Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie
Wydział Informatyki, Elektroniki i Telekomunikacji

Autoreferat rozprawy doktorskiej

mgr inż. Paweł Korus

Analysis of Image Reconstruction Schemes Based on Self-Embedding and Digital Watermarking

Promotor:

prof. dr hab. inż. Andrzej Dziech

Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie
Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Telekomunikacji

al. Mickiewicza 30, 30-059 Kraków, Poland
tel. +48 12 6345582
fax +48 12 6342372

`http://www.agh.edu.pl`
`http://www.iet.agh.edu.pl`
`http://www.kt.agh.edu.pl`
`http://www.kt.agh.edu.pl/~korus/`

© mgr inż. Paweł Korus, 2013
Wszelkie prawa zastrzeżone

Szablon LaTeX © Rafał Stankiewicz

1 Wstęp

Niniejsza rozprawa dotyczy problemu rekonstrukcji oraz uwierzytelniania obrazów cyfrowych. W dobie coraz bardziej powszechnych, w znacznym stopniu zautomatyzowanych narzędzi do retuszu zdjęć, wykonanie przekonywującej modyfikacji ich treści leży w zasięgu ręki przeciętnych użytkowników. Zdjęcia cyfrowe są przy tym coraz częściej stosowane jako materiał dowodowy. Z powyższych względów tematyka badania autentyczności jest obecnie nadzwyczaj aktualna. Potwierdzają to liczne publikacja naukowe, a także szereg komercyjnych produktów dysponujących wspomnianą funkcjonalnością.

Tematem przewodnim rozprawy jest zastosowanie techniki cyfrowych znaków wodnych celem umożliwienia nie tylko lokalizacji złośliwych zmian w obrazie, ale przede wszystkim rekonstrukcji pierwotnego wyglądu zmodyfikowanych fragmentów. Odbywa się to poprzez zapisanie w cyfrowym znaku wodnym informacji referencyjnej, która opisuje oryginalny wygląd obrazu. Dedykowany dekoder jest w stanie, na podstawie analizy tych informacji, przywrócić przybliżoną wersję autentycznej treści. Opisane zastosowanie cyfrowych znaków wodnych nosi nazwę samo-rekonstrukcji (ang. *self-recovery* lub *self-embedding*).

Głównym celem pracy było wykazanie analogii pomiędzy wspomnianym problemem rekonstrukcji obrazu a komunikacją przez kanał z wymazywaniem, oraz zaproponowanie teoretycznego modelu pozwalającego na analizę zachowania oraz osiągalnych granic poprawnej pracy algorytmów samo-rekonstrukcji. Na podstawie zaproponowanego modelu opracowano referencyjny algorytm samo-rekonstrukcji, który posłużył do eksperymentalnej weryfikacji poprawności wyników teoretycznych, oraz do porównania osiągalnej efektywności proponowanego podejścia z alternatywnymi sposobami opisanymi w literaturze światowej.

W pracy sformułowano następującą tezę:

- Możliwe jest modelowanie problemu rekonstrukcji treści obrazów cyfrowych jako komunikację poprzez kanał wymazujący.
- Uzyskany w ten sposób model pozwala na teoretyczną analizę warunków poprawnej rekonstrukcji, a także związanych z tym kompromisów.
- Algorytm samo-rekonstrukcji obrazów oparty na zaproponowanym modelu uzyskuje lepsze wyniki niż istniejące alternatywne rozwiązania.
- Wysoka jakość rekonstrukcji jest możliwa do uzyskania nawet w przypadku rozległych zmian w obrazie.

2 Przegląd literatury oraz motywacja badań

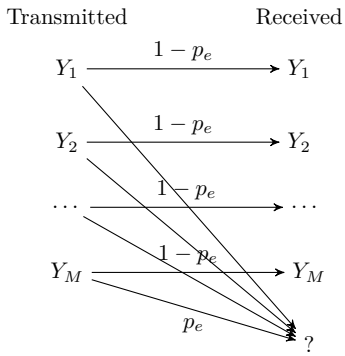
Zastosowanie cyfrowych znaków wodnych do samo-rekonstrukcji obrazów cyfrowych zostało po raz pierwszy zaprezentowane w pracy [24]. Użyte podejście cechowało się jednak pewną naiwnością, gdyż informacja referencyjna opisująca wygląd pojedynczego bloku obrazu, umieszczana była w wybranym innym bloku. Takie podejście prowadzi do łańcucha zależności pomiędzy blokami, co istotnie ogranicza jego stosowalność.

Naturalnym zatem wydaje się rozproszenie informacji referencyjnej po całym obrazie. Podejście takie zastosowano niedawno w [74, 76], gdzie autorzy dzielą obraz na losowe fragmenty, których informacja referencyjna jest generowana z wykorzystaniem pseudo-losowych macierzy (odpowiednio binarnych oraz o rozkładzie normalnym), co rozprasza informację o poszczególnych blokach obrazu po całym fragmencie, do którego obraz należy. Dodatkowo, tak uzyskana informacja referencyjna jest umieszczana w losowo wybranych fragmentach obrazu.

Sam proces rekonstrukcji obrazu odbywać się może na kilka sposobów. Najbardziej powszechnym jest bezpośrednia komunikacja niskiej jakości obrazu referencyjnego jako dane znaku wodnego. Zadanie dekodera polega wtedy na odczycie fragmentów informacji referencyjnej opisujących zmienione bloki, oraz podmianie ich obecnego wyglądu na treść odczytanego wzorca. Alternatywne podejście polegać może na użyciu metody projekcji na zbiory wypukłe [77] bądź z wykorzystaniem próbkowania losowego (ang. *compressive sensing*) [74], gdzie rekonstrukcja odbywa się iteracyjnie. Spotyka się także metody, w których znak wodny zawiera redundancję wygenerowaną na podstawie obrazu przez tradycyjne kody korekcji błędów [42].

Jednym z istotnych problemów jest brak ogólnego modelu, który pozwalałby szacować efektywność opracowywanych rozwiązań. Obecnie opisane w literaturze rozwiązania testowane są najczęściej w jednej wybranej konfiguracji i nie da się na podstawie podanych wyników ocenić wpływu modyfikacji różnych ich parametrów. Utrudnia to zarówno porównanie skuteczności opisanych rozwiązań między sobą a także ich praktyczną implementację, gdyż ciężko jest przewidzieć czy wprowadzenie niezbędnej modyfikacji pozwoli osiągnąć zadowalającą efektywność rekonstrukcji.

Z tego względu, pożądane jest opracowanie modelu teoretycznego, który pozwoli na wyznaczenie teoretycznych granic możliwość odtworzenia obrazu, a także na prostą ocenę wpływu poszczególnych parametrów na uzyskiwane wyniki.



Rysunek 1: M-wartościowy symetryczny kanał z wymazywaniem o prawdopodobieństwie błędu p_e.

