SIM (wykład 5)

# OCHRONA DANYCH MEDYCZNYCH: PODSTAWOWE MECHANIZMY I ZABEZPIECZENIA

*Wykorzystano materiały udostępnione przez Bartosza Boruckiego, Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego, Uniwersytet Warszawski*

# Prawa konstytucyjne (Konstytucja RP z 1997 roku)

(art. 47.)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

(art. 51.)

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

# Dane osobowe

Dane osobowe – informacje charakteryzujące osobę zidentyfikowaną lub pozwalające zidentyfikować daną osobę

(art. 6.)

1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów

*Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883), poprawki z roku 2001 – efekt wdrożenia dyrektywy UE 95/46/WE*

*(w skrócie UODO)*

# Które informacje mogą doprowadzić do identyfikacji osoby?

- Identyfikacja bezpośrednia – jednoznaczne zidentyfikowanie wprost danej osoby na podstawie posiadanych danych
  - przykładowo podanie imienia i nazwiska, adresu
  - ale też: wszystkie elementy dat bezpośrednio powiązanych z jednostką, włączając datę urodzenia, ewentualne daty przystąpienia/odstąpienia (organizacji, leczenia itp.), datę śmierci, oraz liczby określające wiek; numery telefonów i numery faksu; adresy poczty elektronicznej; numery ubezpieczeń społecznych; numery dokumentacji medycznych; numery kont bankowych; numery certyfikatów, licencji, uprawnień; numery identyfikacyjne pojazdów, włączając numery tablic rejestracyjnych; numery seryjne i identyfikacyjne urządzeń; sieciowe adresy URL lub IP; identyfikatory biometryczne, włączając odciski palców, zapis głosu, obrazy fotograficzne pełnej twarzy lub inne porównywalne obrazy
- Identyfikacja pośrednia – jednoznaczne zidentyfikowanie osoby na podstawie relacji wewnątrz wszystkich posiadanych danych lub z wykorzystaniem dodatkowych informacji zewnętrznych
  - na podstawie danych można wywnioskować tożsamość osoby,
  - trzeba więc zapewnić, by np. każdy rekord w zadanym zbiorze danych był nierozróżnialny od co najmniej jednego innego rekordu, a pola zawarte w danych nie powinny być dostępne publicznie w innych zestawach danych
- Dane obrazowe – spory problem

# Identyfikacja na podstawie danych obrazowych

- Zdjęcia
  - rozpoznawanie twarzy
  - porównywanie zdjęć
  - osoby publicznie znane
- Obrazowe dane medyczne
  - rekonstrukcja 3D głowy – twarzy na podstawie CT/MRI
  - widoczna cecha charakterystyczna
- Problem jest zauważalny, ale
  - mało klarownych metod
  - trudno osiągalna jednoznaczność
  - „nadmierne koszty lub działania”

# Ochrona danych osobowych

- Regulacje prawne dotyczące tworzenia i posługiwania się zbiorami danych osobowych, a także pojedynczymi danymi, mające na celu administracyjno-prawną ochronę prawa do prywatności
- Prywatność
  - to jest możliwość jednostki lub grupy osób do utrzymania swoich osobistych danych, zwyczajów, zachowań, preferencji jako nieujawnionych publicznie
  - prawo do uniknięcia niechcianych i/lub nieprzyjaznych ingerencji osób trzecich lub instytucji w sferę życia prywatnego
- Stopniowanie ryzyka
  - imię i nazwisko
    - PESEL, adres zamieszkania
      - dane ubezpieczeniowe, bankowe, ogólnie dostępowe ….
        - dane medyczne

# Dane wrażliwe

- Pojęcie danych wrażliwych
  - grupa szczególnie chronionych danych osobowych
- Dane wrażliwe dotyczą
  - pochodzenia rasowego lub etnicznego
  - poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej
  - **stanu zdrowia**, kodu genetycznego, nałogów lub życia seksualnego
  - skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

(art. 27.)

