Informatyka techniczna i sztuczna inteligencja
Technical informatics and Artificial Intelligence
Engineer of XXI Century'2024

Analysis of using SVD decomposition to hide data in digital images by modifying singular values

Olga Veselska [1], Ruslana Ziubina [2]

[1] *University of Bielsko-Biala, 2 Willowa st., Bielsko-Biala, 43-309, Poland, oveselska@ubb.edu.pl*
[2] *University of Bielsko-Biala, 2 Willowa st., Bielsko-Biala, 43-309, Poland, rziubina@ubb.edu.pl*
* *Corresponding author, oveselska@ubb.edu.pl*

Abstract: This paper presents a study of applying singular value decomposition (SVD) to hide information in digital images. The method uses a modification of selected values in the diagonal matrix Σ obtained by decomposing the image matrix into orthogonal matrices U and V. Changing the principal components r in the Σ matrix allows the data to be hidden while having minimal impact on the visual quality of the image. It was analyzed under what conditions, with different values of r, ensuring maximum imperceptibility of the changes made to the image is possible. The study assessed image quality after modification using the Peak Signal-to-Noise Ratio (PSNR), which measures the difference between the original and modified images. In addition, the Q-determination coefficient was analyzed, which determines how much of an image's information can be preserved with different numbers of principal components while maintaining good visual quality of the image.

Keywords: steganography, SVD decomposition, singular values, data hiding, digital images, principal component modification, image quality.

Analiza wykorzystania dekompozycji SVD do ukrywania danych w obrazach cyfrowych poprzez modyfikację wartości osobliwych

Olga Veselska [1*], Ruslana Ziubina [2]

[1] *Uniwersytet Bielko-Bialski, ul.Willowa 2, Bielskko-Biała, 43-309, Polska, oveselska@ubb.edu.pl*
[2] *Uniwersytet Bielsko-Bialski, ul. Willowa 2, Bielsko-Biała, 43-309, Polska, rziubina@ubb.edu.pl*
* *Corresponding author, oveselska@ubb.edu.pl*

Streszczenie: W artykule zaprezentowano badania nad zastosowaniem dekompozycji wartości osobliwych (SVD) w celu ukrywania informacji w obrazach cyfrowych. Metoda ta wykorzystuje modyfikację wybranych wartości w macierzy diagonalnej Σ uzyskanej w wyniku dekompozycji macierzy obrazu na ortogonalne macierze U i V. Zmiana głównych komponentów r w macierzy Σ pozwala na ukrycie danych, przy jednoczesnym minimalnym wpływie na jakość wizualną obrazu. Przeanalizowano, w jakich warunkach, przy różnych wartościach r, możliwe jest zapewnienie maksymalnej niezauważalności zmian wprowadzonych do obrazu. Badania obejmowały ocenę jakości obrazu po modyfikacji za pomocą współczynnika PSNR (Peak Signal-to-Noise Ratio), który mierzy różnicę między oryginalnym a zmodyfikowanym obrazem. Dodatkowo analizowano współczynnik determinacji Q, który określa, jaką część informacji obrazu można zachować przy różnych liczbach głównych komponentów dla zapewnia wysoki poziom ukrycia informacji przy zachowaniu dobrej jakości wizualnej obrazu.

Słowa kluczowe: steganografia, dekompozycja SVD, wartości osobliwe, ukrywanie danych, obrazy cyfrowe, modyfikacja głównych komponentów, jakość obrazu.

DOI: https://doi.org/10.53052/9788367652292.21

1. Wprowadzenie

Steganografia, czyli sztuka ukrywania informacji w nośnikach cyfrowych, zyskuje na znaczeniu w obszarach bezpieczeństwa informacji, komunikacji oraz ochrony prywatności. Jej głównym celem jest zapewnienie, aby dane były ukryte w taki sposób, że obecność wiadomości pozostaje niezauważona, nawet przy analizie nośnika przez osobę trzecią. W ostatnich latach rozwój algorytmów steganograficznych koncentrował się na efektywnym ukrywaniu danych w obrazach cyfrowych, które są szeroko stosowane jako nośniki informacji dzięki ich wysokiej pojemności i powszechnemu występowaniu.

Jednym z nowoczesnych podejść do steganografii jest wykorzystanie dekompozycji wartości osobliwych (SVD), która pozwala na rozkład macierzy obrazu na macierze ortogonalne oraz macierz diagonalną zawierającą wartości osobliwe [1-3]. Algorytmy steganograficzne bazujące na SVD wykorzystują fakt, że modyfikacja mniejszych wartości osobliwych w macierzy Σ minimalnie wpływa na jakość wizualną obrazu, co umożliwia ukrycie danych w sposób praktycznie niewidoczny dla ludzkiego oka .

