Raport

Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (c. 1)

Wykonali:	**Data Oddania:**
Marcin Cichowski, Jacek Kwieciński	18.04.2021r.

Podstawa opracowania:

Wang Xing-yuan, “Random Numbers Generated from Audio and Video Sources”, Mathematical Problems in Engineering Volume 2013, Article ID 285373, 7 pages

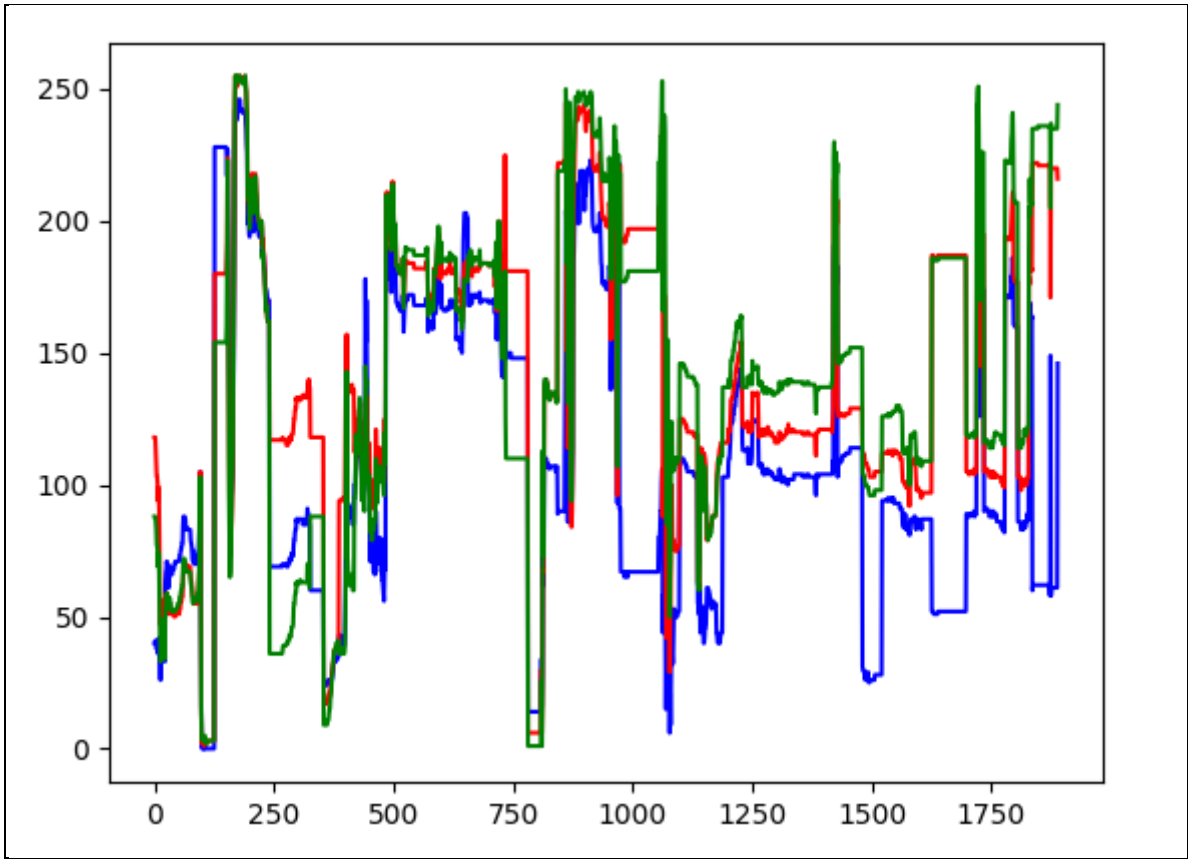
---

Systematyczny przegląd literatury:

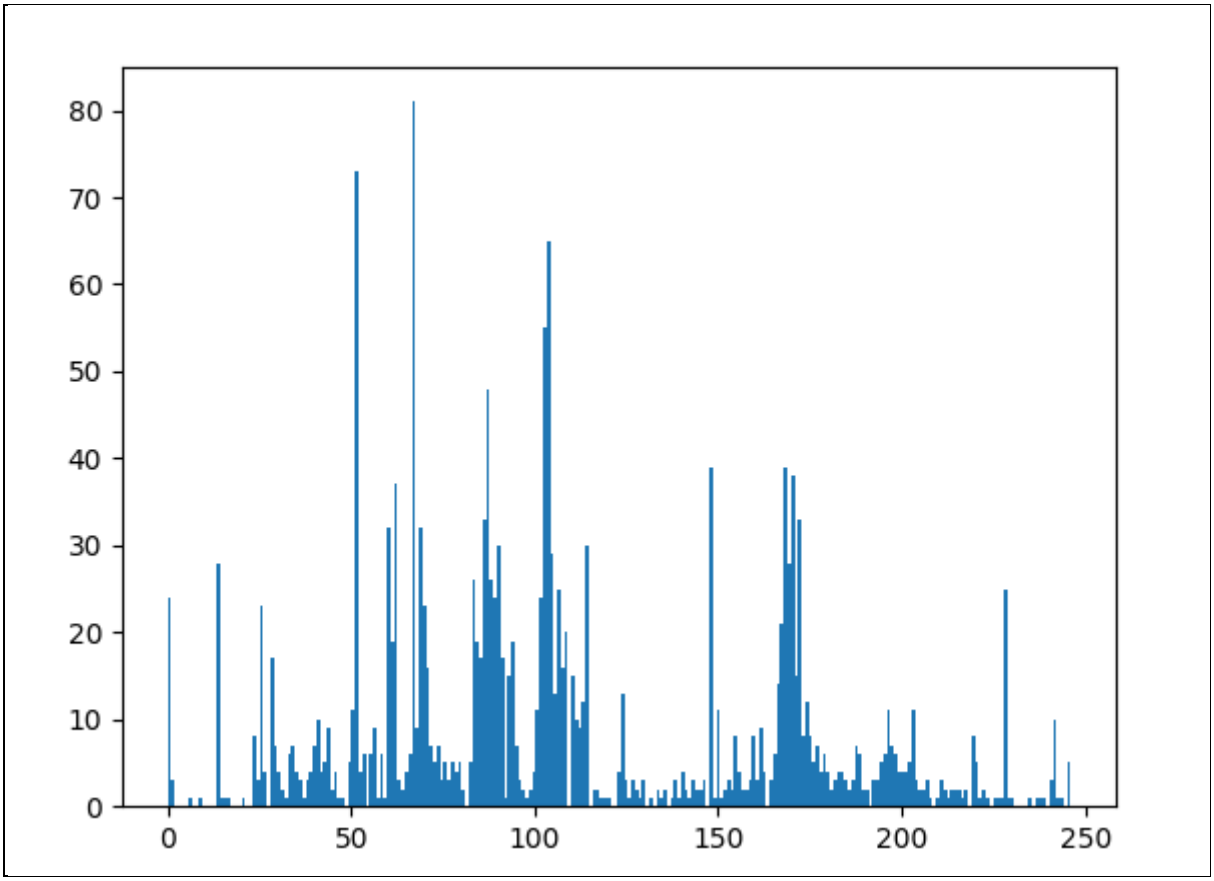
1. Baza danych Biblioteki Politechniki Poznańskiej,
2. Słowa kluczowe: TRNG, Audio, Video, NIST
3. Okres publikacji: 2010-2020,
4. Zdefiniowany pseudokod algorytmu
5. Spełniane testy NIST

Analiza źródła entropii:

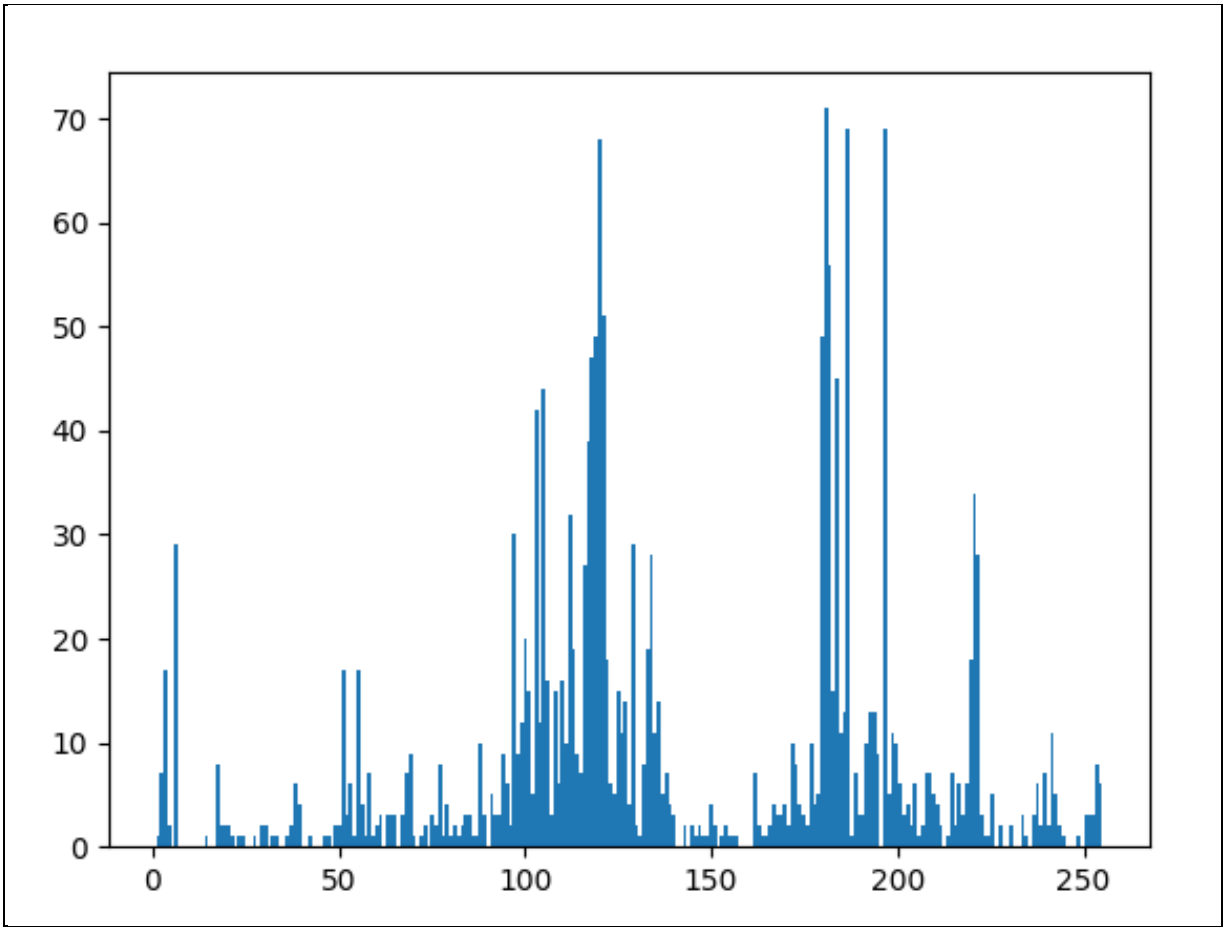
Algorytm jako źródła wykorzystuje informacje o barwie danego punktu klatki wideo zawartej wysokiej rozdzielczości pliku MP4 oraz próbki z uprzednio przygotowanego pliku dźwiękowego WAV wykonywane z częstotliwością 48KHz. Próbki dźwięku ograniczono do pięciu na każde 500 bitów pobranych z pliku audio.



