# Kiedy metody biometryczne stają się niebezpieczne

Khalid Saeed

khalids@wi.pb.edu.pl
http://aragorn.pb.bialystok.pl/~zspinfo/

Wydział Informatyki Politechniki Białostockiej
Wydział Fizyki i Informatyki Stosowanej AGH

# Plan seminarium:

- Zainteresowania i osiągnięcia w dziedzinie *komputerowej analizy obrazów*.
- Zastosowania *macierzy Toeplitza* w redukcji danych oraz przy skutecznym opisie obrazów, a w szczególności obrazów biometrycznych.
- Program komputerowy o zastosowaniach MT

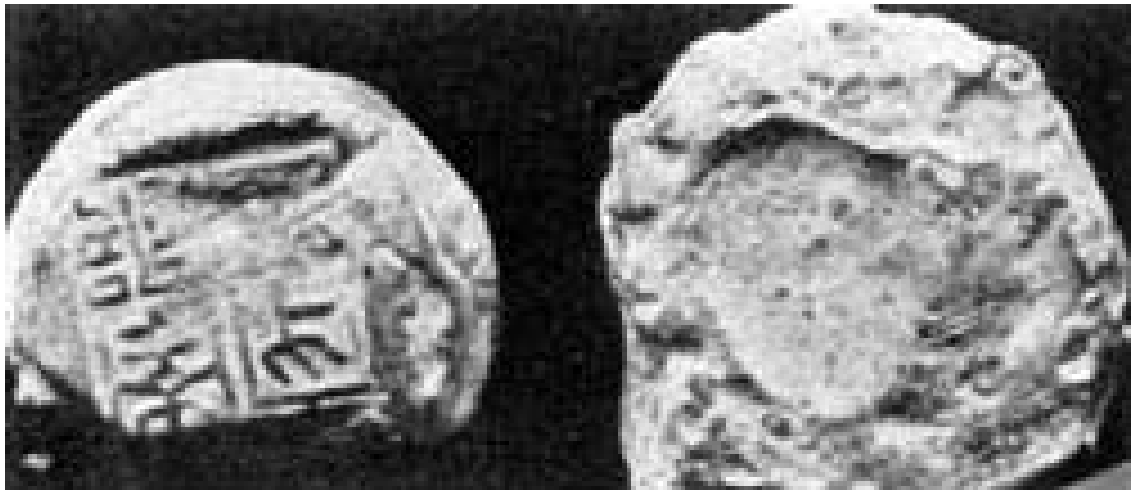
# Co to Biometria?

Biometria oznacza POMIARY BIOLOGICZE
(ang. BIOMETRICS – Biological Measurements)
Nazwa ta pochodzi z greki *BIOS* - życie
i *METRON* - *pomiar*.
*Rozpoznawanie człowieka na podstawie jego cech biologicznych*

# Od kiedy istnieje biometria?

1885-1913 B.C. (Mezopotamia)

Odciski kciuków znaleziono na tablicach glinianych i ceramicznych naczyniach już w starożytnym Babilonie. Ludzie pozostawiali swoje odciski, aby zalegalizować swoje transakcje handlowe.



(*seen in Museum of London*)

*A więc od zawsze wykorzystywano biometrię do identyfikacji człowieka !*

## Systemy biometryczne składają się głównie z następujących elementów:

**1. Skaner (kamera, mikrofon, fotokopiarka, …) -** do skanowania anatomii człowieka

**2. Przetwornik analogowo-cyfrowy oraz odpowiednie oprogramowania -** do zmiany danych analogowych na cyfrowe, zbierania i przetwarzania informacji

**3. Baza danych -** do porównania bieżących danych z bazą w celu uwierzytelniania i identyfikacji człowieka

**W biometrii wyróżniamy dwie kategorie:**

**1. Fizjologiczna (*Cognitive Biometrics* )**
- mierzenie różnych cech indywidualnych człowieka, które zazwyczaj posiada od urodzenia.

***Przykłady***
Odciski palców - *Fingerprints*
Tęczówka - *Iris image* (coloured part of the eye)
Twarz - *Face*
Geometria dłoni - *Hand geometry*
Zapach - *Odor*
Wzorzec naczyniowy - *Vascular pattern*
DNA

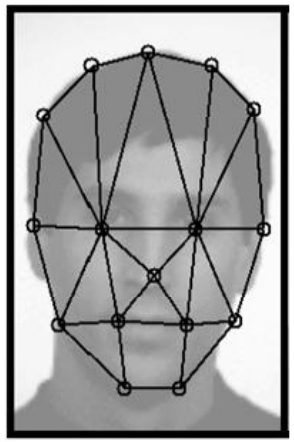
**2. Behawioralna (*Behaviometrics*)**

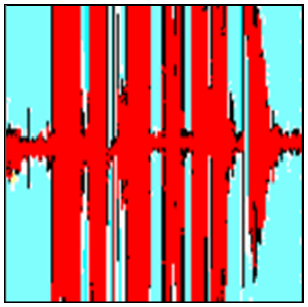
- rejestrowanie zachowania człowieka przy pewnych czynnościach

***Przykłady:***

Mowa i mówca - *Speech and Speaker Recognition*
Podpis - *Signature*
Stukanie na klawiaturze - *Keystroke*
Ruch myszy - *Mouse dynamics*
Chód - *Gait (way of walking)*

# Examples of Biometrics

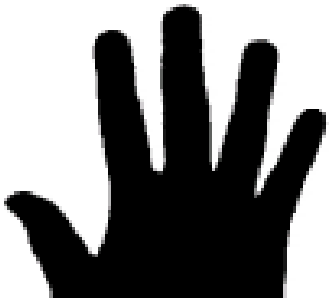


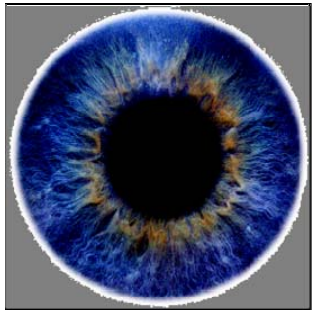


Zdjęcie rentgenowskie kolana

Naczynia krwionośne


Rozstaw zębów






Źródło:[1] oraz opracowanie własne

Dlaczego stosujemy biometrię przy uwierzytelnianiu i identyfikacji człowieka?

- W odróżnieniu od liczbowych haseł czy PIN kodów, biometria prezentuje niepowtarzalne i niezawodne hasła, po prostu każdy człowiek ma swoje cechy/rysy.

Poza tym:

- nietrudno zapomnieć czy zgubić klasyczne hasło,
- łatwa jest również kradzież tradycyjnych haseł.

Ale czy to oznacza, że systemy biometryczne są niezawodne?

A z drugiej strony, co zdecyduje o tym, którą cechę biometryczną należy zastosować? Dlaczego?

