W Y D A W N I C T W O P O L I T E C H N I K I Ś L Ą S K I E J W G L I W I C A C H

ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2018
Seria: ORGANIZACJA I ZARZĄDZANIE z. 130

ODPORNOŚĆ ALGORYTMÓW PODPISYWANIA DOKUMENTÓW CYFROWYCH

Mateusz DUDA[1], Ireneusz J. JÓŹWIAK[2], Jan MACIEJEWSKI[3], Stanisław SAGANOWSKI[4]

[1]Politechnika Wrocławska Wydział Informatyki i Zarządzania, Wrocław; mateusz.duda.x@gmail.com
[2]Politechnika Wrocławska Wydział Informatyki i Zarządzania, Wrocław; ireneusz.jozwiak@pwr.edu.pl
[3]Politechnika Wrocławska Wydział Mechaniczno-Energetyczny, Wrocław; janek.maciejewski25@gmail.com
[4]Politechnika Wrocławska Wydział Informatyki i Zarządzania, Wrocław; stanislaw.saganowski@pwr.edu.pl

Streszczenie: Znakowanie dokumentów jest jednym z najważniejszych sposobów ochrony praw autorskich. W niniejszym artykule zaprezentowano badania odporności wybranych algorytmów podpisywania dokumentów cyfrowych.

Słowa kluczowe: dokument cyfrowy, podpisanie, algorytm, odporność algorytmu.

RESISTANCE OF WATERMARKING AND SIGNING ALGORITHMS OF DIGITAL DOCUMENTS

Abstract: Watermarking information is one of the most important applications of copyright protection. In this article we test resistance of several document watermarking algorithms.

Keywords: digital document, signing, algorithm, resistance.

1. Wprowadzanie

Głównym zadaniem podpisywania dokumentów cyfrowych jest ochrona praw autorskich. Co prawda algorytmy podpisywania dokumentów nie chronią przed ich kopiowaniem, jednak pozwalają zidentyfikować twórcę lub odbiorcę dokumentu. To z kolei pozwala na śledzenie rozpowszechniania konkretnej kopii dokumentu w sieci komputerowej i wykrywanie modyfikacji w dokumencie oryginalnym. Z tego powodu ważne stało się zachowanie podpisu pomimo dokonanych na dokumencie przekształceń. Istnieje wiele algorytmów znakujących dokumenty cyfrowe, jednak żaden z nich nie jest stuprocentowo odporny na

przekształcenia obrazów. Niniejszy artykuł prezentuje odporność wybranych algorytmów znakowania na typowe przekształcenia obrazów rastrowych.

2. Przebieg badań algorytmów podpisywania

Zbiorem Do badań zostały zaimplementowane następujące algorytmy podpisywania: Cox. (Cox et al., 1997), Piva (Barni et al, 1997; Barni et al., 1998; Piva et al., 1997), Ruanaidh (Ruanaidh, Dowling, and Boland, 1996), Ruanaidh blokowy (O'Ruanaidh, Dowling, and Boland, 1996), Nikolaidis (Nikolaidis, and Pitas, 1996; Pitas, 1998), Xia (Xia, Boncelet, and Arce, 1997), Kundur (Kundur, and Hatzinakos, 1998), Dugad (Dugad, Ratakonda, and Ahuja, 1998), Xie (Xie, and Arce, 1998), „Siatki DFT" (modyfikacja algorytmu przedstawionego w pracy (Liber, and Kurek, 2005)).

Badane algorytmy korzystają z różnych metod odczytywania i weryfikowania istnienia znaku wodnego w obrazie. Niektóre metody weryfikowały hipotezę statystyczną, inne sprawdzały pewien zbiór dokumentów. Podpis najbardziej podobny do odczytanego został uznany za osadzony w obrazie.