3 Rekonstrukcja obrazów cyfrowych jako komunikacja poprzez kanał z wymazywaniem

Problem samo-rekonstrukcji treści obrazów cyfrowych można sformułować jako komunikację przez kanał z wymazywaniem. Rozważmy algorytm uwierzytelniania obrazu, który dzieli obraz na niezależne bloki. Do każdego z bloków wstawione zostanie B bitów znaku wodnego o charakterze referencyjnym, oraz 32 -bity znaku wodnego będącego skrótem (podpisem cyfrowym) jego treści, zawartości jego znaku wodnego, lokalizacji bloku wewnątrz obrazu oraz kontekstu autentyczności (np. daty bądź znanego hasła).

Dla każdego bloku generowana jest informacja referencyjna o długości b bitów. W ogólnym przypadku b może być funkcją numeru bloku $b(i)$, co pozwala na dostosowanie rekonstrukcji do treści poszczególnych bloków. W rozprawie rozważone obydwa przypadki, na chwilę obecną zawęźmy jednak rozważanie do stałej wartości b. Dla N bloków obrazu, kompletna informacja referencyjna zawiera zatem Nb bitów. Strumień ten jest następnie dzielony na wielowartościowe symbole o długości B bitów. Na podstawie tych symboli wejściowych, generowane jest dokładnie N symboli wyjściowych - jako znak wodny dla każdego z bloków. Generacja symboli znaku wodnego odbywa się przy pomocy kodowania fontannowego, które automatycznie rozprasza informację nt. każdego z bloków równomiernie po całym obrazie.

Po stronie odbiorczej następuje uwierzytelnienie poszczególnych bloków obrazu poprzez porównanie podpisu zawartego w znaku wodnym z ponownie policzonym podpisem aktualnego stanu bloków. Po uwierzytelnieniu, poszczególne bloki obrazu (a także symbole znaku wodnego) są albo poprawne albo błędne. Zachowanie

to odpowiada transmisji przez kanał wymazujący (rysunek 1) ale kryterium poprawnej transmisji jest odmienne. Do poprawnej rekonstrukcji potrzebne jest zdekodowanie jedynie fragmentów przesyłanej wiadomości. Symbole znaku wodnego opisujące autentyczne fragmenty obrazu można wygenerować ponownie oraz całkowicie wyeliminować tą informację ze wstawionego znaku wodnego. W efekcie, strumień referencyjny może mieć długość znacząco przekraczającą pojemność znaku wodnego.

Przykład działania opisanego algorytmu przedstawiono na rysunku 2. Ilustracja pokazuje również wpływ braku wyrównania pomiędzy długością bloków informacji referencyjnej b a długością symboli znaku wodnego B. W tym przypadku zniszczenie jednego bloku obrazu może powodować konieczność odczytania informacji referencyjnej kilku bloków. Odpowiedni dobór b, B pozwala jednak na uniknięcie tego zjawiska.

Granicę możliwości poprawnej rekonstrukcji można wyznaczyć z warunku na możliwość zdekodowania wiadomości przez kod fontannowy. Należy wziąć jednak pod uwagę zmniejszenie liczby faktycznie potrzebnych symboli, oraz możliwość ponownego użycia autentycznych fragmentów obrazu. Warunek poprawnej rekonstrukcji przyjmuje wtedy postać:

$$\gamma \geqslant \lambda\rho(\lambda, \gamma), \tag{1a}$$

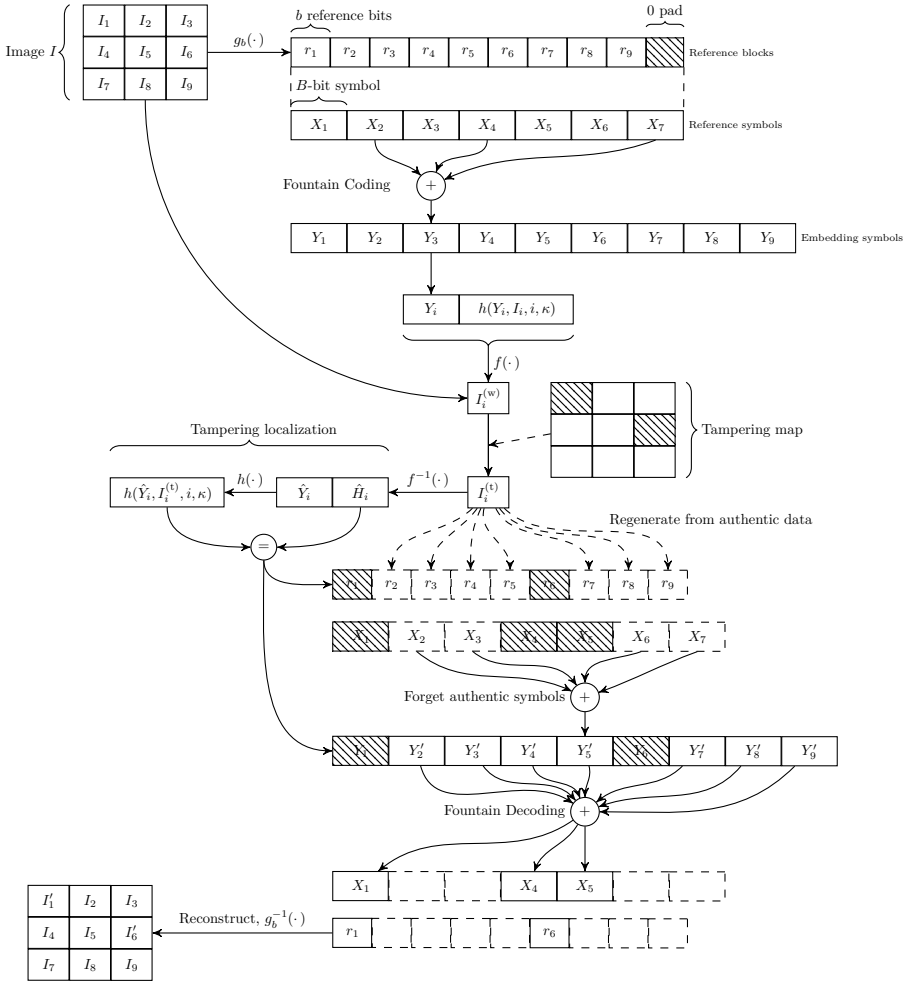
$$\rho(\lambda, \gamma) : \mathbf{R}^+ \times [0, 1] \to [0, 1], \tag{1b}$$

gdzie γ jest współczynnikiem liczby autentycznych do wszystkich bloków obrazu, a $\lambda = \frac{b}{B}$ jest parametrem sterującym jakością rekonstrukcji. $\rho(\lambda, \gamma)$ jest *zapotrzebowaniem rekonstrukcji*, i.e., funkcją opisującą zależność pomiędzy liczbą zniszczonych symboli a częścią strumienia referencyjnego, którą należy odczytać ze znaku wodnego. Zachowanie zapotrzebowania rekonstrukcji na kluczowy wpływ na efektywność działania systemów samo-rekonstrukcji. Jego analiza pozwala na dokładne wyznaczenie granic poprawnej pracy, nawet dla skomplikowanych systemów adaptacyjnych. Pożądane jest aby zapotrzebowanie rekonstrukcji miało charakter liniowy względem współczynnika ingerencji w obraz (tj. współczynnika liczby zmienionych do wszystkich bloków obrazu).