Poniższa tabela odpowiada na te pytania:

| Errors / Biometric | Error Rate | Error Sources | False Positive (Successful theft) | False Negative (Fails to match) |
|---|---|---|---|---|
| Fingerprint | 1 in 500+ | ynedrss, dirt, age | Extremely Difficult | Extremely Difficult |
| Face | no data | lighting, age, glasses, hair | Difficult | Easy |
| Hand | 1 in 500 | hand injury, age | Very Diff. | Medium |
| Speach | 1 in 50 | noise, weather, colds | Medium | Easy |
| Iris tęczówka | 1 in 131,000 | poor lighting | Very Diff. | Very Diff. |
| Retina siatkówka | 1 in 10,000,000 | glasses | Ext. Diff. | Ext. Diff. |
| Signature | 1 in 50 | changing signatures | Medium | Easy |

Źródła: [1], [2] oraz modyfikacja własna

**Więc nie ma optymalnej, idealnej metody biometrycznej.**
**Z tej tabeli wynika, że biometria nie jest niezawodna!**

**Z drugiej strony, co może zagwarantować, że cech człowieka nie można 'ukraść'?**

**Spoofing**[**] **-** ***Fałszowania biometrii***

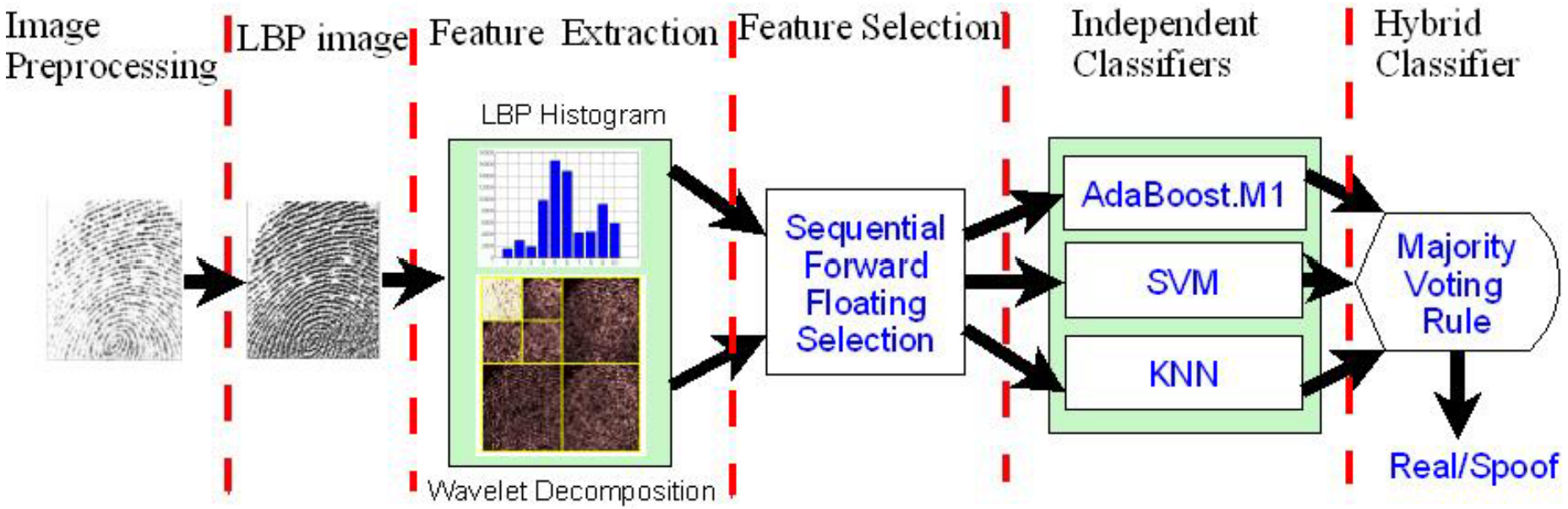
---

** [3] *Spoofing and Anti-Spoofing in Biometrics*, IJBM, vol. 1, no. 2, Inderscience Publishers, UK, 2008.

# Anti-Spoofing

Badacze naukowi oczywiście od razu odpowiedzieli na spoofing stosując nowe metody ‘anti-spoofing’. Wynaleźli więc sposoby zatrzymania fałszerzy.

Zaczęli badać nie tylko obrazu danej cechy biometrycznej, lecz jej żywotność. Badali, na przykład, wzorzec odcisków palca, a równocześnie stosowali czujniki do testowania, czy ten palec jest żywy.



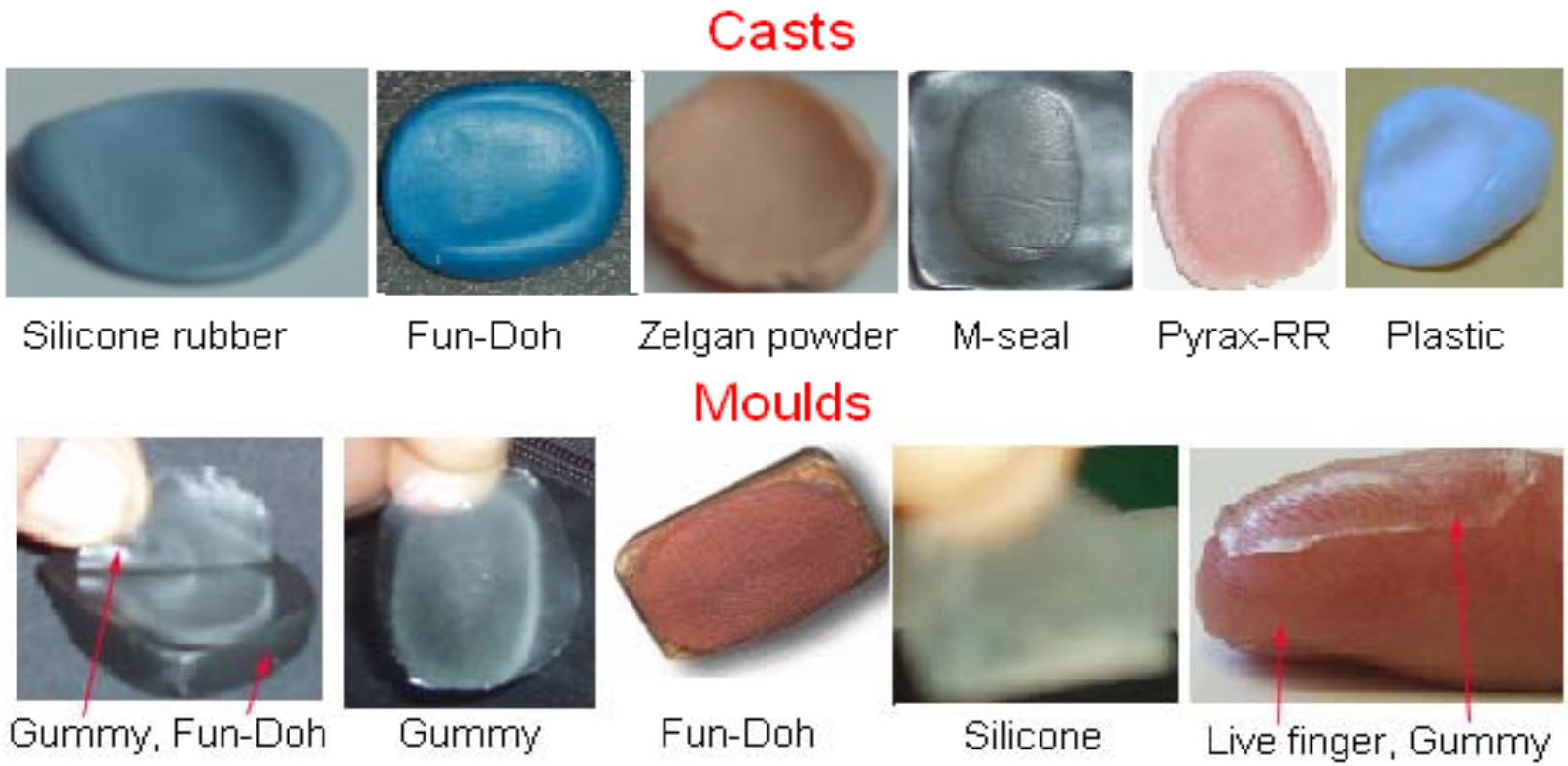

# Liveness detection approach

## Podejście do wykrycia żywotności tkanek palca

Źródło: [3]

# Anti-Spoofing

Dalej jednak fałszowania nie zniknęły, gdyż złodzieje biometrii zastosowali różne sztuczne materiały do stworzenia figur symulujących żywe tkanki – temperatura ciała, krążenie krwi, itp.




# Podrobione palce

Źródło: [3]


Portions of fingerprint images:
(a) Real finger,
(b) Fun-Doh finger,
(c) Gummy finger.

