Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (cz. 1)

Data oddania: 12.04.2021

Wykonali:
Tomasz Wołoszyn Patryk Resler

Podstawa opracowania:
Liang Zhao, Xiaofeng Liao, Di Xiao, Tao Xiang, Qing Zhou, Shukai Duan. „True random number generation from mobile telephone photo based on chaotic cryptography”

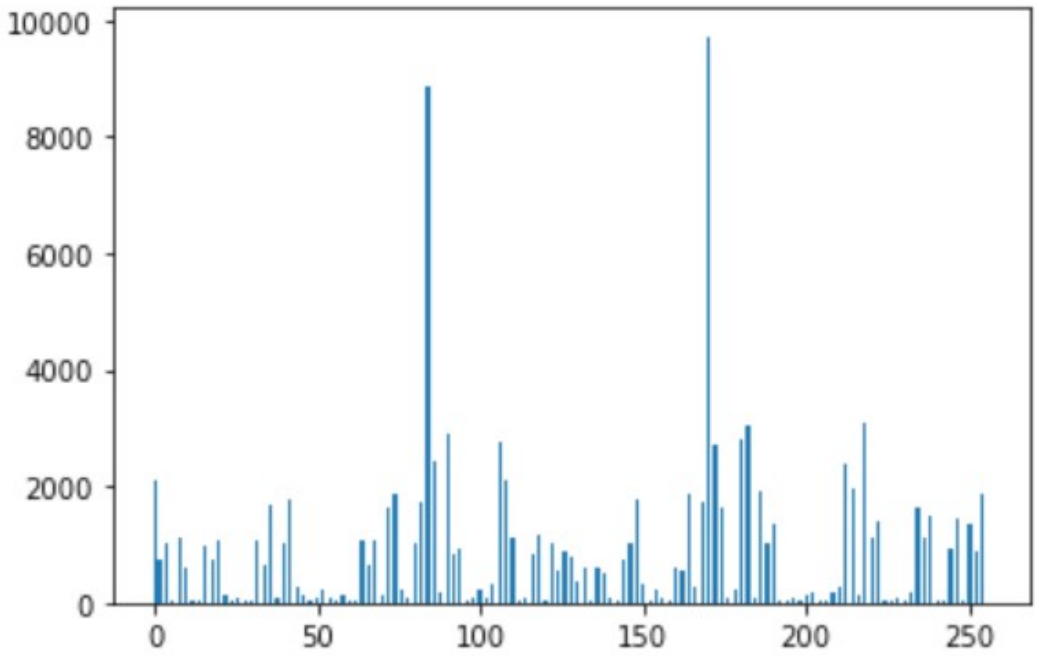
Systematyczny przegląd literatury:

1. Artykuł znaleziony w bazie danych Sciencedirect,
2. Słowa kluczowe: TRNG, Image, Chaos Map, PC,
3. Okres publikacji: 2009 - 2020,
4. Kilka metod implementacji,
5. Przedstawiony wzór.

Analiza źródła entropii:

Algorytm wykorzystuje zdjęcia w celu tworzenia 8 – bitowych sekwencji, które tworzone są z wartości binarnej 0 lub 1 w zależności od występowania piksela na obrazku binarnym 512x512 (kolor szary). Z 3 zdjęć wyciągamy 112347 próbek 8 bitowych.