Badania przeprowadzone w ostatnich latach wykazały, że technika ta, choć obiecująca, wymaga precyzyjnego doboru liczby głównych komponentów r, aby zapewnić odpowiedni kompromis między pojemnością ukrytych danych a jakością obrazu [4, 5]. W niektórych badaniach sugerowano, że optymalna liczba zmodyfikowanych wartości osobliwych zależy od rodzaju obrazu, jego złożoności oraz ilości ukrytej wiadomości [6-9].

W niniejszym artykule przeanalizowano możliwości wykorzystania dekompozycji SVD w steganografii obrazowej. Skoncentrowano się na wpływie modyfikacji wartości osobliwych na jakość wizualną obrazu oraz na zbadaniu, w jakich warunkach możliwe jest osiągnięcie maksymalnej niezauważalności ukrytych danych przy minimalnej degradacji jakości obrazu. Zastosowano wskaźniki PSNR (Peak Signal-to-Noise Ratio) oraz współczynnik determinacji Q, które pozwalają ocenić jakość odtworzonego obrazu i efektywność algorytmu steganograficznego .

2. Zastosowanie dekompozycji SVD w steganografii obrazów

Dekompozycja SVD (Singular Value Decomposition) to matematyczna technika, która pozwala na rozkład macierzy na trzy inne macierze o szczególnych właściwościach. Jest szeroko stosowana w różnych dziedzinach, takich jak analiza danych, kompresja obrazów, rozpoznawanie wzorców i steganografia. Dekompozycja SVD istnieje dla każdej macierzy, niezależnie od jej rozmiaru czy struktury [10, 11]. SVD jest potężnym narzędziem, które umożliwia analizę struktury danyc oraz rozwiązywanie wielu problemów numerycznych w sposób optymalny.

Definicja 1. *Dekompozycja singularna to dekompozycja prostokątnej macierzy rzeczywistej lub zespolonej w postaci $A=U\Sigma V$, gdzie Σ jest diagonalną macierzą m×n z przekątną o nierosnących liczbach singularnych $\sigma_1,\ldots, \sigma_k$, a U i V są ortogonalnymi, odpowiednio, macierzami m×m i n×n*

Definicja 2. *Liczby osobliwe rzeczywistej macierzy $A(m \times n)$ są arytmetycznymi pierwiastkami kwadratowymi z liczb własnych $\lambda_1, \lambda_2,\ldots, \lambda k$ macierzy $A^T A$ i $A A^T$, gdzie $k=min\{m, n\}$*

Liczby osobliwe są oznaczane literą σ i są numerowane w porządku malejącym: $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_k \geq 0$. Liczby osobliwe są natychmiast wprowadzane jako elementy diagonalne macierzy Σ w dekompozycji SVD. Również definicja liczby osobliwej σ jest sformułowana za pomocą zestawu równości $Ax=\sigma y$, $A^T y=\sigma x$, gdzie gdzie n-wymiarowy wektor x i m-wymiarowy wektor y są prawym i lewym wektorem osobliwym. Wektory te tworzą podstawę ortogonalną.

Twierdzenie 1. *Niech A będzie dowolną macierzą m×n, oraz m≥n. Wtedy odwzorowanie $A= U\Sigma V^T$ jest prawdziwe, gdzie macierz U ma wymiar m×m i spełnia zależność $U^T U=I$, macierz V jest kwadratowa rzędu n i spełnia zależność $V^T V=I$, oraz $\Sigma=diag(\sigma_1, \ldots, \sigma_n)$, gdzie $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_n \geq 0$.*
Kolumny $u_1, \ldots, u_m$ macierzy U nazywane są lewymi wektorami osobliwymi (macierzy A). Kolumny $v_1, \ldots, v_n$ macierzy V nazywane są prawymi wektorami osobliwymi. Wartości $\{\sigma i\}_{i=1,\ldots,n}$ nazywane są liczbami osobliwymi. (Gdy m<n, musimy rozważyć macierz A^T).

W steganografii modyfikacja mniejszych wartości osobliwych w macierzy Σ pozwala na ukrycie danych w sposób niemal niezauważalny dla ludzkiego oka, ponieważ najmniej znaczące wartości mają najmniejszy wpływ na ogólną strukturę obrazu [12].Takie podejście do steganografii wykorzystuje mocne strony dekompozycji SVD, takie jak zdolność do odwzorowywania najważniejszych cech obrazu w kilku dominujących wartościach osobliwych, podczas gdy ukryte dane mogą być przechowywane w mniej znaczących komponentach, minimalizując zmiany w obrazie.

2.1 Algorytm dekompozycji SVD w steganografii obrazów

W niniejszej pracy zastosowano dekompozycję SVD do steganografii w obrazach, zgodnie z następującym algorytmem:

1. Obraz, w którym będą ukryte dane, jest przedstawiony w postaci macierzy \(A(m, n)\). Przeprowadzana jest dekompozycja SVD dla macierzy obrazu A(m×n).

$$A=U\Sigma V^{T}, \tag{1}$$

   gdzie Σ - macierz diagonalna, a U i V to macierze ortogonalne.