Granicę możliwości poprawnej rekonstrukcji wyrazić można następującą zależnością:

$$\begin{cases} \gamma \geqslant \lambda\ (1 - \gamma^{\lceil \frac{1}{\lambda} \rceil}), & \text{jeśli } \frac{1}{\lambda} \in \mathbf{N} \text{ lub } \lambda \in \mathbf{N}, \\ \gamma \geqslant \lambda\ (1 - \gamma^{\frac{1}{\lambda}+1}), & \text{w przeciwnym wypadku.} \end{cases} \tag{2}$$

Wynik ten zweryfikowano eksperymentalnie przy pomocy symulacji Monte Carlo. W każdej iteracji eksperymentu obraz chroniony jest z losowo wybraną jakością. Następnie, wprowadzane są zmiany do obrazu o losowo wybranym



Rysunek 2: Działanie proponowanego podejścia do problemu samo-rekonstrukcji.

współczynniku ingerencji. Próby rekonstrukcji, a także teoretycznie wyznaczone granice pomiędzy sukcesem a porażką zaznaczono na rysunku 3. Próby zakończone sukcesem oznaczono zielonymi okręgami, natomiast porażką czerwonymi krzyżykami. Rysunek 3a przedstawia przypadek losowania dowolnego poziomu jakości λ. Z kolei rysunek 3b przedstawia zawężenie do wartości $\lambda \in \mathbf{N}$. We współrzędnych punktów pozostawiono część ułamkową ze względu na czytelność wykresu.

4 Gwarancja parametrów dzięki systemom adaptacyjnym

W pracy rozważono również przypadek adaptacyjnej samo-rekonstrukcji, w której jakością poszczególnych bloków można sterować indywidualnie, tj. $b = b(i)$. W tej sytuacji charakter zachowania zapotrzebowania na rekonstrukcję jest silnie zależny od tego, które bloki obrazu uległy modyfikacji. W przedstawionej analizie zawężono możliwe poziomy jakości λ do liczb naturalnych. W przypadku gdy niszczone są najpierw najważniejsze fragmenty (tj. fragmenty o najwyższej jakości rekonstrukcji), zapotrzebowanie rekonstrukcji ma charakter odcinkowo-liniowy:

$$\rho(\tilde{\gamma}|\Lambda, \mathbf{w}) = \begin{cases} \alpha_1\tilde{\gamma} + \beta_1, & \text{for } \tilde{\gamma} \in (0, w_1^+], \\ \ldots \\ \alpha_s\tilde{\gamma} + \beta_s, & \text{for } \tilde{\gamma} \in (w_{s-1}^+, w_s^+], \\ \ldots \\ \alpha_S\tilde{\gamma} + \beta_S, & \text{for } \tilde{\gamma} \in (w_{S-1}^+, 1]. \end{cases} \tag{3}$$

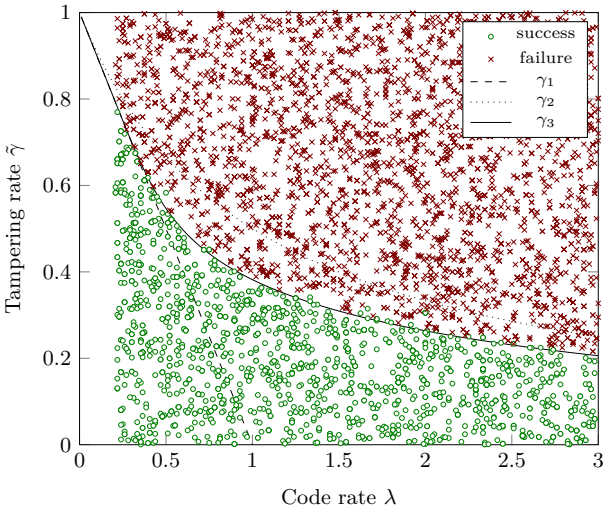
gdzie współczynniki kierunkowe α_s wyznacza się z następującej zależności:

$$\alpha_s = \lambda_s / \sum_{i=1}^{S} w_i \lambda_i, \tag{4}$$

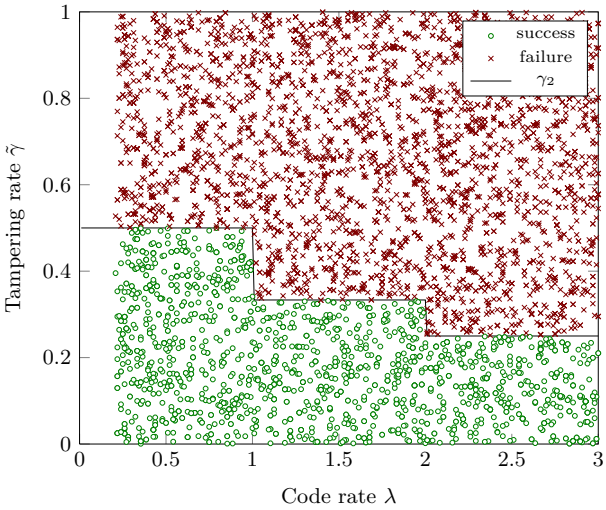
a współczynniki wolne β_s dla kolejnych przedziałów muszą spełniać równanie ciągłości:

$$\beta_s : \bigvee_{s \in \{1,\ldots,S\}} \rho(w_s^+|\lambda, \mathbf{w}) = \lim_{\tilde{\gamma} \to (w_s^+)^+} \rho(\tilde{\gamma}|\lambda, \mathbf{w}). \tag{5}$$

Rysunek 4 pokazuje zachowanie zapotrzebowania na rekonstrukcję dla losowo przypisanych poziomów jakości $\Lambda = [3,\ 2,\ 1]$ występujących z częstotliwością $\mathbf{w} = [0.1429,\ 0.2857,\ 0.5714]$. Rysunek 4a pokazuje odcinkowo-liniowy charakter opisanej zależności, podczas gdy rysunek 4b przedstawia wyniki eksperymentalnej weryfikacji tego zachowania.

