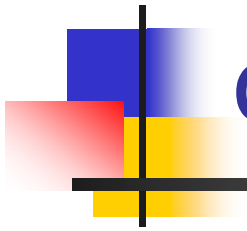
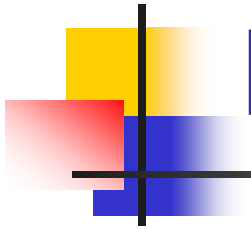


Kryptoanaliza algorytmu chaotycznego szyfrowania obrazu

Karol Jastrzębski

Praca magisterska

Opiekun: dr hab. inż. Zbigniew Kotulski



Plan prezentacji

- Teoria chaosu:
  - Wprowadzenie, cechy układów chaotycznych, pojęcia
- Teoria chaosu w kryptologii:
  - Motywacja, problemy
- Szyfrowanie obrazu:
  - Problem szyfrowania obrazu, chaotyczne szyfrowanie obrazu
- Szyfr Pisarchika:
  - Algorytm, problemy, metoda ataku
- Udoskonalona wersja szyfru Pisarchika:
  - Wprowadzone zmiany, wyniki eksperymentów
- Cechy dobrego szyfru chaotycznego
- Perspektywy

Teoria chaosu - wstęp

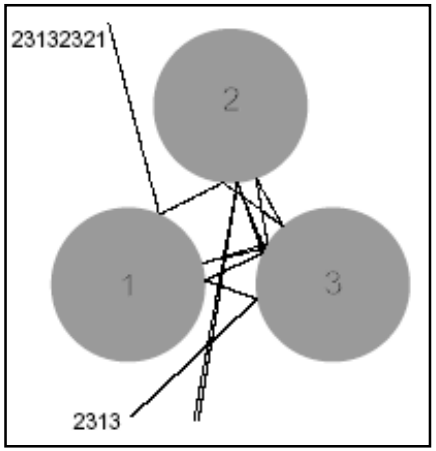
- Dział matematyki zajmujący się opisem układów **zdeterminowanych**, które jednak zachowują się w sposób kapryśny, nieprzewidywalny i na pozór **przypadkowy**

- Taka „losowość”, która daje się opisywać w sposób deterministyczny. Takie równania deterministyczne, które dają „losowość”.

- Jak to możliwe? – niestabilność i mieszanie zapewniają dobre własności statystyczne

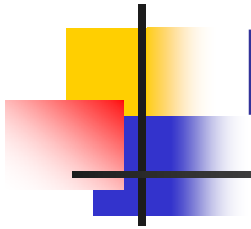
Cechy układów chaotycznych

- Niestabilność – wrażliwość na warunki początkowe („efekt motyla”)



- Mieszanie – trajektoria wędruje po przestrzeni fazowej równomiernie (proporcjonalnie do miary obszaru); obszary przestrzeni są asymptotycznie statystycznie niezależne

- Typowa orbita układu jest nieokresowa (więc i nieskończona)

