Politechnika Warszawska

Wydział Elektroniki i Technik Informacyjnych

Analiza zniekształceń procesu „print-scan” w metodach steganografii zdjęć drukowanych

Włodzimierz Kasprzak

Maciej Stefańczyk

Jan Popiołkiewicz

Instytut Automatyki i Informatyki Stosowanej Politechnika Warszawska

W.Kasprzak@elka.pw.edu.pl

Biometria 2012

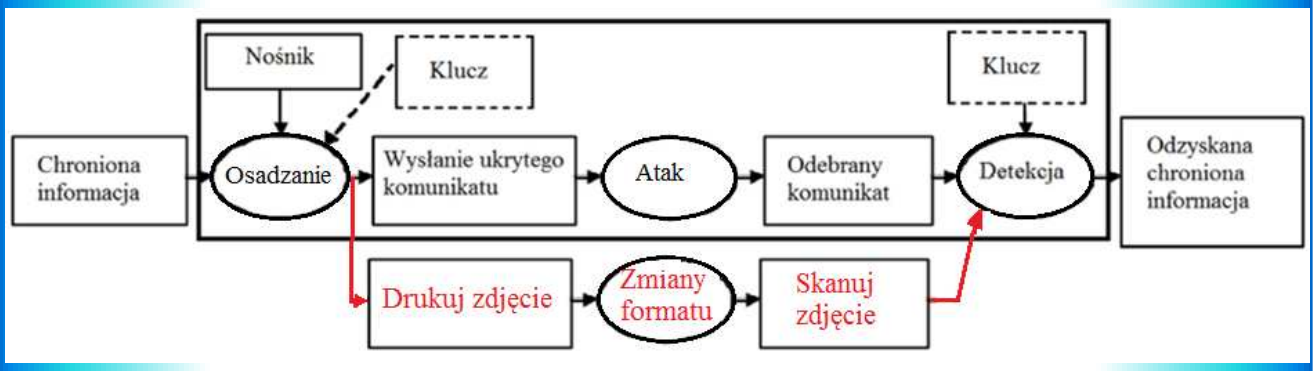
Warszawa, 13.12.2012

Treść

1. Steganografia zdjęcia tożsamości
2. Proces „drukuj-skanuj”
3. Metoda Fujitsu
4. Metoda DFM
5. Metoda BPCS
6. Osadzanie w siatce trójkątów
7. Wnioski

1. System steganograficzny

Schemat systemu steganograficznego i szczególnego problemu „**drukuj-skanuj**” **(PS)** (”print-scan”):

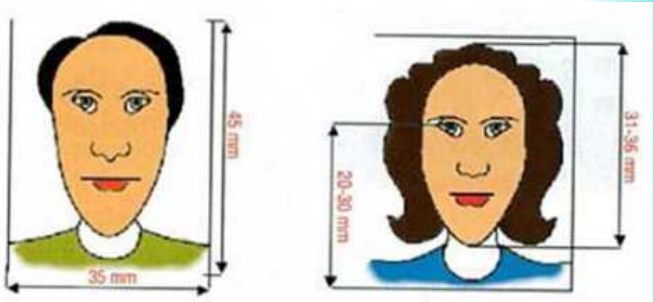


Rozmiar zdjęcia

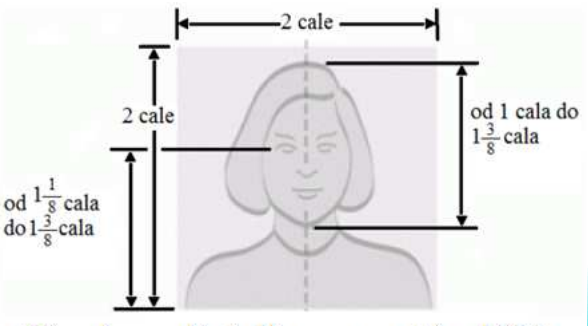
Rozdzielczość –

co najmniej 300 dpi, czyli

w pionie 530 pikseli, w poziomie 415 pikseli.



Polska instrukcja MSWiA z 2007 r. [MSWIA]



Wymiary zdjęć dla paszportów USA

2. Proces „drukuj-skanuj” w steganografii

Rozpatrywany schemat przetwarzania zdjęcia:

1. Wykonujemy zdjęcie twarzy (otrzymujemy obraz cyfrowy bez kompresji) – jest to **nośnik**
2. Wstawiamy stego-obiekt
3. Drukujemy obraz (na papierze lub karcie PVC)
4. Skanujemy papierowy wydruk (otrzymujemy obraz cyfrowy)
5. Detekcja - odczytujemy lub potwierdzamy obecność stego-obiektu

Przykład - skanowanie zdjęcia

Zdjęcie zeskanowane czytnikiem dokumentu tożsamości:

Zdjęcie oryginalne

a) w świetle białym (widoczne nadruki);

b) w podczerwieni IR

c) wersja OVD (po wycięciu warstwy nadruku) ;

d) w ultrafiolecie (UV)

Osadzanie i detekcja

Proces osadzania stego-obiektu:

1. Opcjonalna synchronizacja obrazu
2. Opcjonalne szyfrowanie informacji ukrywanej
3. Osadzanie informacji ukrytej

Proces detekcji stego-obiektu:

1. Opcjonalna synchronizacja obrazu
2. Dekodowanie informacji ukrytej
3. Opcjonalne odszyfrowanie informacji ukrytej

Synchronizacja

Etap synchronizacji obrazu u odbiorcy ma na celu wyeliminowanie wpływu następujących przekształceń obrazu:

przesunięcie, przeskalowanie i obrót,

które zaszły w wyniku procesu „drukuj-skanuj”, jakiemu podlegał obraz na dokumencie tożsamości.