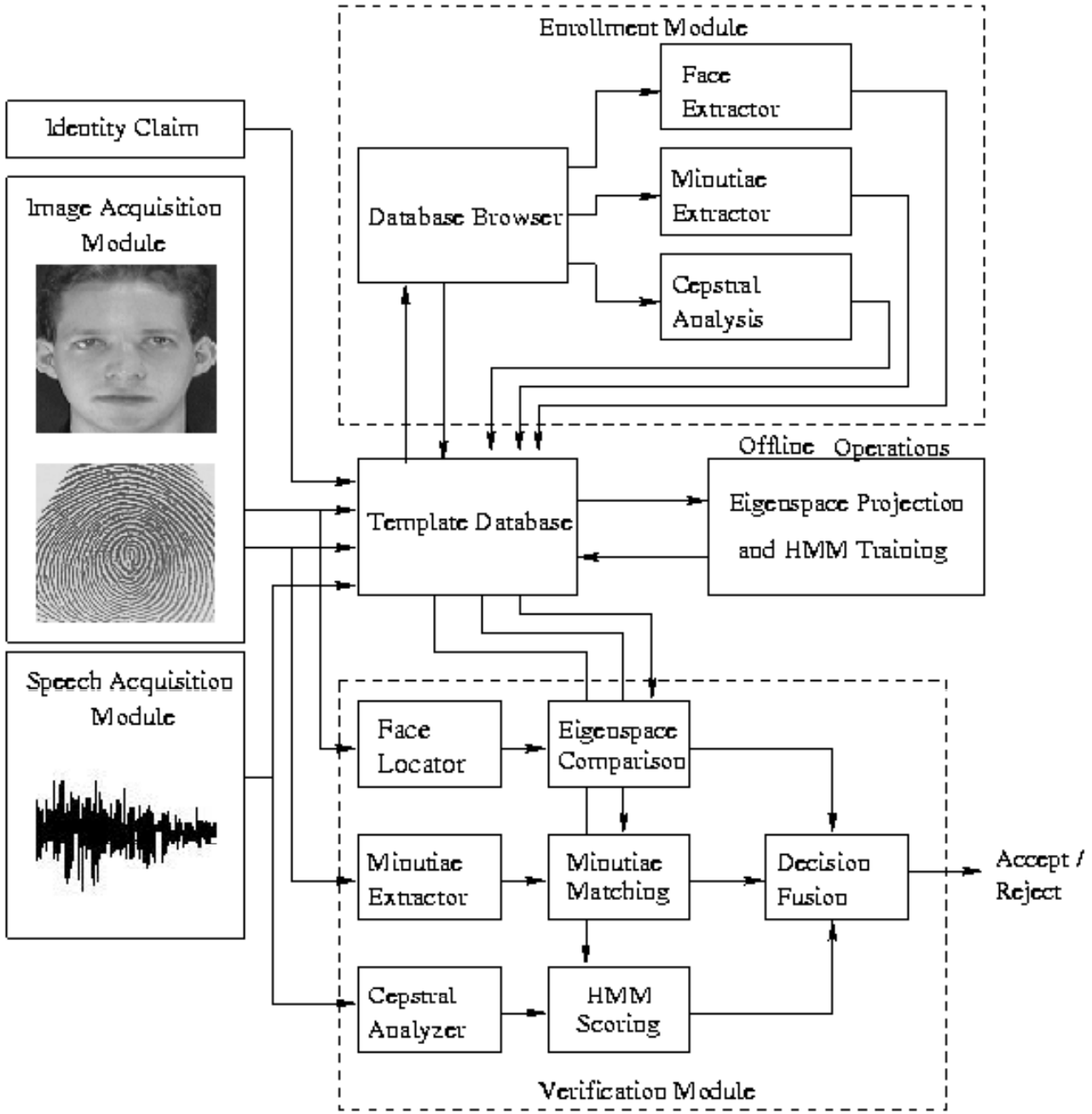
**Badania i wyniki różnych eksperymentów okazały, że nie ma żadnego systemu biometrycznego, który może być zastosowany sam i zdałby egzamin!**

## Jakie więc widzimy rozwiązanie? Co zrobić, aby nie dopuścić do sfałszowania naszych cech biometrycznych?

Multi-modelowe systemy wyglądają na najlepszy sposób ochrony danych człowieka i są chyba najlepszym rozwiązaniem.

# Jain's Model of MULTIBIOMETRICS

Jain opracował model składający się z 3-ch metod jako 'Fusion Biometric System' [2], [4].


Enrollment Module
Face Extractor
Minutiae Extractor
Cepstral Analysis
Database Browser
Identity Claim
Image Acquisition Module
Speech Acquisition Module
Template Database
Offline Operations
Eigenspace Projection and HMM Training
Face Locator
Eigenspace Comparison
Minutiae Extractor
Minutiae Matching
Decision Fusion
Accept / Reject
Cepstral Analyzer
HMM Scoring
Verification Module

Kiedy zintegrujemy dwie lub więcej metod w jeden system, to stworzymy nowy problem – złożone systemy obliczeniowo !!
Jednak, na to znajdują się różne rozwiązania – algorytmy do REDUKCJI DANYCH.
Najważniejszym zadaniem takich algorytmów jest stworzenie modelu matematycznego, który zapewnia:

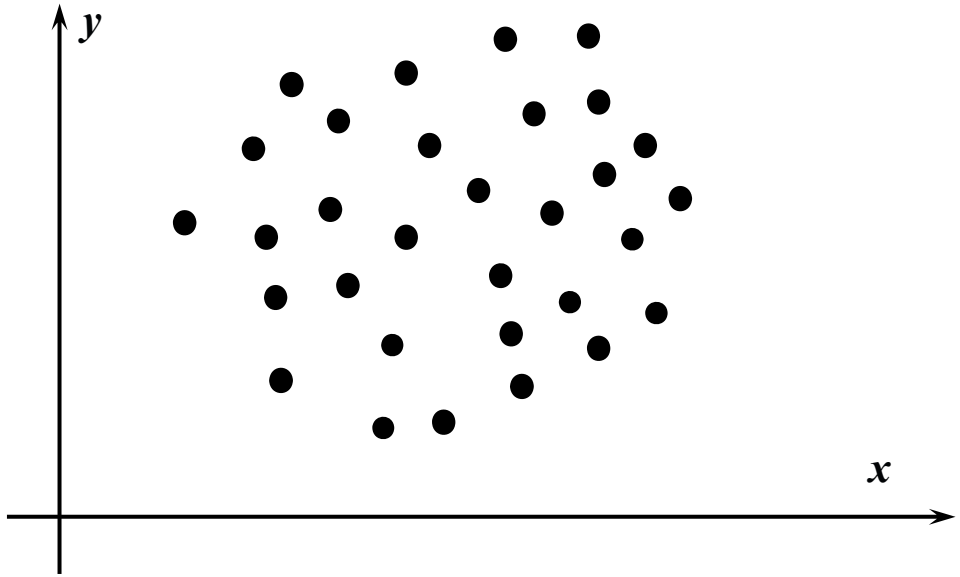
- zmniejszenie obliczeń
- otrzymanie wersji danych bez strat informacji o danym obiekcie.

W tym celu opracowałem model matematyczny na podstawie macierzy TOEPLITZ’a i ich minimalnych wartości własnych.

