Zastosowanie zaawansowanych metod sztucznej inteligencji do wybranych problemów bezpieczeństwa informacji

Marcin Plata

Katedra Podstaw Informatyki, Politechnika Wrocławska

Opiekunowie naukowi:
prof. dr hab. inż. Marek Klonowski
dr inż. Piotr Syga

IPI PAN, 23 listopada 2020

- Bezpieczeństwo **w** AI:
  - ataki typu *adversarial examples*,
  - trening modeli w sposób zwiększający ich odporność,
  - *Generative Adversarial Networks* (GAN),
  - ...
- AI **w** bezpieczeństwie – metody AI w problemach z bezpieczeństwa:
  - autoryzacja biometryczna,
  - problem podszywania się (*spoofing*), np. *deepfake*,
  - steganografia, znakowanie wodne,
  - techniki ochrony prywatności,
  - wspomaganie kryminalistyki (*information forensics*),
  - zapobieganie atakom typu *phishing*,
  - wykrywanie anomalii w sieci,
  - ...

- Bezpieczeństwo **w** AI:
  - ataki typu *adversarial examples*,
  - trening modeli w sposób zwiększający ich odporność,
  - *Generative Adversarial Networks* (GAN),
  - ...
- AI **w** bezpieczeństwie – metody AI w problemach z bezpieczeństwa:
  - autoryzacja biometryczna,
  - problem podszywania się (*spoofing*), np. *deepfake*,
  - steganografia, znakowanie wodne,
  - techniki ochrony prywatności,
  - wspomaganie kryminalistyki (*information forensics*),
  - zapobieganie atakom typu *phishing*,
  - wykrywanie anomalii w sieci,
  - ...

Watermarking – technologie znaków wodnych:

- **MP**, P. Syga,
  Robust Spatial-spread Deep Neural Image Watermarking
  [IEEE TrustCom 2020, CORE A]
- **MP**, P. Syga
  Robust watermarking with double detector–discriminator approach
  [złożona na CVPR 2021]

Biometria:

- Identyfikacja na podstawie mimiki twarzy:
  MP, P. Syga, M. Klonowski
  How to Save Your Face: a Facial Recognition Method Robust Against Image Reconstruction
  [IEEE BTAS 2019]
- Voice Spoofing:
  R. Białobrzeski, M. Kośmider, M. Matuszewski, **MP**, A. Rakowski
  Robust Bayesian and Light Neural Networks for Voice Spoofing Detection
  [INTERSPEECH 2019, CORE A]

  Rozwiązanie zajęło 5-te miejsce w konkursie ASVspoof 2019.
- Identyfikacja na podstawie kształtu dłoni:
  MP, M. Klonowski, P. Syga
  User authorization based on hand geometry without special equipment
  [Pattern Recognition, Vol. 73, 2018]

Cel:

Dodanie do kopii obrazu (wideo, ścieżki dźwiękowej) niezauważalnych zmian (wplecenie wiadomości), które umożliwią jej identyfikację.

Atak:

Takie przekształcenie treści, aby uniemożliwić identyfikację bez istotnego pogarszania własności wizualnych obrazu. Największe obecnie wyzwanie to kompresja, np. JPEG.

Istotne jest zapewnienie balansu między:

- odpornością na ataki (*robustness*),
- przejrzystością/jakością obrazu (*transparency*),
- pojemnością wiadomości (*capacity*),
- *złożoność obliczeniowa (complexity)*.

Watermarking $\neq$ steganografia.

Cel:

Dodanie do kopii obrazu (wideo, ścieżki dźwiękowej) niezauważalnych zmian (wplecenie wiadomości), które umożliwią jej identyfikację.

Atak:

Takie przekształcenie treści, aby uniemożliwić identyfikację bez istotnego pogarszania własności wizualnych obrazu. Największe obecnie wyzwanie to kompresja, np. JPEG.

Istotne jest zapewnienie balansu między:

- odpornością na ataki (*robustness*),
- przejrzystością/jakością obrazu (*transparency*),
- pojemnością wiadomości (*capacity*),
- *złożoność obliczeniowa (complexity)*.

Watermarking $\neq$ steganografia.

Cel:

Dodanie do kopii obrazu (wideo, ścieżki dźwiękowej) niezauważalnych zmian (wplecenie wiadomości), które umożliwią jej identyfikację.

Atak:

Takie przekształcenie treści, aby uniemożliwić identyfikację bez istotnego pogarszania własności wizualnych obrazu. Największe obecnie wyzwanie to kompresja, np. JPEG.

Istotne jest zapewnienie balansu między:

- odpornością na ataki (*robustness*),
- przejrzystością/jakością obrazu (*transparency*),
- pojemnością wiadomości (*capacity*),
- *złożoność obliczeniowa (complexity)*.

Watermarking $\neq$ steganografia.

Cel:

Dodanie do kopii obrazu (wideo, ścieżki dźwiękowej) niezauważalnych zmian (wplecenie wiadomości), które umożliwią jej identyfikację.

Atak:

Takie przekształcenie treści, aby uniemożliwić identyfikację bez istotnego pogarszania własności wizualnych obrazu. Największe obecnie wyzwanie to kompresja, np. JPEG.

Istotne jest zapewnienie balansu między:

- odpornością na ataki (*robustness*),
- przejrzystością/jakością obrazu (*transparency*),
- pojemnością wiadomości (*capacity*),
- *złożoność obliczeniowa (complexity)*.

Watermarking $\neq$ steganografia.

- LSB – Least Significant Bits
- Transformaty – Dyskretna Transformata Cosinusowa (DCT), transformaty falkowe, Tranformata Fouriera
- Rozkład według wartości osobliwych (SVD)
- Pierwsze rozwiązanie „end-to-end” oparte na sieciach neuronowych:
  J. Zhu, R. Kaplan, J. Johnson, L. Fei-Fei,
  HiDDeN: Hiding Data With Deep Networks,
  ECCV 2018

M. Plata, P. Syga, *Robust Spatial-spread Deep Neural Image Watermarking* [IEEE TrustCom 2020]

Opis:

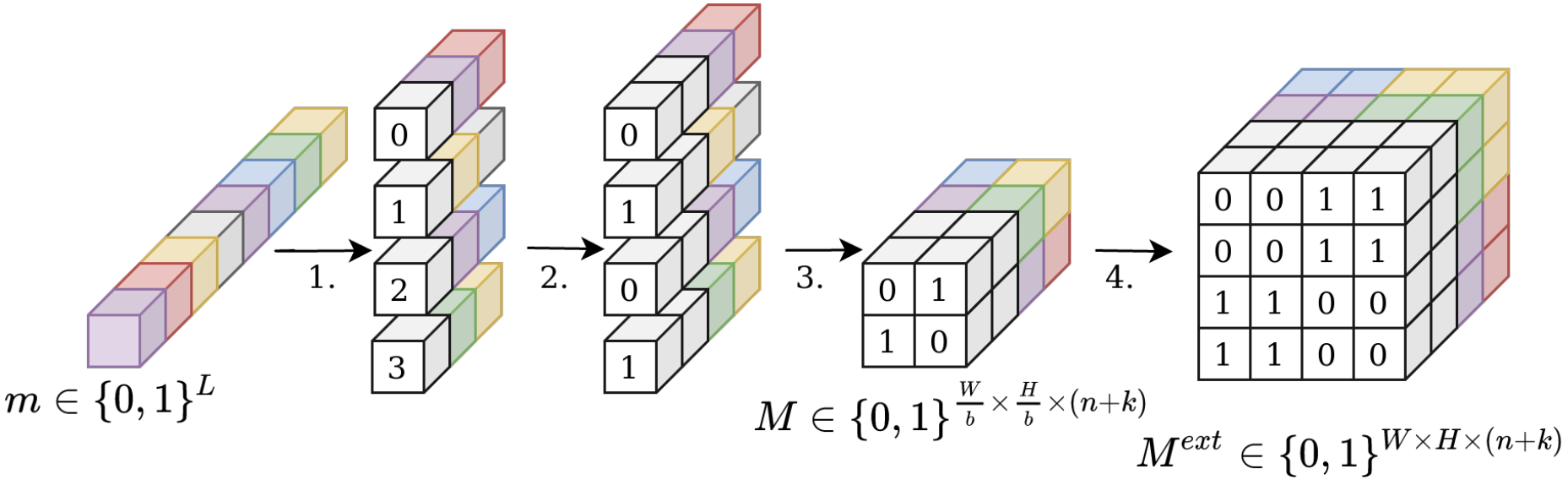
- Moduł do rozprzestrzenienia wiadomości w domenie przestrzennej.
- Opracowanie funkcji kosztu do trenowania nowego modułu.
- Wzrost odporności modelu przy utrzymaniu pojemności i jakości obrazu.
- Uwzględnienie nowych typów ataku.
- Analiza i pogrupowanie ataków pod kątem ich typu, co ułatwia zbalansowany wybór ataków do treningu sieci.