1. **Zabrania się przetwarzania** danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również **danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym** oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

*Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883), poprawki z roku 2001 – efekt wdrożenia dyrektywy UE 95/46/WE*

# Przetwarzanie informacji wrażliwych

Dopuszczalne jest gdy

- osoba, której dane dotyczą, wyrazi na to zgodę na piśmie
- inna ustawa zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony
- jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów
- dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą
- jest to niezbędne do prowadzenia badań naukowych, pod warunkiem anonimizacji danych

# Dokumentacja medyczna w ZOZ

Rozporządzenie Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania:

- par.52 ust.2 – Udostępnienie dokumentacji następuje w trybie zapewniającym zachowanie poufności i ochrony danych osobowych
- par.57 ust.2 – Dokumentację prowadzoną w postaci elektronicznej udostępnia się z zachowaniem jej integralności oraz ochrony danych osobowych
- par.60 – Dokumentację prowadzoną w postaci elektronicznej uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:
  - **zapewniona jest jej dostępność wyłącznie dla osób uprawnionych**
  - **jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem**
  - **są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana**

# Ochrona medycznych danych osobowych

- Sprzeczność celów
  - oczekiwania instytucjonalne – najszerszy możliwy dostęp do danych
  - oczekiwania indywidualne – minimalizacja rozprzestrzeniania się danych
- Konieczność zapewnienia ochrony z uwzględnieniem zachowania równowagi
  - które dane są identyfikujące?
  - jakie metody i mechanizmy?
- Przykład zabezpieczeń prawnych w USA:  PHI (Protected Health Information – chronione dane zdrowotne) – w ramach HIPAA, zawiera wszystkie dane medycznego rekordu pacjenta , płatności, dodatkowe usługi itp.
- HIPAA - Health Insurance Portability and Accountability Act of 1996
  - Uchwała kongresu Stanów Zjednoczonych 1996
  - Szczegółowa dokumentacja wyznaczająca reguły i zalecenia przetwarzania i udostępniania danych medycznych
  - The Privacy Rule – dokument uzupełniający HIPAA z 2002 roku, federalne prawo ochrony prywatności danych zdrowotnych

# Dane medyczne chronione według HIPAA

- Imię i nazwisko – włączając aktualne, wcześniejsze oraz panieńskie nazwisko matki
- Adres pocztowy – wraz ze wszystkimi geograficznymi regionami mniejszymi niż województwo, włączając powiat, miasto, dzielnicę, kod pocztowy i odpowiadające im kody geograficzne
- Wszystkie elementy dat (z wyłączeniem roku) dla dat bezpośrednio powiązanych z jednostką, włączając datę urodzenia, ewentualne daty przystąpienia/odstąpienia (organizacji, leczenia itp.), datę śmierci, oraz liczby określające wiek poniżej 89 lat wraz ze wszystkimi elementami dat (włączając rok), które mogą na taki wiek wskazywać, z wyłączeniem zbiorczej kategorii wiekowej „90 i powyżej”.
- Numery telefonów i numery faksu
- Adresy poczty elektronicznej (e-mail)
- Numery ubezpieczeń społecznych
- Numery dokumentacji medycznych
- Numery kont bankowych
- Numery certyfikatów, licencji, uprawnień
- Numery identyfikacyjne pojazdów, włączając numery tablic rejestracyjnych
- Numery seryjne i identyfikacyjne urządzeń
- Sieciowe adresy URL (Universal Resource Locator)
- Sieciowe adresy IP (Internet Protocol)
- Identyfikatory biometryczne, włączając odciski palców i głosu
- Obrazy fotograficzne pełnej twarzy lub inne porównywalne obrazy
- Inne unikalne numery identyfikacyjne, charakterystyki lub kody

# Medyczne dane osobowe a nauka

- Udostępnianie osobowych danych medycznych w celach naukowych jest zgodne z prawem

(*Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli) jest* to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone

- Jednostka naukowa
  - przetwarza dane osobowe
  - podlega UODO
  - musi zapewnić ochronę i bezpieczeństwo danych
- Zaleca się jednak postępowanie zgodne z HIPAA
  - zredukowanie danych tak aby nie były danymi osobowymi

# Bezpieczeństwo vs. poufność

Trzy elementy ryzyka

- Ryzyko utraty prywatności – ingerencja w życie prywatne pacjenta
- Ryzyko utraty bezpieczeństwa – nieautoryzowany dostęp do danych
- Ryzyko utraty poufności – nieautoryzowane udostępnienie danych

# Anonimizacja

- Znaczenie słowa „anonymous”
  - nienazwany lub niezidentyfikowany
  - nieznanego autorstwa lub pochodzenia
  - nie posiadający indywidualności, niewyróżniający się, nierozpoznawalny