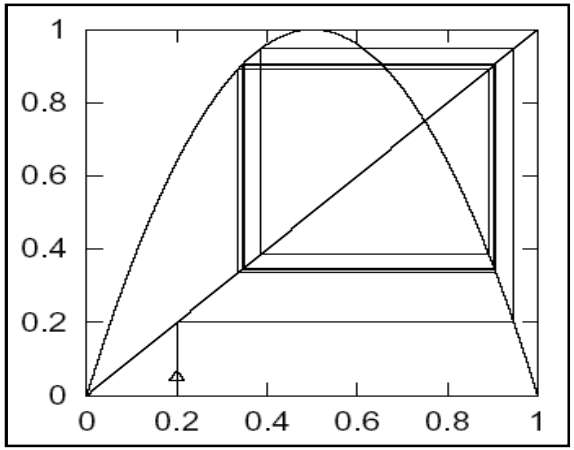


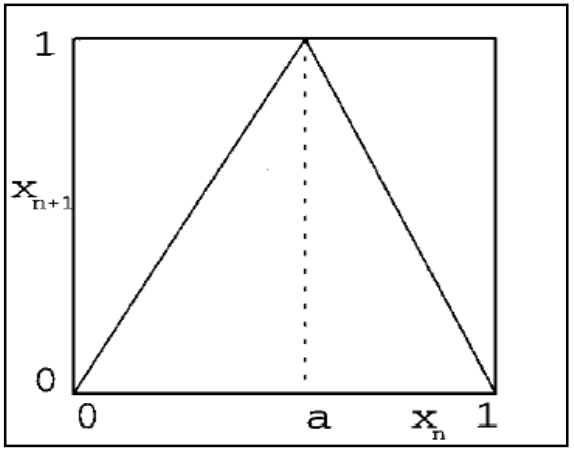
Pojęcia

- Wykładnik Lapunowa – miara liczbowa chaotyczności układu; układ jest chaotyczny, gdy posiada dodatni wykładnik Lapunowa
- Atraktor – podzbiór przestrzeni fazowej, do którego dąży typowa trajektoria
- Bifurkacja – skokowa zmiana własności układu przy ciągłej zmianie parametru sterującego

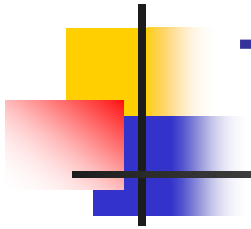
Teoria chaosu w kryptologii (1/3)

- Układy ciągłe i dyskretne w czasie
- Układy dyskretne – mapy zależne od parametru sterującego



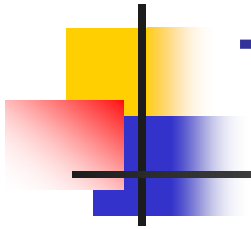


- Szyfrowanie – wielokrotne iterowanie mapy, klucz – para (parametr p, warunek początkowy x_0)



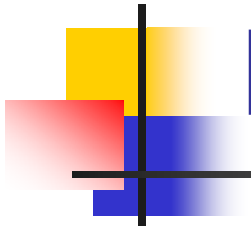
Teoria chaosu w kryptologii (2/3)

- Dowiedziono braku bezpieczeństwa większości proponowanych szyfrów
- Najczęstsze błędy (zwłaszcza wśród starszych publikacji) to brak odporności na atak z wybranym tekstem jawnym lub słabości związane z kluczem (mały rozmiar przestrzeni, słabe klucze)
- Duża liczba pomysłów matematycznych, niewielka – szczegółowych, formalnych specyfikacji technicznych, popartych dokładną analizą bezpieczeństwa i efektywności
- Niewielkie zainteresowanie ze strony „poważnej” kryptologii



Teoria chaosu w kryptologii (3/3)

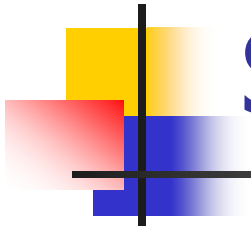
- Zalety
  - Dobra matematyczna teoria
  - Dziedzina stosunkowo nowa – duże „pole do popisu”
  - Głębokie analogie pomiędzy własnościami układów chaotycznych a cechami dobrych kryptosystemów (dyfuzja, konfuzja, własności statystyczne, ...)
- Wady
  - Nowe podejście – nowe ataki, nowe kryteria bezpieczeństwa
  - Niski poziom części publikacji
  - Trudności implementacyjne – teoria operuje liczbami rzeczywistymi i nieskończonością



Problemy implementacyjne

- Przedstawienie liczby rzeczywistej i przenoszenie błędów
  - Rozwiązania: implementacja własnej arytmetyki, zwiększanie precyzji, niewielka liczba iteracji

- *Dynamical degradation* – pogorszenie własności statystycznych powodowane dyskretyzacją
  - Skutki: krótkie cykle, słabe klucze, możliwość odgadnięcia „rozdzielczości” klucza
  - Rozwiązania: istnieją algorytmy perturbacji, poprawiające własności układu