M. Plata, P. Syga, *Robust Spatial-spread Deep Neural Image Watermarking* [IEEE TrustCom 2020]

Opis:

- Moduł do rozprzestrzenienia wiadomości w domenie przestrzennej.
- Opracowanie funkcji kosztu do trenowania nowego modułu.
- Wzrost odporności modelu przy utrzymaniu pojemności i jakości obrazu.
- Uwzględnienie nowych typów ataku.
- Analiza i pogrupowanie ataków pod kątem ich typu, co ułatwia zbalansowany wybór ataków do treningu sieci.

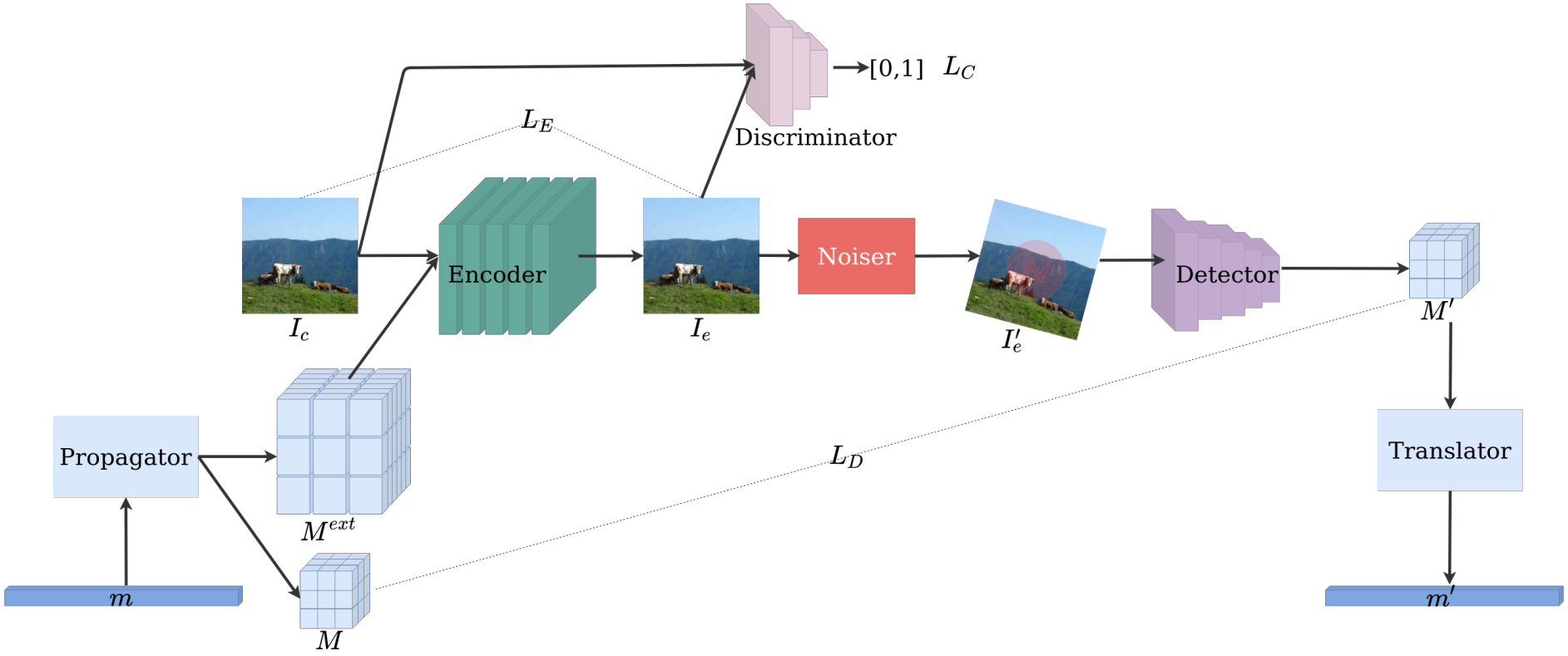
Architektura modułu *Propagator*:



$$s_i = bin_n(i) \| (m_{ki}, m_{ki+1} \ldots, m_{ki+k-1})$$

$$i \in \{0, 1, \ldots, \frac{L}{k} - 1\}$$

Architektura metody *Spatial*:



Funkcja kosztu między oryginalnym i zakodowanym obrazem:

$$L_E(I_c, I_e) = \mathrm{MSE}(I_c, I_e) = \frac{1}{H \cdot W \cdot \mathrm{Ch}} ||I_c - I_e||_2^2, \tag{1}$$

Funkcja kosztu między zakodowaną i odczytaną wiadomością:

$$L_D^{mean}(M, M') = \frac{b^2}{H \cdot W} \sum_{h=0}^{H_b} \sum_{w=0}^{W_b} Mean(|M_{hw} - M'_{hw}|) = \frac{b^2}{H \cdot W \cdot (n+k)} ||M - M'||_1 \tag{2}$$

$$L_D^{var}(M, M') = \frac{b^2}{H \cdot W} \sum_{h=0}^{H_b} \sum_{w=0}^{W_b} Var(|M_{hw} - M'_{hw}|). \tag{3}$$

Funkcja kosztu między oryginalnym i zakodowanym obrazem:

$$L_E(I_c, I_e) = \mathrm{MSE}(I_c, I_e) = \frac{1}{H \cdot W \cdot \mathrm{Ch}} ||I_c - I_e||_2^2, \tag{1}$$

Funkcja kosztu między zakodowaną i odczytaną wiadomością:

$$L_D^{mean}(M, M') = \frac{b^2}{H \cdot W} \sum_{h=0}^{H_b} \sum_{w=0}^{W_b} Mean(|M_{hw} - M'_{hw}|) = \frac{b^2}{H \cdot W \cdot (n+k)} ||M - M'||_1 \tag{2}$$

$$L_D^{var}(M, M') = \frac{b^2}{H \cdot W} \sum_{h=0}^{H_b} \sum_{w=0}^{W_b} Var(|M_{hw} - M'_{hw}|). \tag{3}$$

Funkcja kosztu dla *adversarial training*:

$$L_C(I_c, I_e) = log(1 - C(I_e)) + log(C(I_c)). \tag{4}$$

Chcemy zminimalizować:

Dla enkodera E i dekodera D:

$$\mathbb{E}_{I_c,M}[\lambda_E L_E + \lambda_D^{mean} L_D^{mean} + \lambda_D^{var} L_D^{var} + \lambda_C L_C], \tag{5}$$

Dla dyskriminatora C:

$$\mathbb{E}_{I_c}[-L_C]. \tag{6}$$

Funkcja kosztu dla *adversarial training*:

$$L_C(I_c, I_e) = log(1 - C(I_e)) + log(C(I_c)). \tag{4}$$

Chcemy zminimalizować:

Dla enkodera E i dekodera D:

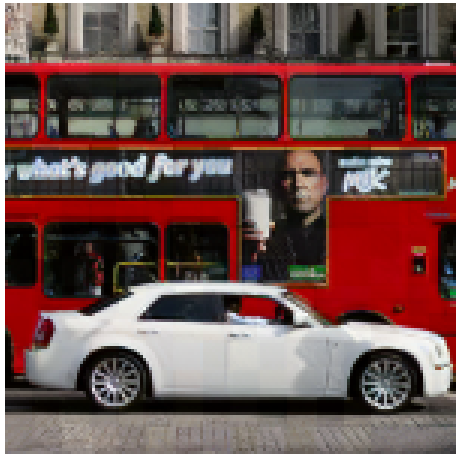
$$\mathbb{E}_{I_c,M}[\lambda_E L_E + \lambda_D^{mean} L_D^{mean} + \lambda_D^{var} L_D^{var} + \lambda_C L_C], \tag{5}$$