- **Anonimizacja** danych to przekształcenie danych osobowych, po którym nie można ( w rozsądnym wymiarze czasowym) już przyporządkować poszczególnych informacji osobistych lub rzeczowych określonej lub możliwej do zidentyfikowania osobie fizycznej

- Podejście 1:  usuwanie informacji identyfikacyjnych
  - deidentyfikacja (*de-identification*)/depersonalizacja (*de-personalization*)
  - pseudonimizacja (*pseudonymization*)

- Podejście 2:  zapewnienie niejednoznaczności danych
  - uniejednoznacznianie (nadawanie niejednoznaczności, *ambiguation*)

# Anonimizacja - deidentyfikacja

- Deidentyfikacja to proces usuwania z danych informacji identyfikacyjnych
  - pola jawnie identyfikacyjne (lista)
  - informacje zawarte w polach opisowych – tekst dowolny – szczególnie w dokumentacji medycznej
- Proces deidentyfikacji
  - pola dobrze zdefiniowane można bezpośrednio usunąć
  - w polach dowolnych trzeba znaleźć
    - powtarzające się informacje z pól jawnie identyfikujących
    - inne dane identyfikacyjne (nazwiska, numery, itp.)
- Problem tekstów dowolnych
  - jakiego rodzaju informacji szukać?
  - jak szukać tych informacji?
  - zależność od języka
  - zależność od dziedziny

# Metody deidentyfikacji tekstów dowolnych

- Wyszukiwanie proste
  - wyszukiwanie informacji usuniętych z pól jawnie identyfikujących, wraz z odmianami (np. Nowak, Nowaka, Nowakowi,  Nowakiem …)
  - wyszukiwanie znaczników tożsamości (Dr, Pan, Pani, p., …)
  - wyszukiwanie informacji geograficznych (np. adresy)
  - wyszukiwanie numerów
- Wyszukiwanie odwrotne
  - klasyfikowanie poszczególnych słów jako odpowiednich części mowy i zdania
  - klasyfikowanie sensu poszczególnych terminów specjalistycznych
  - usuwanie pozostałych, niesklasyfikowanych informacji
  - słowniki
  - lingwistyka obliczeniowa
  - przetwarzanie języka naturalnego

# Anonimizacja – pseudonimizacja (kodowanie)

- Pseudonimizacja to proces zastępowania pól identyfikacyjnych pseudonimami
- Pseudonim może być generowany dla pojedynczego pola lub dla zestawu pól
- Najistotniejsze cechy pseudonimizacji
  - różne zestawy danych dotyczące zadanego pacjenta zawsze posiadają jednakowy pseudonim – możliwość grupowania danych pacjenta
  - dane identyfikacyjne są zastępowane pseudonimami (kodami), a zatem zestaw danych przestaje podlegać kategorii danych osobowych
- Zadania stawiane przed algorytmami pseudonimizacji
  - powtarzalność procesu – zawsze jednakowy pseudonim dla danego pacjenta
  - unikalność pseudonimów – wyjątkowy pseudonim dla każdego pacjenta
  - odporność na ataki słownikowe (*brute-force*)

# Metody pseudonimizacji

- Podział
  - pseudonimizacja odwracalna (dwukierunkowa)
  - pseudonimizacja nieodwracalna (jednokierunkowa)
- Metody
  - pseudonimy losowe
    - generacja unikalnego losowego kodu
    - skojarzenie „pacjent ↔ pseudonim” zapamiętywane w postaci listy mapującej
    - odwracalność za pośrednictwem listy
    - bezpieczeństwo – lista mapująca
  - symetryczne i niesymetryczne algorytmy szyfrujące
    - pseudonim generowany poprzez zaszyfrowanie danych identyfikujących
    - odwracalność poprzez deszyfrację
    - bezpieczeństwo – klucz szyfrujący
    - DES, AES, RSA, …
- Funkcje mieszania
    - pseudonim generowany w postaci nowego ciągu znaków
    - na bazie funkcji mieszającej
    - niemożliwe skojarzenie pseudonim → pacjent (algorytm nieodwracalny)
    - możliwe skojarzenie pacjent → pseudonim (ponowne zakodowanie)
    - SHA, MD5, …