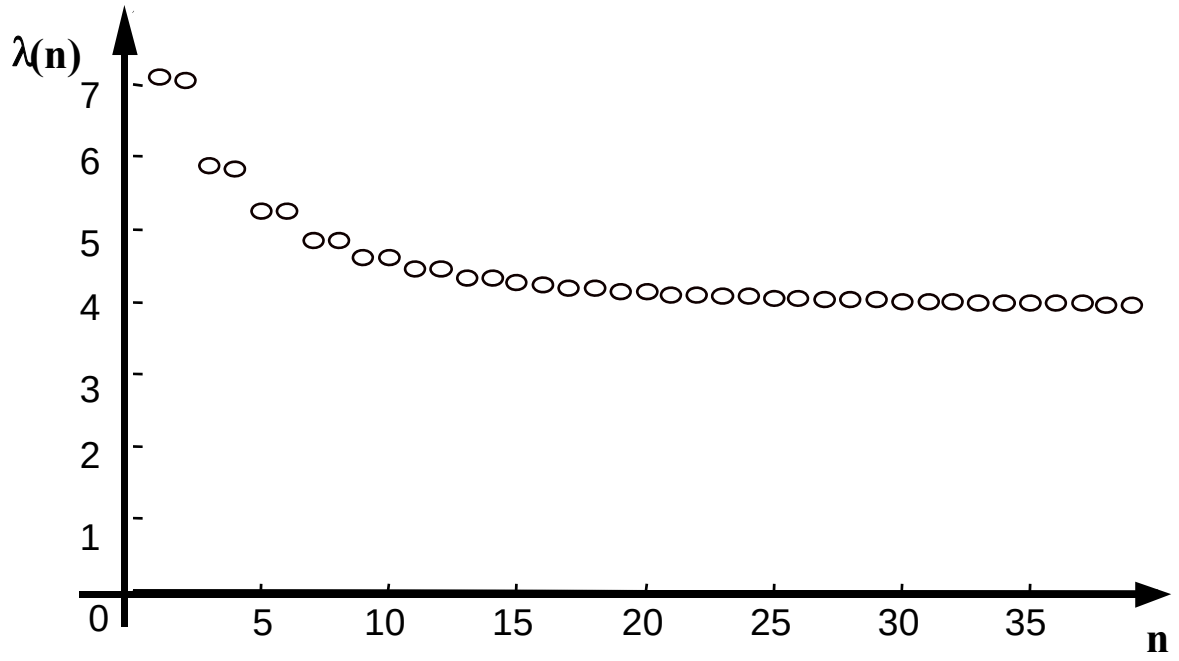
Dane liczby rzeczywiste

$$a_i \; i = 1, 2, ..., n$$

rozmieszczone na płaszczyźnie *x*-*y* według jakiegoś kryterium mogą na przykład reprezentować współrzędne danego obrazu.

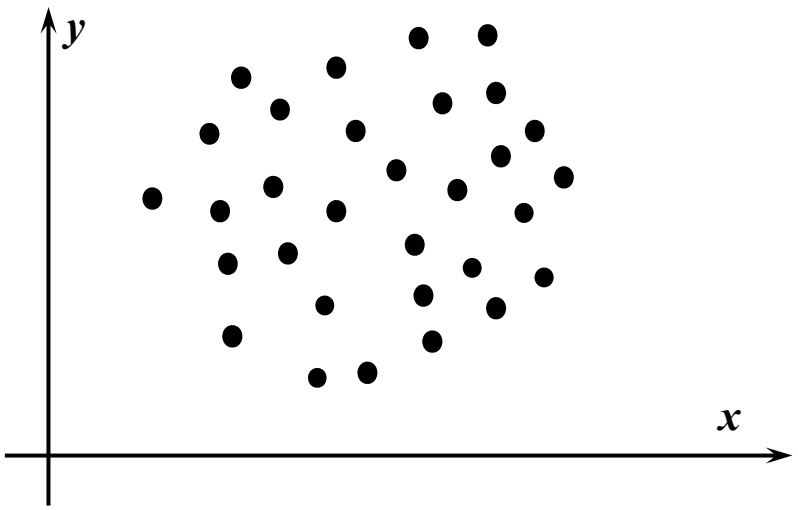


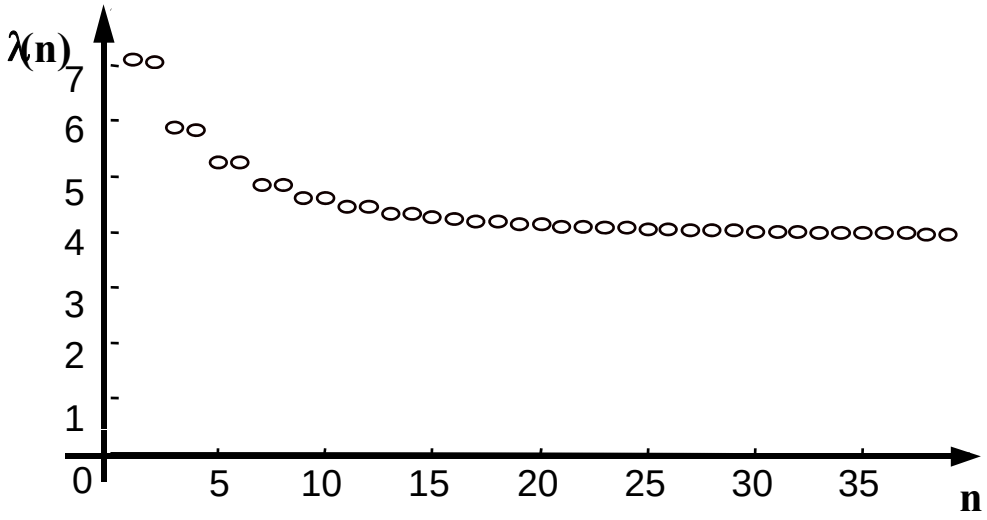
Te punkty mogą być uporządkowane tak, aby tworzyły poniższy wykres.




Zostaje to wykonane według następującej transformaty:

$$(x_i, y_i) \Rightarrow \lambda_i$$


y
x


λ(n)
7
6
5
4
3
2
1
0
5
10
15
20
25
30
35
n

Wykonuje się to korzystając z macierzy Toeplitza.

---

Historia

Brune Function → Determinants →
→ D and λ of TM with complex numbers →
→ TM with real elements

Rational function → Taylor series → TM and submatrices→ λ for each submatrix

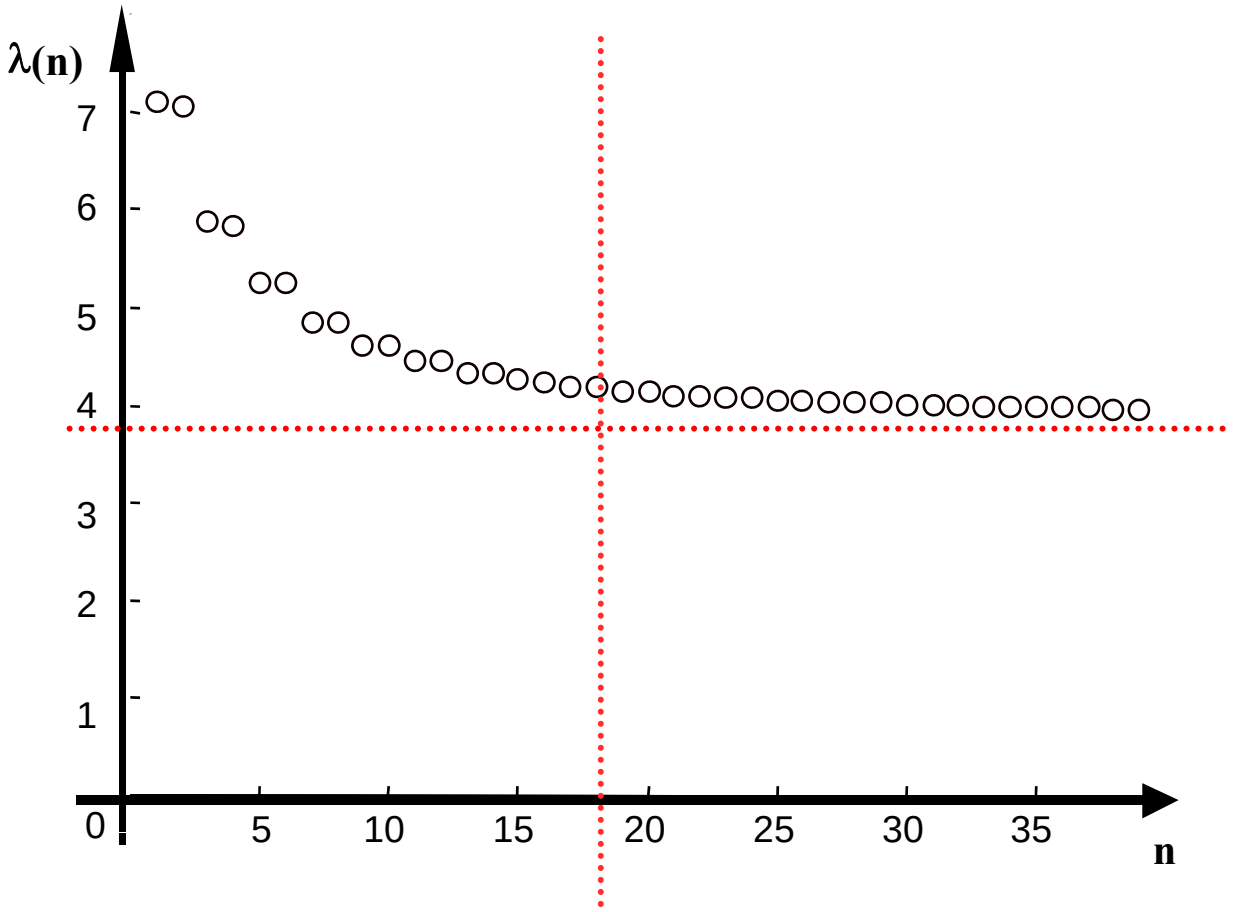
$$\lambda_0 \geq \ldots \geq \lambda_i \geq \ldots \geq \lambda_n$$