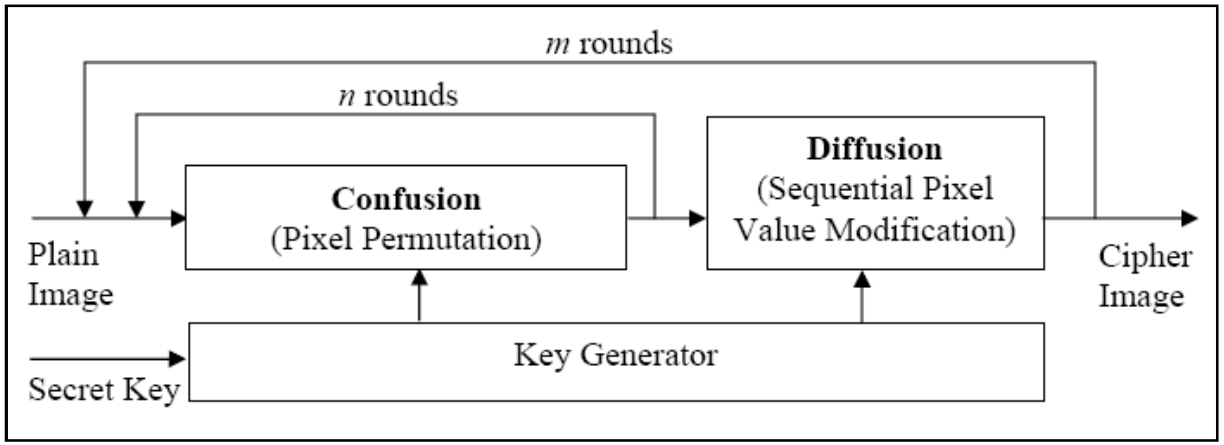


Szyfrowanie obrazu

- Zagadnienia:
  - Wysoka nadmiarowość i duża objętość danych
  - Szybkość działania
  - Silna korelacja sąsiadujących pikseli
  - Szyfrowanie a kompresja
  - Bity ważniejsze i mniej ważne
  - Czasami dopuszczalny częściowy wyciek informacji
- Dobry szyfr:
  - Duża szybkość działania
  - Szyfrogram silnie zależny od zmian klucza i obrazu jawnego
  - Szyfrogram ma płaski histogram kolorów, brak w nim korelacji pomiędzy pikselami
  - Odporny na znane ataki

Chaotyczne szyfrowanie obrazu

- Dowiedziono słabości większości szyfrów
- Szyfry oparte bądź na zmianie wartości pikseli, bądź na ich permutowaniu
- Friedrich zaproponował ogólną architekturę:



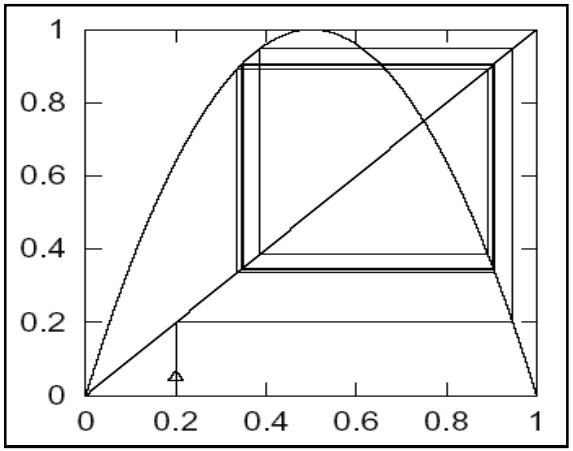
Szyfr Pisarchika (1/4)

- Źródło: A. N. Pisarchik, N. J. Flores-Carmona, M. Carpio-Valadez, *Encryption and decryption of images with chaotic map lattices* (Sierpień 2006)