Dla algorytmów osadzających ciągi binarne posłużono się współczynnikiem podobieństwa. Próg weryfikacji został ustalony na poziomie 0,2. Dla algorytmu Xia posłużono się czynnikiem korelacji z progiem weryfikacji 0,1. Dla pozostałych algorytmów wykorzystano metody weryfikacji hipotezy statystycznej właściwe dla badanego algorytmu. Wyniki badań wybranych algorytmów przedstawiono w tabeli 1. W tabeli 1 zestawiono długości znaków (w bitach) ukrytych w obrazach testowych. Algorytmy, których badanie nie dotyczy zostały w tabeli pominięte.

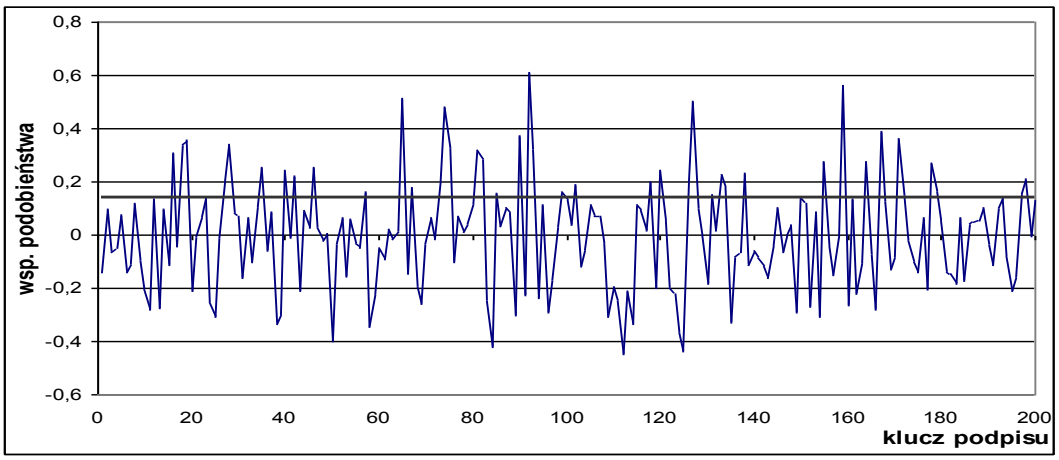
Tabela 1.
Długości znaków (w bitach) ukrytych w obrazach testowych

Algorytm	Baboon	Boats	Koło	Krzyż	Lena	Pierścień	X
Ruanaidh	80						
Ruanaidh	88	215	48	48	262	96	200
Kundur	3281						
Xie	341						

Badanie polegało na odczytaniu znaków wodnych z podpisanych obrazów. W tabeli 2 prezentowane są rezultaty weryfikacji prawdziwych podpisów.

Tabela 2.
Wyniki testu weryfikacji prawdziwego podpisu

Algorytm	Baboon	Boats	Koło	Krzyż	Lena	Pierścień	X
Cox	+	+	+	+	+	+	+
Piva	+	+	+	-	+	+	-
Ruanaidh	+	+	+	+	+	+	+
Ruanaidh blokowy	+	+	+	+	+	+	+
Nikolaidis	+	+	-	-	+	+	+
Xia	+	+	+	+	+	+	+
Kundur	+	+	-	-	+	-	-
Dugad	+	+	+	+	+	+	+
Xie	+	+	-	+	+	+	+
Siatki DFT	+	+	-	+	+	+	-



Rysunek 1. Diagram podobieństwa 200 podpisów Piva w obrazie Krzyż.