# Macierze Töeplitza*

W swojej prostej formie, macierz Töeplitza jest taką macierzą hermitowską, która ma *stałe i równe wartości na diagonalu o ujemnym nachyleniu.*

$$C = \begin{bmatrix} c_0 & c_{-1} & c_{-2} & \cdots & c_{-n+1} \\ c_1 & c_0 & c_{-1} & \ddots & \vdots \\ c_2 & c_1 & c_0 & \ddots & c_{-2} \\ \vdots & \ddots & \ddots & \ddots & c_{-1} \\ c_{n-1} & \cdots & c_2 & c_1 & c_0 \end{bmatrix}$$

* Von Otto Töeplitz (Gottengen), "Uber Die Fourier'sche Entwickelung Positiver Funktionen," Aus einem an Herrn Caratheodory gerichteten Briefe, Rendiconti del Circolo Matematico di Palermo, vol. 32 (1911), pp. 191-192.

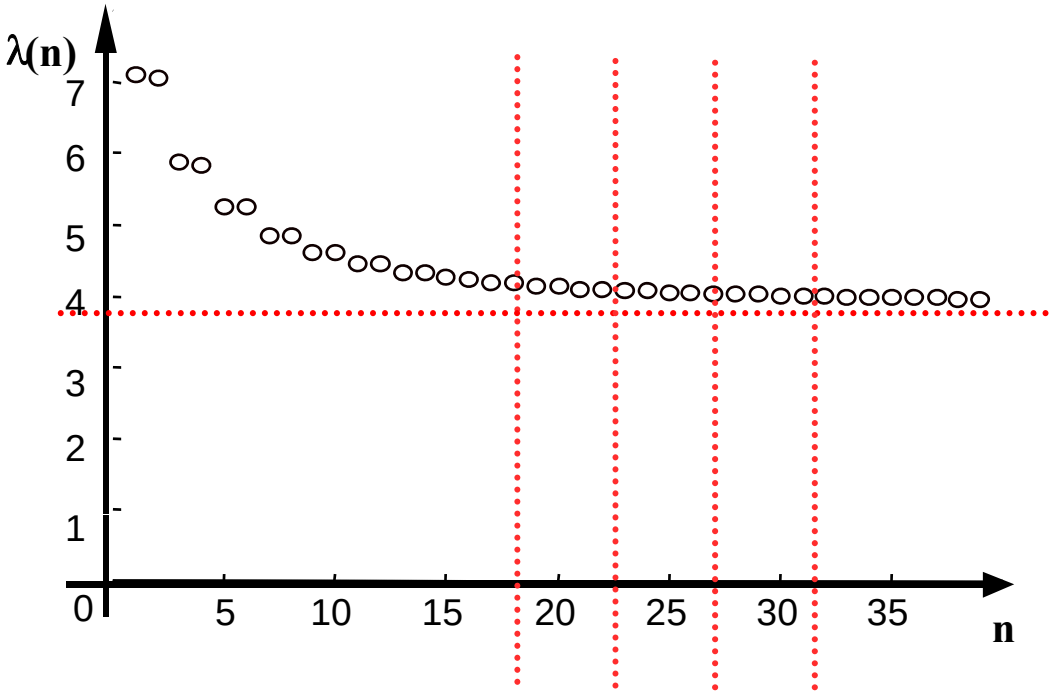



*Zachowanie minimalnych wartości własnych macierzy Töeplitza*.

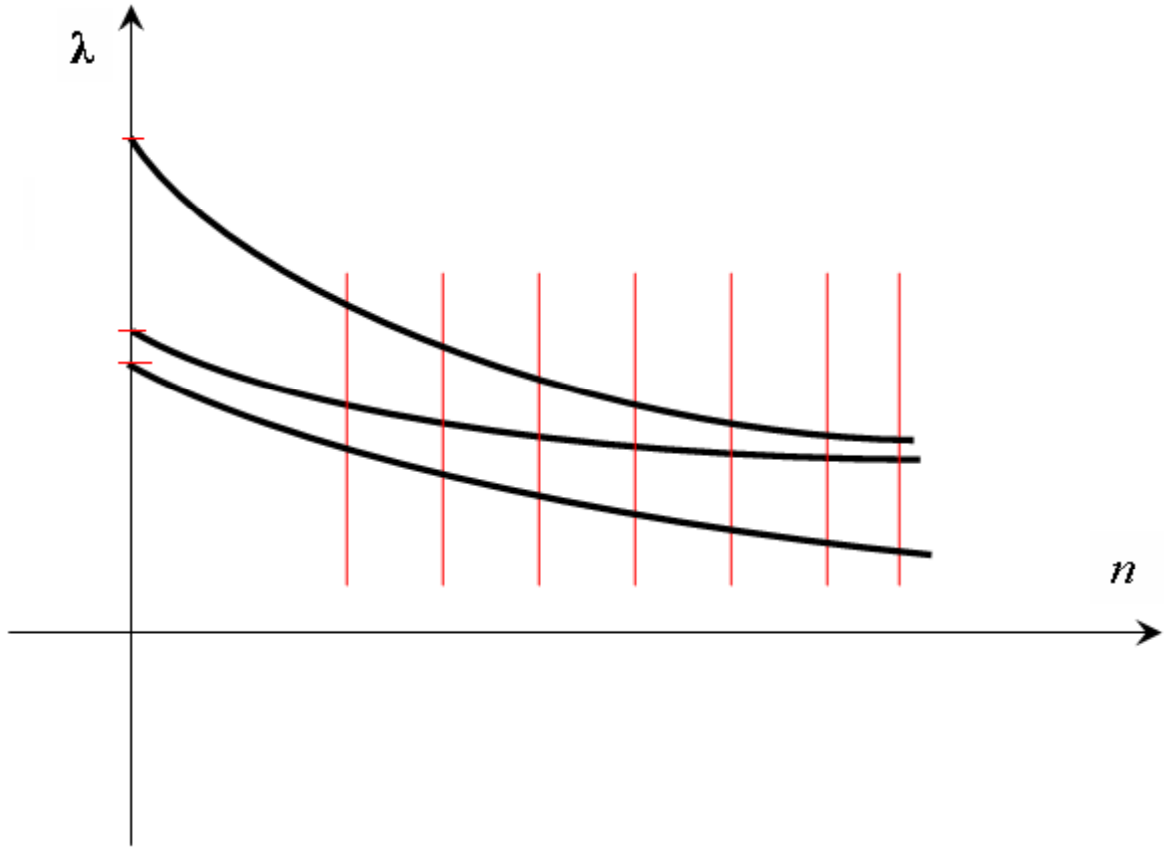
$$\lambda_0 \geq \ldots \geq \lambda_i \geq \ldots \geq \lambda_n$$

Spowoduje to zmniejszenie wymaganych danych wejściowych oraz zminimalizowanie elementów wektora cech dla danego obrazu w danej klasie.