# Anonimizacja – usuwanie jednoznaczności

- Przetworzenie danych w taki sposób, aby przy jednoczesnym zapewnieniu jak największej informatywności danych, uzyskać wystarczający poziom niejednoznaczności
- Klasyfikacja oceny stopnia niejednoznaczności
  - niejednoznaczność zadanego zestawu wartości cech na przestrzeni populacji (jak również w danym zestawie danych)
  - efekt dodania konkretnej wartości cechy do zadanego zestawu wartości cech
  - dostępność danej cechy na zewnątrz danych (tzn. potencjalny „koszt” wejścia w posiadanie wartości danej cechy)
- Pojęcie k-anonimowości
  - zestaw danych jest *k*-anonimowy, gdy każdy rekord w obrębie tych danych jest nierozróżnialny od co najmniej *k*-1 innych rekordów

# Usuwanie jednoznaczności - przykłady

- usunięcie nazwisk

| Nazwisko | Adres | Wiek | Diagnoza |
|---|---|---|---|
| *** | Warszawa | 26 | Zapalenie płuc |
| *** | Kraków | 42 | Nadciśnienie |
| *** | Zakopane | 47 | Cukrzyca |
| *** | Radom | 28 | Astma |

- grupowanie (na polach adres i wiek)
  - adres jest zastępowany wyższą jednostką administracyjną
  - wiek określony przedziałem

| Nazwisko | Adres | Wiek | Diagnoza |
|---|---|---|---|
| *** | woj. Mazowieckie | 20-29 | Zapalenie płuc |
| *** | woj. Małopolskie | 40-49 | Nadciśnienie |
| *** | woj. Małopolskie | 40-49 | Cukrzyca |
| *** | woj. Mazowieckie | 20-29 | Astma |