- Proponowana mapa: odwzorowanie logistyczne

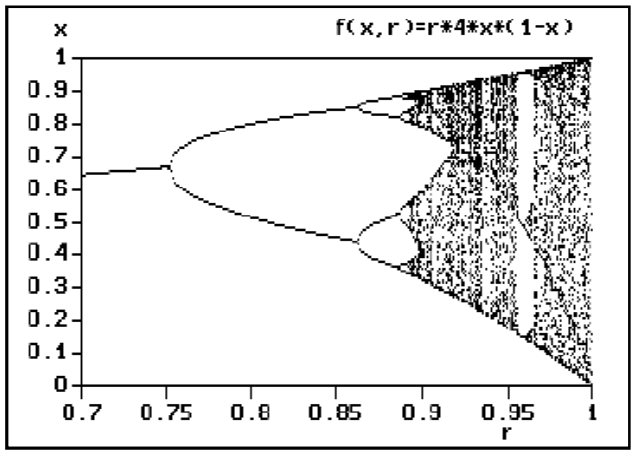
$$x_{n+1} = a x_n (1 - x_n)$$

dla $3.57 < a < 4.0$



Szyfr Pisarchika (2/4)

- Dla różnych wartości parametru *a* istnieją jednoznacznie określone $x_{\min}, x_{\max}$, będące granicami atraktora



- Zamiana wartości kolorów pikseli na liczby zmiennoprzecinkowe i z powrotem ($\delta x = x_{\max} - x_{\min}$):

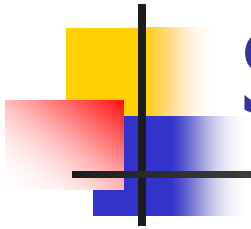
$$x_c = x_{\min} + \delta x \left(\frac{C_c}{255} \right)$$

$$C_c = round\left((x_c - x_{\min}) \frac{255}{\delta x} \right)$$

Szyfr Pisarchika (3/4)

- Szyfrowanie:
  1. Zamieniamy składowe kolorów pikseli na liczby zmiennoprzecinkowe.
  2. Dla każdego piksela: bierzemy piksel poprzedni jako wartość początkową dla mapy, iterujemy mapę *n* razy i dodajemy tę wartość do wartości bieżącego piksela.
  3. Jeżeli suma wykracza poza przedział $[x_{\min}, x_{\max}]$, dokonuje się normalizacji poprzez odjęcie δx.
  4. Zamieniamy liczby zmiennoprzecinkowe skojarzone z pikselami na kolory.

- Klucz szyfru:
  - para liczb (*n*, *a*) = (liczba iteracji, parametr sterujący mapy)

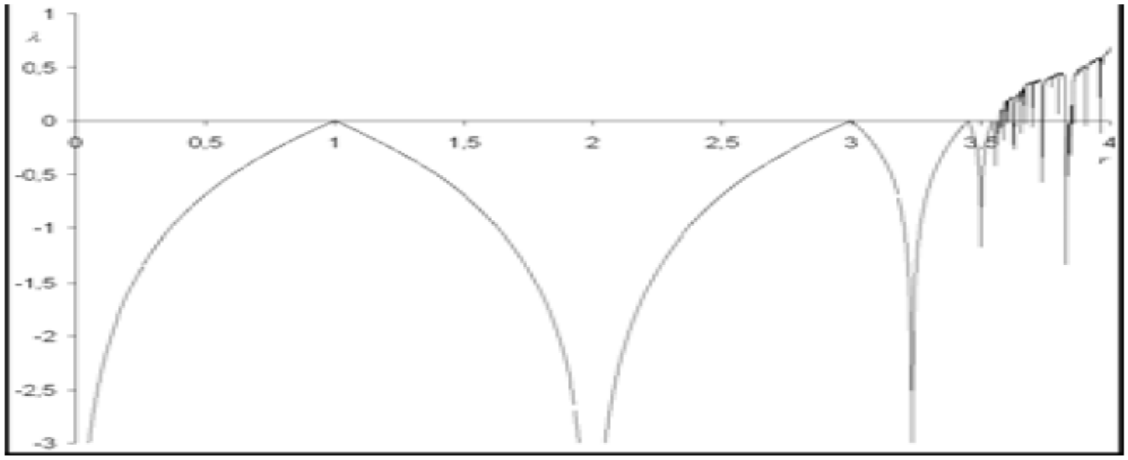


Szyfr Pisarchika (4/4)

- Deszyfrowanie:
  1. Zamieniamy składowe kolorów pikseli na liczby zmiennoprzecinkowe.
  2. Dla każdego piksela: bierzemy piksel poprzedni jako wartość początkową dla mapy, iterujemy mapę n razy i odejmujemy tę wartość od wartości bieżącego piksela.
  3. Jeżeli różnica jest mniejsza od zera, należy ją znormalizować poprzez dodanie δx.
  4. Zamieniamy liczby zmiennoprzecinkowe skojarzone z pikselami na kolory.