Dla dyskriminatora C:

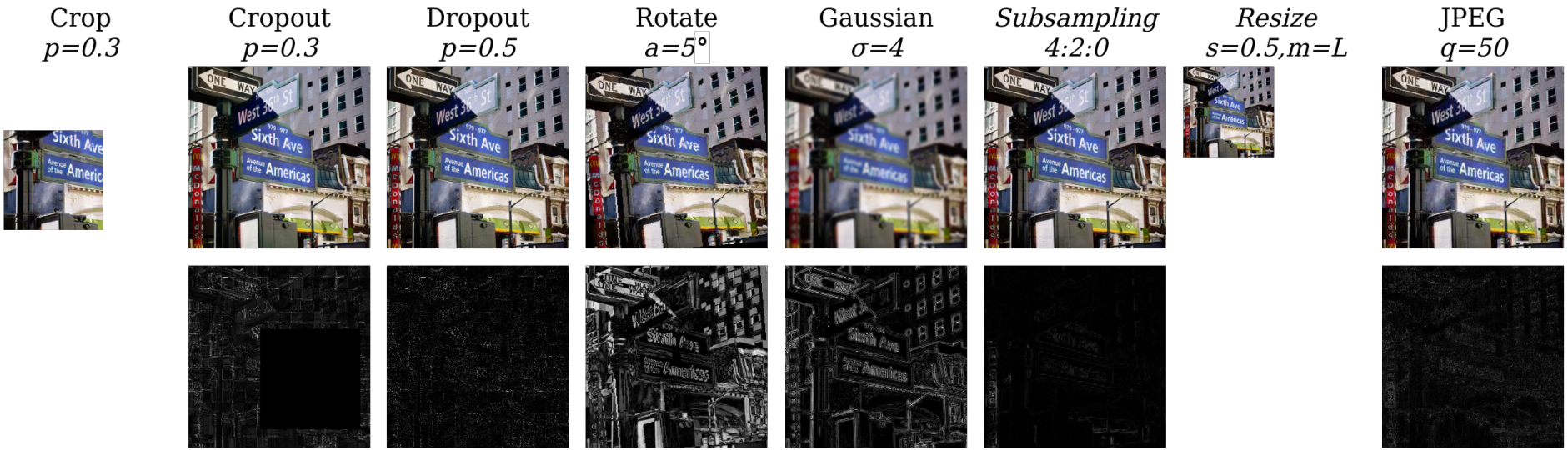
$$\mathbb{E}_{I_c}[-L_C]. \tag{6}$$

Wyniki jakości obrazu dla metody *Spatial*:
$PSNR(Y) = 30.19dB$, $PSNR(Cb) = 37.81dB$, $PSNR(Cr) = 37.46dB$

Wyniki jakości obrazu dla metody *Spatial*:



Wizualizacja ataków:



Wyniki selektywnego doboru ataków do modułu *Noiser*:

Attacks	Noiser Layers		
	Identity	Crop([0.3, 0.9]) Dropout([0.3, 0.9])	Gaussian({3, 5}) Subsampling(4:2:0)
Identity	0.999	0.991	0.985
Crop(p=0.3)	0.847	0.894	0.833
Cropout(p=0.3)	0.793	0.875	0.672
Dropout(p=0.5)	0.530	0.972	0.574
Rotate(α=5°)	0.754	0.821	0.780
Gaussian(σ=5)	0.823	0.564	0.981
Subsampling(4:2:0)	0.524	0.623	0.980
Resize(s=0.5, m=L)	0.511	0.532	0.735
JPEG(q=95)	0.502	0.512	0.783

M. Plata, P. Syga
Robust watermarking with double detector–discriminator approach
[złożona na CVPR 2021]

Opis:

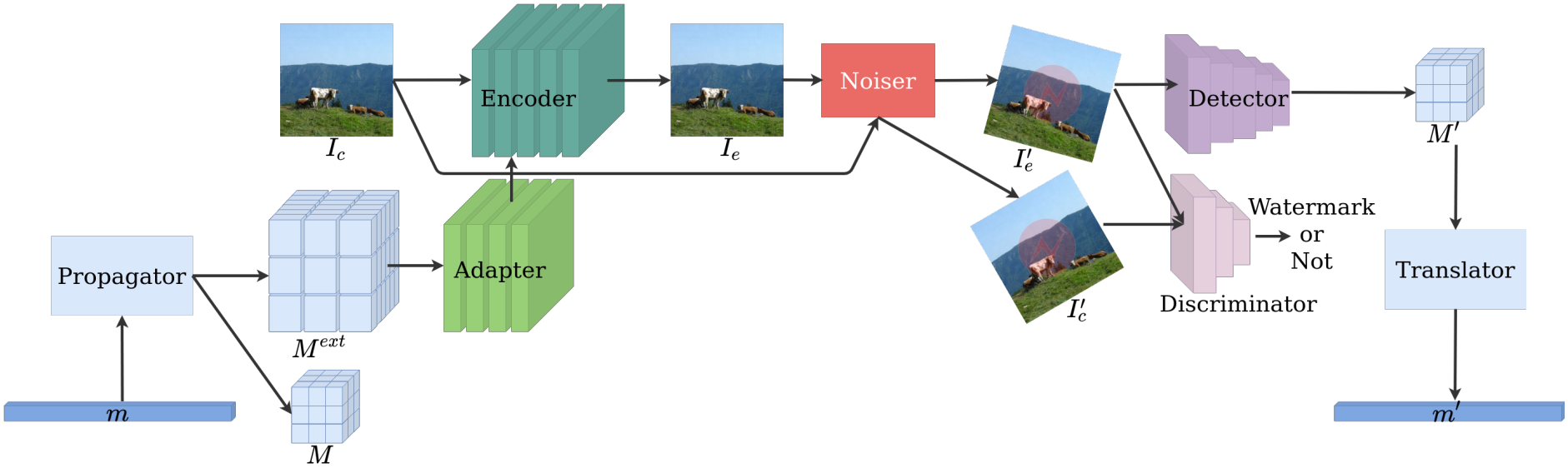
- Nowy moduł do wykrywania obecności znaku wodnego.
- Propozycja nowej formuły testowej.
- Dodatkowy moduł – *Adapter*.
- Wzrost odporności modelu przy utrzymaniu pojemności i jakości.
- Adaptacja rozwiązania do wideo.

M. Plata, P. Syga
Robust watermarking with double detector–discriminator approach
[złożona na CVPR 2021]

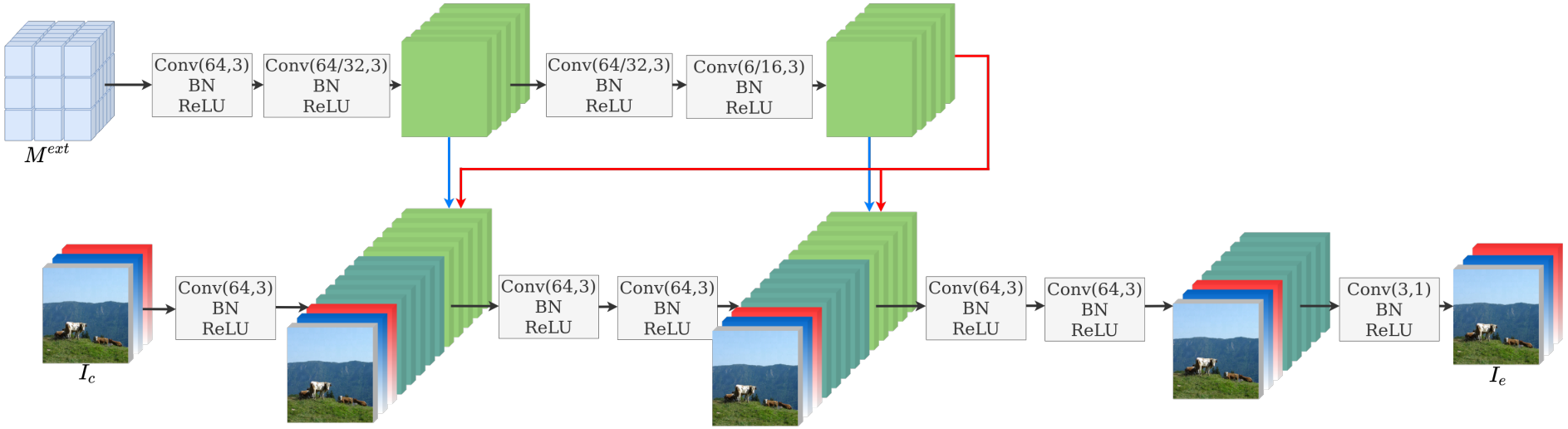
Opis:

- Nowy moduł do wykrywania obecności znaku wodnego.
- Propozycja nowej formuły testowej.
- Dodatkowy moduł – *Adapter*.
- Wzrost odporności modelu przy utrzymaniu pojemności i jakości.
- Adaptacja rozwiązania do wideo.

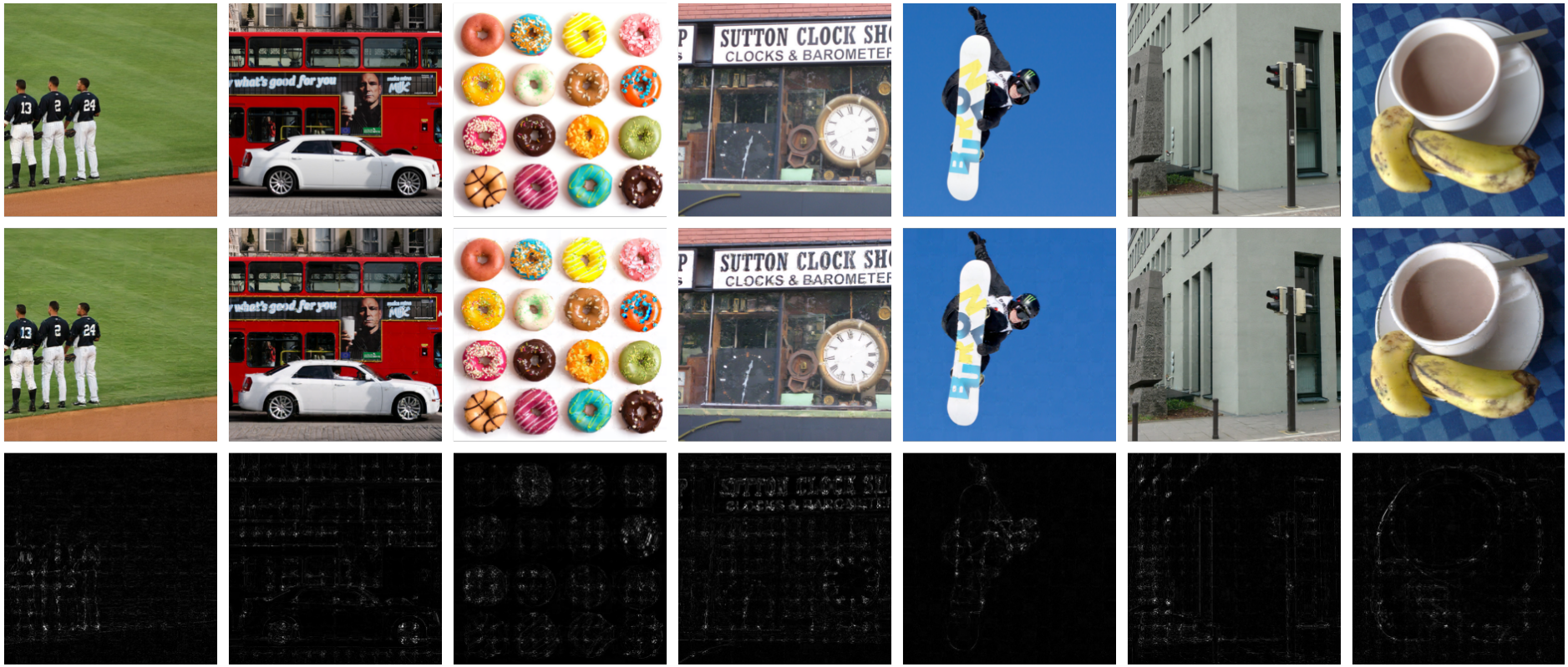
Architektura metody *DDD-WM*:



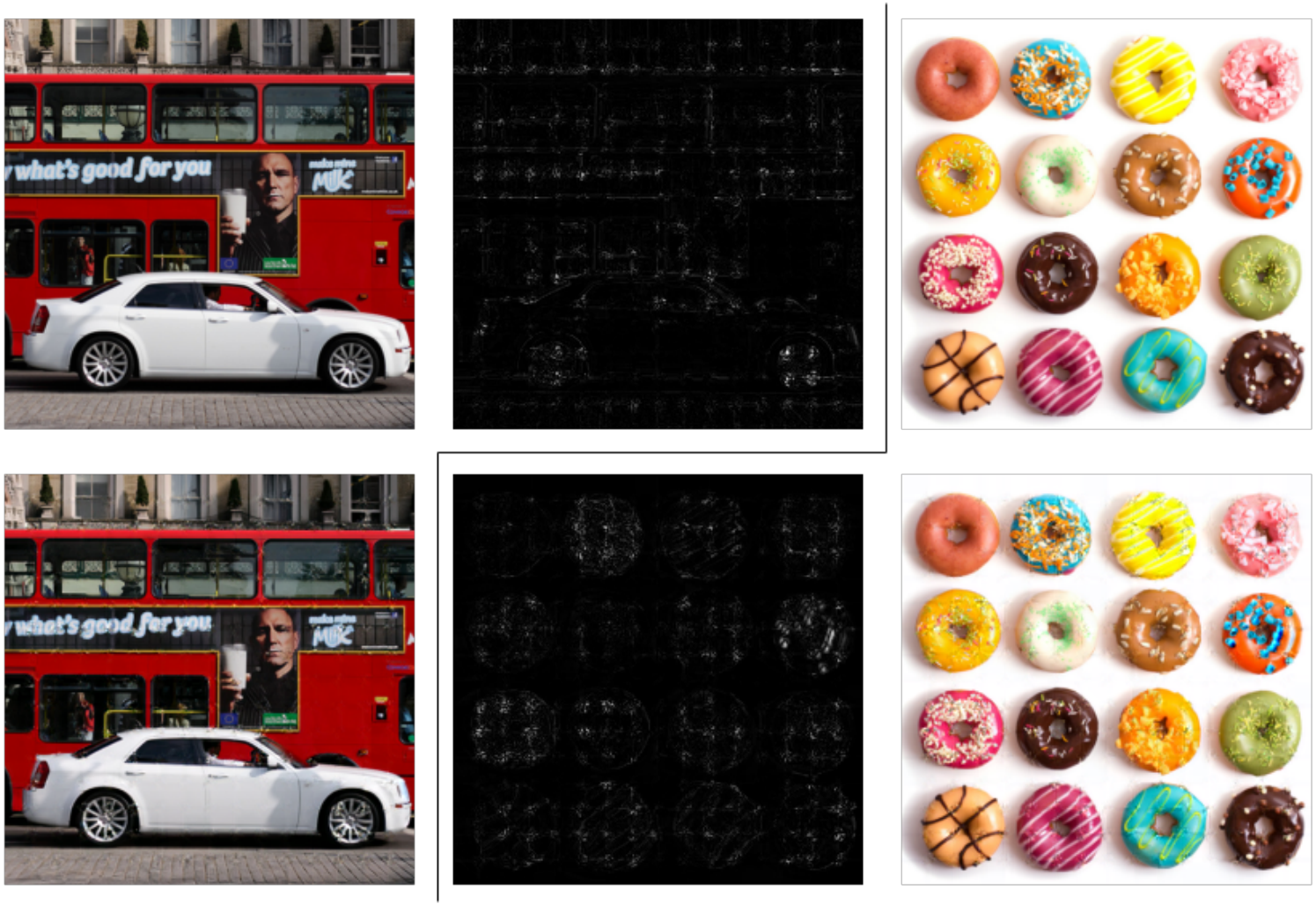
Architektura modułu do kodowania w *DDD-WM*:



Wyniki jakości obrazu dla metody *DDD-WM*:
$PSNR(Y) = 31.57dB$, $PSNR(Cb) = 44.04dB$, $PSNR(Cr) = 44.90dB$



Wyniki jakości obrazu dla metody *DDD-WM*:



Wyniki odporności:

Attacks	DDD-WM			Spatial	HiDDeN	DADW	RedMark	RaviGAN
	Plain	Sparse	w/o A					
No attack	1.000	1.000	1.000	1.000	1.000	1.000	1.000	-
Crop($p = 0.3$)	0.860	0.831	0.834	0.832	**1.000**	**1.000**	-	-
Cropout($p = 0.3$)	0.921	0.902	0.892	0.902	**0.940**	-	0.925	-
Dropout($p = 0.5$)	0.981	0.856	0.963	0.972	**1.000**	**1.000**	≈0.99	-
Rotate($\alpha = 5°$)	**0.956**	0.716	0.884	0.842	-	-	-	-
Gaussian($\sigma = 2$)	**0.991**	0.935	0.981	0.986	0.960	0.600	0.5	-
Gaussian($\sigma = 4$)	**0.989**	0.974	0.984	0.982	0.820	0.500	0.5	-
Subsampling(4:2:0)	**0.993**	0.991	0.985	0.984	-	-	-	-
Resize($s = 0.5$, $m = N$)	**0.913**	0.793	0.849	0.849	-	0.671	0.819	-
Resize($s = 0.5$, $m = L$)	0.886	0.658	0.898	**0.908**	-			-
JPEG($q = 50$)	0.902	**0.935**	0.829	0.831	0.670	0.817	0.746	-
MJPEG	0.968	**0.981**	0.746	-	-	-	-	0.965
MPEG	0.945	**0.951**	0.689	-	-	-	-	0.932

Walidacja podejścia DDD-WM:

- TP, gdy I_{en} oraz $Discriminator(I_{en}) > t$.
- FP, gdy I_{co} oraz $Discriminator(I_{co}) > t$.
- $TIR = Pr(\text{poprawny klucz}|TP)$.
- $FIR = Pr(\text{błędny klucz}|TP)Pr(I_{en}) + Pr(FP)Pr(I_{co})$.

Wyniki odporności mierzone nową metodą:

Attacks	Double			Naïve		
	TIR	FIR_{en}	FIR_{co}	TIR	FIR_{en}	FIR_{co}
No attack	0.999	0.001	0.000	0.999	0.001	0.005
Crop($p = 0.3$)	0.219	**0.122**	**0.000**	0.219	0.594	0.707
Cropout($p = 0.3$)	0.550	**0.193**	**0.001**	0.556	0.372	0.720
Dropout($p = 0.5$)	0.940	0.007	0.008	0.951	0.004	0.006
Rotate($\alpha = 5°$)	0.983	0.016	**0.000**	0.979	0.009	0.119
Gaussian($\sigma = 2$)	0.950	0.000	0.474	0.998	0.000	**0.130**
Gaussian($\sigma = 4$)	0.956	0.001	0.410	0.999	0.001	**0.005**
Subsampling(4:2:0)	0.971	0.000	0.000	0.975	0.000	0.001
Resize($s = 0.5, m = N$)	0.630	**0.119**	**0.602**	0.645	0.284	0.717
Resize($s = 0.5, m = L$)	0.540	**0.126**	0.701	0.542	0.371	0.707
JPEG($q = 50$)	0.712	0.069	**0.000**	0.712	0.044	0.118

Źródło: www.findbiometrics.com

Definicja

Technologia umożliwiająca identyfikację użytkowników w systemie na podstawie ich cech biologicznych, np. rysy twarzy, odcisk palca, kontur dłoni, tęczówka oka.

Rozważane modele biometryczne:

- Weryfikacja - do mierzenia skuteczności wykorzystujemy *False Accept Rate* (FAR) and *False Reject Rate* (FRR).
- Identyfikacja - do mierzenia skuteczności wykorzystujemy *Identification Rate* (IR). W teorii mówi się również o n krotnej weryfikacji - $FAR_{Id} = 1 - (1 - FAR)^{n-1}$ i $FRR_{Id} = FRR$.

Problemy:

- Dane niezbywalne.
- Nie ma opcji „reset hasła".
- Mogą być pobrane bez wiedzy użytkowania.
- Kwestie prywatności – *reconstruction attack*.

Rozważane modele biometryczne:

- Weryfikacja - do mierzenia skuteczności wykorzystujemy *False Accept Rate* (FAR) and *False Reject Rate* (FRR).
- Identyfikacja - do mierzenia skuteczności wykorzystujemy *Identification Rate* (IR). W teorii mówi się również o n krotnej weryfikacji - $FAR_{Id} = 1 - (1 - FAR)^{n-1}$ i $FRR_{Id} = FRR$.

Problemy:

- Dane niezbywalne.
- Nie ma opcji „reset hasła".
- Mogą być pobrane bez wiedzy użytkowania.
- Kwestie prywatności – *reconstruction attack*.

M. Plata, P. Syga, M. Klonowski,
How to Save Your Face: a Facial Recognition Method Robust Against Image Reconstruction [IEEE BTAS 2019]

Opis:

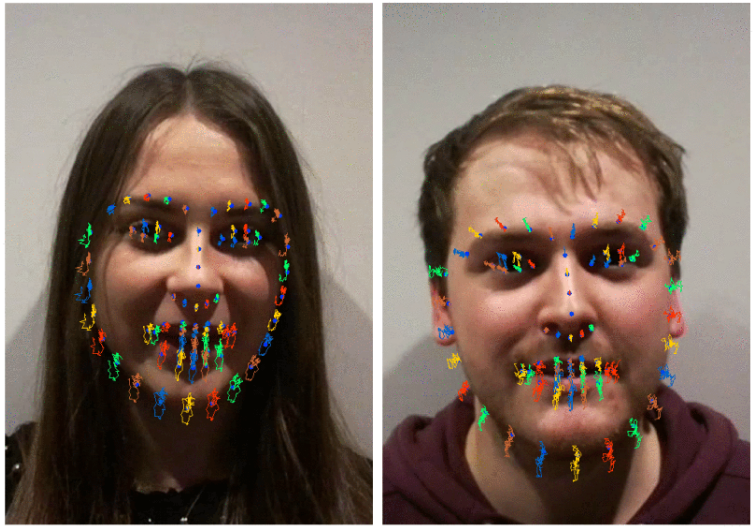
- Identyfikacja osób na podstawie mimiki twarzy.
- Zwiększenie prywatności metod opartych o rozpoznawanie twarzy.
- Do bazy zapisujemy jedynie znormalizowany wektor przesunięć, nie zapisujemy położenia punktów początkowych.
- W celu zwiększenia prywatności usuwamy najbardziej skorelowane cechy z cechami statycznymi.
- Rozwiązanie jest *text-dependent* - każdy użytkownik wypowiada tę samą frazę.