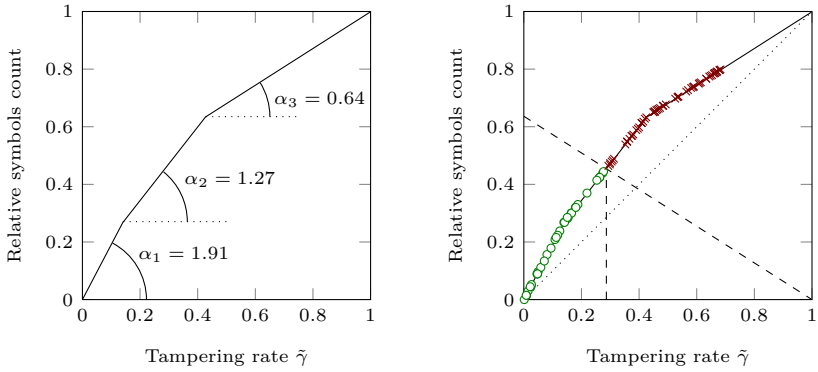


(a) Dowolna jakość obrazu



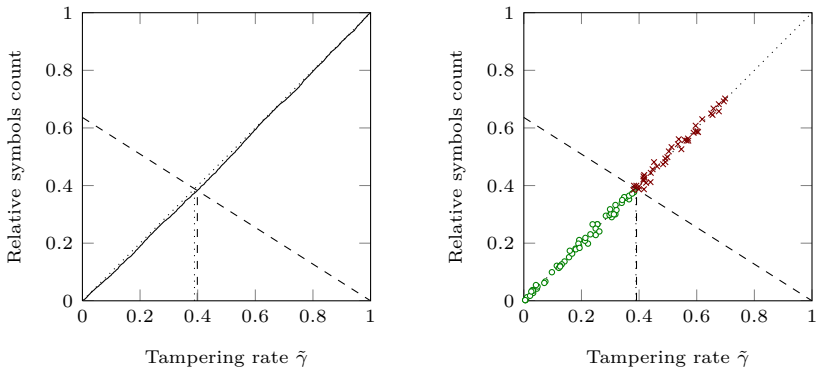
(b) Jakość obrazu $\lambda \in \mathbf{N}^+$

Rysunek 3: Eksperymentalna weryfikacja poprawności wyznaczonych granic teoretycznych. Każdy punkt odpowiada pojedynczej iteracji eksperymentu.



(a) Odcinkowo-liniowy charakter ρ (b) Weryfikacja eksperymentalna

Rysunek 4: Zachowanie zapotrzebowania na rekonstrukcję dla przypadku zniszczeń w najważniejszych obszarach zdjęcia.

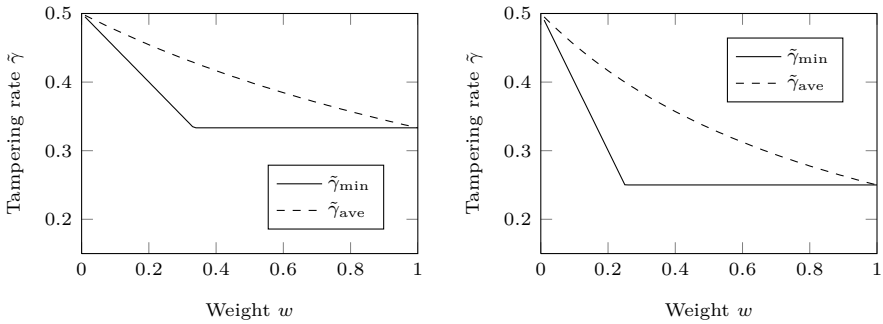


(a) Liniowy wzrost ρ; przykładowa realizacja (b) Weryfikacja eksperymentalna

Rysunek 5: Zachowanie zapotrzebowania na rekonstrukcję dla przypadku zniszczeń w losowych obszarach zdjęcia.

W przypadku losowych zmian w obrazie zapotrzebowanie na rekonstrukcję ma charakter niewielkich oscylacji względem oczekiwanego liniowego wzrostu. Przypadek ten przedstawiono na rysunku 5.

Z analizy zachowania zapotrzebowania na rekonstrukcję można wyciągnąć



(a) $\lambda_1 = 2,\ \lambda_2 = 1$ (b) $\lambda_1 = 3,\ \lambda_2 = 1$

Rysunek 6: Ilustracja braku poprawy pesymistycznego współczynnika ingerencji w obraz dla przypadku dwóch zdefiniowanych poziomów jakości rekonstrukcji.

wniosek, że pomimo chęci poprawy maksymalnego dopuszczalnego współczynnika ingerencji w obraz poprzez zastosowanie do części obrazu rekonstrukcji o niższej jakości (czyli w efekcie skrócenia strumienia bitów informacji referencyjnej), parametr ten niekoniecznie musi ulec poprawie. W przypadku zmian dotykających najważniejszych fragmentów zdjęcia poprawa nie będzie zauważalna do momentu, w którym liczba bloków o wysokiej jakości nie będzie stanowiła wyraźniej mniejszości. Przykładowo, dla przypadku dwóch poziomów jakości $\lambda_1 > \lambda_2$ o częstotliwościach występowania:

$$\mathbf{w} = [w, 1 - w], \tag{6}$$

parametryzowanych przez $w \in [0, 1]$, graniczny współczynnik ingerencji dla $w \in (\frac{1}{1+\lambda_1}, 1]$ jest stały oraz zależny wyłącznie od λ_1. Zjawisko to przedstawiono na rysunku 6.

Na podstawie powyższych modeli zachowania zapotrzebowania na rekonstrukcję w rozprawie zaproponowano algorytm gwarancji wybranych parametrów samo-rekonstrukcji. Jako wejście traktowane są: maksymalny pożądany współczynnik ingerencji w obraz dla zadanego typu zniszczeń oraz mapa ważności fragmentów obrazu. Na podstawie podanej mapy, algorytm automatycznie zagwarantuje najwyższą jakość rekonstrukcji dla wybranych fragmentów zdjęcia, oraz dostosuje jakość pozostałych tak, aby możliwe było spełnienie warunku na zadany współczynnik ingerencji. Przykład praktycznego zastosowania opisanego mechanizmu przedstawiono na rysunku 7, gdzie w przypadku systemu adaptacyjnego gwarancja wysokiego poziomu jakości dotyczy tablicy rejestracyjnej pojazdu.

(a) Bez adaptacji, 32.2 dB

(b) Z adaptacją, 33.0 dB

(c) Bez adaptacji, 32.2 dB

(d) Z adaptacją, 33.0 dB

Rysunek 7: Porównanie wpływu adaptacji jakości wybranych fragmentów zdjęcia na czytelność tablicy rejestracyjnej pojazdu.

Jest ona wyraźnie wyższa (kosztem jakości tła) niż w przypadku algorytmu nie stosującego adaptacji.

5 Optymalizacja jakości

W rozprawie rozważono również mechanizmy optymalizacji jakości rekonstrukcji. W szczególności zbadano wpływ zastąpienia równomiernego słownika kwantyzacji poprzez optymalny słownik Lloyda-Maxa [49] oraz wpływ zastosowania kilku klas treści, różniących się pomiędzy sobą poziomem tekstury wewnątrz bloku. Opracowano również mechanizm wyznaczania optymalnej alokacji precyzji reprezentacji współczynników widma. Jego zastosowanie pozwala na automatyczne wyznaczenie optymalnej precyzji dla dowolnego zadanego budżetu długości informacji referencyjnej poszczególnych bloków.