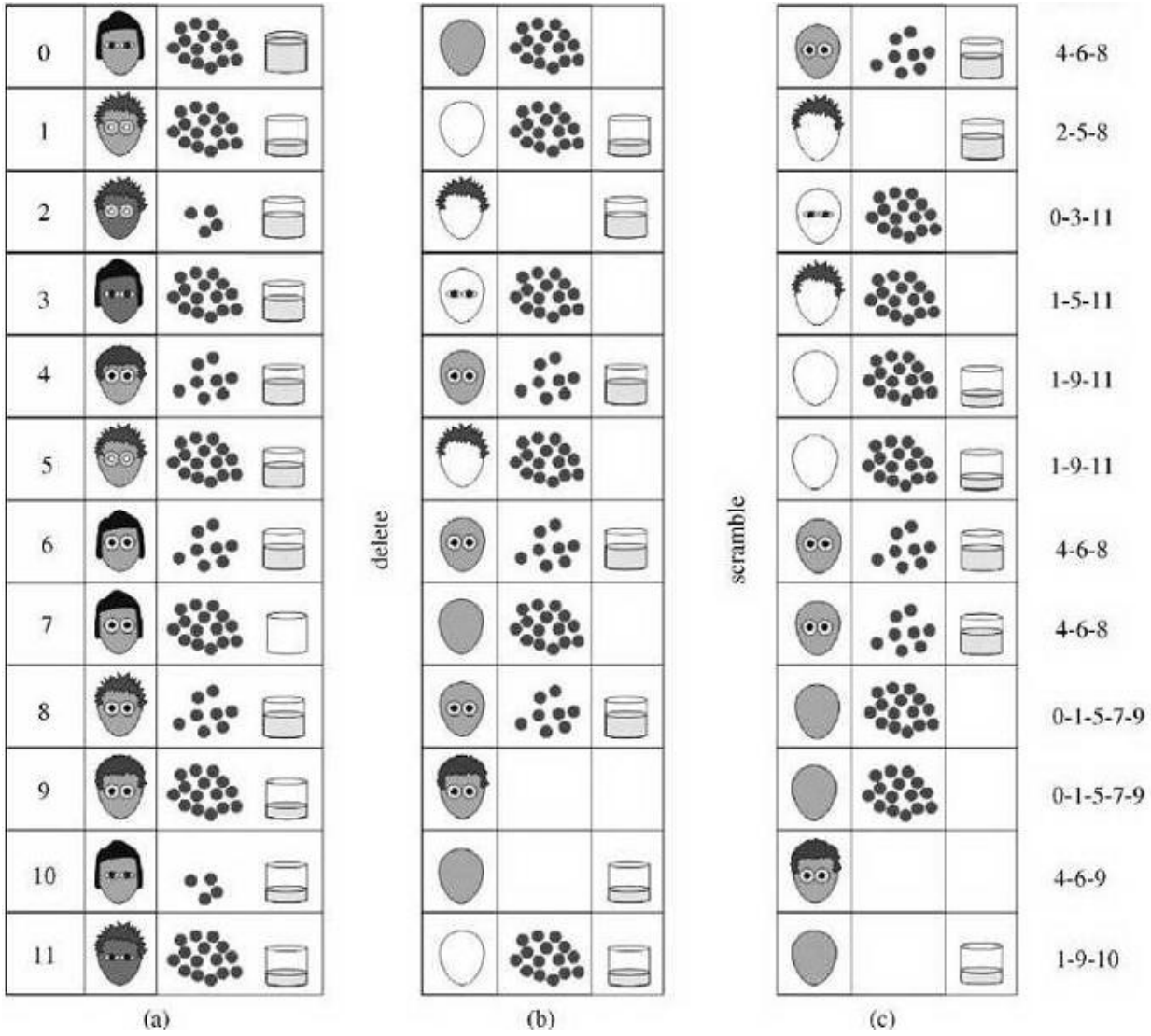
poziom 2-anonimowości

# Usuwanie części informacji

(a) początkowa baza danych z 5 cechami: włosy, kolor oczu, kolor skóry, wynik badania hemoglobiny, wynik badania moczu

(b) baza niejednoznaczna o poziomie 3-anonimowości

(c) losowe przemieszanie rekordów; liczby wskazują początkowe rekordy do których pasuje zanonimizowany rekord




*L.Ohno-Machado, P.Silveira, S.Vinterbo, „Protecting patient privacy by quantifiable control of discosures in disseminated databases", Int. J. of Med. Informatics 73 (2004)*

# Digital Imaging and Communication In Medicine (DICOM) - anonimizacja

- Standard opracowany przez American College of Radiology oraz National Electrical Manufacturers Association
- Nagłówek
  - grupy
  - elementy
  - np. (0010,0030) – grupa 0010 to dane osobowe pacjenta, element 0030 to data urodzenia pacjenta
- Dane obrazowe
  - binarne dane obrazowe zależne od urządzenia diagnostycznego
  - dodatkowe obrazy (np. zrzuty ekranu)

# Anonimizacja w DICOM (cel naukowy)

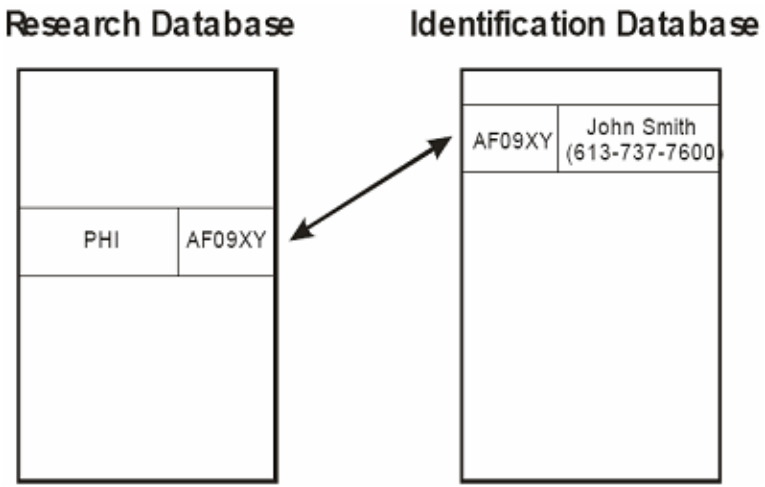
- Standard podaje zalecenia które znaczniki powinny podlegać procesowi deidentyfikacji – suplement nr 55.
- W zależności od zastosowania pola podane w standardzie mogą być niewystarczające
- Zalecana procedura postępowania (R.Noumeir, A.Lemay, (2007) Pseudonymization of radiology data for research purposes, J Dig Im 20(3), 2007)
  - atrybuty prywatne mogą zostać skasowane, gdyż wykorzystywane są jedynie przez sprzęt diagnostyczny, na którym powstały dane
  - atrybuty powiązane z instytucją, technikami i lekarzami mogą zostać usunięte, gdyż przeważnie nie są wymagane do celów innych niż wewnętrzne
  - opis badania, opis serii oraz informacje o protokole muszą pozostać, gdyż zawierają istotne informacje np. do przetwarzania obrazów
  - historia i komentarze pacjenta powinny zostać wyczyszczone, gdyż jako pola wolego tekstu mogą zawierać informacje identyfikacyjne, natomiast ich znaczenie naukowe jest niewielkie
  - wszystkie unikalne identyfikatory (UID) powinno się zastąpić pseudonimami – nowymi unikalnymi identyfikatorami; formaty poszczególnych identyfikatorów są opisane w standardzie DICOM
  - identyfikator badania oraz numer dostępu (*accession number*) powinny zostać usunięte
  - imię i nazwisko pacjenta, godzina urodzenia, inne identyfikatory pacjenta, inne nazwy pacjenta, MRL (*medical record locator*), grupa etniczna oraz zawód są usuwane
  - data urodzenia jest uniejednoznaczniana poprzez usunięcie dnia urodzenia
  - waga pacjenta, płeć oraz wzrost są zachowywane lub również uniejednoznaczniane, gdyż mogą być kluczowe dla algorytmów przetwarzania
  - identyfikator pacjenta jest zastępowany pseudonimem