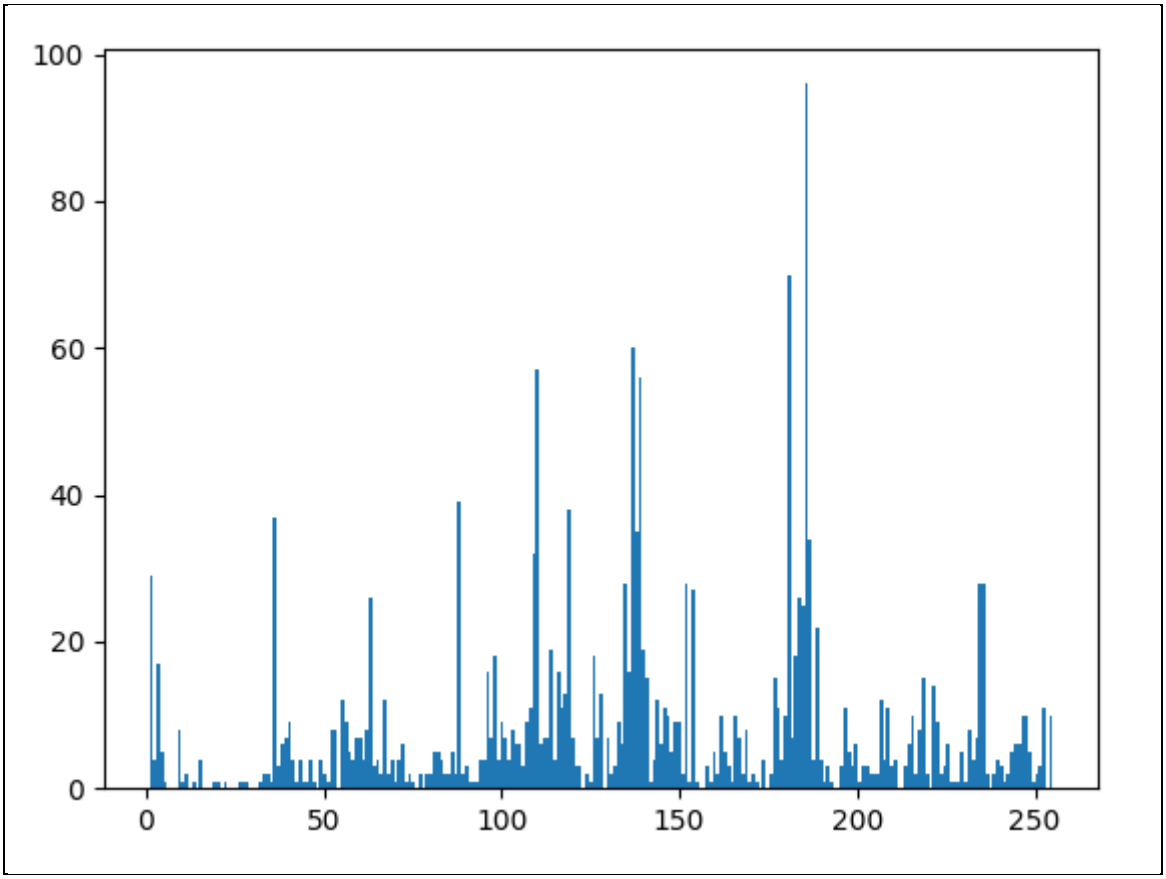
Rys1. Wykres wartości RGB w pliku wejściowym.