Przykład poprawy jakości związany z zastosowaniem wymienionych technik przedstawiono na rysunkach 8 oraz 8. Ilustracje przedstawiają wycinek obrazu oryginalnego o pełnej jakości oraz trzech obrazów referencyjnych, które pokazują jakiej jakości będą poszczególne fragmenty w przypadku ich rekonstrukcji. Przedstawiono wariant uzyskany przy pomocy jednorodnego słownika (zniekształcenia na poziomie 30,54 dB) a także dwa warianty uzyskany przy pomocy słownika Lloyda-Maxa. Pierwszy wariant odpowiada jednej, ogólne klasie treści - stosowanej do wszystkich bloków obrazu (31,40 dB). Drugi wariant wykorzystuje 3 klasy treści - dla bloków o mało, średnio oraz bardzo intensywnej teksturze (32,24 dB).

6 Eksperymentalna ocena efektywności

W ramach przeprowadzonych badań dokładnie przetestowano jakość rekonstrukcji kilkunastu różnych wariantów proponowanego algorytmu. Dokładne wyniki można znaleźć w pełnej wersji rozprawy. W niniejszym podsumowaniu zawężono prezentowane wyniki do porównania efektywności z najlepszymi rozwiązaniami opisanymi dotychczas w literaturze światowej. Celem wiarygodnego porównania, zaimplementowano 5 wybranych algorytmów. Algorytmy te skonfigurowano w analogiczny sposób, tj. użyto identycznej metody wstawiania znaku wodnego oraz identycznej ilości danych znaku wodnego. Dzięki temu wszystkie algorytmu uzyskały ten sam poziom zniekształceń spowodowanych znakiem wodnym - 37.9 dB. Dla każdego z algorytmów wygenerowano zbiór 48 zabezpieczonych obrazów cyfrowych. Następnie, obrazy te były zmieniane w ten sam sposób dla każdego z algorytmów, celem porównania jakości rekonstrukcji w identycznych warunkach. Eksperyment powtórzono dla różnych wartości współczynnika ingerencji w obraz. Uzyskane wyniki zebrano w tabeli 1.

W przeprowadzonym eksperymencie wzięto pod uwagę dwie klasy algorytmów. Po pierwsze, są to algorytmy o stałym poziomie jakości (proponowany, a także [76] oraz [73]). Po drugie są to algorytmy o zmiennym poziomie jakości, zależnym od faktycznie zaobserwowanych zmian w obrazie. W przypadku niewielkich zmian w obrazie (tj. dla współczynnika ingerencji w obraz na poziomie kilku-kilkunastu pro-

(a) lena, oryginał

(b) lena, jednorodny słownik, 30.54 dB

Rysunek 8: Porównanie jakości obrazu referencyjnego dla obrazu *lena*.

(c) lena, słownik Lloyda-Maxa, 1 klasa treści, 31.40 dB

(d) lena, słownik Lloyda-Maxa, 3 klasy treści, 32.24 dB

Rysunek 8: Porównanie jakości obrazu referencyjnego dla obrazu *lena*.

Tablica 1: Porównanie jakości rekonstrukcji najlepszych rozwiązań opisanych w literaturze.

Algorytm	**Jakość rekonstrukcji PSNR [dB]**						$\tilde{\gamma}_{\max}$
	0.050	0.100	0.200	0.300	0.400	0.475	
[74]	37.2	34.8	31.7	29.1	28.1	27.0	0.60
[75]	37.3	35.6	33.3	31.6	30.2	29.2	0.54
[76]-B	31.8	31.7	31.7	28.7	28.7	25.8	0.66
[73]	28.5	28.4	28.4	28.4	28.4	28.4	0.59
[76]-A	40.7	40.7	40.7	-	-	-	0.24
Proponowany	36.4	36.4	36.4	36.4	36.4	36.4	0.50

cent powierzchni obrazu) alternatywne rozwiązania potrafią sobie poradzić lepiej. W szczególności uwagę należy tutaj zwrócić na algorytm [76]-A, który przywraca treść obrazu z pełną możliwą dokładnością - w zakresie umożliwionym siłą wstawiania znaku wodnego. Algorytm ten cechuje się jednak odpornością na zmiany poniżej współczynnika ingerencji na poziomie 24% procent powierzchni obrazu. W przypadku bardziej rozległych zmian w obrazie, proponowane rozwiązanie znacząco przewyższa jakością rozwiązania alternatywne. Przy rekonfiguracji proponowanego algorytmu do poziomu jakości odpowiadającego systemowi [76]-A, możliwa jest rekonstrukcja aż do 33% zmienionych obszarów zdjęcia.

Przykładowy efekt rekonstrukcji (przy zmienionym poziomym pasie w środku obrazu) dla rozważonych algorytmów pokazano na rysunku 9. Współczynnik ingerencji w obraz wynosi 28% powierzchni obrazu.

7 Podsumowanie

W rozprawie poruszono problem samo-rekonstrukcji obrazów cyfrowych, tj. możliwości odtworzenia pierwotnej treści zmienionych obszarów zdjęcia na podstawie informacji referencyjnej zapisanej w samym obrazie przy pomocy cyfrowego znaku wodnego. Najważniejszym wynikiem rozprawy jest nowy model problemu rekonstrukcji obrazów cyfrowych. Model ten jednoznacznie pokazuje na istniejące analogie z teorią komunikacji przez kanał wymazujący. Praktyczna implementacja opisanego modelu wykorzystuje nowy sposób rozpraszania informacji referencyjnej po obrazie, bazujący na cyfrowych kodach fontannowych. Jego zastosowanie prowadzi do algorytmu o lepszej wydajności niż istniejące rozwiązania.

W ramach przeprowadzonych badań dokonano teoretycznej analizy problemu prowadzącej do wzorów pozwalających na wyznaczenie granic możliwości

(a) Obraz oryginalny

(b) Proponowany, 30.82 dB

(c) [74], 23.55 dB

Rysunek 9: Przykładowy efekt rekonstrukcji obrazu *6882* ze zbioru *bows*.

(d) [76]-B, 24.73 dB

(e) [75], 25.11 dB

(f) [73], 21.40 dB

Rysunek 9: Przykładowy efekt rekonstrukcji obrazu *6882* ze zbioru *bows*.

rekonstrukcji dla dowolnej konfiguracji procesu rekonstrukcji. Wprowadzono pojęcie *zapotrzebowanie rekonstrukcji*, które opisuje zależność pomiędzy zniszczoną powierzchnią obrazu a ilością potrzebnej informacji referencyjnej. Analiza zachowania zapotrzebowania rekonstrukcji pozwala na dokładne wyznaczenie granic możliwości poprawnego odtworzenia treści. Dotyczy to także systemów adaptacyjnych, w których jakość rekonstrukcji wybierana jest indywidualnie dla każdego z bloków obrazu. Wynikiem przeprowadzonej analizy jest także obserwacja, że wbrew powszechnie panującemu przekonaniu, wprowadzenie dodatkowych poziomów o niższej jakości nie musi prowadzić do polepszenia zdolności do odtworzenia obrazu.