2. Modyfikacja wybranych wartości w macierzy Σ w celu ukrycia danych. Najmniej znaczące bity w elementach Σ mogą zostać zamienione na bity wiadomości, którą chcemy ukryć. Dzięki temu zmiany w obrazie będą trudne do zauważenia.
3. Zrekonstruowanie obrazu po modyfikacji macierzy Σ.

$$A'=U\Sigma'VT, \tag{2}$$

   gdzie Σ ′ to macierz Σ po modyfikacji, a A′ to nowy obraz z ukrytą wiadomością.

4. Aby odzyskać ukrytą wiadomość, wystarczy ponownie przeprowadzić dekompozycję SVD na obrazie A′, a następnie odczytać zmodyfikowane wartości w macierzy Σ.

2.1.1 Przeprowadzenie SVD na macierzy obrazu A

Załóżmy, że mamy prosty obraz o rozmiarze 3x3 reprezentowany przez macierz jasności pikseli A:

$$A = \begin{pmatrix} 200 & 202 & 198 \\ 203 & 205 & 202 \\ 201 & 199 & 200 \end{pmatrix}$$

Obliczamy SVD dla macierzy A. Wynikiem będzie: A=UΣVT

$$U = \begin{pmatrix} -0.577 & -0.577 & 0.577 \\ -0.577 & 0.789 & 0.211 \\ -0.577 & -0.211 & -0.789 \end{pmatrix}, \quad \Sigma = \begin{pmatrix} 600 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0.5 \end{pmatrix}, \quad V^T = \begin{pmatrix} -0.577 & -0.577 & -0.577 \\ 0.789 & -0.211 & -0.577 \\ -0.211 & -0.789 & 0.577 \end{pmatrix}$$

2.1.2 Modyfikacja wybranych wartości w Σ w celu ukrycia wiadomości

Załóżmy, że chcemy ukryć jedną literę wiadomości, np. 'H'. Wartość ASCII dla litery 'H' to 72, co w systemie binarnym wygląda tak: 01001000.

Zmienimy na najmniej znaczące bity wybranych wartości w macierzy Σ. Weźmy na przykład pierwsze dwa największe elementy w Σ: 600 i 3.

600 binarnie: 1001011000. Zmieniamy najmniej znaczący bit, żeby ukryć pierwszą cyfrę wiadomości 0 — pozostaje 1001011000.

3 binarnie: 11. Zmieniamy najmniej znaczący bit, żeby ukryć drugą cyfrę wiadomości 1 — otrzymujemy 11.

Po zakończeniu modyfikacji macierz Σ′ może wyglądać tak:

$$\Sigma' = \begin{pmatrix} 600 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0.5 \end{pmatrix}$$

2.1.3. Rekonstrukcja obrazu po modyfikacji Σ

Nowy obraz po modyfikacji można obliczyć jako A′=UΣ′VT

Wartości w macierzy A ′ mogą nieznacznie różnić się od oryginalnych, ale różnica powinna być na tyle mała, że zmiany będą niezauważalne dla oka.

2.1.4. Odzyskiwanie ukrytej wiadomości

Aby odzyskać wiadomość, należy ponownie przeprowadzić SVD na zmodyfikowanym obrazie A′, aby uzyskać macierz Σ′, a następnie odczytać najmniej znaczące bity z jej wartości.

Wartości z Σ′: 600 (binarnie: 1001011000), 3 (binarnie: 11).

Po odczytaniu najmniej znaczących bitów: 01, co odpowiada pierwszym dwóm bitom wiadomości 01001000, czyli 'H'.

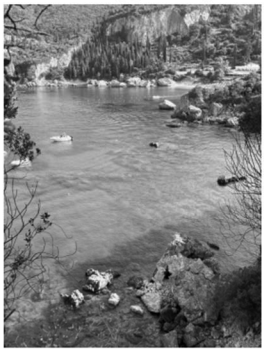
3. Przykład zastosowania SVD w steganografii

W steganografii najczęściej używane obrazy do osadzania danych to te, które mają dużą ilość szczegółów i różnorodność kolorów lub intensywności pikseli, co utrudnia dostrzeżenie zmian wprowadzone przez ukrycie danych. Najecęszciej są to obrazy naturalne i fotografie, dlatego że obrazy przedstawiające złożone sceny, takie jak krajobrazy, przyroda, portrety czy zdjęcia codziennych scen, mają wiele drobnych detali, które skutecznie maskują ukryte dane. Ze względu na dużą ilość szczegółów i naturalne „szumy", są często wykorzystywane do osadzania danych bez ryzyka wykrycia zmian. Rowniesz ostatnim czasem bardzo aktualne używanie do osadzania danych obrazów medycznych (np. obrazy MRI). Obrazy medyczne, takie jak MRI czy CT, są bardzo szczegółowe i używane w aplikacjach, gdzie ukrywanie danych (np. dodatkowe metadane pacjenta).