Rozpatrujemy trzy przypadki:

1) Brak synchronizacji (tzn. nie jest wymagana)
2) Dopasowanie ramki obrazu
3) Dopasowanie poprzez wykrycie punktów szczególnych obrazu.

Metody steganograficzne

Badamy stosowanie wybranych metod steganograficznych dla zabezpieczania zdjęć tożsamości na dokumencie drukowanym:

1. Metoda Fujitsu – osadzanie w dziedzinie obrazu
2. Metoda DFM – osadzanie w dziedzinie transformaty Fouriera-Mellina
3. Metoda BPCS („bit plane complexity segmentation") – osadzanie w dziedzinie składowych bitowych obrazu
4. Osadzanie w sieci trójkątów obrazu – synchronizacja metodą punktów szczególnych

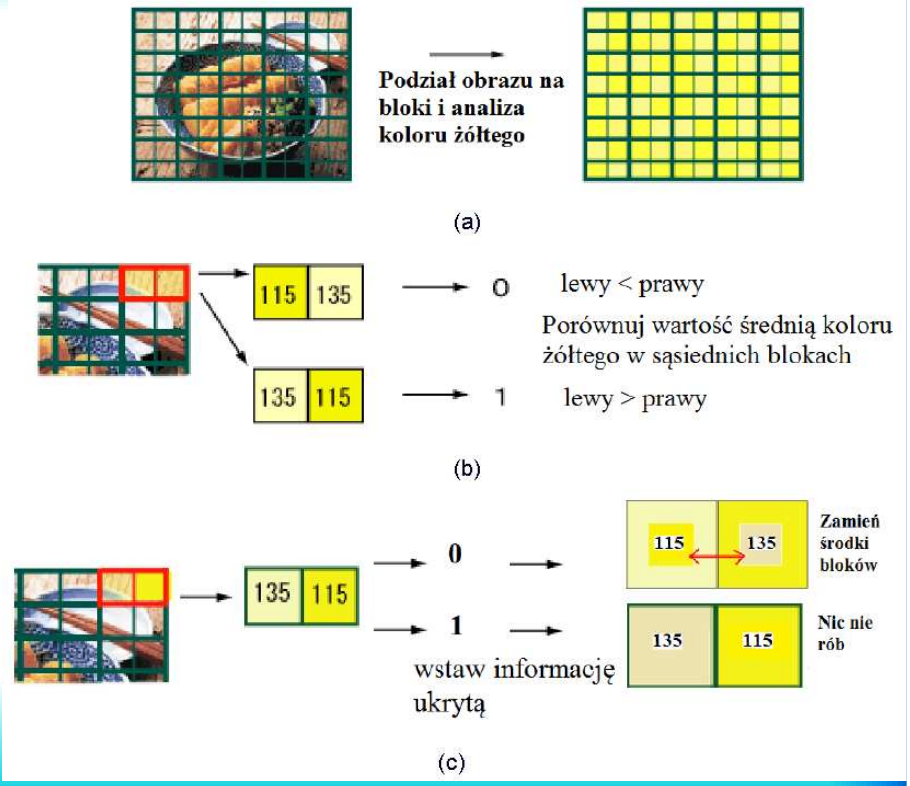
3. Metoda Fujitsu

Idea osadzania:

(a) skanowanie blokami

(b) detekcja średniej wartości 2 bloków (8x8)

(c) wstawianie bitu.



Osadzanie i detekcja

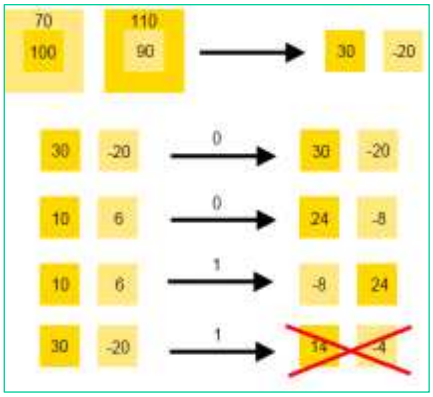
Nasza implementacja:

- równomierna zmiana wartości środków bloków (4x4) dla osiągnięcia minimalnej wymaganej odległości zamiast ich zamiany.

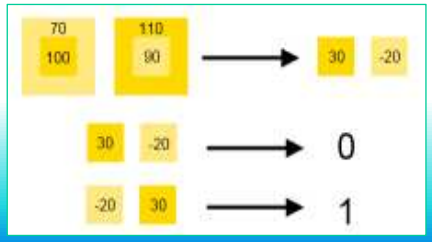
Osadzanie bitu:

(np. minimum odległości = 32;

zmiana +/- 16)



Detekcja bitu:



Metoda Fujitsu - wyniki

α	2	4	8	16	32
PSNR	46.5	45.5	43.4	39.9	35.6

Miara zakłóceń (PSNR) wprowadzanych przez osadzenie informacji w zależności od siły wstawienia (α) (= minimalna wymagana odległość)

zdjęcie oryginalne | obrócone o 27° | obrócone (korekcja) o -27° | przycięte

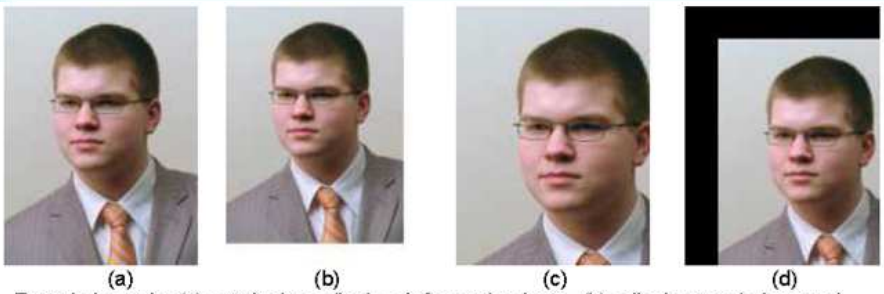
Kąt obrotu:	-90°	-60°	-45°	-30°	-15°	0°	15°	30°	45°	60°	90°
α = 2	90%	86	88	89	90	91	90	89	87	85	90%
α = 8	95%	94%	93	95	95	96	95	95	94	93	95%
α = 32	97%	96	95	96	97	96	96	96	95	95	97%

Procentowa ilość poprawnie odczytanych bitów stego-obiektu przy dwukrotnym obrocie

Kąt obrotu:	-1°	-0.8°	-0.6°	-0.4°	-0.2°	0°	0.2°	0.4°	0.6°	0.8°	1°
α = 2	61%	63	70	78	88	97	90	79	71	63	61%
α = 8	70%	72%	81	87	94	97	94	87	81	72	69%
α = 32	76%	80	91	93	96	97	96	93	90	80	75%

Procentowa ilość poprawnie odczytanych bitów stego-obiektu przy obrocie z przycięciem

Metoda Fujitsu – wyniki (2)



(a) (b) (c) (d)

Test skalowania: (a) oryginalne zdjęcie z informacją ukrytą, (b) zdjęcie przeskalowane i dopełnione białym kolorem, (c) zdjęcie przeskalowane i przycięte, (d) zdjęcie przesunięte.

Przeskalo-wanie:	10 %	30 %	50 %	70 %	90 %	100 %	110 %	130 %	150 %	170 %	200 %
$\alpha = 2$	47%	72	87	90	94	96	96	96	96	96	98%
$\alpha = 8$	47%	85%	94	96	97	97	97	97	97	97	97%
$\alpha = 32$	47%	93	96	96	97	97	97	97	97	97	97%

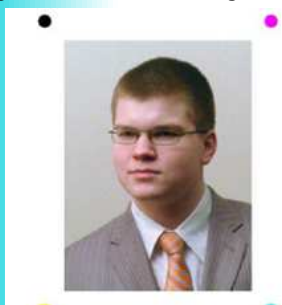
Procentowa ilość poprawnie odczytanych bitów informacji przy dwukrotnym przeskalowaniu

Zmiana szerokości (piksele):	-10	-8	-6	-4	-2	0	2	4	6	8	10
$\alpha = 2$	51%	51	55	55	70	97	70	52	49	51	51%
$\alpha = 8$	50%	51%	55	56	75	97	75	55	49	51	51%
$\alpha = 32$	50%	51	51	55	83	97	83	55	48	50	59%

Procentowa ilość poprawnie odczytanych bitów informacji przy przeskalowaniu i dopełnieniu białym kolorem lub przycięciu

Wyniki – proces PS (3)

Synchronizacja 4 znacznikami:



Zdjęcie wraz ze znacznikami

(a) (b)

Przykład (a) wydrukowanego i (b) zeskanowanego zdjęcia

Proces PS: zdjęcie 300x400, drukarka atramentowa lub wywołanie w fotolabie (254 dpi, 3x4cm).

Kąt obrotu:	0°	10°	20°	30°	40°	50°	60°	70°	80°	90°
$\alpha = 2$	68%	67	66	66	65	64	62	60	59	58
$\alpha = 8$	82%	82%	82	81	79	77	74	71	68	66
$\alpha = 32$	96%	96	96	96	96	95	93	90	89	88

Procentowa ilość poprawnie odczytanych bitów stego-obiektu poddanego procesowi PS

2. Metoda DFM

Metoda DFM to wstawianie stego-obiektu w dziedzinie dyskretnej transformaty Fouriera – Mellina.

Jest to dziedzina niezmiennicza ze względu na przekształcenia afiniczne obrazu (przekształcenia RST – obrót, skalowanie, przesunięcie).

2-wymiarowa DFT

- **DFT dla obrazu 2D**

$$F_{uv} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cdot e^{(-i2\pi\frac{u}{M})x}\cdot e^{(-i2\pi\frac{v}{N})y}$$