Zaproponowano także mechanizm adaptacyjnej samo-rekonstrukcji, zdolny do gwarantowania zadanego poziomu jakości rekonstrukcji oraz zadanego poziomu odporności na zmiany obrazu. W ww. celu opracowano algorytm wyznaczania przyporządkowania poziomów jakości do bloków obrazu, którego zadaniem jest maksymalizacja jakości obrazu przy spełnieniu podanych wymagań. Ze względu na potrzebę przygotowania informacji referencyjnej o różnej jakości dla różnorodnych treści, zaproponowano formalny sposób wyznaczania alokacji bitów strumienia referencyjnego.

Istotnym wkładem jest także wyczerpująca ocena efektywności najlepszych rozwiązań opisanych w literaturze światowej. Testy przeprowadzono w tych samych warunkach testowych, dla porównywalnych konfiguracji rozważonych algorytmów.

Otrzymane wyniki dają podstawę do kontynuacji badań nad systemami uwierzytelniania i rekonstrukcji obrazów cyfrowych. W szczególności, kolejnym etapem jest opracowanie praktycznego systemu, zdolnego do efektywnej pracy na obrazach cyfrowych kompresowanych stratnie, np. z wykorzystaniem formatu JPEG. Prototypowy system MITIS (ang. *malicious image tampering identification system*) oparty na przedstawionym modelu, został nagrodzony Srebrną Gwiazdą Policji przez ekspertów wymiaru sprawiedliwości podczas międzynarodowych targów technologii policyjnych EUROPOLTECH, które odbyły się w kwietniu 2013 r. w Warszawie. Rozszerzenie opisanego modelu o zjawiska występujące przy pracy z obrazami kompresowanymi stratnie opisane pokrótce w dodatku E do rozprawy.

Literatura

[1] The sipi dataset, university of southern california. `http://sipi.usc.edu/database/`. Visited on 26 March 2012.

[2] Photoshop cs6 / content-aware fill. `http://www.adobe.com/products/photoshop/content-aware-fill.html`. Visited on 29 July 2012.

[3] Datamark. `http://www.datamark.com.sg/`. Visited on 29 July 2012.

[4] Handy photolab / touch retouch. `http://www.handyphotolab.com/application_tr`. Visited on 29 July 2012.

[5] The dataset from the 2nd bows contest. `http://bows2.ec-lille.fr/`, 2007. Visited on 26 March 2012.

[6] Chowdary. B. Adsumilli, Mylène. C. Q. Farias, Sanjit. K. Mitra, and Marco. Carli. A robust error concealment technique using data hiding for image and video transmission over lossy channels. *IEEE Transactions on Circuits and Systems for Video Technology*, 15(11):1394–1406, 2005. doi: 10.1109/TCSVT.2005.856933.

[7] Sergio Bravo-Solorio and Asoke K. Nandi. Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities. *Signal Processing*, 91(4):728 – 739, 2011. ISSN 0165-1684. doi: 10.1016/j.sigpro.2010.07.019.

[8] Sergio Bravo-Solorio, Chang-Tsun Li, and Asoke K. Nandi. Watermarking with low embedding distortion and self-propagating restoration capabilities. In *Proc. of IEEE International Conference on Image Processing*, Orlando, FL, 2012. URL `http://sbravo.x10.mx/home/repo/bravo-icip12.pdf`.

[9] Sergio Bravo-Solorio, Chang-Tsun Li, and Asoke K. Nandi. Watermarking method with exact self-propagating restoration capabilities. In *Proc. of IEEE International Workshop on Information Forensics and Security*, Tenerife, 2012. URL `http://sbravo.x10.mx/home/repo/bravo-wifs12.pdf`.

[10] Richard P. Brent, Shuhong Gao, and Alan G. B. Lauder. Random Krylov spaces over finite fields. *SIAM Journal on Discrete Mathematics*, 16(2): 276–287, February 2003. ISSN 0895-4801. doi: 10.1137/S089548010139388X.

[11] Chin-Chen Chang, Yi-Hsuan Fan, and Wei-Liang Tai. Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, 41(2):654 – 661, 2008. ISSN 0031-3203. doi: 10.1016/j.patcog.2007.06.003.

[12] Abbas Cheddad. *Steganoflage : A New Image Steganography Algorithm*. PhD thesis, University of Ulster, 2009. URL `http://theses.eurasip.org/theses/443/steganoflage-a-new-image-steganography-algorithm/`.

[13] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt. A secure and improved self-embedding algorithm to combat digital document forgery. *Signal Processing*, 89:2324–2332, December 2009. ISSN 0165-1684. doi: 10.1016/j.sigpro.2009.02.001.

[14] Brian Chen and Gregory W. Wornell. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4):1423–1443, 2001. doi: 10.1109/18.923725.

[15] Fan Chen, Hongjie He, Yaoran Huo, and Hongxia Wang. Self-recovery fragile watermarking scheme with variable watermark payload. In YunQing Shi, Hyoung-Joong Kim, and Fernando Perez-Gonzalez, editors, *Digital Forensics and Watermarking*, volume 7128 of *Lecture Notes in Computer Science*, pages 142–155. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-32204-4. doi: 10.1007/978-3-642-32205-1_13.

[16] Minghua Chen, Yun He, and R.L. Lagendijk. A fragile watermark error detection scheme for wireless video communications. *IEEE Transactions on Multimedia*, 7(2):201–211, 2005. doi: 10.1109/TMM.2005.843367.

[17] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. *Digital Watermarking and Steganography*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2nd edition, 2007. ISBN 0123725852, 9780123725851.

[18] Ingemar J. Cox, Gwenaël Doërr, and Teddy Furon. Watermarking is not cryptography. In YunQing Shi and Byeungwoo Jeon, editors, *Digital Watermarking*, volume 4283 of *Lecture Notes in Computer Science*, pages 1–15. Springer Berlin Heidelberg, 2006. ISBN 978-3-540-48825-5. doi: 10.1007/11922841_1.

[19] Chenwei Deng, Weisi Lin, Bu-Sung Lee, and Chiew Tong Lau. Robust image coding based upon compressive sensing. *IEEE Transactions on Multimedia*, 14(2):278–290, 2012. doi: 10.1109/TMM.2011.2181491.

[20] D.L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, 52(4):1289–1306, 2006. doi: 10.1109/TIT.2006.871582.

[21] Joachim J. Eggers, Robert Bäuml, Roman Tzschoppe, and Bernd Girod. Scalar costa scheme for information embedding. *IEEE Transactions on Signal Processing*, 51(4):1003–1019, 2003. doi: 10.1109/TSP.2003.809366.