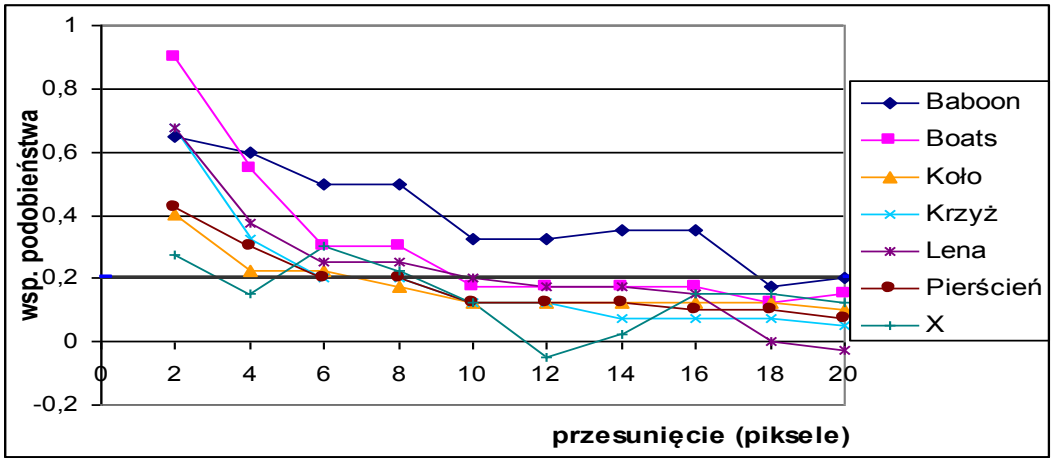
Z badań wynika, że wszystkie podpisy zostały poprawnie wykryte w obrazach Baboon, Boats, Lena. Najwięcej błędów zostało popełnionych podczas weryfikacji obrazów Koło, Krzyż, Pierścień, X. W przypadku podpisu Piva wykryto wiele fałszywych podpisów, choć osadzony był tylko jeden (rysunek 1).

W teście odporności podpisów na translacje cykliczne obrazów wykorzystano przekształcenie polegające na przesunięciu pikseli obrazu w prawo o zadaną wartość. Po przesunięciu piksele znajdujące się skrajnie z prawej strony i nie mieszczące się w obrębie rysunku były przenoszone na lewą stronę. W tabeli 3 przedstawiono na ilu obrazach udało się rozpoznać podpis.

Tabela 3.
Wyniki testów odporności podpisów na translacje

Algorytm	Przesunięcie (piksele)									
	2	4	6	8	10	12	14	16	18	20
Piva	2	1	-	-	-	1	1	-	-	-
Ruanaidh	7	6	7	6	2	1	1	1	-	1
Xie	2	1	-	1	-	1	-	-	-	-
Siatki DFT	5	5	5	5	5	5	5	5	5	5

Badanie wykazało, że większość podpisów jest słabo odporna na translacje cykliczne. Szczególnie dotyczy to algorytmów osadzających podpis w przestrzeni geometrycznej obrazu i transformaty falkowej. Bardzo odporny w przypadku obrazu Baboon okazał się podpis Ruanaidh.. Na innych obrazach jego odporność była jednak znacznie słabsza (Rysunek 2). Podpis Siatki DFT jest całkowicie odporny na translacje cykliczne, ponieważ jest osadzany w komponentach amplitudowych współczynników dyskretnej transformaty Fouriera (DFT).



Rysunek 2. Wartość współczynnika podobieństwa podpisu Ruanaidh po translacjach cyklicznych obrazu.

W teście odporności podpisów przy obrotach obrazów użyto przekształcenia polegającego na obrocie obrazu wokół środka obrotu znajdującego się w środku obrazu. Wymiary oryginalne obrazów były zachowane. Puste obszary były wypełniane kolorem czarnym. Wykonano dwa rodzaje obrotów: o kąt 1-10 stopni oraz o kąt 90, 180 i 270 stopni. W tabeli 4 przedstawiono na ilu obrazach udało się rozpoznać podpis.

