ramli (MCS-SBR). This algorithm is used to reduce the computational time and compression ratio, as well as to increase resistance to known-plaintext attack brute-force attack. The procedures included the integration of two processes, i.e. compression process followed by encryption processes. The method of compression process employed the integration of discrete cosine transform (DCT) and quantization process. This was possible from algebraic perspective as quantized DCT still retained its orthonormal characteristic, just as standard DCT function. As for the encryption process, multi chaos system, consisting of logistic map and Arnold?s cat map, was used. Each of these functioned as random number generation to get a key stream and random permutation respectively. For this purpose, 3 logistic map were used with one key stream formula based on Galois field (256) in order to increase resistance to

known-plaintext attack and brute-force attack. The subsequent procedures included practical examination and theoretical evaluation.
The results of the practical examination are as follow: the average time complexity is reduced, which increases the compression time; the average percentage of the compression ratio is 2,35 higher; the resulted key space is 8,6  1012 greater; the sensitivity level is 2  10−10 lower; and the histogram is almost flat. The result of theoretical evaluation by National Institute of Standards and Technology (NIST) indicates that the function of random number generator really produces random numbers, shown by 𝑃. 𝑣𝑎𝑙𝑢𝑒 = 0,43277 ≥ 0,01. Based on the results of the practical examination and theoretical evaluation, it can be concluded that the algorithm of MCS-SBR video encryption is highly resistant to known-plaintext attack and brute-force attack.