[22] Dominik Engel, Thomas Stütz, and Andreas Uhl. A survey on jpeg2000 encryption. *Multimedia Systems*, 15:243–270, 2009. ISSN 0942-4962. doi: 10.1007/s00530-008-0150-0.

[23] Jessica Fridrich. Robust hash functions for digital watermarking. In *Proc. of the International Conference on Information Technology: Coding and Computing*, pages 178–183, 2000. doi: 10.1109/ITCC.2000.844203.

[24] Jessica Fridrich and Miroslav Goljan. Images with self-correcting capabilities. In *Proc. of IEEE International Conference on Image Processing*, 1999. doi: 10.1109/ICIP.1999.817228.

[25] Gürkan Gür, Yücel Altug, Emin Anarim, and Fatih Alagöz. Image error concealment using watermarking with subbands for wireless channels. *IEEE Communications Letters*, 11(2):179–181, 2007. doi: 10.1109/LCOMM.2007.061055.

[26] Ammar M. Hassan, Yassin M. Y. Hasan, Ayoub Al-Hamadi, Mohamed A. A. Wahab, and Bernd Michaelis. A novel public key self-embedding fragile watermarking technique for image authentication. In *Proc. of IEEE International Conference on Image Processing*, pages 1253–1256, 2009. ISBN 978-1-4244-5653-6. doi: 10.1109/ICIP.2009.5413551.

[27] Hong-Jie He, Jia-Shu Zhang, and Heng-Ming Tai. Self-recovery fragile watermarking using block-neighborhood tampering characterization. In Stefan Katzenbeisser and Ahmad-Reza Sadeghi, editors, *Information Hiding*, volume 5806 of *Lecture Notes in Computer Science*, pages 132–145. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-04430-4. doi: 10.1007/978-3-642-04431-1_10.

[28] Hongjie He and Jiashu Zhang. Cryptoanalysis on majority-voting based self-recovery watermarking scheme. In *Proc. International Conference on Multimedia Information Networking and Security*, 2009. doi: 10.1109/MINES.2009.218.

[29] Hongjie He, Jiashu Zhang, and Hongxia Wang. Synchronous counterfeiting attacks on self-embedding watermarking schemes. *International Journal of Computer Science and Network Security*, 6(1B):251–257, 2006.

[30] HongJie He, Fan Chen, Heng-Ming Tai, Ton Kalker, and Jiashu Zhang. Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme. *IEEE Transactions on Information Forensics and Security*, 7(1):185–196, 2012. doi: 10.1109/TIFS.2011.2162950.

[31] Matthew J. Holliman and Nasir D. Memon. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 9(3):432–441, 2000. doi: 10.1109/83.826780.

[32] Wien Hong and Tung-Shou Chen. A novel data embedding method using adaptive pixel pair matching. *IEEE Transactions on Information Forensics and Security*, 7(1):176–184, 2012. doi: 10.1109/TIFS.2011.2155062.

[33] Yaoran Huo, Hongjie He, and Fan Chen. Alterable-capacity fragile watermarking scheme with restoration capability. *Optics Communications*, 285: 1759–1766, 2012. doi: 10.1016/j.optcom.2011.12.044.

[34] Paweł Korus and Andrzej Dziech. A novel approach to adaptive image authentication. In *Proc. of IEEE International Conference on Image Processing*, Brussels, 2011. doi: 10.1109/ICIP.2011.6116243.

[35] Paweł Korus and Andrzej Dziech. Reconfigurable self-embedding with high quality restoration under extensive tampering. In *Proc. of IEEE International Conference on Image Processing*, Orlando, FL, 2012. doi: 10.1109/ICIP.2012.6467329.

[36] Paweł Korus and Andrzej Dziech. Efficient method for content reconstruction with self-embedding. *IEEE Transactions on Image Processing*, 22(3):1134–1147, March 2013. doi: 10.1109/TIP.2012.2227769.

[37] Paweł Korus, Wojciech Szmuc, and Andrzej Dziech. A scheme for censorship of sensitive image content with high-quality reconstruction ability. In *Proc. of IEEE International Conference on Multimedia and Expo*, Singapore, 2010. doi: 10.1109/ICME.2010.5583410.

[38] Paweł Korus, Jarosław Białas, Piotr Olech, and Andrzej Dziech. A high-capacity annotation watermarking scheme. In *Multimedia Communications, Services and Security*, volume 149 of *Communications in Computer and Information Science*, pages 1–9. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-21512-4. doi: 10.1007/978-3-642-21512-4_1.

[39] Paweł Korus, Lucjan Janowski, and Piotr Romaniak. Automatic quality control of digital image content reconstruction schemes. In *Proc. of IEEE International Conference on Multimedia and Expo*, Barcelona, 2011. doi: 10.1109/ICME.2011.6011872.

[40] Paweł Korus, Jarosław Białas, and Andrzej Dziech. A new approach to high-capacity annotation watermarking based on digital fountain codes. *Multimedia Tools and Applications*, pages 1–19, 2012. ISSN 1380-7501. doi: 10.1007/s11042-011-0986-8.

[41] Koert Kuipers. Bnb - branch and bound solver for a mixed-integer nonlinear programming. `http://www.mathworks.com/matlabcentral/fileexchange/95-bnb`, 2003.

[42] Jaejin Lee and Chee Sun Won. Authentication and correction of digital watermarking images. *Electronics Letters*, 35(11):886–887, 1999. doi: 10.1049/el:19990642.

[43] Jaejin Lee and Chee Sun Won. Image integrity and correction using parities of error control coding. In *Proc. of IEEE International Conference on Multimedia and Expo*, volume 3, pages 1297–1300, 2000. doi: 10.1109/ICME.2000.871004.

[44] Tien-You Lee and Shinfeng D. Lin. Dual watermark for image tampering detection and recovery. *Pattern Recognition*, 41:3497–3506, 2008. doi: 10.1016/j.patcog.2008.05.003.

[45] Guangzhen Li, Yoshimichi Ito, Xiaoyi Yu, Naoko Nitta, and Noboru Babaguchi. A discrete wavelet transform based recoverable image processing for privacy protection. In *Proc. of IEEE International Conference on Image Processing*, pages 1372–1375, 2008. doi: 10.1109/ICIP.2008.4712019.

[46] Guangzhen Li, Yoshimichi Ito, Xiaoyi Yu, Naoko Nitta, and Noboru Babaguchi. Recoverable privacy protection for video content distribution. *EURASIP Journal on Information Security*, 2009, January 2009. ISSN 1687-4161. doi: 10.1155/2009/293031.

[47] Ching-Yung Lin and Shih-Fu Chang. Sari: Self-authentication-and-recovery image watermarking system. In *ACM International Conference on Multimedia*, pages 628–629, New York, NY, USA, 2001. ISBN 1-58113-394-4. doi: 10.1145/500141.500266.

[48] Anna Lisowska. Smoothlets - multiscale functions for adaptive representation of images. *IEEE Transactions on Image Processing*, 20(7):1777–1787, 2011. doi: 10.1109/TIP.2011.2108662.