- **Faktoryzacja: 2 x 1D FFT**

$f(x,y)$ → $F(x,v)$ → $F(u,v)$

wiersze kolumny

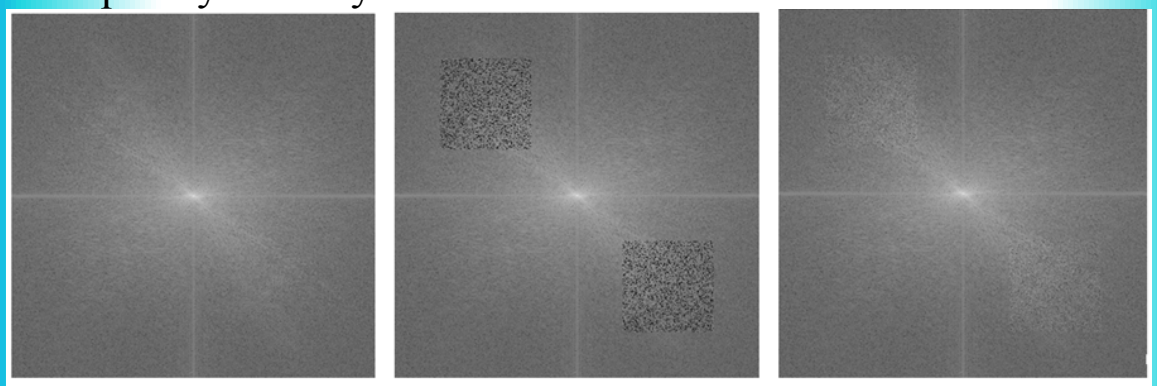
- Przesunięcie sygnału w dziedzinie obrazu nie wpływa na **amplitudę** współczynników Fouriera (niezmienniczość względem przesunięcia).
- **Skalowanie i obrót zmieniają też współczynniki Fouriera:** → przekształcenie **LogPolar** (logarytm reprezentacji biegunowej).

Wstawianie w dziedzinie widma

Stego-obiekt (znak po zakodowaniu) osadzany jest w zakresie średnich częstotliwości widma amplitudowego.

Wstawianie informacji „*r*” : $\mathbf{c}' = \mathbf{c}(1+\alpha\, \boldsymbol{r})$

gdzie **c** to wektor współczynników, ***r*** to zakodowana wiadomość a α współczynnik siły wstawienia.



Spektrogram 2D obrazu nośnika

Spektrogram po wstawieniu informacji ukrytej

Spektrogram obrazu po zniekształceniu procesu drukuj-skanuj

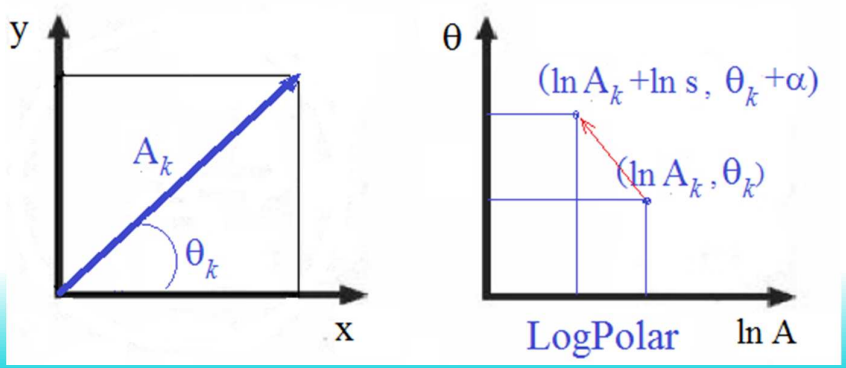
Transformata Fouriera- Mellina

- **Obrót i skalowanie** powodują jedynie przesunięcie w przestrzeni **LogPolar** dla widma sygnału:

$$F_k^{polar} = A_k \cdot e^{-i\theta_k} \qquad \ln F_k = \ln A_k + i \cdot \theta_k$$

$$s \cdot F_k = s \cdot A_k \cdot e^{-i\theta_k} \qquad e^{-i\alpha}(s \cdot F_k) = s \cdot A_k \cdot e^{-i(\theta_k+\alpha)}$$

$$\ln(e^{-i\alpha}(s \cdot F_k)) = \ln s + \ln A_k - i(\theta_k + \alpha)$$



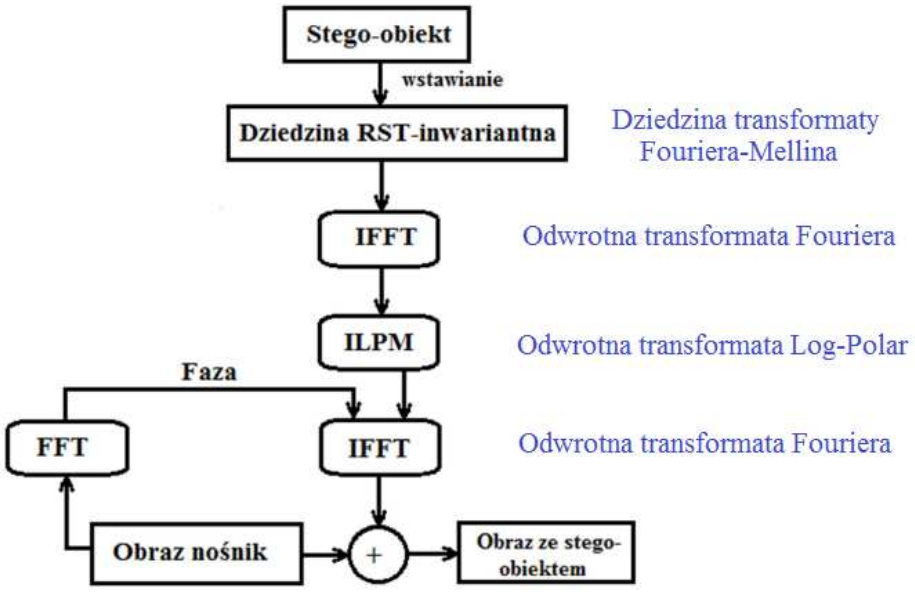
Transformata Fouriera-Mellina (2)