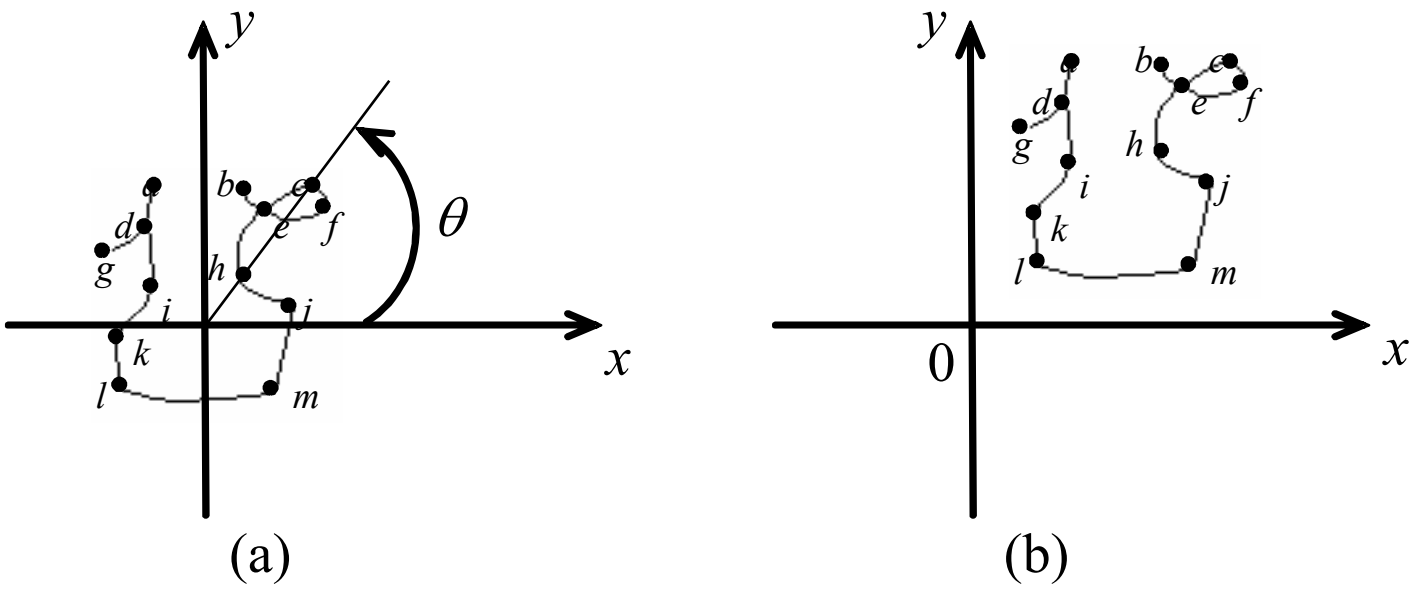
Redukcja ta wynika z istotnego faktu, iż wektor cech zawiera ***relację między cechami, a nie same cechy, jak w metodach klasycznych. Każdy kawałek wykresu przekazuje taką samą informację.***



… więc informacja jest podobna na wykresie jednego obrazu, ale różni się od informacji innych obrazów w danej klasie. Zatem wykresy te mogą stać się idealnym ANOTATOREM (deskryptorem).



Jak budować (konstruować) macierze Töeplitza z punktów charakterystycznych obrazu?

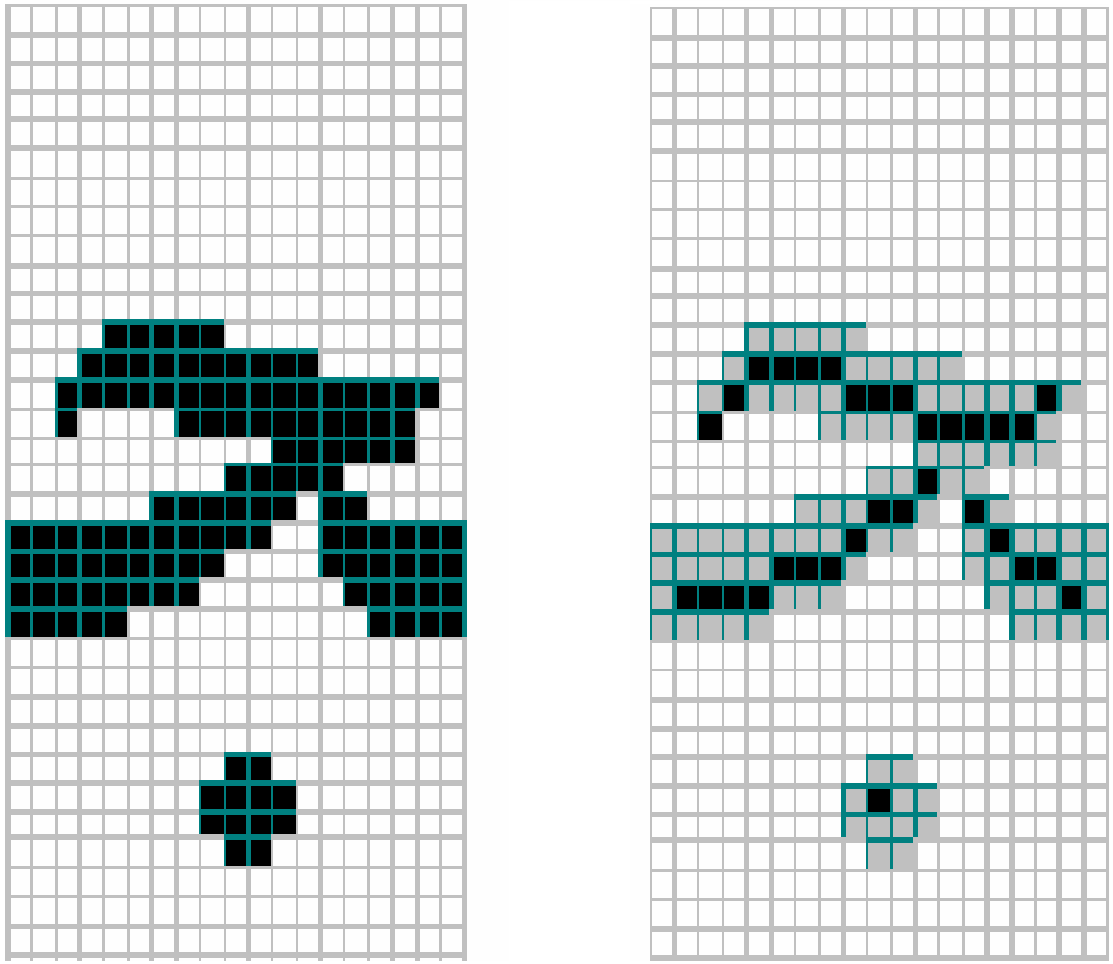



*Punkty charakterystyczne na płaszczyźnie biegunowej (a) oraz kartezjańskiej (b).*

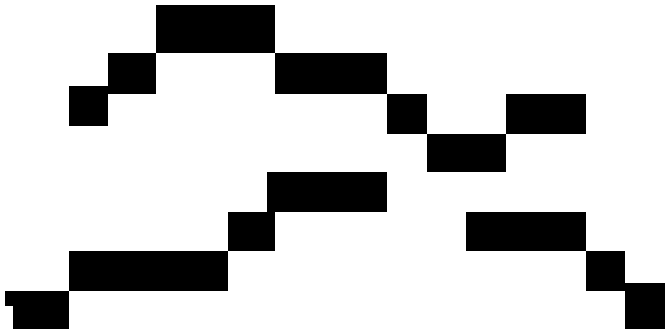
Źródło: [5]

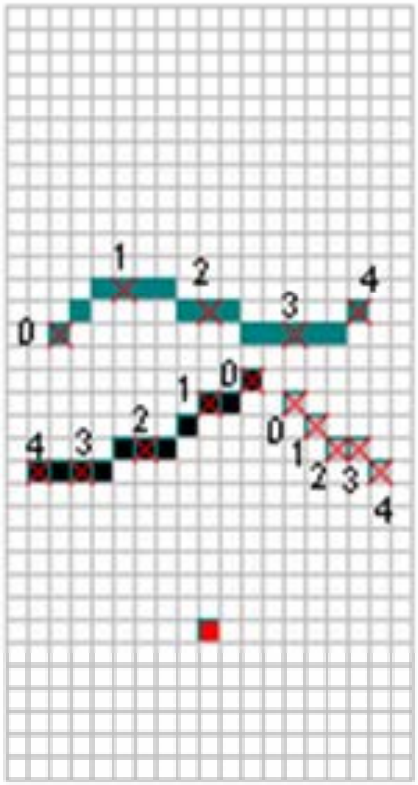
Pozycje *n* punktów charakterystycznych leżących na każdej linii obrazu są wykryte, gdzie *n* zależy od klasy badanego obrazu.

