Generator Liczb Losowych

Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (cz. 1)

Wykonali:

Waldemar Wagner, Krystian Tworzewski

Data oddania:

15.04.2021 r.

Podstawa opracowania:

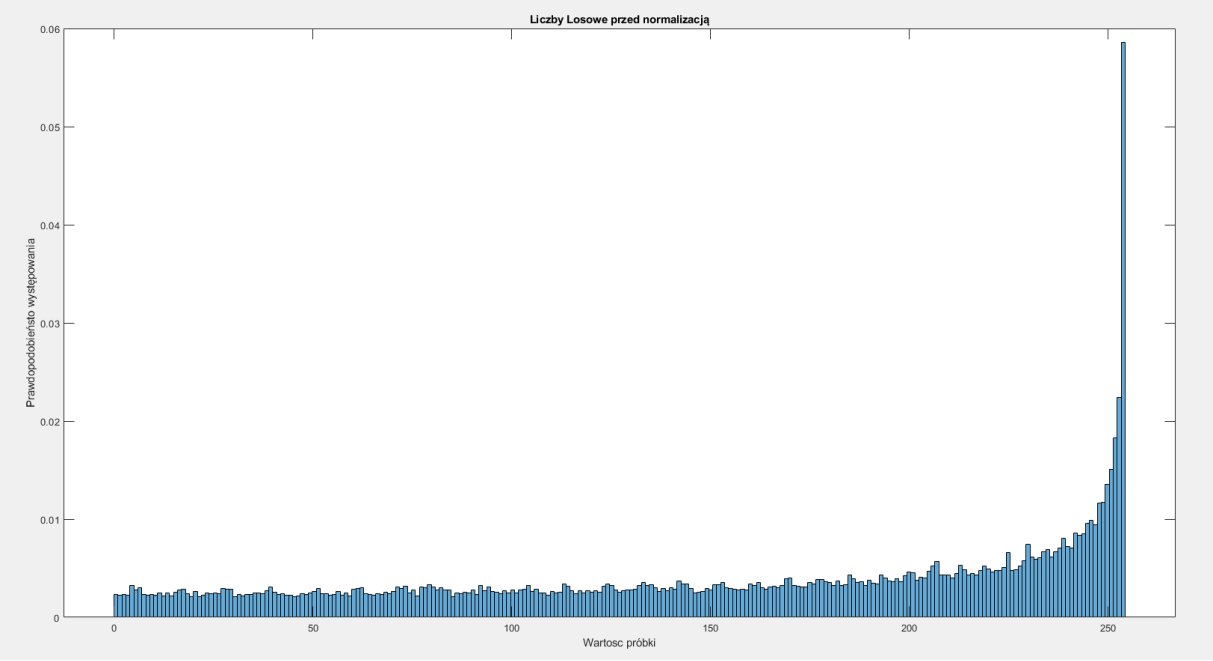
H. Zhu , C. Zhao , X. Zhang , L. Yang, „A novel iris and chaos-based random number generator", Computers & Security, vol. 36, pp. 40-48, July 2013.

Systematyczny przegląd literatury:

1. baza danych ScienceDirect Journals,
2. Słowa kluczowe: TRNG, PC, NIST, chaotic function,
3. okres publikacji: 2010-2020,
4. post-processing,
5. spełnione testy NIST

Analiza źródła entropii:

Do stworzenia generatora liczb losowych została wykorzystana cecha różnorodności i nieprzewidywalności tęczówki ludzkiego oka. Na zdjęcie tęczówki oka zostały nałożony algorytm wykrywania krawędzi o nazwie „Canny edge detector". Wykorzystane zostało położenie wcześniej wykrytych krawędzi do wygenerowania współrzędnych punktów, które zostały poddane działaniu funkcji matematycznej.