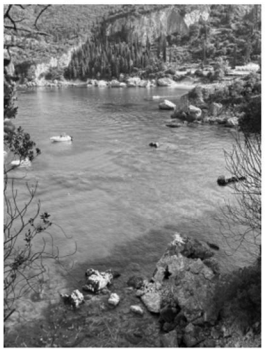
W oparciu o powyższe, do eksperymentu wybrano trzy rodzaje obrazów: obraz 1 „Natura", obraz 2 „Portret", obraz 3 „Fotografia medyczna MRI". Po przeprowadzeniu dekompozycji SVD dla macierzy obrazu A, wybrano do modyfikacji najmniejsze wartości w macierzy Σ, aby ukryć wiadomość o długości 100 znaków. W celu obliczenia dekompozycji SVD, współczynnika determinacji Q oraz wskaźnika PSNR, opracowano i zaimplementowano odpowiednie programy w środowisku programistycznym Python.

Steganografia wykorzystująca dekompozycję wartości pojedynczej (SVD) została zaimplementowana w celu ukrycia wiadomości w obrazie. Dane zostały ukryte poprzez modyfikację wartości osobliwych w macierzy Σ, a wyniki zostały wyświetlone na czterech obrazach: oryginalnym obrazie i trzech obrazach o różnym stopniu modyfikacji.

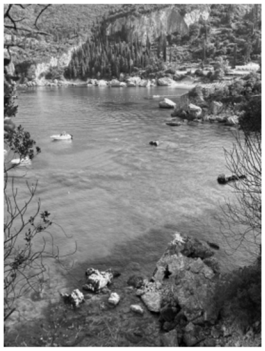
Rys. 1(a) Oryginalny obraz



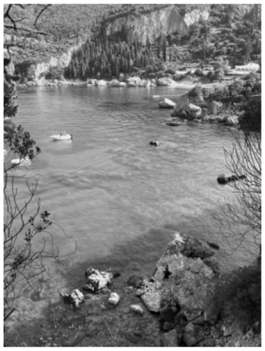
Rys. 1(b) Modyfikacja (10% wartości Σ)



Rys. 1(c) Modyfikacja (50% wartości Σ)



Rys. 1(d) Modyfikacja (100% wartości Σ)



