INTISARI

PENGEMBANGAN *TRUE RANDOM NUMBER GENERATOR* BERBASIS CITRA MENGGUNAKAN ALGORITME KAOTIS

Dian Arief Risdianto
14/369609/PA/16395

Keamanan sebagian besar sistem kriptografi bergantung pada *key generation* yang tidak dapat diprediksi menggunakan *Random Number Generator* yang nondeterministik. PRNG (Pseudorandom Number Generator) menghasilkan deret random number dengan pola berulang dalam jangka waktu tertentu dan dapat diprediksi jika kondisi awal dan algoritme diketahui. TRNG (True Random Number Generator) mengekstrak entropi dari sumber fisik yang tidak dapat diprediksi untuk menghasilkan bilangan acak yang nondeterministik. Namun, sebagian besar sistem tersebut memiliki biaya, kompleksitas, dan tingkat kesulitan yang relatif tinggi. Jika kamera diarahkan pada adegan yang acak, deret *random number* yang dihasilkan dapat diasumsikan acak pula. Namun, kerugian kamera digital sebagai sumber angka acak terletak pada pola bias yang dihasilkan. Deret *raw* tanpa pemrosesan lebih lanjut dapat memiliki pola *noise* yang tetap. Dengan menerapkan pengolahan citra digital dan juga algoritme kaotis, kamera digital dapat digunakan untuk menghasilkan *true random number*. Dalam penelitian ini, untuk *preprocessing* data citra digunakan metode algoritme *floyd-steinberg*. Untuk menyelesaikan masalah terdapatnya beberapa piksel hitam atau putih berurutan yang muncul di area citra yang diproses, digunakan algoritme *arnold-cat map* sedangkan operasi XOR digunakan untuk mengkombinasi data dan membangkitkan *true random number*. Pengujian statistik NIST, analisis *scatterplot* dan histrogram menunjukan penggunaan metode ini mampu menghasilkan *true random number* yang benar-benar acak.

Kata kunci—*TRNG, PRNG, Arnold's Map, Floyd-Steinberg*

ABSTRACT

DEVELOPMENT OF TRUE RANDOM NUMBER GENERATOR BASED ON IMAGE WITH CHAOTIC ALGORITHM

Dian Arief Risdianto
14/369609/PA/16395

The security of most cryptographic systems depends on key generation using a nondeterministic RNG. PRNG generates a random numbers with repeatable patterns over a period of time and can be predicted if the initial conditions and algorithms are known. TRNG extracts entropy from physical sources to generate random numbers. However, most of these systems have relatively high cost, complexity, and difficulty levels. If the camera is directed to a random scene, the resulting random number can be assumed to be random. However, the weakness of a digital camera as a source of random numbers lies in the resulting refractive pattern. The raw data without further processing can have a fixed noise pattern. By applying digital image processing and chaotic algorithms, digital cameras can be used to generate true random numbers. In this research, for preprocessing image data used method of floyd-steinberg algorithm. To solve the problem of several consecutive black or white pixels appearing in the processed image area, the arnold-cat map algorithm is used while the XOR operation is used to combine the data and generate the true random number. NIST statistical tests, scatter and histrogram analyzes show the use of this method can produce truly random numbers.

Keywords— *TRNG, PRNG, Arnold's Map, Floyd-Steinberg*