Problemy z szyfrem Pisarchika (1/3)

- Wybór mapy
  - W przedziale $a \in (3.57, 4.00)$ istnieją ujemne wykładniki Lapunowa



  - Nie wiadomo, skąd brane są wartości $x_{\min}$ i $x_{\max}$
  - Brak odniesienia do problemu dynamicznej degradacji

Problemy z szyfrem Pisarchika (2/3)

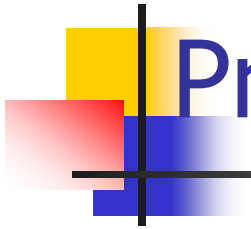
- Normalizacja
  - Jej konstrukcja jest niepoprawna. Niech:

$$x_{\max} = 0.9 \qquad x_{\min} = 0.1 \qquad \delta x = 0.9 - 0.1 = 0.8$$

+	**0.1**	**0.9**
0.1	0.2	$1.0 - \delta x = 0.2$
0.9	$1.0 - \delta x = 0.2$	$1.8 - \delta x = 1.0$

–	**0.1**	**0.9**
0.1	0.0	$-0.8 + \delta x = 0.0$
0.9	0.8	0.0

  - Taka normalizacja nie ma prawa działać

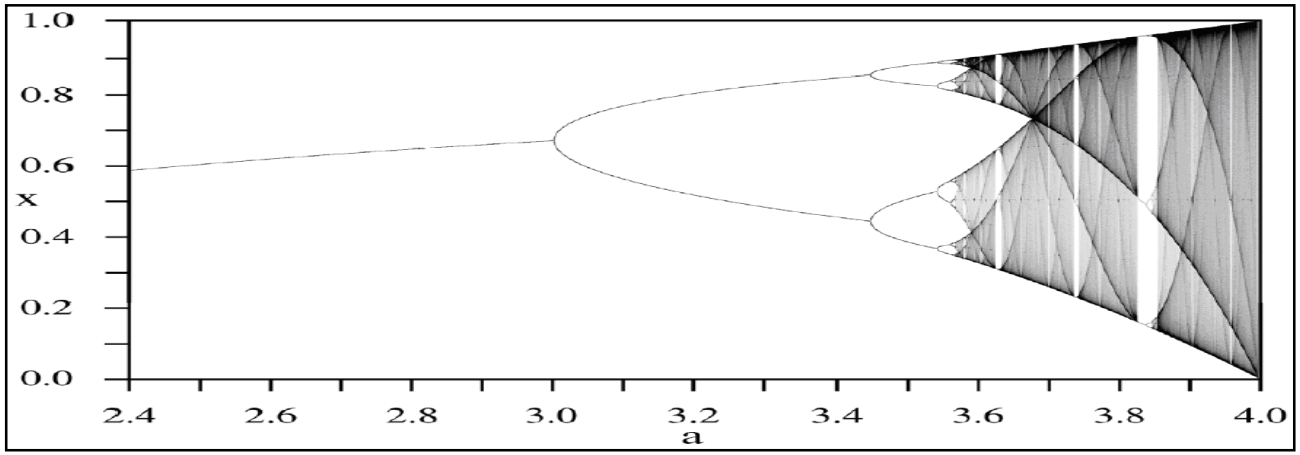


Problemy z szyfrem Pisarchika (3/3)

- Zamiana kolorów na liczby zmiennoprzecinkowe i na odwrót
  - Użycie operatora *round(.)* powoduje obcięcie liczby, a więc utratę informacji
  - W procesie deszyfrowania mapa jest iterowana z innym warunkiem początkowym, niż w procesie szyfrowania
  - Uniemożliwia to odszyfrowanie obrazu (można to pokazać numerycznie)
  - Należy przyjąć, że szyfrogramem jest zbiór liczb zmiennoprzecinkowych
- Przestrzeń klucza
  - Nie zdefiniowano typów liczbowych, jakich należy użyć w implementacji – uniemożliwia to analizę rozmiaru przestrzeni klucza