- Ponowna **transformata Fouriera** prowadzi do **amplitud współczynników niezmienniczych** ze względu na **obrót i skalowanie.**

$$DFT[\ln F_k] = [B_k \cdot e^{-i\rho_k}], k = 0,\ldots,M-1$$

$$DFT[\ln(e^{-i\alpha}(s \cdot F_k))] = [B_k \cdot e^{-i(\rho_k+\sigma)}], k = 0,\ldots,M-1$$

Osadzanie w metodzie DFM

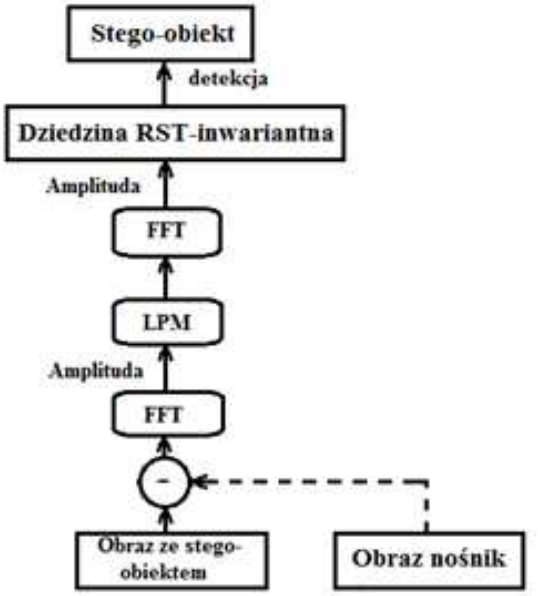


Schemat osadzania informacji, w którym unika się transformacji obrazu nośnika do dziedziny RST-inwariantnej.

Detekcja w metodzie DFM

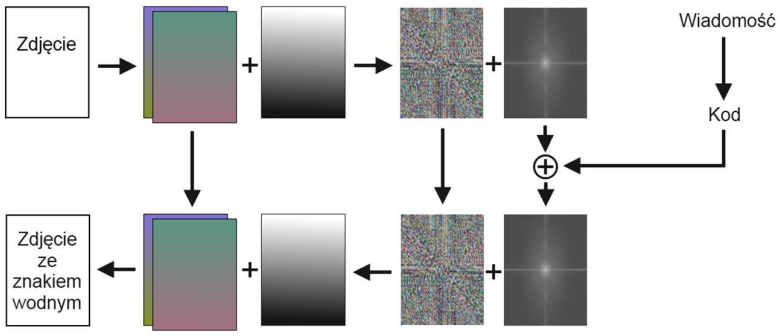
Jeżeli podczas detekcji informacji dostępny jest oryginalny obraz-nośnik to należy go odjąć od obrazu ze stego-obiektem.

Jeżeli obraz oryginalny nie jest dostępny to należy zastosować filtr pasmowy – imitując proces odjęcia obrazu-nośnika.

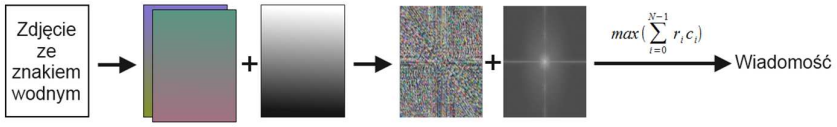


Idea osadzania i detekcji

Osadzanie w dziedzinie widma amplitudowego:



Detekcja znaku – maksymalna korelacja amplitudy widma obrazu z kodem znaku: $k = \sum_{i=0}^{N-1} r_i c_i$



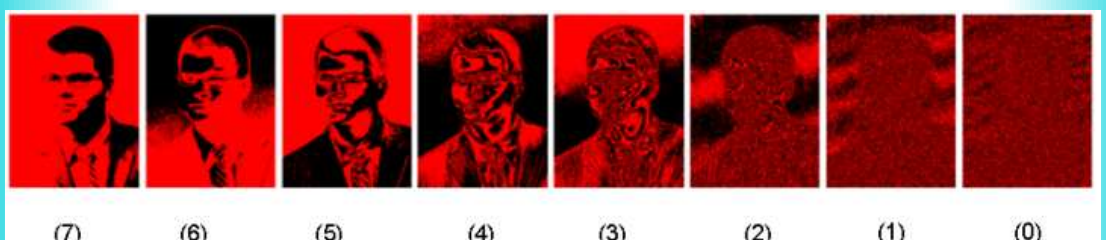
Wyniki testów DFM

- Odporność metody na przekształcenia afiniczne została potwierdzona – możliwe było odczytanie informacji po przeskalowaniu (nawet 5-krotnym zmniejszeniu) lub obróceniu obrazu.
- Stwierdzono dużą wrażliwość metody na błędy powodowane interpolacją obrazu.

5. Metoda BPCS

Osadzanie informacji w metodzie BPCS:

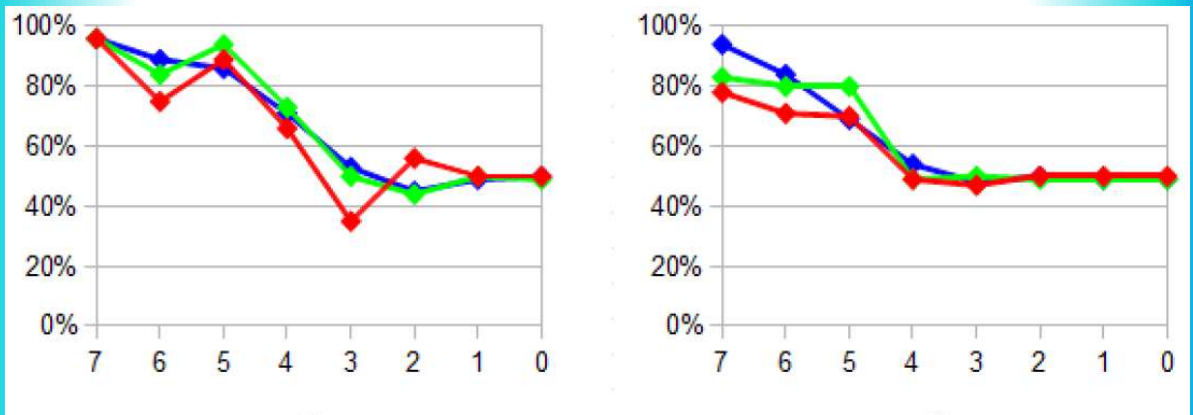
1. Kodowanie składowej koloru kodem Graya
2. Podzielenie obrazu na warstwy odpowiadające bitom (0-7)
3. Wyróżnienie w każdej warstwie bloków 8x8
4. Ocena złożoności bloku: częstość zmian 0→1 i 1→0 w wierszach i kolumnach bloku.
5. Wybór bloków o dużej złożoności (np. > 0.3) i zastąpienie ich blokiem ukrywanej informacji (kolejne 64 bity).



Zdjęcie testowe (tu składowa czerwona barwy) podzielone zostało na warstwy binarne odpowiadające bitom słowa w kodzie Graya

Wyniki testów BPCS

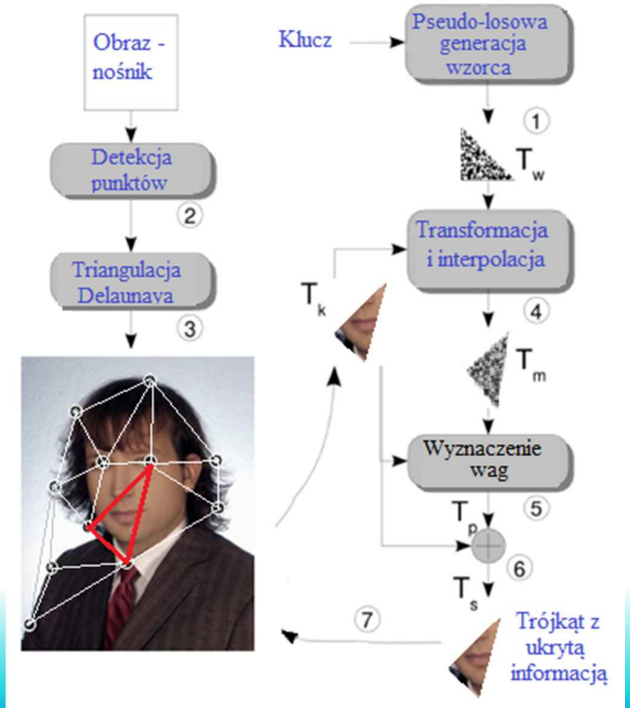
- Wyniki testów nie są zachęcające.
- Stwierdzono dużą wrażliwość metody na błędy powodowane procesem PS – zarówno zmiany geometrii obrazu, jak i zmiany koloru i rozdzielczości reprezentacji.



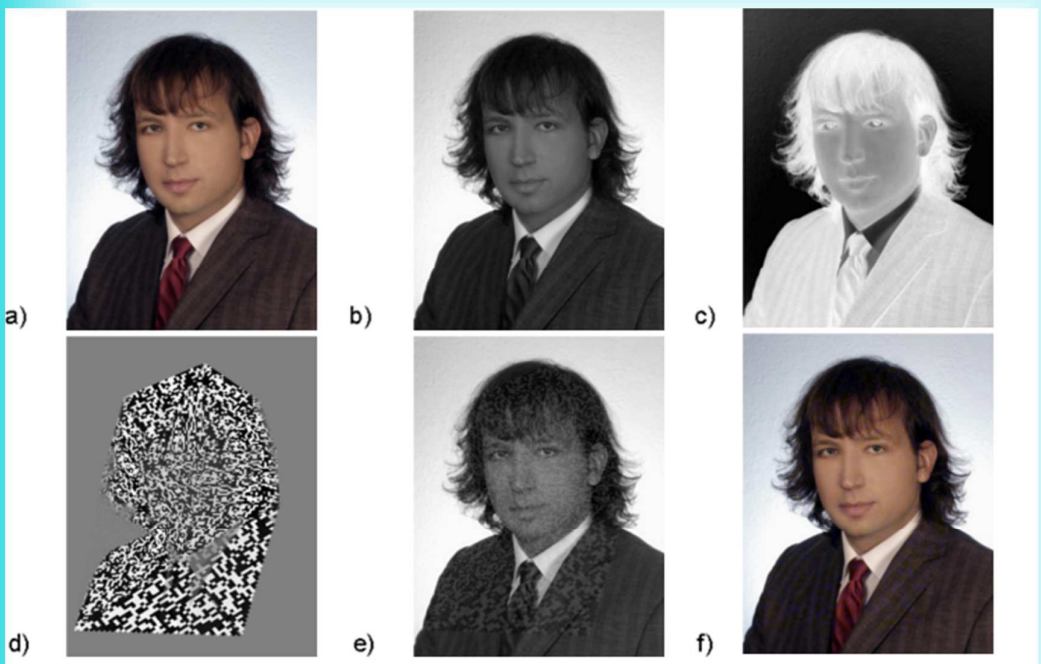
Procent poprawnie odczytanych bitów w procesie PS w zależności od warstwy (kod Graya) dla (a) naświetlarki i (b) drukarki atramentowej (linie odpowiadają poszczególnym składowym koloru)