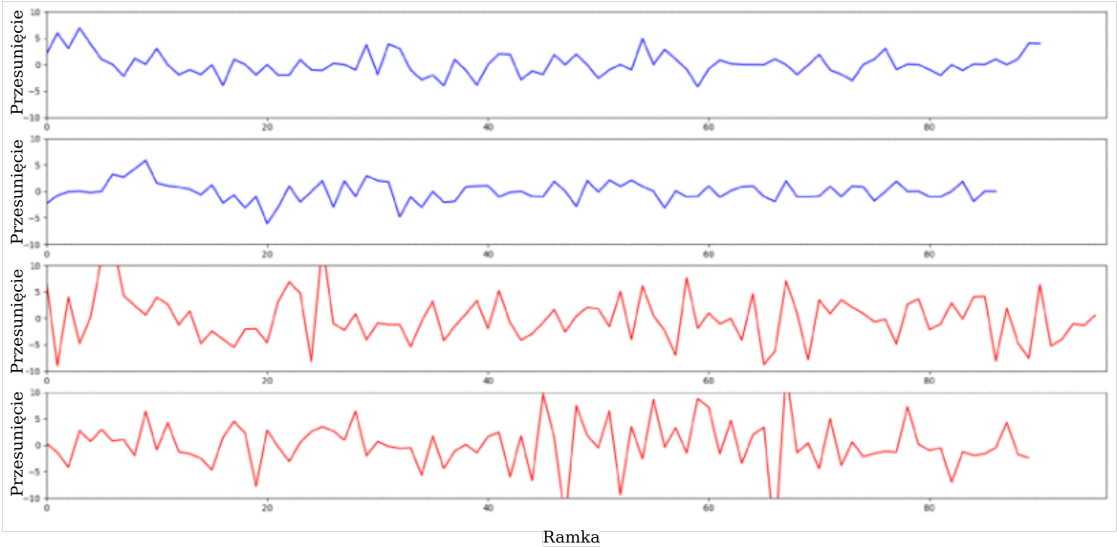
M. Plata, P. Syga, M. Klonowski,
How to Save Your Face: a Facial Recognition Method Robust Against Image Reconstruction [IEEE BTAS 2019]

Opis:

- Identyfikacja osób na podstawie mimiki twarzy.
- Zwiększenie prywatności metod opartych o rozpoznawanie twarzy.
- Do bazy zapisujemy jedynie znormalizowany wektor przesunięć, nie zapisujemy położenia punktów początkowych.
- W celu zwiększenia prywatności usuwamy najbardziej skorelowane cechy z cechami statycznymi.
- Rozwiązanie jest *text-dependent* - każdy użytkownik wypowiada tę samą frazę.

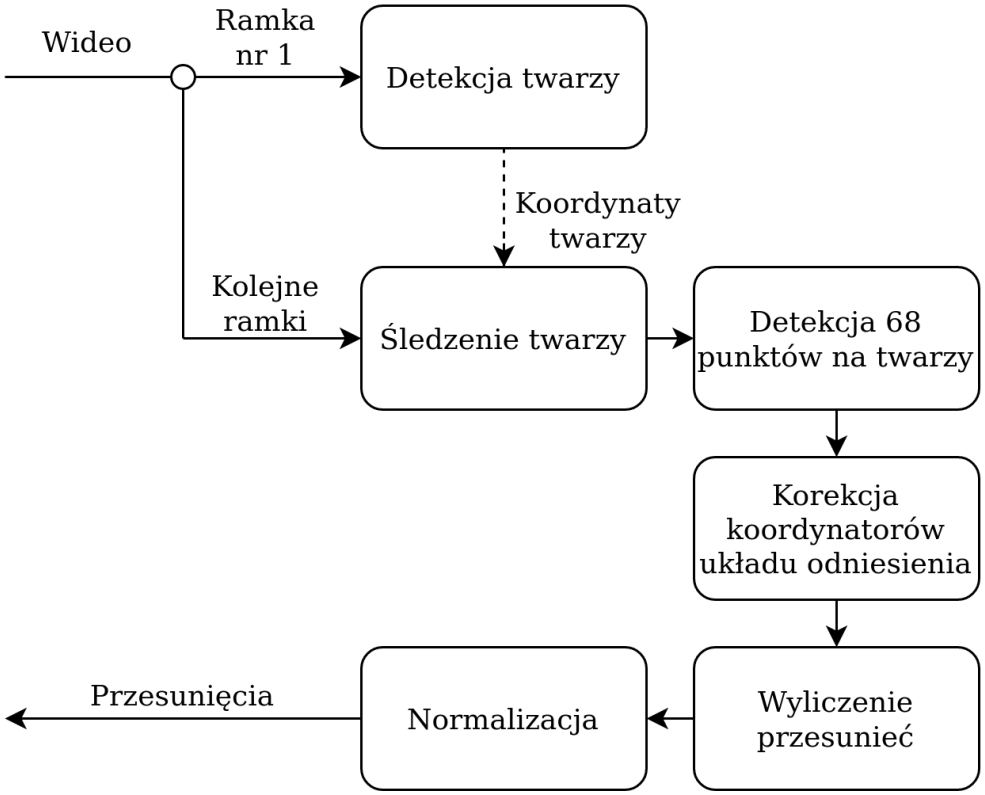
Wizualizacja otrzymanych cech biometrycznych:





Algorytm:

Detekcja cech biometrycznych:



Porównanie cech biometrycznych:

$D^{2N \times F}$ - wektor cech

$E^{2N \times F}$ - wektor cech

$$s_n^{DE} = DTW(D_n, E_n) \; \forall_{n \in \{1,\ldots,2N\}}$$

Określenie podobieństwa wektorów:

$$SVM(s^{DE}) : \mathbb{R}^{2N} \rightarrow [0, 1]$$

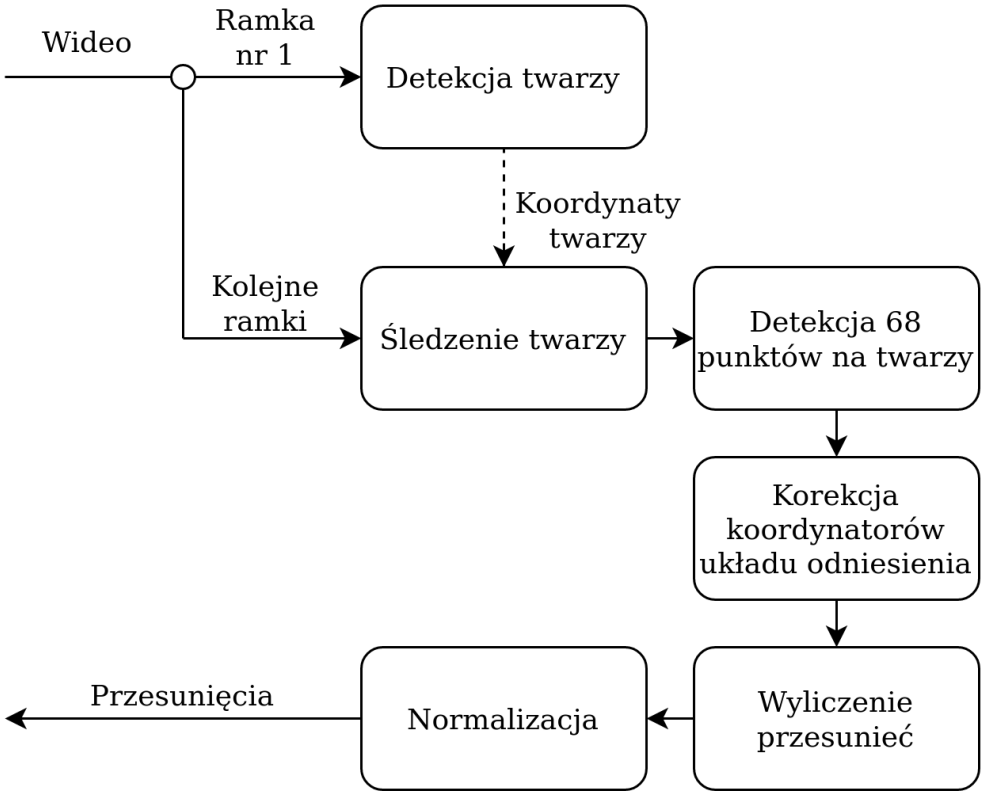
Trenowanie metody SVM:

$$x_i = s^{DE}$$

$$y_i = \begin{cases} 1, & \text{gdy D i E ten sam użytkownik} \\ 0, & \text{w p.p.} \end{cases}$$

Algorytm:

Detekcja cech biometrycznych:



Porównanie cech biometrycznych:

$D^{2N\times F}$ - wektor cech

$E^{2N\times F}$ - wektor cech

$$s_n^{DE} = DTW(D_n, E_n)\ \forall_{n\in\{1,\ldots,2N\}}$$

Określenie podobieństwa wektorów:

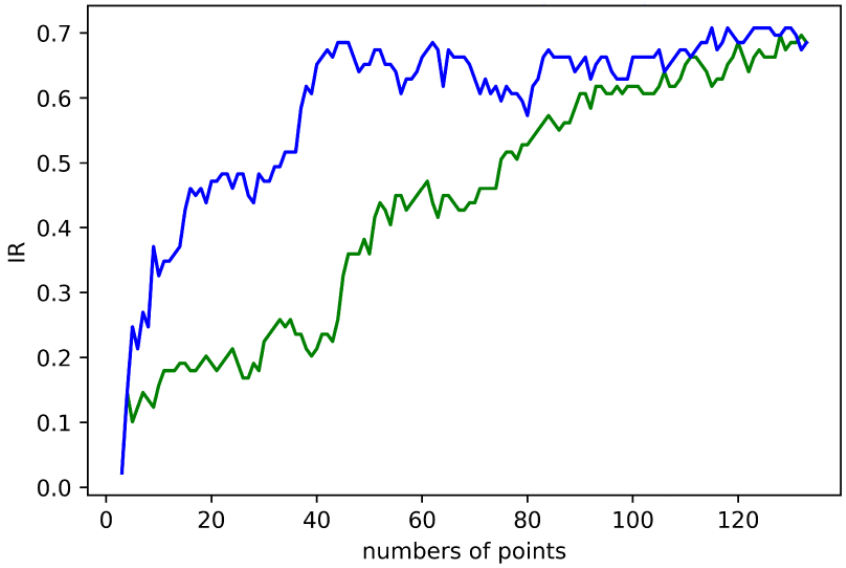
$$SVM(s^{DE}) : \mathbb{R}^{2N} \rightarrow [0,1]$$

Trenowanie metody SVM:

$$x_i = s^{DE}$$

$$y_i = \begin{cases} 1, & \text{gdy D i E ten sam użytkownik} \\ 0, & \text{w p.p.} \end{cases}$$

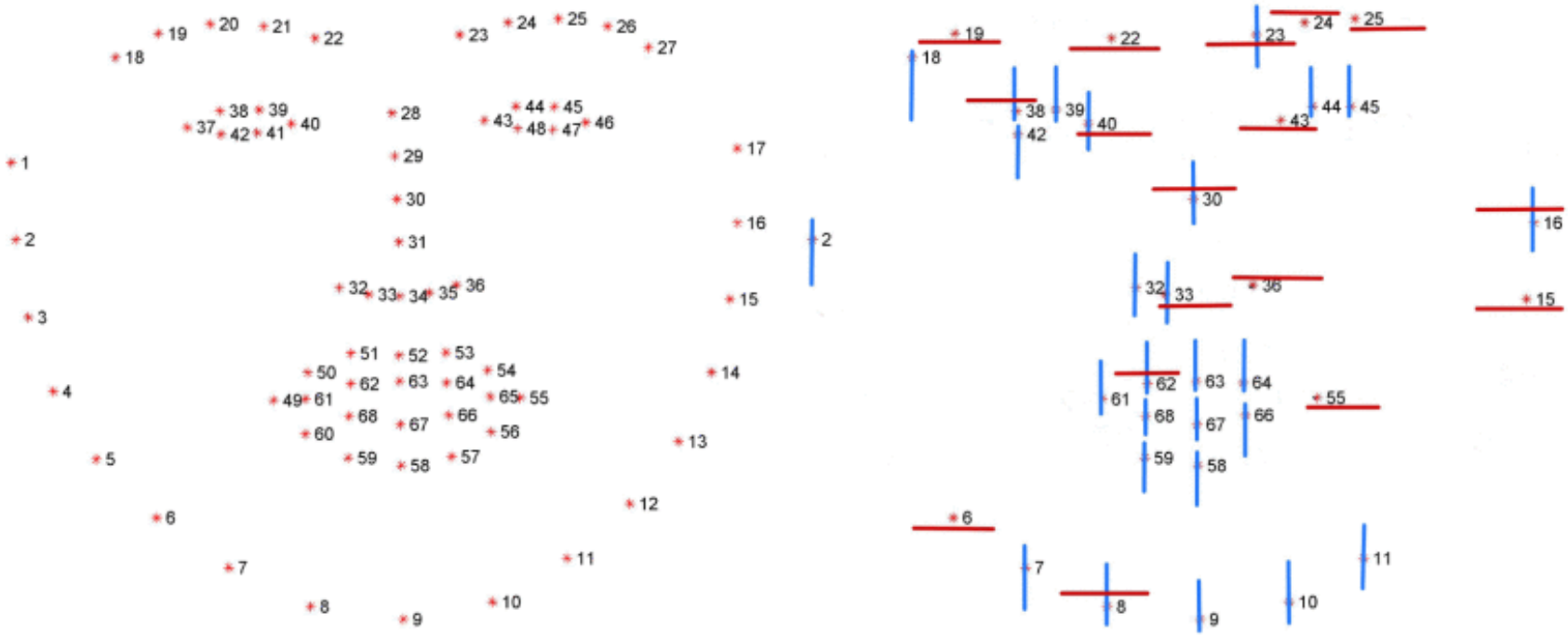
Wyniki, usuwanie cech (nie)skorelowanych:



niebieski - nieskorelowane usuwane najpierw
zielony - skorelowane usuwane najpierw

- Eksperymenty przeprowadzone dla próbki 34 użytkowników.
- $IR = 70.78\%$ dla 115 cech i 3 sampli w zapisanych bazie.
- $IR = 68.54\%$ dla 44 cech i 3 sampli w zapisanych bazie.
- przy uśnięciu 50 najbardziej skorelowanych cech: $IR > 50\%$.

44 cechy dla których algorytm osiąga $IR = 68.54\%$:



(a) (b)

R. Białobrzeski et al., *Robust Bayesian and Light Neural Networks for Voice Spoofing Detection* [INTERSPEECH 2019]

Opis metody:

- Rozwiązanie „lekkie", do wykorzystania w urządzeniach o małych zasobach.
- Łączy dwa podejścia:
  - Bayesowskie sieci neuronowe - warstwa Flipout,
  - Light Convolutional Neural Network - warstwa Max Feature Map.
- *Attack-Out Cross-Validation*.
- Wizualizacja złożoności wariantów ataku.

Rozważany atak:

- atak typu odtwarzanie (*replay attack*),
- dostęp fizyczny (PA),
- trzy warianty jakości odtwarzania (*high*, *medium*, *low*),
- trzy warianty odległości atakującego od mówcy (*10-50cm*, *50-100cm*, *>100cm*).

R. Białobrzeski et al., *Robust Bayesian and Light Neural Networks for Voice Spoofing Detection* [INTERSPEECH 2019]

Opis metody:

- Rozwiązanie „lekkie”, do wykorzystania w urządzeniach o małych zasobach.
- Łączy dwa podejścia:
  - Bayesowskie sieci neuronowe - warstwa Flipout,
  - Light Convolutional Neural Network - warstwa Max Feature Map.
- *Attack-Out Cross-Validation*.
- Wizualizacja złożoności wariantów ataku.

Rozważany atak:

- atak typu odtwarzanie (*replay attack*),
- dostęp fizyczny (PA),
- trzy warianty jakości odtwarzania (*high*, *medium*, *low*),
- trzy warianty odległości atakującego od mówcy (*10-50cm*, *50-100cm*, *>100cm*).

R. Białobrzeski et al., *Robust Bayesian and Light Neural Networks for Voice Spoofing Detection* [INTERSPEECH 2019]

Opis metody:

- Rozwiązanie „lekkie”, do wykorzystania w urządzeniach o małych zasobach.
- Łączy dwa podejścia:
  - Bayesowskie sieci neuronowe - warstwa Flipout,
  - Light Convolutional Neural Network - warstwa Max Feature Map.
- *Attack-Out Cross-Validation*.
- Wizualizacja złożoności wariantów ataku.