Metoda ataku

- Parametr *a* jednoznacznie determinuje wartości $x_{\min}, x_{\max}$



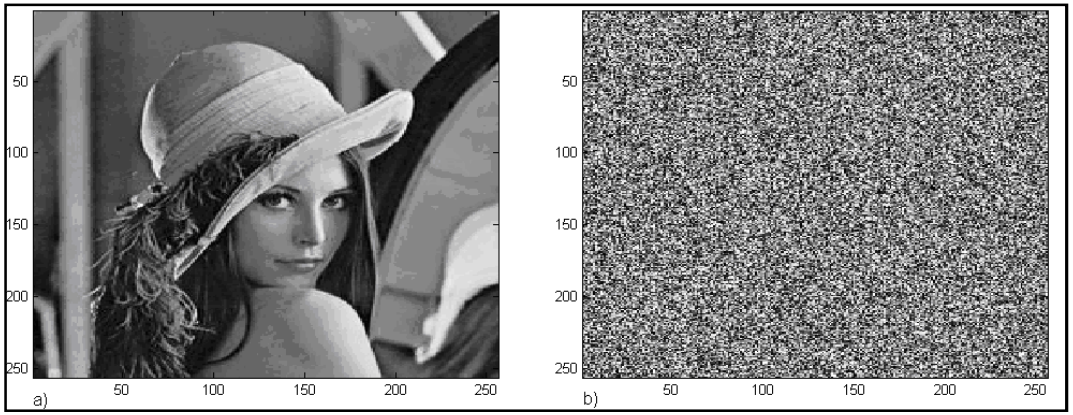
- Wyszukanie wartości największej i najmniejszej w ciągu przesyłanych liczb zmiennoprzecinkowych nie jest problemem
- Znalezione wartości dobrze przybliżają $x_{\min}, x_{\max}$
- Mając te wartości można znaleźć *a* – konieczna do przeszukania przestrzeń klucza maleje o ok. 2^{64}

Udoskonalona wersja szyfru

- Mapa odcinkami liniowa – chaotyczna w całym zakresie zmian parametru sterującego
- Użyto algorytmu perturbacji, wykorzystującego generator liczb pseudolosowych z ziarnem *s*.
- Konwersja na składowe kolorów następuje przed i po wykonaniu iteracji na mapie – dzięki temu pozostałe operacje arytmetyczne są działaniami w grupie $\mathbf{Z}_{256}$
- Normalizacja dokonywana jest poprzez dodawanie lub odejmowanie liczby 256.
- Kluczem jest para (*a*, *s*), a rozmiar przestrzeni klucza to ok. 2^{118}

Wyniki eksperymentów (1/2)

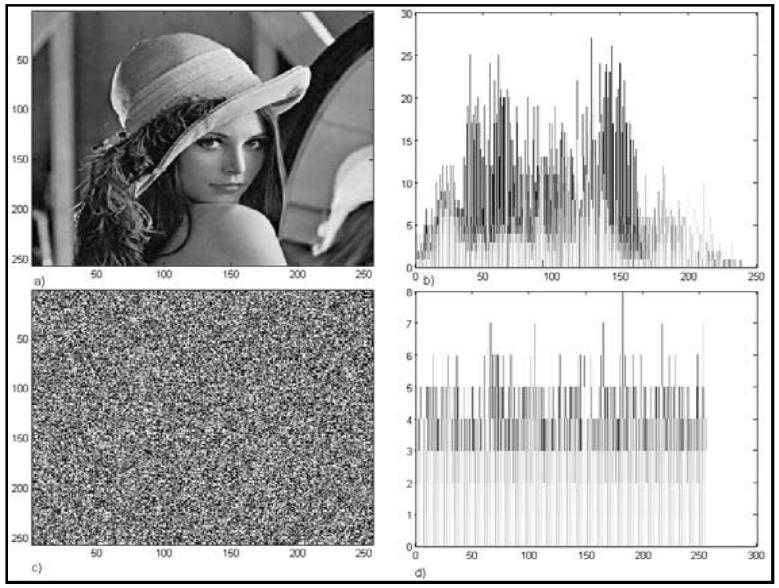
- Szyfrogram jest nieczytelny już przy niewielkiej liczbie iteracji