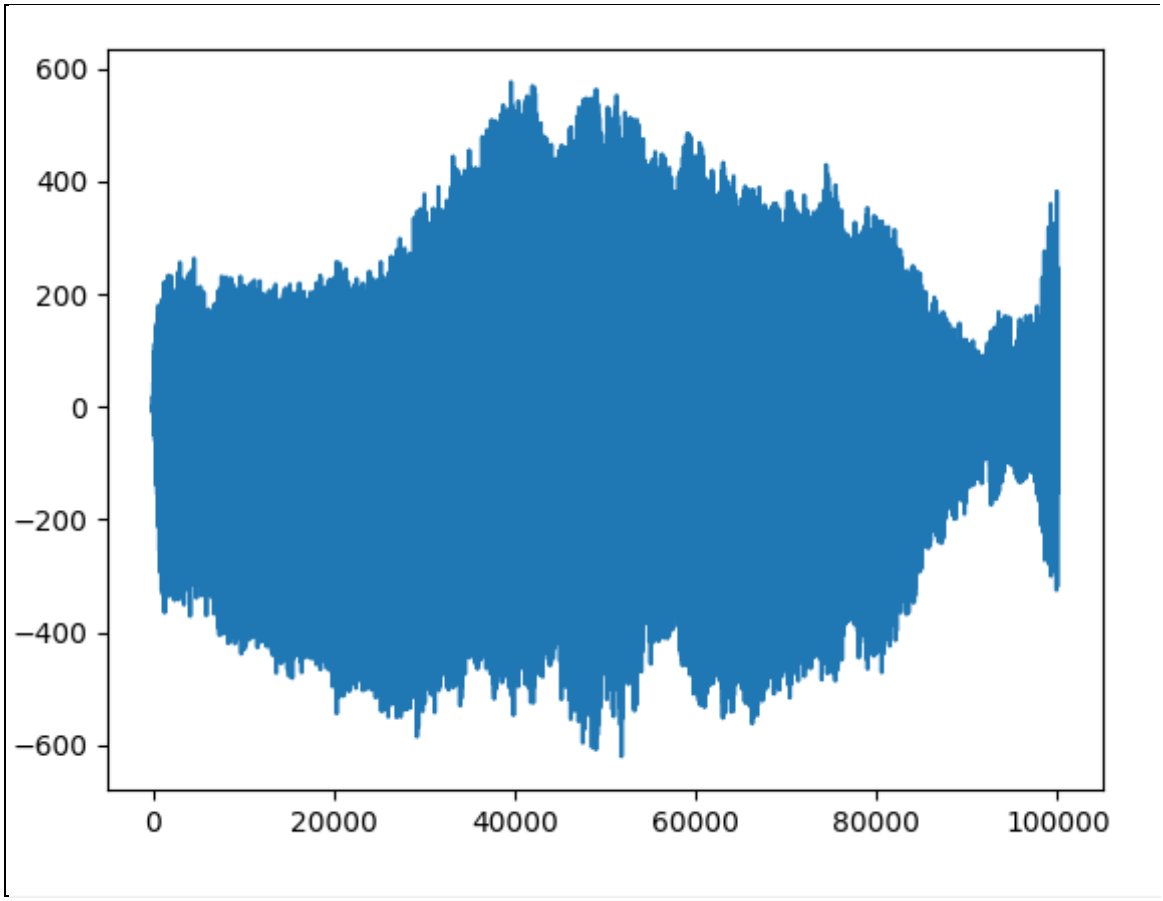
Rys 2. Histogram wartości B z pliku wejściowego.



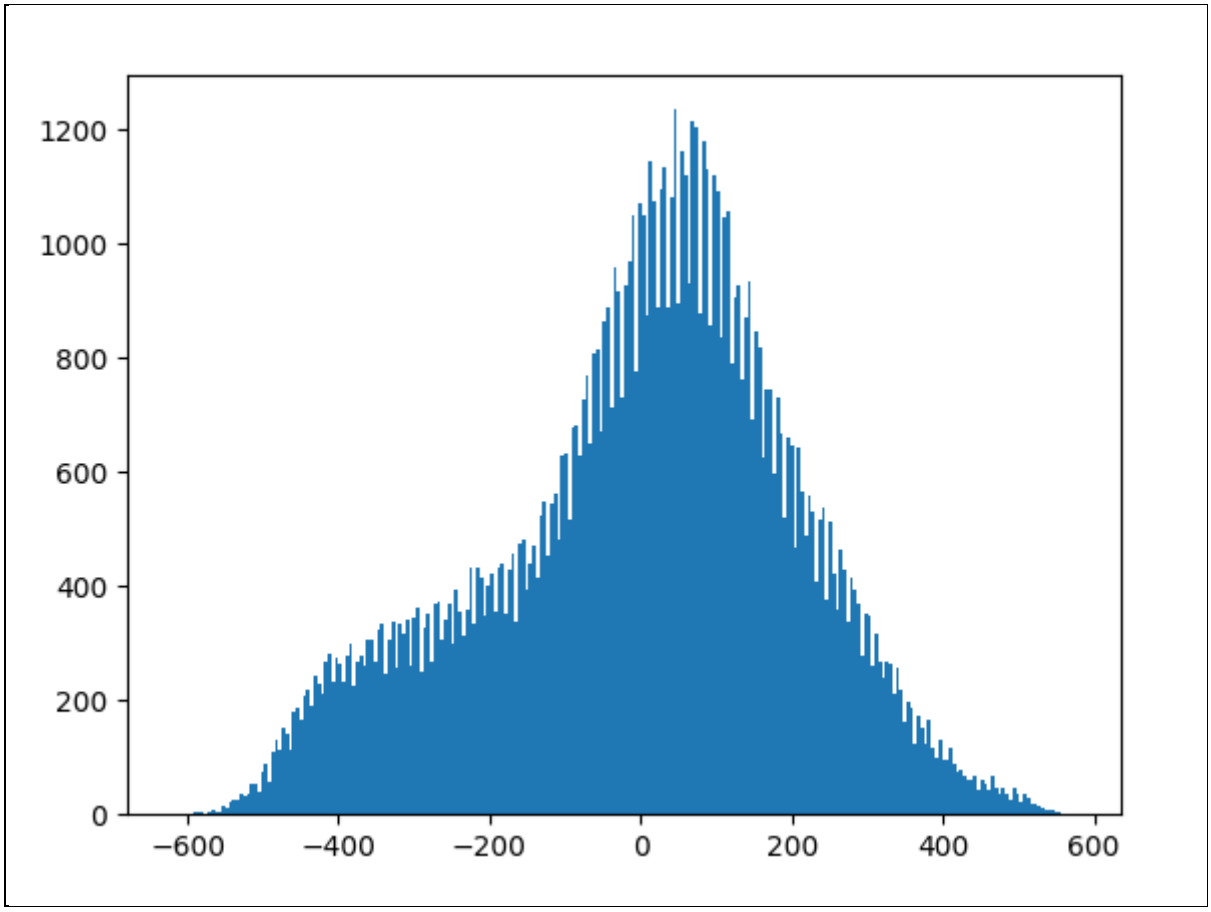
Rys 3. Histogram wartości R z pliku wejściowego.