Rysunek 1. Obraz 1 „Natura”z różnym stopniem modyfikacji wartości Σ

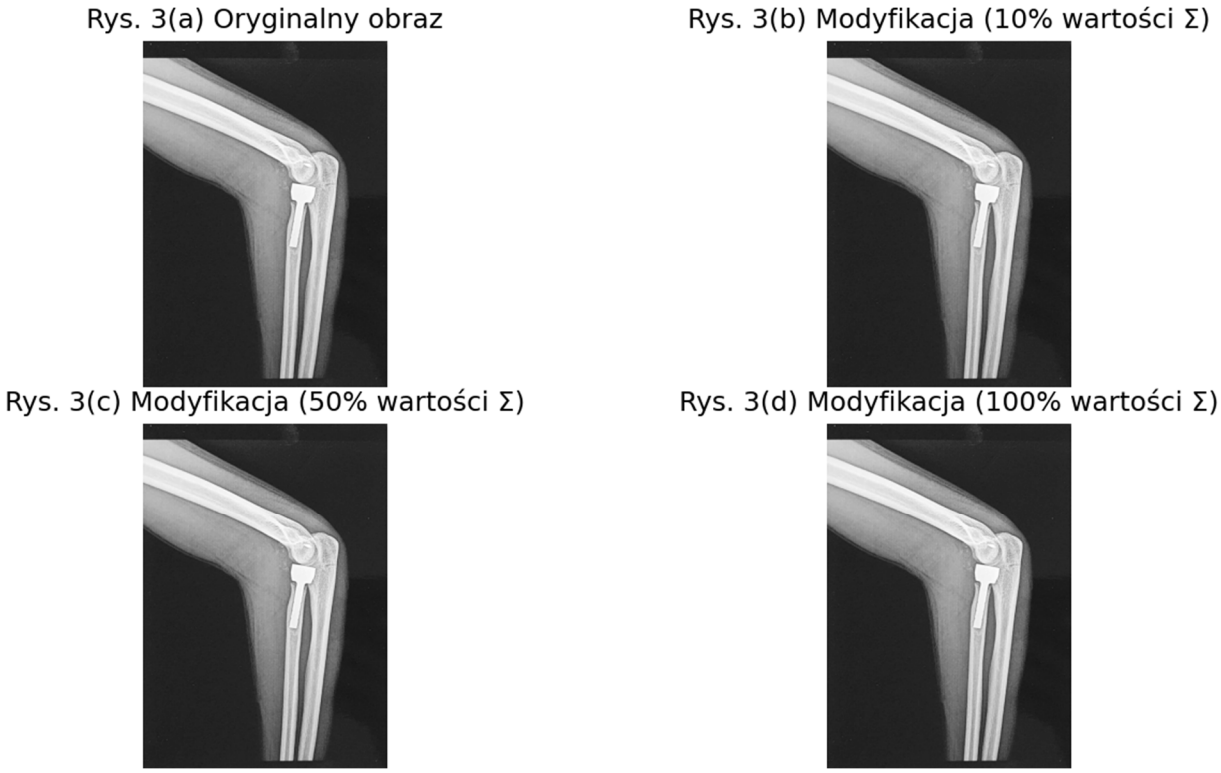
Rys. 2(a) Oryginalny obraz

Rys. 2(b) Modyfikacja (10% wartości Σ)

Rys. 2(c) Modyfikacja (50% wartości Σ)

Rys. 2(d) Modyfikacja (100% wartości Σ)

Rysunek 2. Obraz 2 „Portret” z różnym stopniem modyfikacji wartości Σ



Rysunek 3. Obraz 3 „Fotografia medyczna MRI"z różnym stopniem modyfikacji wartości Σ

Na rysunkach 1(a), 2(a), 3(a) przedstawiono oryginalne obrazy, bez żadnych modyfikacji, co stanowi bazę do porównania z modyfikowanymi wersjami. Na rysunkach 1(b), 2(b), 3(b) modyfikowano jedynie 10% wartości w macierzy Σ. W tej wersji zmiany w obrazie są praktycznie niewidoczne dla ludzkiego oka. Oznacza to, że steganograficzne ukrywanie danych jest mało zauważalne. Na rysunkach 1(c), 2(c), 3(c) modyfikowano 50% wartości w macierzy Σ. W tej wersji obraz zaczyna wykazywać pewne widoczne zmiany w strukturze, co świadczy o tym, że większa liczba modyfikacji zaczyna wpływać na jakość obrazu. Niemniej jednak zmiany są umiarkowane i wciąż mogą być trudne do wykrycia bez szczegółowej analizy. Na rysunkach 1(d), 2(d), 3(d) modyfikowano 100% wartości w macierzy Σ. W tej wersji obraz jest wyraźnie zniekształcony. Jakość obrazu znacznie się pogorszyła, co oznacza, że steganografia staje się coraz bardziej widoczna, gdy modyfikujemy większość wartości osobliwych.

4. Zależność współczynnika determinacji od liczby głównych komponentów

W steganografii, celem jest ukrycie pewnej informacji w obrazie bez widocznych zmian w jego jakości. Przeprowadzenie SVD umożliwia dekompozycję obrazu na macierze U, Σ i V, gdzie modyfikacja macierzy Σ (wartości osobliwych) pozwala na ukrycie danych. Kryterium zmiany jakości w macierzy A jest współczynnik determinacji zbliżony do jedności, obliczany według wzoru (1).

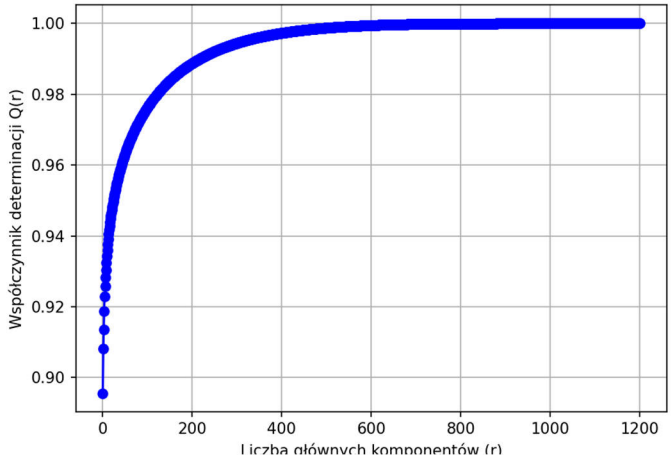
$$Q(r) = \frac{\sum_{k=1}^{r} \lambda_k}{\sum_{k=1}^{n} \lambda_k} \tag{3}$$

gdzie:

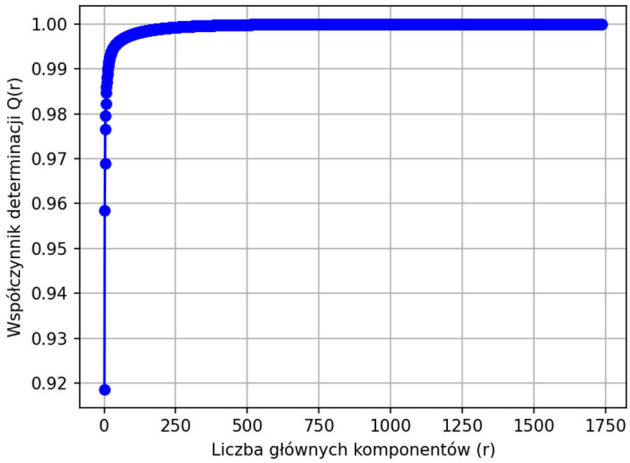
- λk to wartości osobliwe (elementy macierzy Σ),
- r to liczba głównych komponentów,
- n to całkowita liczba wartości osobliwych.