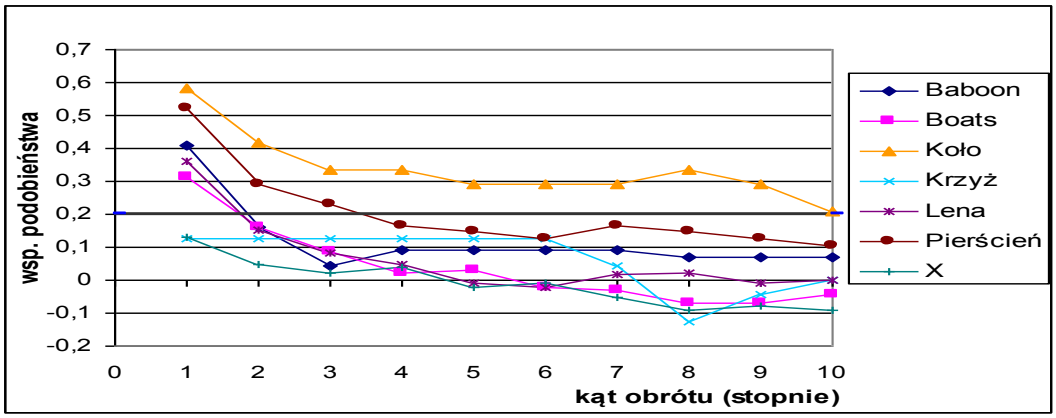
Tabela 4.
Wyniki testów odporności podpisów na obroty

Algorytm	Kąt obrotu												
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**90**	**180**	**270**
Piva	-	2	-	2	-	2	1	-	1	-	2	2	2
Ruanaidh	7	6	5	5	3	3	1	2	-	-	-	-3[1]	-
Ruanaidh blokowy	5	2	2	1	1	1	1	1	1	1	1	2	1
Xie	2	-	-	-	-	1	-	1	-	-	2	1	2

Uwagi:
[1] – współczynnik podobieństwa był równy -1 (odczytano bitową negację podpisu).

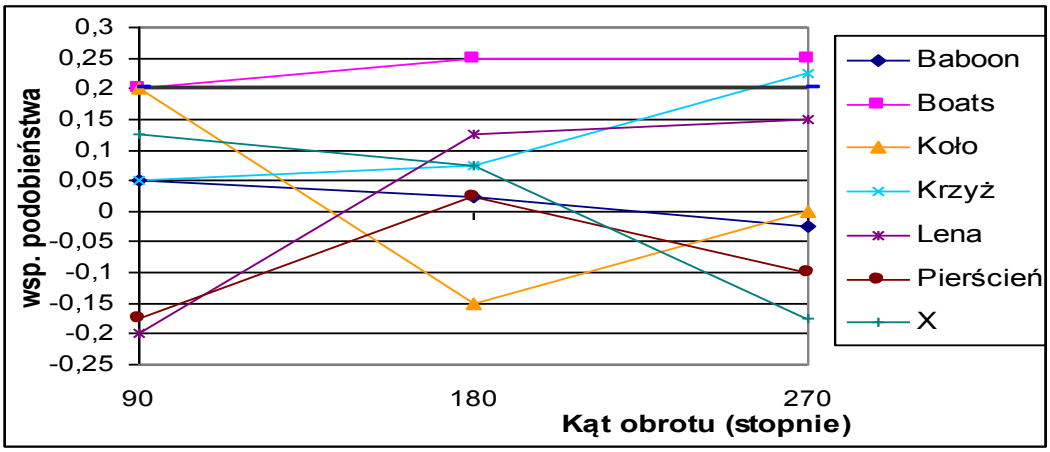
Badanie wykazało, że większość podpisów jest nieodporna na rotacje o mały kąt. Algorytmy Ruanaidh i Ruanaidh blokowy uzyskały bardzo dobre rezultaty dla obrazu Koło, ale na pozostałych obrazach były znacznie mniej odporne (Rysunek 3). Podpis Xie był

odporny na obroty o kąty 90,180 i 270 tylko w przypadku obrazu Boats. Pozwala to przypuszczać, że wykrycie podpisu na tym jednym obrazie było przypadkowe (rysunek 4).



Rysunek 3. Wartość współczynnika podobieństwa podpisu Ruanaidh blokowy po obrotach obrazu.

W teście odporności podpisów przy kompresji stratnej zastosowano przekształcenie polegające na kompresowaniu podpisanych obrazów algorytmem JPEG. Następnie obrazy dekompresowano i próbowano odczytać podpis. Badania wykonano dla 10 współczynników kompresji. W tabeli 5 przedstawiono wyniki porównań algorytmów podpisywania.