Rys 4. Histogram wartości G z pliku wejściowego.



Rys 5. Wykres wartości dźwięku z pliku wejściowego



Rys 6. Histogram wartości dźwięku

Entropia wyliczona zgodnie ze wzorem: $e = -\sum i\ pi\ log2\ (pi\ )$

Dla powyższych rozkładów odpowiednio dla wartości składowej

B = 6.8112 bita

G = 6.9186 bita

R = 6.6798 bita

Metoda poprawy właściwości statycznych:

Aby przetworzyć odpowiednio dane wejściowe wybierane są początkowe wartości współrzędnych punktu w obrazie (domyślnie punkt centralny) na podstawie wartości RGB tego punktu wybierane są następne wartości współrzędnych x oraz y dla nowego punktu z którego pobierane są wartości RGB do generowania bitu losowego. Poza wartościami barw punktu klatki wideo dodane są wartości dźwięku z pliku WAV odpowiednio:

SN1 = sound byte$j$ [10 + ($R * i$ + ($G \ll 2$) + B + runcnt)% ($K/2$)];

SN2 = sound byte$j$ [15 + ($R * i$ + ($G \ll 3$) + B + runcnt)% ($K/2$)];

SN3 = sound byte$j$ [20 + ($R * i$ + ($G \ll 4$) + B + runcnt)% ($K/2$)];