Podczas zastosowania SVD do steganografii obrazów, współczynnik determinacji Q mierzy, jak blisko oryginalny obraz i zmodyfikowany obraz po zmnianie liczby wartości osobliwych są do siebie podobne. Q znacząco mniejsze od 1 oznacza, że rekonstrukcja nie jest dokładna, co sugeruje, że znaczna część informacji została utracona w procesie

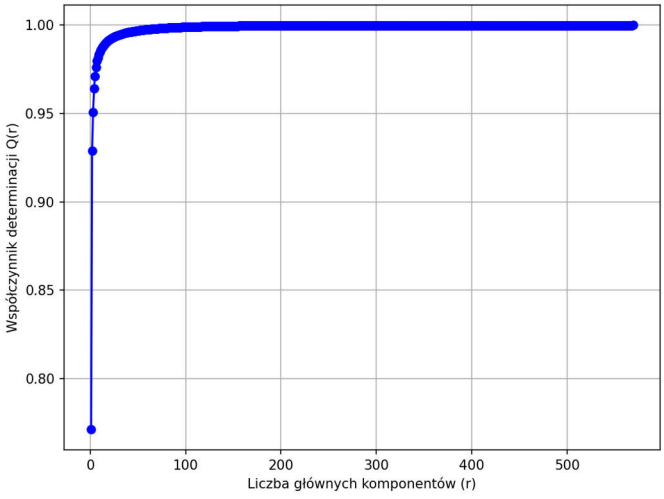
redukcji wymiarów. Wartości Q(r) zbliżają się do 1, gdy r rośnie i obejmuje coraz więcej głównych komponentów, co oznacza lepszą jakość obrazu. Współczynnik determinacji Q pokazuje, jaka część oryginalnej informacji obrazu jest zachowywana po modyfikacji wybranych komponentów w macierzy Σ podczas procesu dekompozycji SVD. Analiza wartości Q w zależności od liczby głównych komponentów r pozwala ocenić, w jakim stopniu modyfikacje macierzy Σ wpływają na jakość obrazu, a tym samym na to, jak wiele informacji można ukryć, minimalizując zauważalne zmiany w obrazie.



a)



c)



c)

Rysunek 4. Zależność współczynnika determinacji Q od liczby głównych komponentów r: a)- dla obraza 1 „Natura" b) -dla obraza 2 „Portret" , c) - dla obraza 3 „Fotografia medyczna MRI"

Jak widać na powyższych rysunkach, potencjał do osadzania wiadomości jest największy na zdjeczach natury, ponieważ w tym celu można zmodyfikować więcej głównych komponentów. Dla obraza 1 „Natura" zakres ten wynosi od 0 do 400 r, dla obraza 2 „Portret" od 0 do 200 r, a dla obraza 3 „Fotografia medyczna MRI" od 0 do 50 r. Z analizy powyższych wyników wynika, że potencjał do osadzania danych za pomocą modyfikacji głównych komponentów w macierzy Σ zależy w dużej mierze od rodzaju obrazu. Obrazy o złożonych teksturach, takie jak krajobrazy, są mniej wrażliwe na modyfikacje i pozwalają na bezpieczne wprowadzenie większej ilości informacji, zachowując przy tym dobrą jakość wizualną. Z kolei obrazy o bardziej jednorodnych strukturach, takie jak portrety czy obrazy medyczne, wymagają ostrożniejszego podejścia, ponieważ są bardziej podatne na degradację jakości przy modyfikacjach większej liczby głównych komponentów. Dzięki tym analizom można wnioskować, że w zależności od rodzaju obrazu należy dostosować zakres modyfikacji liczby głównych komponentów, aby zrównoważyć ilość ukrytych danych i zachowanie odpowiedniej jakości wizualnej.