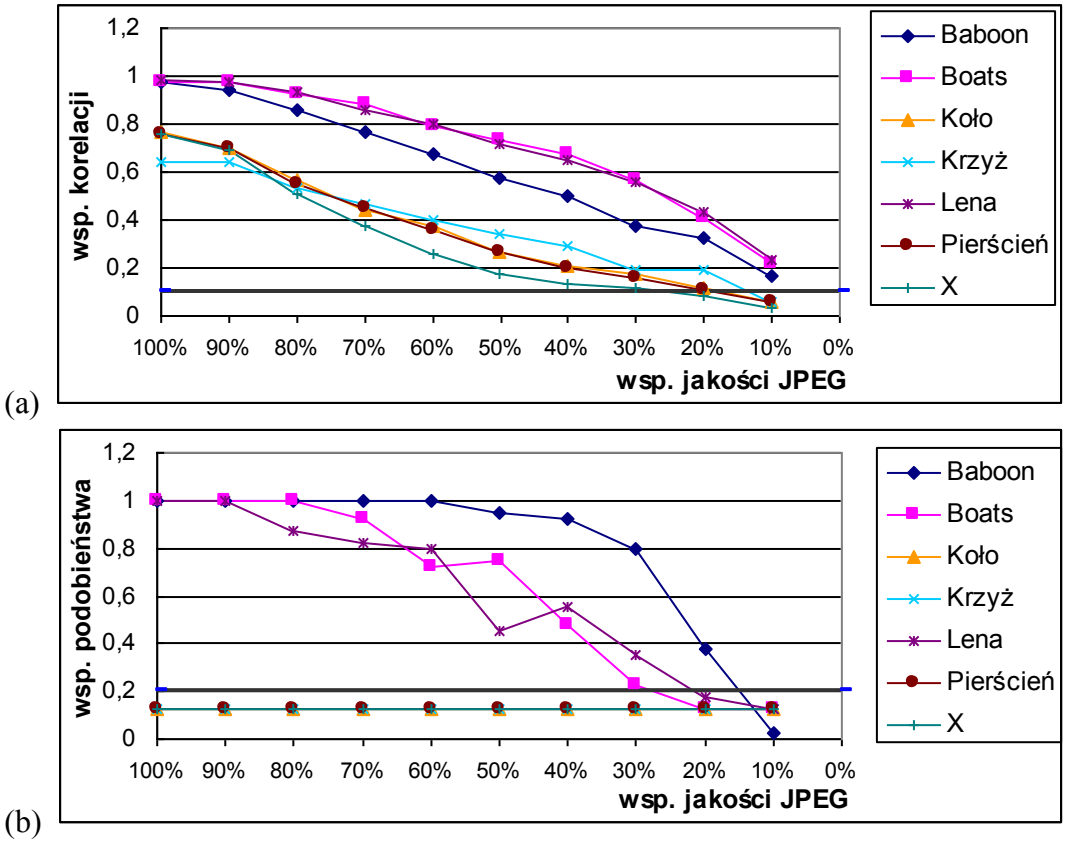


Rysunek 4. Wartość współczynnika podobieństwa podpisu Xie po obrotach obrazu.

Tabela 5.
Wyniki testów odporności podpisów na kompresję JPEG

Algorytm	Współczynnik jakości JPEG [%]									
	100	90	80	70	60	50	40	30	20	10
Cox	7	7	6	6	6	6	6	6	6	6
Ruanaidh	7	7	7	7	7	7	7	7	7	7
Nikolaidis	5	-	1	1	-	-	-	-	-	-
Xia	7	7	7	7	7	7	7	7	6	3
Kundur	3	3	3	3	3	3	3	3	1	-

Badanie pokazało, że większość podpisów bardzo dobrze znosi kompresję JPEG. Podpis Ruanaidh został rozpoznany we wszystkich obrazach przy wszystkich współczynnikach kompresji. W przypadku pozostałych algorytmów podpisywania problemy z rozpoznaniem podpisu najczęściej dotyczyły obrazów Koło, Krzyż, Pierścień, X. Algorytm Nikolaidis okazał się praktycznie nieodporny na kompresję stratną. Na wykresach na rysunku 5 przedstawiono wyniki weryfikacji podpisów osadzanych w przestrzeni transformaty falkowej. Odporność tych podpisów zwykle była bardzo dobra w przypadku obrazów będących zdjęciami (Baboon, Boats, Lena).