# Systemy bezpieczeństwa

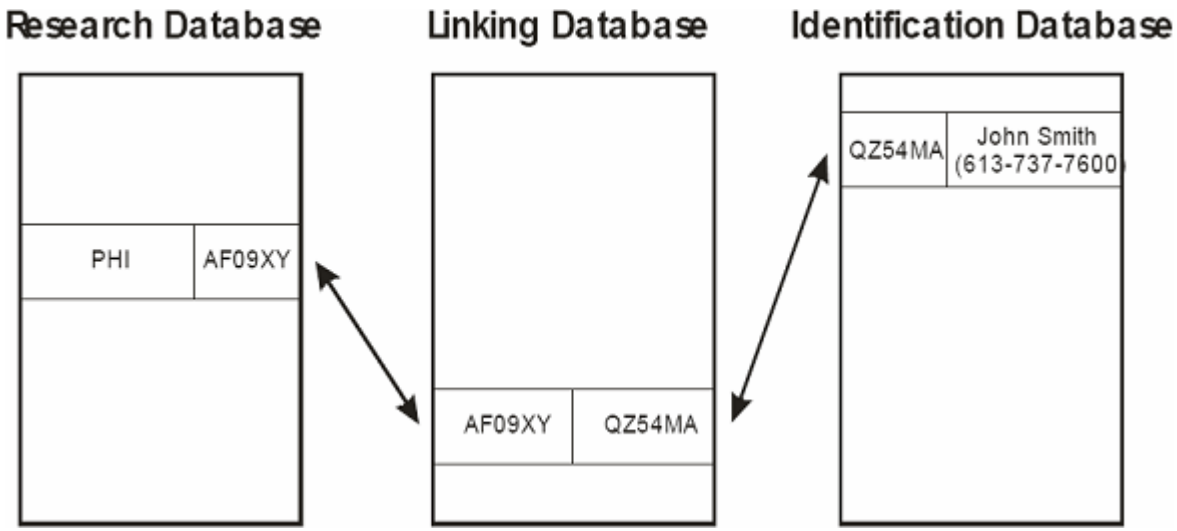
- Poszczególne metody anonimizacji stosuje się głównie w celu udostępniania danych
- W systemach medycznych (przechowujących i przetwarzających dane medyczne) bazuje się na połączeniu wielu metod w celu zwiększenia poziomu bezpieczeństwa
- Model separacji (najczęściej stosowany)
  - Dane są poddawane procesowi depersonalizacji – dane identyfikujące są oddzielane od pozostałych danych
  - Oba zestawy danych przechowywane są osobno (również fizycznie)
  - Skojarzenie danych identyfikujących z resztą danych realizowane za pośrednictwem pseudonimizacji
  - Część identyfikacyjna danych jest rzadziej potrzebna i może być obwarowana silniejszymi zabezpieczeniami
  - Część anonimowych danych może być udostępniana