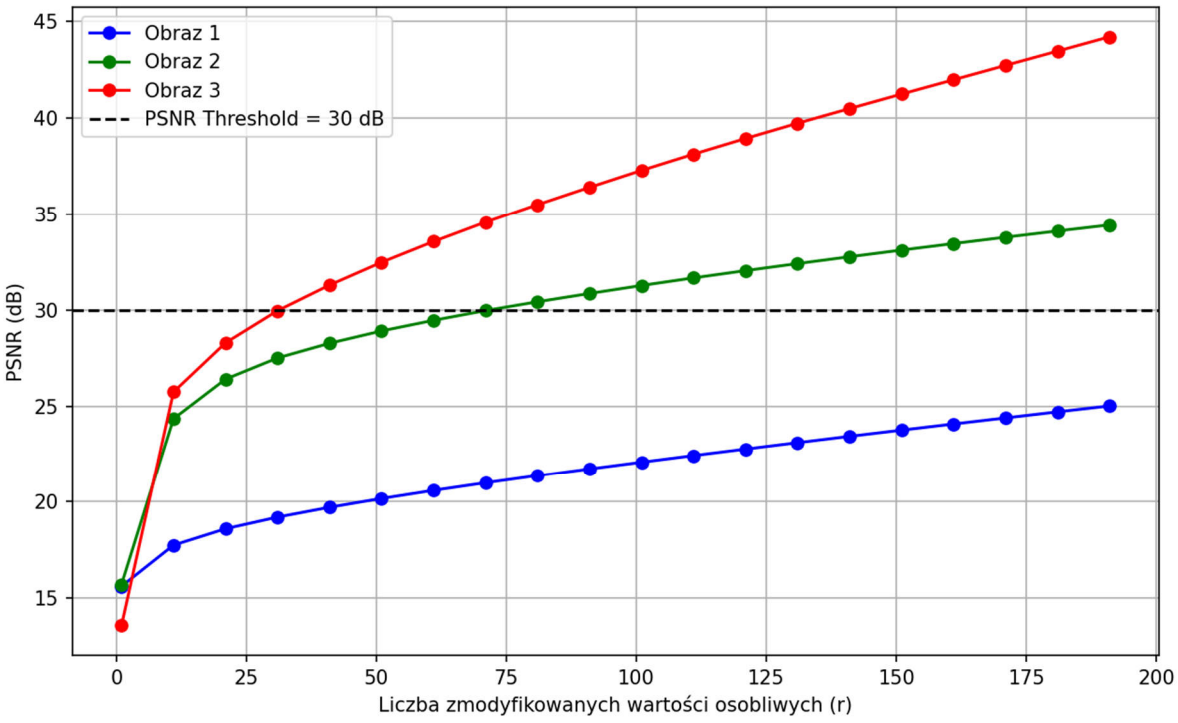
5. Zależności jakości obrazu od liczby zmodyfikowanych wartości osobliwych

Dla dokładnej oceny jakości obrazu po modyfikacji zastosowano wskaźnik PSNR (ang. Peak Signal-to-Noise Ratio). Wartość PSNR pozwala określić, jak bardzo zmieniony obraz różni się od obrazu oryginalnego i jest obliczana według wzoru (4).

$$\mathrm{PSNR} = 10 \cdot \log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right), \tag{4}$$

gdzie MAX to maksymalna możliwa wartość piksela obrazu, a MSE to średni błąd kwadratowy między obrazem oryginalnym a stego.

Po obliczeniu PSNR dla trzech obrazów uzyskano zależność jakości obrazu od liczby zmodyfikowanych wartości pojedynczych r, a wyniki przedstawiono na rysunku 5.



Rysunek 5. Zależność wskaźnika PSNR od liczby zmodyfikowanych wartości osobliwych

Próg PSNR (Peak Signal-to-Noise Ratio) wynoszący 30 dB jest powszechnie uznawany za minimalną wartość, przy której różnice między oryginalnym a zmodyfikowanym obrazem są trudno zauważalne dla ludzkiego oka. PSNR mierzy stosunek między maksymalną możliwą wartością sygnału (jasności pikseli) a poziomem szumu (błędem wprowadzonym przez modyfikację obrazu).

Dla obrazów, ogólne zasady interpretacji PSNR są takie:

- PSNR ≥ 30 dB - Zmiany są praktycznie niezauważalne. Obraz wygląda bardzo podobnie do oryginału.
- 20 dB ≤ PSNR < 30 dB - Można dostrzec pewne różnice, ale obraz wciąż jest akceptowalnej jakości.
- PSNR < 20 dB -Widoczne artefakty lub degradacja obrazu.

Wartość PSNR jest obliczana dla różnych liczby modyfikowanych wartości osobliwych r w dekompozycji SVD. Umieszczenie linii poziomej na poziomie 30 dB pomaga wskazać, przy jakiej liczbie zmodyfikowanych wartości *r* jakość obrazu zaczyna być dostrzegalnie gorsza.

Każdy obraz, oznaczony innym kolorem na rys. 5, wykazuje ze wraz z wzrostem liczby r, wskaźnik PSNR maleje. Oznacza to, że większa liczba zmodyfikowanych wartości osobliwych powoduje większe zniekształcenia w obrazie. Początkowo, dla małych wartości r, zmiany są niemal niezauważalne, PSNR jest wysoki. W miarę jak zwiększamy r, PSNR maleje, co oznacza większą degradację jakości obrazu.