Histogram zmiennych losowych generowanych przez źródło szumu



Entropia wyliczona zgodnie ze wzorem e = $\sum i\ pi\ log2\ (pi)$ dla powyższego rozkładu wynosi 5,95764

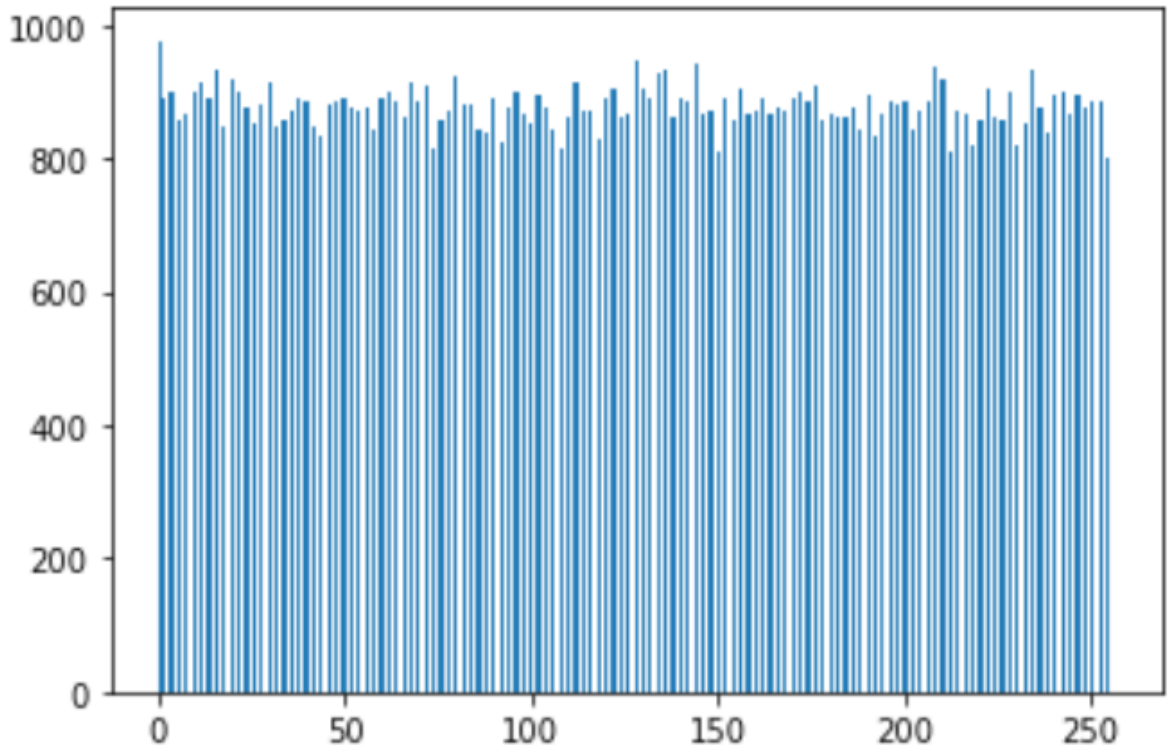
Metoda poprawy właściwości statystycznych:

Wykorzystana metoda zwana „Arnold cat map” (Metoda 3.1 z artykułu), polega na wytworzeniu mapy chaotycznej 2D wyrażonej wzorem :

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

Zmienne p oraz q to dodatnie integery, ich wartości to p=1, q=1 wykorzystane jako sekretny klucz. Zmienna N ustawiona na 512. Oryginalny obraz binarny jest iterowany 7 razy, dzięki czemu uzyskujemy wiarygodną losowość.

Histogram zmiennych losowych generowanych po post-processingu



Entropia wyliczona zgodnie ze wzorem e = $\sum i\ pi\ log2\ (pi)$ dla powyższego rozkładu wynosi 6,99914

Bibliografia:

- Artykuł: Liang Zhao, Xiaofeng Liao, Di Xiao, Tao Xiang, Qing Zhou, Shukai DuanTrue random number generation from mobile telephone photo based on chaotic cryptography
- Artykuł: Xiao D, Liao X, Deng S. One-way Hash function construction based on the chaotic map with changeable-parameter. Chaos, Soliton and Fractals 2005;24(1):65–71.
- Artykuł: Chen G, Chen Y, Liao X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. Chaos, Solitons and Fractals 2007;31(3):571–9.
- Dokumentacja Numpy i Scipy
- Dokumentacja PILLOW