Rysunek 5. Wyniki weryfikacji podpisów w obrazach po kompresji JPEG: (a) Xia, (b) Kundur.

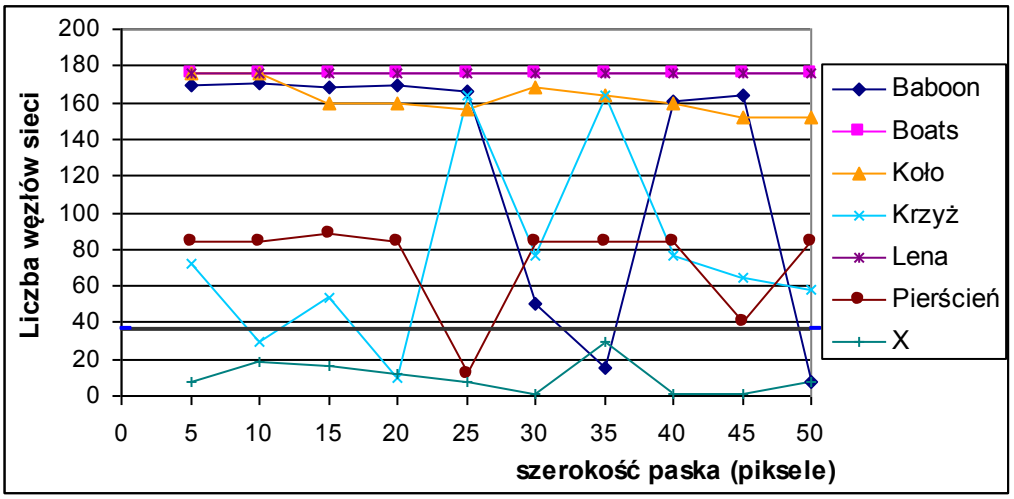
3. Kadrowanie obrazów

Wspomaganie W teście odporności podpisów na kadrowanie wykorzystano przekształcenie polegające na wycięciu z lewej strony obrazu pionowego pasa. Oryginalne wymiary obrazu były zachowane. Puste miejsce było wypełniane kolorem czarnym. Badanie przeprowadzono dla różnych szerokości pasa. W tabeli 6 przedstawiono wyniki porównań algorytmów podpisywania.

Tabela 6.
Wyniki testów odporności podpisów na obcinanie brzegu obrazu

Algorytm	Szerokość pasa (piksele)									
	5	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
Cox	5	4	3	3	3	2	1	1	2	1
Ruanaidh	7	7	7	7	6	6	6	6	6	6
Xia	7	7	7	7	7	7	7	7	7	7
Siatki DFT	6	5	6	5	5	6	5	6	6	5

Badanie pokazało, że wszystkie algorytmy są odporne na ten rodzaj przekształcenia. Jest to zgodne z oczekiwaniami – zmiany w obrazie były stosunkowo niewielkie i miały charakter lokalny. Stosunkowo najgorsze wyniki uzyskał algorytm Cox – podpis został rozpoznany po wszystkich przekształceniach tylko na jednym obrazie. Algorytm Siatki DFT poprawnie wykrywał podpis w obrazach Boats, Koło, Lena. Podczas wykrywania podpisu w pozostałych obrazach zachowywał się niestabilnie (rysunek 6).



Rysunek 6. Liczba wykrytych węzłów siatki podpisu osadzonego metodą Siatki DFT po wycięciu z obrazu pionowego paska.

4. Podsumowanie

Badania wykazały, że podpisy osadzone w obrazach dwupoziomowych są znacznie mniej odporne na często stosowane operacje, w szczególności na kompresję stratną. Stwierdzono, że znaki osadzane metodą Siatki DFT cechują się wysoką odpornością na translacje i ograniczoną odpornością na obroty, kadrowanie oraz kompresję JPEG.