Jako przykład
rozpatrzymy obraz litery „ ***dzim”*** z alfabetu arabskiego
z trzema liniami

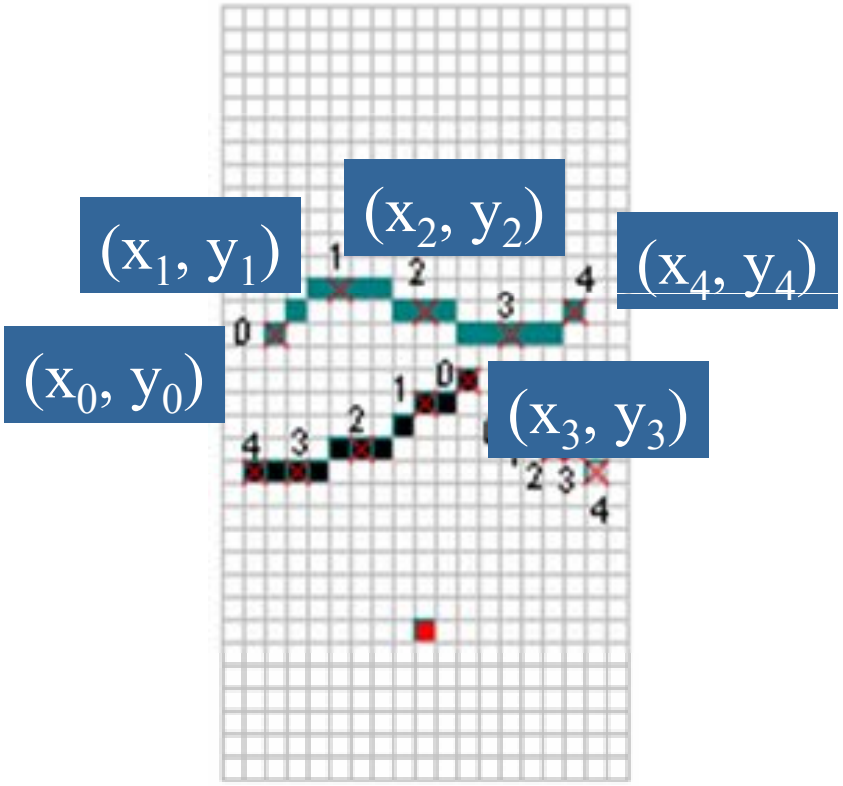


*a po ścienianiu i fragmentacji*

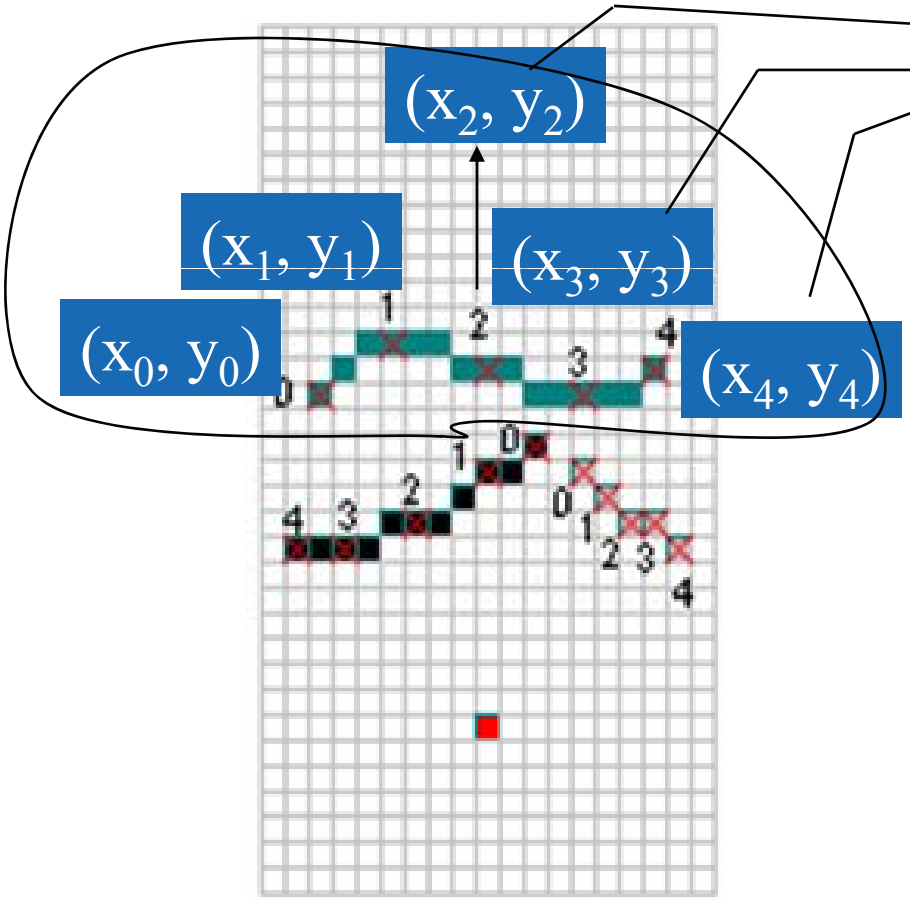



0
1
2
3
4
4
3
2
1
0
0
1
2
3
4

# Wybranie punktów charakterystycznych



# Wczytanie współrzędnych punktów
# ... w tym przykładzie, dla jednej linii




| | | | | |
|---|---|---|---|---|
| $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
| $y_0$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ |

# Tworzenie funkcji wymiernej

| | | | | |
|---|---|---|---|---|
| $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ |
| $y_0$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ |

$$f(s)=\frac{P(s)}{Q(s)}=\frac{x_0+x_1s+x_2s^2+x_3s^3+x_4s^4+\ldots}{y_0+y_1s+y_2s^2+y_3s^3+y_4s^4+\ldots}$$

# Rozwijanie w szereg Taylora

$$f(s)=\frac{P(s)}{Q(s)}=\frac{x_0+x_1s+x_2s^2+x_3s^3+x_4s^4+\ldots}{y_0+y_1s+y_2s^2+y_3s^3+y_4s^4+\ldots}$$



$$T(s)=c_0+c_1s+c_2s^2+\ldots+c_is^i+\ldots$$

# Stworzenie macierzy Töeplitza i obliczanie minimalnych wartości własnych dla jej podmacierzy

$$C_0 = c_0 = \frac{x_0}{y_0} \quad \text{daje} \quad \lambda_0 \qquad C_1 = \begin{bmatrix} c_0 & c_1 \\ c_1 & c_0 \end{bmatrix} \quad \text{daje} \quad \lambda_1$$

$$C_2 = \begin{bmatrix} c_0 & c_1 & c_2 \\ c_1 & c_0 & c_1 \\ c_2 & c_1 & c_0 \end{bmatrix} \quad \text{daje} \quad \lambda_2$$