Rozważany atak:

- atak typu odtwarzanie (*replay attack*),
- dostęp fizyczny (PA),
- trzy warianty jakości odtwarzania (*high*, *medium*, *low*),
- trzy warianty odległości atakującego od mówcy (*10-50cm*, *50-100cm*, *>100cm*).

Eksperymenty z siecią Bayesowska:

Type	Full datastet		20% of the dataset	
	min-tDCF	*ERR (%)*	*min-tDCF*	*ERR (%)*
		Fold 0		
Bayes	0.02561	0.00961	**0.04821**	**0.01536**
Non	**0.00912**	**0.00399**	0.05075	0.01667
		Fold 1		
Bayes	0.00014	7.36e−5	**0.00029**	**0.00014**
Non	**7.36e−5**	**3.68e−5**	0.00066	0.00042
		Fold 2		
Bayes	0.00072	0.00029	0.00315	0.0012
Non	**0.00018**	**9.09e−5**	**0.00261**	**0.00075**

Wyniki dla całego systemu (*ensemble*):

Dataset	*Development*		*Evaluation*	
Model	*min-tDCF*	*ERR (%)*	*min-tDCF*	*ERR (%)*
		Baseline models:		
LFCC-GMM	0.2554	11.96	0.3017	13.54
CQCC-GMM	0.1953	9.87	0.2454	11.04
Bayesian NN	0.0316	1.18	0.0433	1.66
LCNN	0.0516	2.46	0.0600	2.33
Ensemble	**0.0170**	**0.78**	**0.0219**	**0.88**

M. Klonowski, M. Plata, P. Syga,
User authorization based on hand geometry without special equipment
[Pattern Recognition, Vol. 73, 2018]

Opis metody:

- System do weryfikacji oraz identyfikacji oparty o kontur dłoni.
- Rozwiązuje bazuje na klasycznych metodach przetwarzania obrazów.
- Materiał biometryczny pobrany skanerem biurowym.
- Zapisuje jedynie 62 obliczonych cech do bazy.
- Rozwiązanie cechuje się wysoką skutecznością.

Wyniki:

Baza autorska (60 osób $\times$ 5–10 próbek, wzorzec z 3 próbek):

- $FAR = 0.00\%$, $FRR = 1.19\%$
- $IR = 100.00\%$

Bosphorus Hand Database (738 osób $\times$ 3 próbki, wzorzec z 2 próbek):

- $FAR = 0.41\%$, $FRR = 1.41\%$
- $IR = 99.86\%$

M. Klonowski, M. Plata, P. Syga,
User authorization based on hand geometry without special equipment
[Pattern Recognition, Vol. 73, 2018]

Opis metody:

- System do weryfikacji oraz identyfikacji oparty o kontur dłoni.
- Rozwiązuje bazuje na klasycznych metodach przetwarzania obrazów.
- Materiał biometryczny pobrany skanerem biurowym.
- Zapisuje jedynie 62 obliczonych cech do bazy.
- Rozwiązanie cechuje się wysoką skutecznością.

Wyniki:

Baza autorska (60 osób $\times$ 5–10 próbek, wzorzec z 3 próbek):

- $FAR = 0.00\%$, $FRR = 1.19\%$
- $IR = 100.00\%$

Bosphorus Hand Database (738 osób $\times$ 3 próbki, wzorzec z 2 próbek):

- $FAR = 0.41\%$, $FRR = 1.41\%$
- $IR = 99.86\%$

M. Klonowski, M. Plata, P. Syga,
User authorization based on hand geometry without special equipment
[Pattern Recognition, Vol. 73, 2018]

Opis metody:

- System do weryfikacji oraz identyfikacji oparty o kontur dłoni.
- Rozwiązuje bazuje na klasycznych metodach przetwarzania obrazów.
- Materiał biometryczny pobrany skanerem biurowym.
- Zapisuje jedynie 62 obliczonych cech do bazy.
- Rozwiązanie cechuje się wysoką skutecznością.

Wyniki:

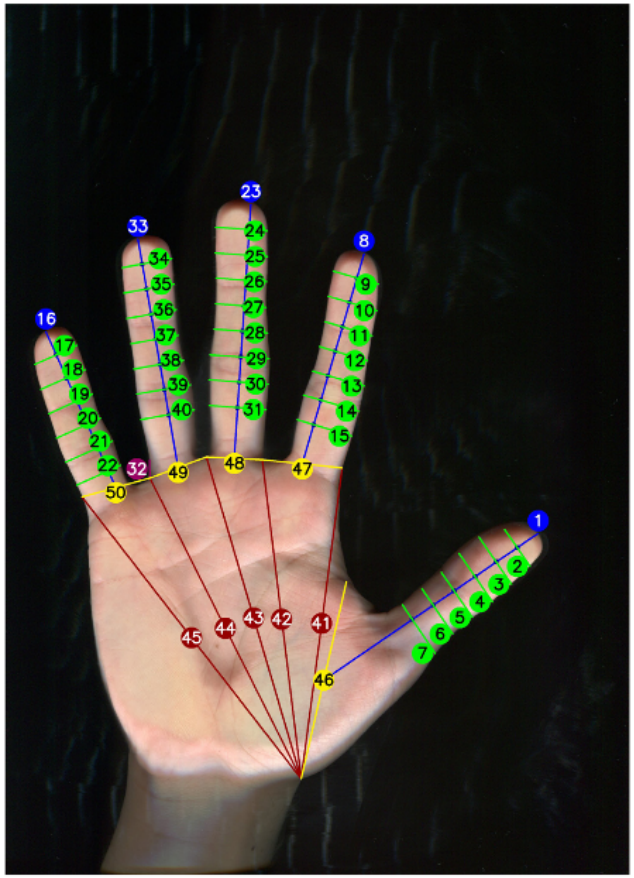
Baza autorska (60 osób $\times$ 5–10 próbek, wzorzec z 3 próbek):

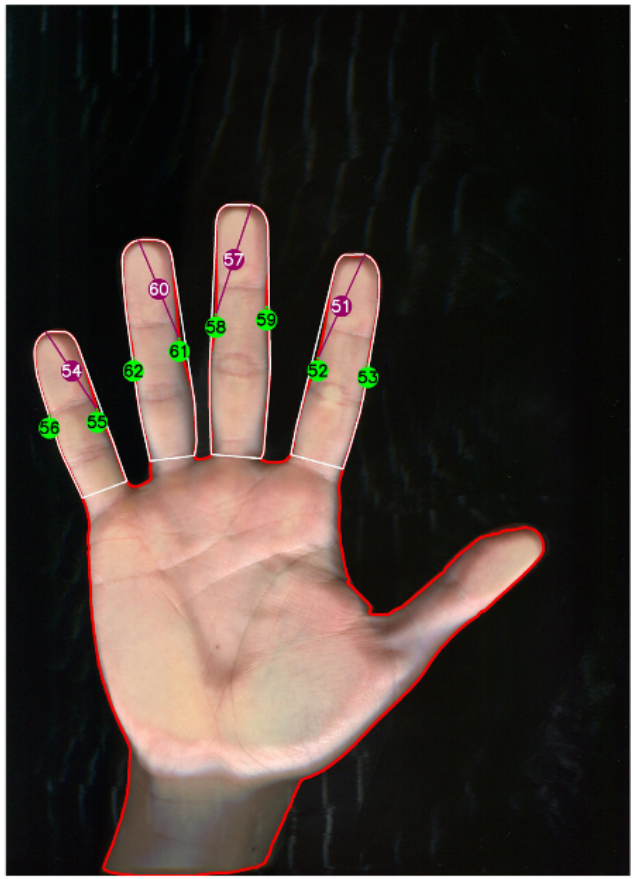
- $FAR = 0.00\%$, $FRR = 1.19\%$
- $IR = 100.00\%$

Bosphorus Hand Database (738 osób $\times$ 3 próbki, wzorzec z 2 próbek):

- $FAR = 0.41\%$, $FRR = 1.41\%$
- $IR = 99.86\%$

Zestaw 62 cech biometrycznych definiujących użytkownika na podstawie konturu dłoni:





Dziękuję za uwagę.