Znaki osadzane metodą Siatki DFT mogą być użyte jako wzorce, według koncepcji przedstawionej w pracy S. Pereiry i T. Puna (Pereira, and Pun, 2000). Wykazali oni, że znaki osadzane w przestrzeni transformaty Fouriera są odporne na translacje, obroty i skalowanie.

W takim podejściu siatka może być osadzona w obrazie razem z innym znakiem wodnym. Siatka nie przenosi wiadomości, ale jej analiza pozwala stwierdzić, jakim operacjom był poddany obraz. Dzięki temu możliwe jest odwrócenie dokonanych transformacji oraz odczytanie drugiego znaku zawierającego właściwą wiadomość.

Bibliografia

1. Barni, M., Bartolini, F., Cappellini, V., Piva, A. (1997). Robust watermarking of still images for copyright protection. *Proceedings of 13th International Conference on Digital Signal Processing*, 2, pp.499 – 502, doi: 10.1109/ICDSP.1997.628384.
2. Barni, M., Bartolini, F., Cappellini, V., Piva, A. (1998). A DCT-domain system for robust image watermarking. *Signal Processing,* 66(3), pp. 357-372.
3. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing,* 6(12), pp. 1673-1687, doi: 10.1109/83.650120.
4. Dugad, R., Ratakonda, K., Ahuja, N. (1998). A new wavelet-based scheme for watermarking images. *Proceedings 1998 International Conference on Image Processing.* ICIP98, 2, pp. 419-423, doi: 10.1109/ICIP.1998.723406.
5. Kundur, D., Hatzinakos, D. (1998). Digital watermarking using multiresolution wavelet decomposition. *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'98, 5*, pp. 2969-2972, doi: 10.1109/ICASSP.1998.678149.
6. Liber, A., Kurek, W. (2005). Niedostrzegalne sygnatury cyfrowe obrazów rastrowych odporne na procesy drukowania i skanowania. W *Współczesne problemy informatyki. Problemy analizy i projektowania sieci komputerowych*. Legnica: Wydaw. Wyższej Szkoły Menedżerskiej, pp.175-200.
7. Nikolaidis, N., Pitas, I. (1996). Copyright protection of images using robust digital signatures. *Proceedings - ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing*, 4, pp. 2168-2171, doi: 10.1109/ICASSP.1996.545849.
8. O'Ruanaidh, J.J.K., Dowling, W.J., Boland, F.M. (1996). Watermarking digital images for copyright protection. *IEE Proceedings - Vision, Image and Signal Processing*, 143(4), pp.250-256.
9. Pereira, S., Pun, T. (2000). Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*, 9(6), pp. 1123-1129, doi: 10.1109/83.846253.
10. Pitas, I. (1998). A method for watermark casting on digital image. *IEEE Transactions on Circuits and Systems for Video Technology*, 8(6), pp. 775-780, doi: 10.1109/76.728421.

11. Piva, A., Barni, M., Bartolini, F., Cappellini, V. (1997). DCT-based watermark recovering without resorting to the uncorrupted original image. *Proceedings of International Conference on Image Processing*, 1, pp. 520-523, doi: 10.1109/ICIP.1997.647964.
12. Ruanaidh, J.J.K.O., Dowling, W.J., Boland, F.M. (1996). Phase watermarking of digital images. *Proceedings of 3rd IEEE International Conference on Image Processing*, 3, pp. 239-242, doi: 10.1109/ICIP.1996.560428.
13. Xia, X.G., Boncelet, C.G., Arce, G.R. (1997). A multiresolution watermark for digital images. *Proceedings of International Conference on Image Processing*, 1, pp. 548-551, doi: 10.1109/ICIP.1997.647971.
14. Xie, L., Arce, G.R. (1998). Joint wavelet compression and authentication watermarking. *Proceedings 1998 International Conference on Image Processing. ICIP98*, 2, pp. 427-431, doi: 10.1109/ICIP.1998.723409.