[49] Stuart Lloyd. Least Squares Quantization in PCM. *IEEE Transactions on Information Theory*, 28(2):129 – 137, mar 1982. ISSN 0018-9448. doi: 10.1109/TIT.1982.1056489.

[50] Michael Luby. Lt codes. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 271–280, Washington, DC, USA, 2002. IEEE Computer Society. ISBN 0-7695-1822-2. doi: 10.1109/SFCS.2002.1181950.

[51] David J. MacKay. *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003. ISBN 978-0521642989. URL `http://www.inference.phy.cam.ac.uk/mackay/itila/`.

[52] David J. MacKay. Fountain codes. *IEE Proceedings Communication*, 152(6), 2005. doi: 10.1049/ip-com:20050237.

[53] Antonis Mouhtaropoulos, Chang-Tsun Li, and Marthie Grobler. Proactive digital forensics: The ever-increasing need for standardization. In *Proc. of 2012 European Intelligence and Security Informatics Conference (EISIC)*, Odense, 2012. doi: 10.1109/EISIC.2012.66.

[54] Zhenxing Qian and Guorui Feng. Inpainting assisted self recovery with decreased embedding data. *IEEE Signal Processing Letters*, 17(11):929–932, November 2010. ISSN 1070-9908. doi: 10.1109/LSP.2010.2072991.

[55] Zhenxing Qian and Tong Qiao. Image self-embedding with large-area restoration capability. In *Proc. of IEEE International Multimedia Information Networking and Security Conference*, pages 649–652, 2010. doi: 10.1109/MINES.2010.141.

[56] Zhenxing Qian, Guorui Feng, Xinpeng Zhang, and Shuozhong Wang. Image self-embedding with high-quality restoration capability. *Digital Signal Processing*, 21(2):278–286, March 2011. ISSN 1051-2004. doi: 10.1016/j.dsp.2010.04.006.

[57] Chuan Qin, Chin-Chen Chang, and Pei-Yu Chen. Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. *Signal Processing*, 92(4):1137 – 1150, 2012. ISSN 0165-1684. doi: 10.1016/j.sigpro.2011.11.013.

[58] Amir Said. Measuring the strength of partial encryption schemes. In *International Conference on Image Processing*, pages II: 1126–1129, 2005. doi: 10.1109/ICIP.2005.1530258.

[59] Gerald Schaefer and Michal Stich. Ucid - an uncompressed colour image database. In *Storage and Retrieval Methods and Applications for Multimedia 2004*, Proceedings of SPIE, pages 472–480, 2004. URL `http://homepages.lboro.ac.uk/~cogs/datasets/UCID/ucid.html`.

[60] Gerard Sierksma. *Linear and Integer Programming - Theory and Practice*. Marcel Dekker, 2-nd edition, 2002. ISBN 978-0824706739.

[61] David Slepian and Jack Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4):471–480, July 1973. ISSN 0018-9448. doi: 10.1109/TIT.1973.1055037.

[62] Jun Tian. Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8):890–896, 2003. doi: 10.1109/TCSVT.2003.815962.

[63] Hui Wang, Anthony T. S. Ho, and Xi Zhao. A novel fast self-restoration semi-fragile watermarking algorithm for image content authentication resistant to jpeg compression. In *Proceedings of the 10th international conference on Digital-Forensics and Watermarking*, IWDW'11, pages 72–85, Berlin, Heidelberg, 2012. Springer-Verlag. ISBN 978-3-642-32204-4. doi: 10.1007/978-3-642-32205-1_8.

[64] Ming-Shi Wang and Wei-Che Chen. A majority-voting based watermarking scheme for color image tamper detection and recovery. *Computer Standards & Interfaces*, 29(5):561–570, 2007. ISSN 0920-5489. doi: 10.1016/j.csi.2006.11.009.

[65] Shuenn-Shyang Wang and Sung-Lin Tsai. Automatic image authentication and recovery using fractal embedding and image inpainting. *Pattern Recognition*, 41:701–712, 2008. doi: 10.1016/j.patcog.2007.05.012.

[66] Aaron D. Wyner and Jacob Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Transactions on Information Theory*, 22:1–10, 1976. doi: 10.1109/TIT.1976.1055508.

[67] Shao Yafei, Zhang Li, Wu Guowei, and Lin Xinggang. Reconstruction of missing blocks in image transmission by using self-embedding. In *Proc. Int Intelligent Multimedia, Video and Speech Processing Symp*, pages 535–538, 2001. doi: 10.1109/ISIMP.2001.925451.

[68] Chun-Wei Yang and Jau-Ji Shen. Recover the tampered image based on vq indexing. *Signal Processing*, 90:331–243, 2010. doi: 10.1016/j.sigpro.2009.07.007.

[69] Xiaoyi Yu, Kenta Chinomi, Takashi Koshimizu, Naoko Nitta, Yoshimichi Ito, and Noboru Babaguchi. Privacy protecting visual processing for secure video surveillance. In *Proc. of IEEE International Conference on Image Processing*, pages 1672–1675, 2008. doi: 10.1109/ICIP.2008.4712094.

[70] Wei Zhang, S.S. Cheung, and Minghua Chen. Hiding privacy information in video surveillance system. In *Proc. of IEEE International Conference on Image Processing*, volume 3, 2005. doi: 10.1109/ICIP.2005.1530530.

[71] Xinpeng Zhang and Shuozhong Wang. Fragile watermarking with error free restoration capability. *IEEE Transactions on Multimedia*, 10(8), 2008. doi: 10.1109/TMM.2008.2007334.

[72] Xinpeng Zhang and Shuozhong Wang. Fragile watermarking scheme using a hierarchical mechanism. *Signal Processing*, 89:675–679, 2009. doi: 10.1016/j.sigpro.2008.10.001.

[73] Xinpeng Zhang, Shuozhong Wang, and Guorui Feng. Fragile watermarking scheme with extensive content restoration capability. In *Proc. of International Workshop on Digital Watermarking*, 2009. doi: 10.1007/978-3-642-03688-0_24.

[74] Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. *IEEE Transactions on Information Forensics and Security*, 6(4):1223–1232, 2011. doi: 10.1109/TIFS.2011.2159208.

[75] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng. Self-embedding watermark with flexible restoration quality. *Multimedia Tools and Applications*, 54:385–395, 2011. ISSN 1380-7501. doi: 10.1007/s11042-010-0541-z.

[76] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng. Reference sharing mechanism for watermark self-embedding. *IEEE Transactions on Image Processing*, 20(2):485–495, 2011. doi: 10.1109/TIP.2010.2066981.

[77] Xunzhan Zhu, Anthony T.S. Ho, and Pina Marziliano. A new semi fragile image watermarking with robust tampering restoration using irregular sampling. *Signal Processing : Image Communication*, 22(5), 2007. doi: 10.1016/j.image.2007.03.004.