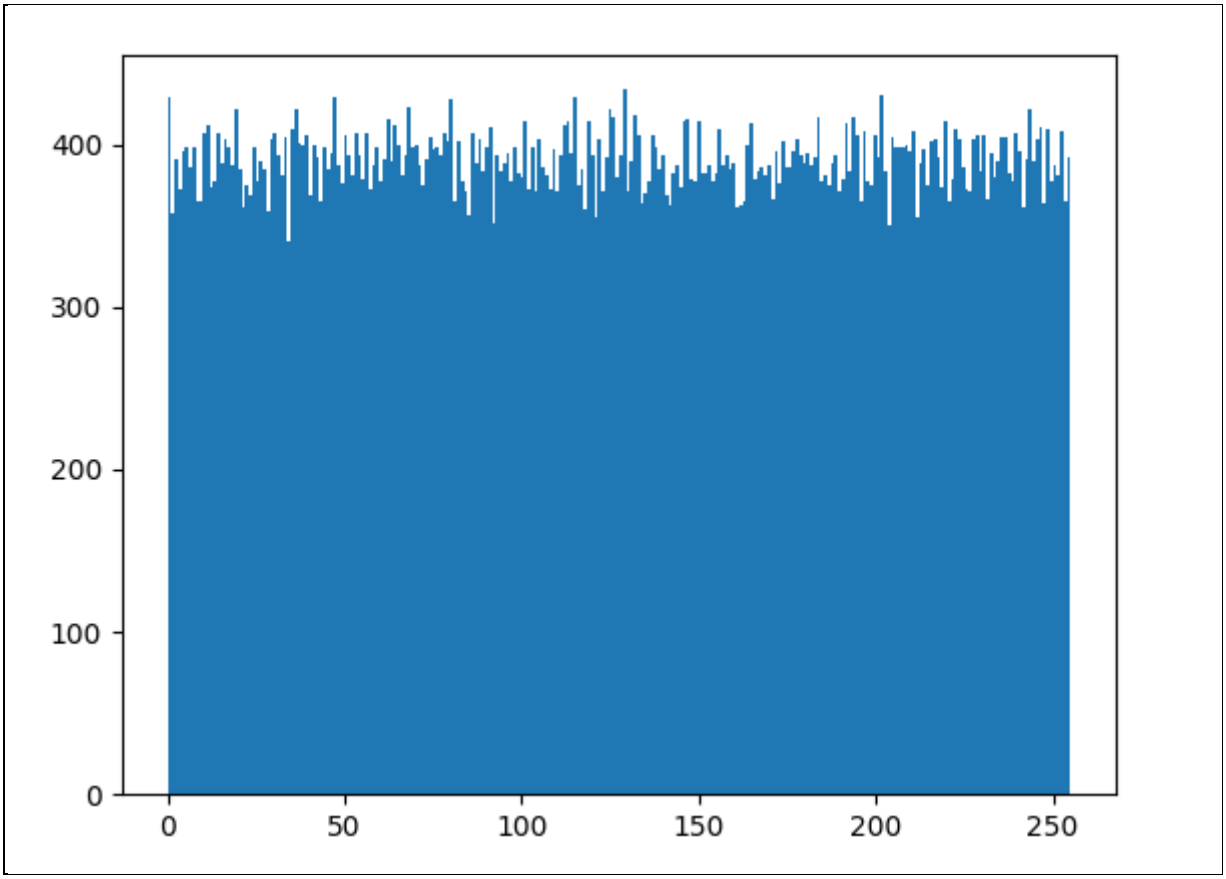
SN4 = sound byte$j$ [5 + ($R * i$ + ($G \ll 1$) + B + runcnt)% ($K/2$)];

SN5 = sound byte$j$ [25 + ($R * i$ + ($G \ll 5$) + B + runcnt)% ($K/2$)];

Wartości te są odpowiednio wykorzystywane w generowaniu bitu losowego razem z wartościami barw wybranego punktu z klatki wideo. Generowanie bitu jest przeprowadzane ze wzoru:

$$\text{bit}[i] = 1\&(R \oplus G \oplus B \oplus R1 \oplus G1 \oplus B1 \oplus R2 \oplus G2 \oplus B2 \oplus SN1 \oplus SN2 \oplus \cdots \oplus SNn)$$

Odpowiednio po wygenerowaniu 100 tysięcy liczb 8 bitowych



Rys 7. Histogram wartości wylosowanych

Entropia wylosowanych liczb wynosi: 7.99862 bita

Uwagi:

W ułatwieniu implementacji została wykorzystana konwersja pliku mp4 na dodatkowy plik wav zawierający wyłącznie wartości dźwięku. Prędkość generowania liczb wynosi około 30 minut na milion liczb. Generator nie jest skomplikowany, przy małym nakładzie danych wejściowych możemy wygenerować bardzo dużo liczb. Generator otrzymuje podobne rezultaty dla różnych plików wejściowych natomiast gorzej działa dla filmów animowanych, ponieważ wartości kolorystyczne zawarte w klatce są częściej powielane.