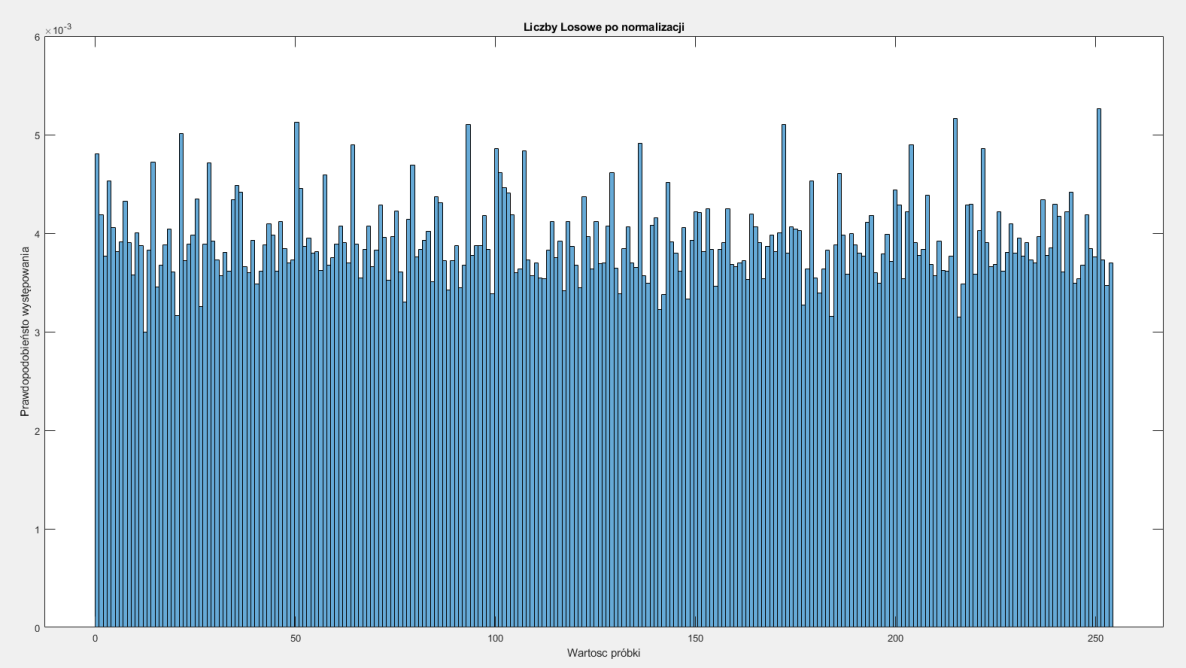


Entropia wyliczona zgodnie ze wzorem: $e = -\sum i\ pi\ log2\ (pi\ )$, dla powyższego rozkładu wynosi 7.6539 bita.

Metoda poprawy właściwości statystycznych:

Aby zebrane dane stały się prawdziwie losowe używana jest funkcja chaotyczna $x_n = f(a_n, b_n) = \cos(a_n \, x \, b_n)$, gdzie (a_n, b_n) to współrzędne punktu o wartości „1" na obrazie po detekcji krawędzi. Aby sekwencja losowa była bardziej równomierna używamy funkcji $y_n = \frac{1}{\pi}\arccos(x)$.

Wylosowane liczby są z przedziału [0;1], więc każda z nich została pomnożona przez 255 i zaokrąglona do wartości całkowitej, aby uzyskane liczby były 8-bitowe.



Entropia wyliczona zgodnie ze wzorem: $e = -\sum i \; pi \; log2 \; (pi \;)$, dla powyższego rozkładu wynosi 7.9871 bita.

Uwagi:

1. Zdjęcie używane w generatorze powinno być dobrej jakości, a także w skali szarości aby uzyskać jak największą liczbę krawędzi, co wiąże się potem z liczbą uzyskach liczb.
2. W celu wygenerowania 100 tyś. liczb losowych zostało użyte 8 zdjęć i czas generowania wyniósł 8 sekund. Dla miliona liczb ten czas wynosił około 63 sekund i wykorzystane zostało 80 zdjęć.
3. Najwięcej czasu potrzebnego do wygenerowania liczb wykorzystuje algorytm detekcji krawędzi (98% czasu).
4. Kod programu i potrzebne pliki dostępne są pod linkiem: https://github.com/skrb7/Bezpieczenstwo-Systemow-Teleinformatycznych