Enkripsi citra digital dengan skema permutasi dan difusi menggunakan MS Map = Digital image encryption with permutation and diffusion schemes using MS Map

Priya Arif Abdul Azis, author

Abstrak

Dengan perkembangan teknologi, diperlukan perlindungan terhadap data digital untuk menghindari manipulasi dan perubahan data. Dalam penelitian ini, dilakukan pengamanan data digital berupa citra digital dengan teknik kriptografi (enkripsi dan dekripsi). Proses enkripsi dan dekripsi menggunakan fungsi chaos MS map dengan melakukan dua skema yaitu skema permutasi dan skema difusi secara berurutan sehingga dibutuhkan keystream untuk masing-masing skema yaitu keystream permutasi dan keystream difusi yang dilanjutkan dengan operasi XOR terhadap masing-masing piksel citra digital.
Hasil uji coba dan analisis, menunjukkan rata-rata waktu proses enkripsi relatif sama dengan proses dekripsi, tingkat sensitivitas keystream mencapai 10-17 untuk nilai awal 0 dan 1016 untuk parameter r dan, keystream yang dibangkitkan merupakan barisan acak karena lulus uji NIST, citra terdekripsi berdistribusi uniform karena histogram berbentuk flat, citra terenkripsi sama dengan citra asli ditunjukkan dengan nilai PSNR = dan piksel-piksel citra terenkripsi tidak korelasi. Maka algoritma enkripsi yang dikembangkan dengan menggunakan MS map berskema permutasi dan difusi tahan terhadap serangan bruteforce attack, statistical attack, dan diferensial attack.
.....
With the development of technology, protection of digital data is needed to avoid data manipulation and change. In this study, digital data security will be carried out in the form of digital images with cryptographic techniques (encryption and decryption). The process of encryption and decryption uses the chaos MS map function by carrying out two schemes, namely permutation schemes and sequential diffusion schemes so that each sequence is needed for permutation and diffusion parameters, which will be XORed against each pixel of the digital image.
Trial and analysis results show that the average encryption process time is relatively the same as the decryption process, the keystream sensitivity level reaches 1017 for the initial values 0 and 1016 for parameters r and, keystream the generated is a random sequence because it passed the NIST test, the decrypted image is uniformly distributed because the histogram is flat, the encrypted image with the original image is indicated by the value of PSNR = and the pixels of the encrypted image are not correlated. Then the encryption algorithm developed using MS map with permutation and diffusion schemes is resistant to bruteforce attack, statistical attack, and differential attacks.