6. Osadzanie w siatce trójkątów

Proces osadzania stego-obiektu w siatce trójkątów



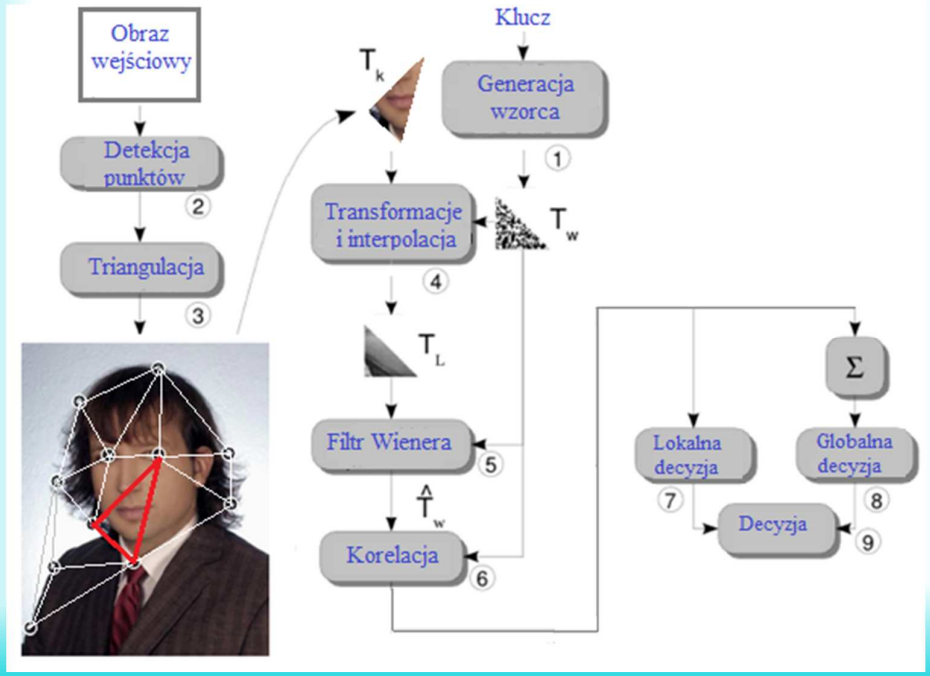
Osadzanie informacji



Kolejne fazy osadzania informacji w obrazie: a) obraz wejściowy, b) wybrany kanał (RGB-B) c) maska wagowa, informacja osadzana będzie najmocniej w obszarach o niskim nasyceniu koloru niebieskiego, d) obraz kodowy pomnożony przez maskę wag, e) wyjściowy kanał przy mocy osadzania ustawionej na 0.08, f) obraz wynikowy (PSNR 35dB).

Detekcja w siatce trójkątów

Badanie korelacji ukrytej informacji ze znanym wzorcem



Operator Harrisa

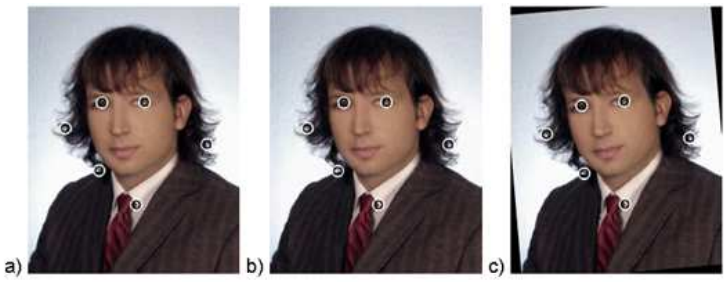
Operator Harrisa-Stephensa

Wyznaczane są średnie gradienty I_x, I_y funkcji obrazu w otoczeniu punktu (x, y). Tworzona jest macierz kowariancji gradientów:

$$A(x, y) = \begin{bmatrix} \sum_W (I_x(x_k, y_k))^2 & \sum_W I_x(x_k, y_k) I_y(x_k, y_k) \\ \sum_W I_x(x_k, y_k) I_y(x_k, y_k) & \sum_W (I_y(x_k, y_k))^2 \end{bmatrix}$$

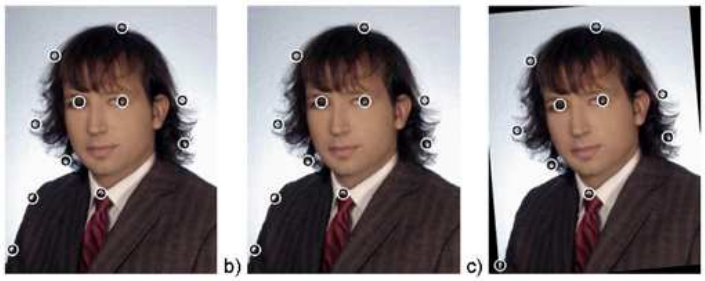
Punkt charakterystyczny wykrywany jest wtedy, gdy obie wartości własne macierzy A są porównywalnie duże.