Natomiast,

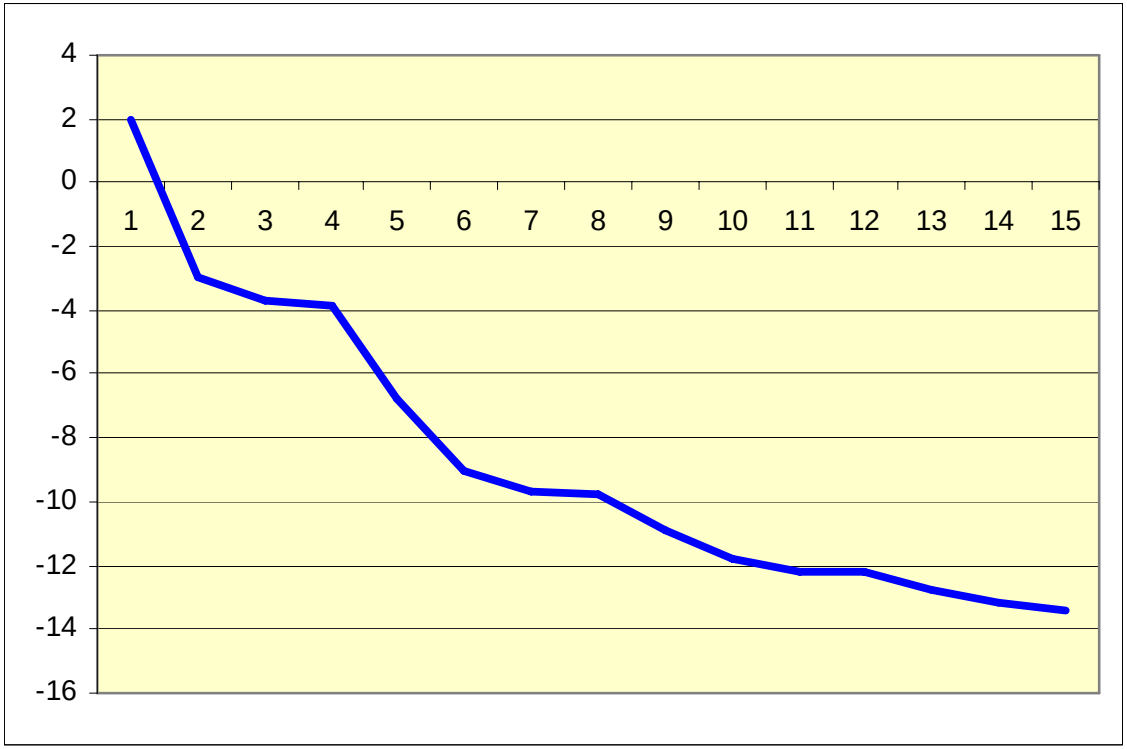
$$C_k = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_k \\ c_1 & c_0 & c_1 & \ddots & \vdots \\ c_2 & c_1 & c_0 & \ddots & c_2 \\ \vdots & \ddots & \ddots & \ddots & c_1 \\ c_k & \cdots & c_2 & c_1 & c_0 \end{bmatrix} \quad \text{daje } \lambda_k =, \ldots \text{itd.}$$

Otrzymane minimalne wartości własne stworzą szereg:

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_1 & c_0 & c_1 & \ddots & \vdots \\ c_2 & c_1 & c_0 & \ddots & c_2 \\ \vdots & \ddots & \ddots & \ddots & c_1 \\ c_{n-1} & \cdots & c_2 & c_1 & c_0 \end{bmatrix} \longrightarrow \begin{matrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_i \end{matrix}$$

$$\uparrow$$

$$T(s) = c_0 + c_1 s + c_2 s^2 + \ldots + c_i s^i + \ldots$$




$$\lambda_0$$

$$\lambda_1$$

$$\vdots$$

$$\lambda_n$$

$$FV = [\lambda_0, \lambda_1, \ldots, \lambda_n]$$

Szereg tych minimalnych wartości własnych maleje monotonicznie do określonej granicy.

$$\lambda_0 \geq \ldots \geq \lambda_i \geq \ldots \geq \lambda_n$$

$$\lim_{n \to \infty} \lambda^n = \min \Re f(s)$$

Ten fakt jest udowodniony zarówno teoretycznie
jak i eksperymentalnie.

Granica tutaj nie ma żadnego znaczenia chociaż w specyficznych zagadnieniach teorii obwodów elektronicznych oraz w filtrach cyfrowych odgrywa ważną rolę.

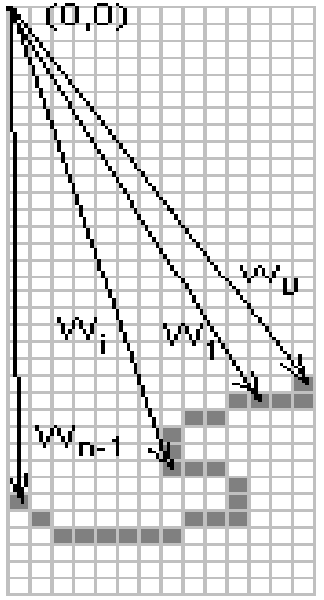
Są jeszcze inne sposoby wprowadzania danych do macierzy Töeplitza, czyli obliczania współczynników szeregu Taylora, bez konieczności dzielenia wielomianów:

1) $$c_i = \sqrt{x_i^2 + y_i^2}$$

2) $$c_0 = |r_0| - |r_i|, \quad c_1 = |r_1| - |r_2|, \ldots, c_n = |r_n|$$

3) $$c_i = |r_i| e^{j\varphi_i} \qquad \text{gdzie} \quad \begin{cases} |r_i| = \sqrt{x_i^2 + y_i^2} \\ \varphi_i = \tan^{-1} \dfrac{y_i}{x_i} \end{cases}$$

## *Różnica długości kolejnych wektorów*

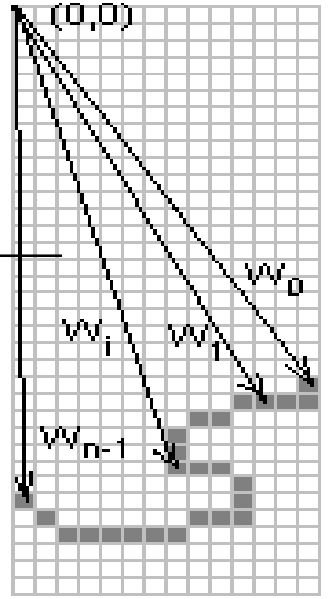



$$T(s) = c_0 + c_1 s + c_2 s^2 + \ldots + c_i s^i + \ldots$$

# *Różnica długości kolejnych wektorów*

$$c_i = \left|W_{i-1}\right| - \left|W_i\right|$$

$$i = 1,2,\ldots,n-1$$




$$T(s) = c_0 + c_1 s + c_2 s^2 + \ldots + c_i s^i + \ldots$$

… Żeby opis i analiza były skuteczne, prawidłowe ścienianie jest bardzo ważne.

Opracowałem algorytm do szkieletyzacji liter alfabetów, który został rozszerzony, żeby ścieniać dowolny obraz.

# Literatura


[1] Strike Force:
http://www.strikeforcetech.com/solutions/biometrics/asp.
September 2008.

[2] A. K. Jain and A. Ross, ”Multibiometric Systems", Comm.
ACM, vol. 47, no. 1, pp. 34-40, January 2004.

[3] K. Saeed (EiC), ”Spoofing and Anti-Spoofing in Biometrics”, IJBM-International Journal of Biometrics, vol. 1, no. 2, Inderscience Publishers, UK, 2008.

[4] A. K. Jain and S. Pankanti, ”A Touch of Money,” *IEEE*
Spectrum, vol. 43, no. 7, pp. 22-27, July 2006.

[5] K. Saeed, ”Image Analysis for Object Recognition,” Bialystok Technical University Press, Bialystok, Poland, 2004.

D Z I Ę K U J Ę