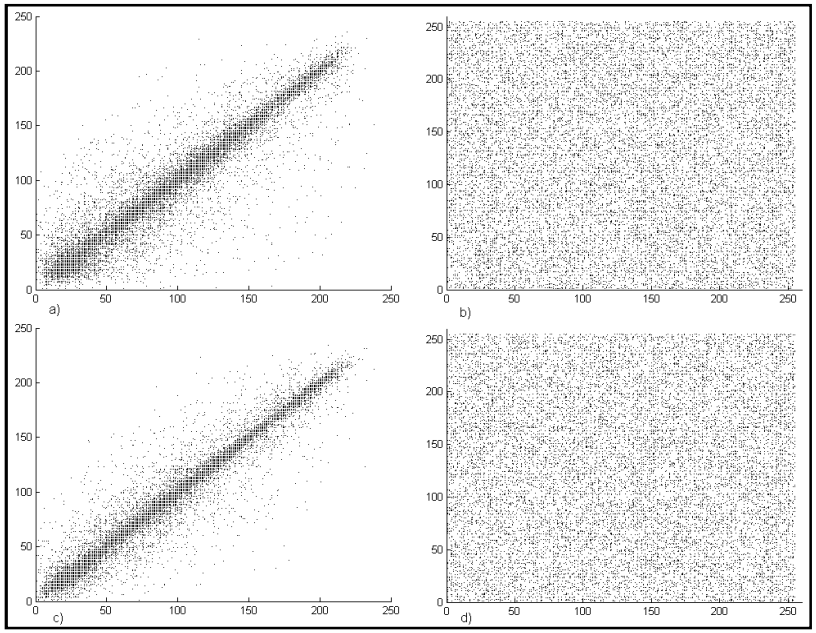


- Szyfr jest czuły na zmianę wartości klucza
- Szyfr nie jest czuły na zmianę tekstu jawnego

Wyniki eksperymentów (2/2)

- Histogram szyfrogramu jest wypłaszczony

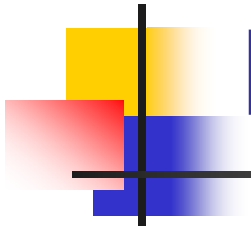




- Korelacja pomiędzy sąsiednimi pikselami zanika

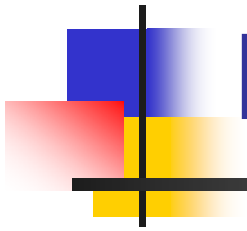
Cechy dobrego szyfru chaotycznego

- Szczegółowa formalna specyfikacja
- Rozpatrzone efekty związane z tzw. dynamiczną degradacją
- Jasno zdefiniowany klucz – jeśli kluczem jest parametr sterujący mapy, nie powinno się używać kluczy, dla których mapa nie jest chaotyczna
- Uważnie oszacowany rozmiar przestrzeni klucza
- Dobre własności statystyczne szyfrogramu dla każdego klucza i każdego tekstu jawnego
- Sprawdzona odporność na podstawowe klasy ataków
- Analiza efektywności



Perspektywy

- Próby zdefiniowania układów chaotycznych dyskretnych w czasie i w przestrzeni
  - Zamiast ciągłych map – ich dyskretne wersje, jako dobrze mieszające permutacje skończonych zbiorów
  - Dyskretne wykładniki Lapunowa jako miara chaotyczności tych permutacji (w granicy przechodzące w zwyczajne wykładniki Lapunowa dla układów ciągłych w przestrzeni)
- Nieliniowe permutacje, dobrze i szybko „mieszające” dane
  = S-boxy szyfrów blokowych (DES, AES)
- Nowe narzędzia matematyczne do konstrukcji szyfrów konwencjonalnych?



Dziękuję za uwagę

Pytania?