Testy – detekcja punktów



a) b) c)

Wyniki działania detektora Harrisa; wielkość bloku = 5, jakość = 0.05; a) obraz odniesienia, b) obraz po dodaniu szumu, c) obraz obrócony



a) b) c)

Wyniki działania detektora Shi-Tomasi: wielkość bloku = 5. jakość = 0.05: w porównaniu do detektora Harrisa widoczna większa liczba punktów; a) obraz odniesienia, b) obraz po dodaniu szumu, c) obraz obrócony

Wyniki detekcji punktów i trójkątów

Blok	2		5		8	
Jakość	Punkty	Trafne	Punkty	Trafne	Punkty	Trafne
0,01	18,2	53,5	17,7	67,7	17,3	63,8
0,02	14,6	56,0	14,6	69,1	14,0	75,0
0,05	10,8	55,4	11,2	79,6	11,3	77,0
0,08	9,0	60,2	10,4	82,0	10,3	80,5

Zestawienie wyników dla detektora Shi-Tomasi

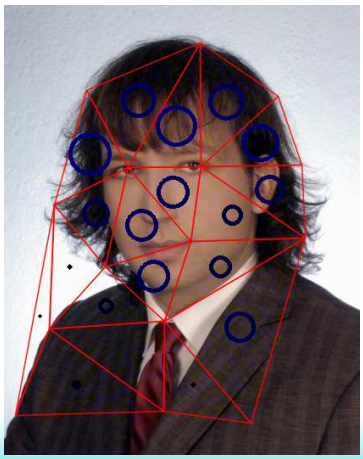
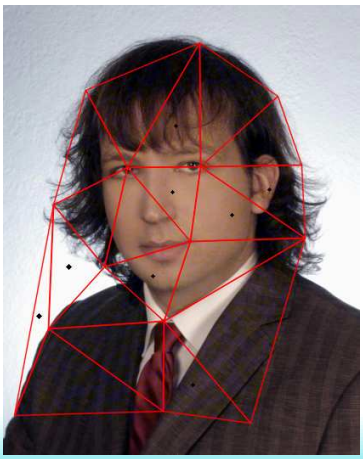
Kanał	Siła wst.	Obraz oryg.	Obrót 5°	Szum	Barwa		Nasycenie		Jasność	
					-25	+25	-10	+10	-10	+10
RGB-B	0,02	100	82	45	100	100	82	93	92	50
RGB-B	0,05	100	82	77	38[1]	72	38	85	70[1]	0
YUV-U	0,02	100	82	54	64[1]	72	50	85	100[1]	82
YUV-U	0,05	100	82	20	12[1]	85[1]	36[1]	69	85[1]	42

[1] *Kod staje się widoczny gołym okiem*

Stosunek ilości trójkątów z wykrytym kodem do wszystkich trójkątów na obrazie przy zastosowaniu różnych zniekształceń na wejściu.

Przykład detekcji - weryfikacji trójkątów

Wynik weryfikacji obecności ustalonego kodu w podanym zdjęciu; wielkość okręgu oznacza współczynnik korelacji (im większy okrąg tym lepiej); a) wysokie współczynniki dla prawidłowego kodu, b) wszystkie współczynniki o bardzo niskiej wartości dla kodu nieprawidłowego.

a)  b) 

7. Wnioski

Metoda Fujitsu

- Odporna na przekłamanie koloru w procesie PS (do 90% ukrytej informacji zostało odczytane).
- Wymagana jest synchronizacja obrazu
- Dość duża odporność na utratę informacji w wyniku zmiany rozdzielczości – interpolację.

DFM

- Odporna na przekształcenia afiniczne obrazu (RST).
- Mało odporna na zmiany koloru i rozdzielczości.

Wnioski (2)

BPCS

- Wyniki testów wskazują, że jej zastosowanie w steganografii dokumentów drukowanych nie jest zasadne.

Osadzanie w siatce trójkątów

- Potwierdzono odporność metody na zniekształcenia wszelkiego rodzaju w procesie PS (geometrii i barwy).
- Wymaga znajomości w odbiorniku klucza kodowego przesyłanej informacji.

Literatura

[FU2002] M. S. Fu and O. C. Au, “Data hiding watermarking in halftone images, *IEEE Trans. Image Process.*, vol. 11, no. 4, pp. 477–484, Apr. 2002

[FUJ04] Fujitsu Laboratories’ Printable Steganography,
http://www.fujitsu.com/global/news/pr/archives/month/2004/20040630-01.html
http://jp.fujitsu.com/group/labs/techinfo/techguide/list/steganography.html

[KAN 10] X. Kang, J. Huang, W. Zeng, Efficient general print-scanning resilient data hiding based on uniform log-polar mapping, *IEEE Transactions on Information Forensics Security* vol. 5(1), pp. 1–12, 2010

[PRA08] A. Pramila, A. Keskinarkaus, T. Seppänen, Watermark robustness in the print-cam process, *Proc. IASTED Signal Processing, Pattern Recognition, and Applications*, pp. 60-65, 2008

[ROS2001] J. Rosen and B. Javidi, “Hidden images in halftone pictures,” *Appl. Opt.*, vol. 40, no. 20, pp. 3346–3353, Jul. 2001.

[RUA98] J.J.K.O Ruanaidh, T. Pun, Rotation, scale, and translation invariant spread spectrum digital image watermarking, *Signal Processing*, vol. 66, no. 3, pp. 303–318, 1998

[SOL99] V. Solachidis, I. Pitas, Circularly Symmetric Watermark Embedding in 2D DFT Domain, *IEEE Trans. Image Processing*, vol. 10, no.11, pp. 1741–1753, Nov. 2001.

[SOL04] K. Solanki, U. Madhow, B.S. Manjunath, S. Chandrasekaran, Estimating and undoing rotation for print-scan resilient data hiding, *Proceedings IEEE ICIP*, Singapore, 2004.