6. Wnioski

Artykuł przedstawia analizę wykorzystania dekompozycji wartości osobliwych (SVD) jako metody steganograficznej do ukrywania danych w obrazach cyfrowych. Głównym celem pracy jest zbadanie, w jaki sposób można zastosować modyfikację wartości osobliwych w macierzy obrazu, aby skutecznie i niezauważalnie ukryć informacje. Analiza efektywności algorytmu opierała się na różnych poziomach modyfikacji wartości osobliwych i ich wpływie na jakość obrazu. Metoda jest skuteczna w ukrywaniu danych, przy czym przy niewielkich zmianach wartości osobliwych różnice między oryginalnym a zmodyfikowanym obrazem są praktycznie niedostrzegalne. Jakość obrazu po modyfikacjach mierzono za pomocą wskaźnika PSNR (Peak Signal-to-Noise Ratio). Wyniki pokazały, że dopóki PSNR pozostaje powyżej 30 dB, jakość obrazu jest akceptowalna, a ukryte dane są dobrze zamaskowane.

Wyniki eksperymentów przeprowadzonych w artykule potwierdzają, że potencjał do ukrywania danych za pomocą modyfikacji wartości osobliwych w macierzy Σ zależy w dużej mierze od rodzaju obrazu. Z analizy tych wyników wynika, że obrazy o złożonych teksturach, takie jak krajobrazy, mają większy potencjał do ukrywania informacji, ponieważ są mniej podatne na zauważalne zmiany w wyniku modyfikacji większej liczby głównych komponentów. Z kolei obrazy o bardziej jednorodnych strukturach, takie jak portrety czy obrazy medyczne, wymagają bardziej konserwatywnego podejścia, aby nie zniekształcać istotnych szczegółów wizualnych. Metoda wykorzystująca dekompozycję SVD do steganografii oferuje dobrą równowagę pomiędzy skutecznością ukrywania danych a jakością obrazu. Dzięki modyfikacjom wartości osobliwych możliwe jest ukrycie danych bez wprowadzania widocznych zniekształceń. Algorytm SVD, w połączeniu z technikami steganograficznymi, zapewnia potencjalnie bezpieczny sposób ukrywania danych w obrazach cyfrowych.

Acknowledgement:

The work was fulfilled within the framework of Erasmus+ project "The transferable training model - the best choice for training IT business leaders" (project no. 2023-2-PL01-KA220-HED-000179445). Namely, the work contributes to the project results concerning studying use cases of AI and IoT good practices (work packages 2 and 3).

Literatura

1. N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, “Image steganography: A review of the recent advances,” IEEE Access, vol. 9, pp. 23409–23423, 2021.
2. J. H. Kim et al., "Neural Network-Assisted SVD Steganography for High-Capacity Data Hiding," IEEE Transactions on Image Processing, 2023.
3. Kumar, P., & Kaur, M. (2017). Performance analysis of image steganography using singular value decomposition. Journal of Information Security and Applications, 34, 55–65. DOI: 10.1016/j.jisa.2017.02.003
4. P. L. Gonzalez et al., "Hybrid Watermarking Using SVD and Adaptive Embedding Techniques," Computers & Security, 2020.
5. Bhatnagar, G., Wu, Q. J., & Raman, B. (2012). A new robust watermarking scheme based on SVD and wavelet transform. Pattern Recognition, 45(12), 4041–4051. DOI: 10.1016/j.patcog.2012.05.019
6. Singh, P., & Kumar, R. (2013). Image steganography using SVD and wavelet difference reduction. International Journal of Computer Applications, 73(10), 15–19. DOI: 10.5120/12816-9905
7. Liu, F., & Liu, Y. (2014). An improved SVD-based watermarking scheme for protecting rightful ownership. Multimedia Tools and Applications, 72(3), 2331–2352. DOI: 10.1007/s11042-013-1469-9
8. Patel, H., & Tailor, H. (2016). A novel steganography method using discrete wavelet transform and singular value decomposition. International Journal of Computer Science and Network Security, 16(2), 77–83.
9. Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474–481. DOI: 10.1109/49.668971
10.] F. K. Zaidan, “Digital image steganography scheme based on DWT and SVD,” Diyala Journal of Engineering Sciences, vol. 13, no. 4, pp. 10–17, 2020
11. Y. Wang and H. Zhou, "An Improved SVD-Based Steganographic Algorithm for Medical Image Security," Journal of Information Security and Applications, 2021.
12. N. A. Ahmed et al., "Optimized Steganography Based on SVD and Genetic Algorithms," Multimedia Tools and Applications, 2022.