# Przykład separacji i pseudonimizacji

- Jednowarstwowej



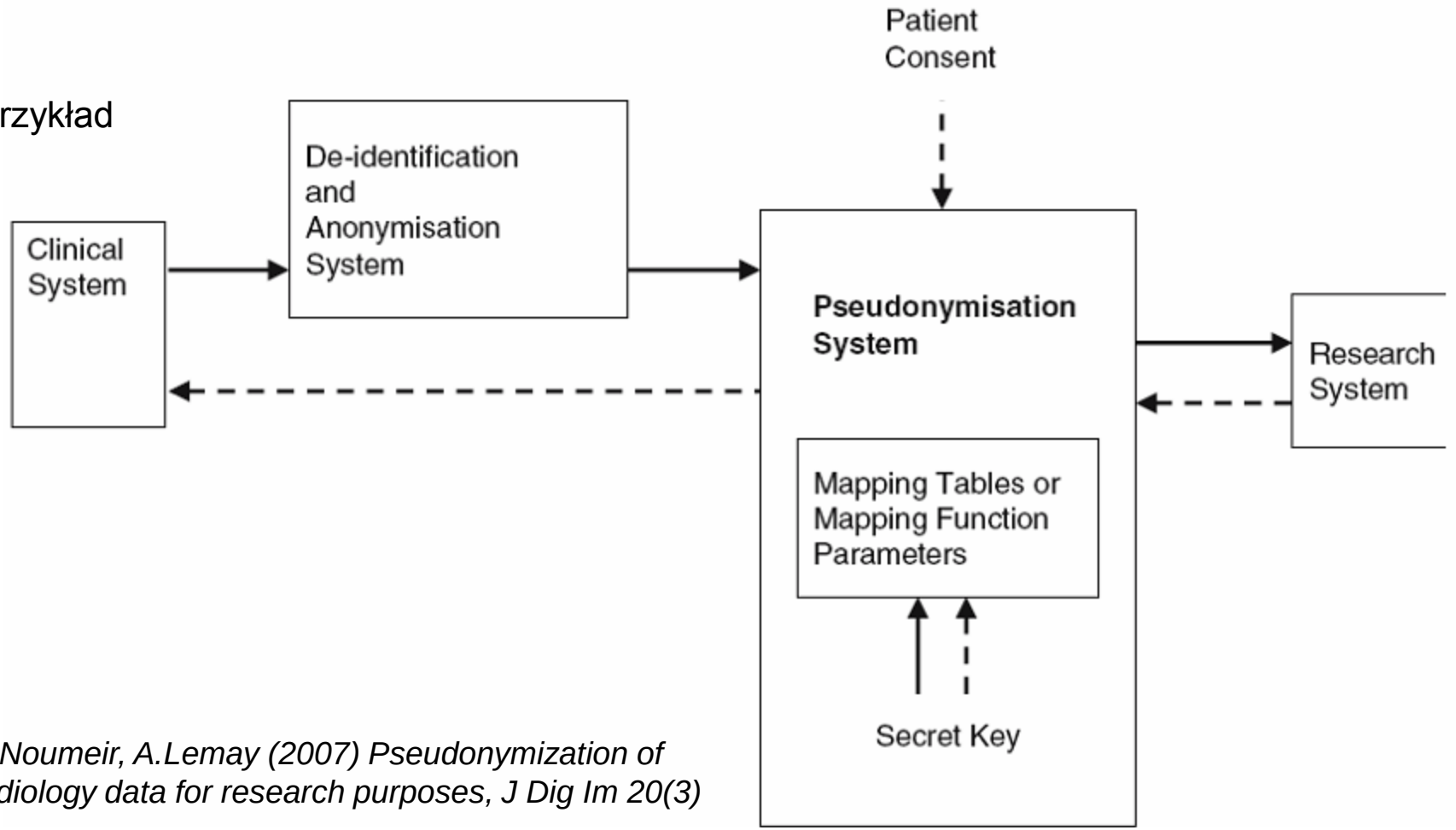

- Dwuwarstwowej



# Systemy złożone

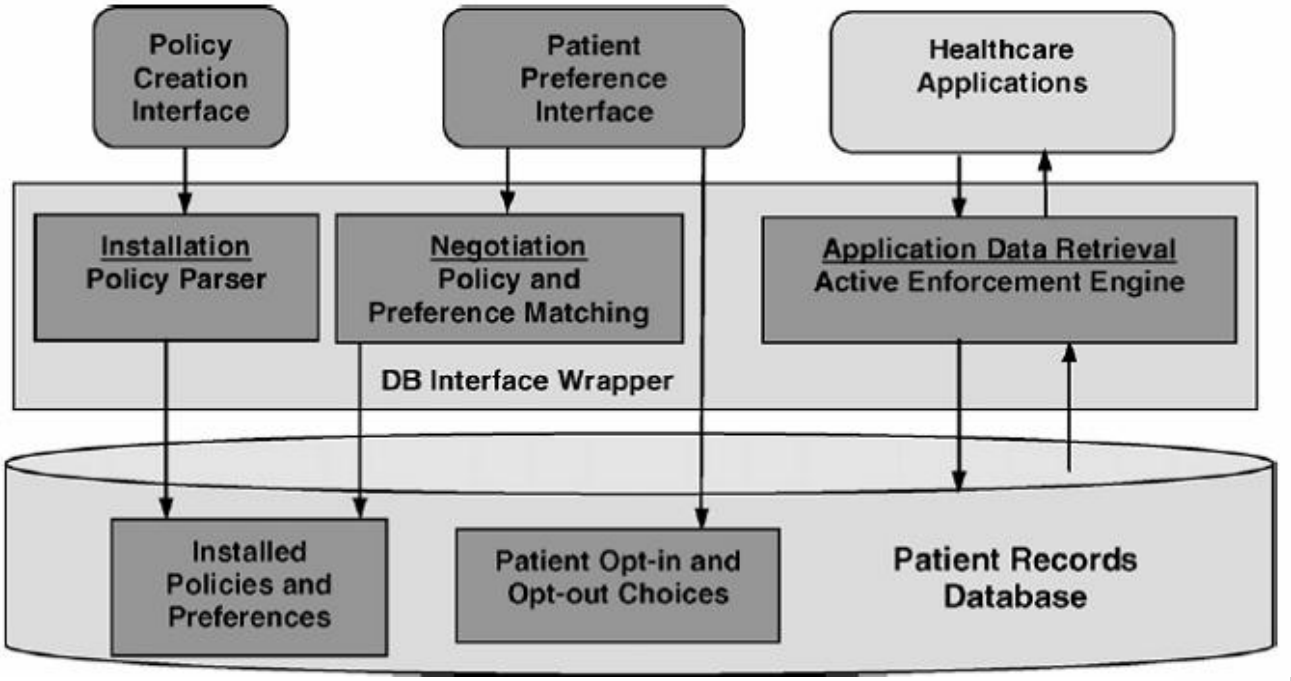
Jednoczesne stosowanie wielu metod (deidentyfikacja + pseudonimizacja +uniejednoznacznianie)

przykład

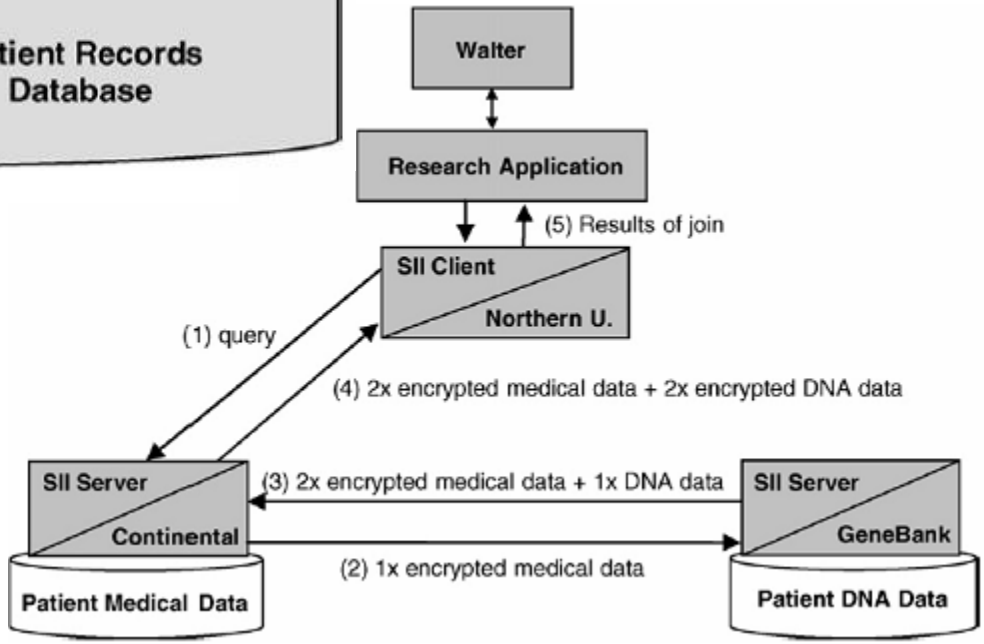



*R.Noumeir, A.Lemay (2007) Pseudonymization of radiology data for research purposes, J Dig Im 20(3)*

# Przykład systemu złożonego



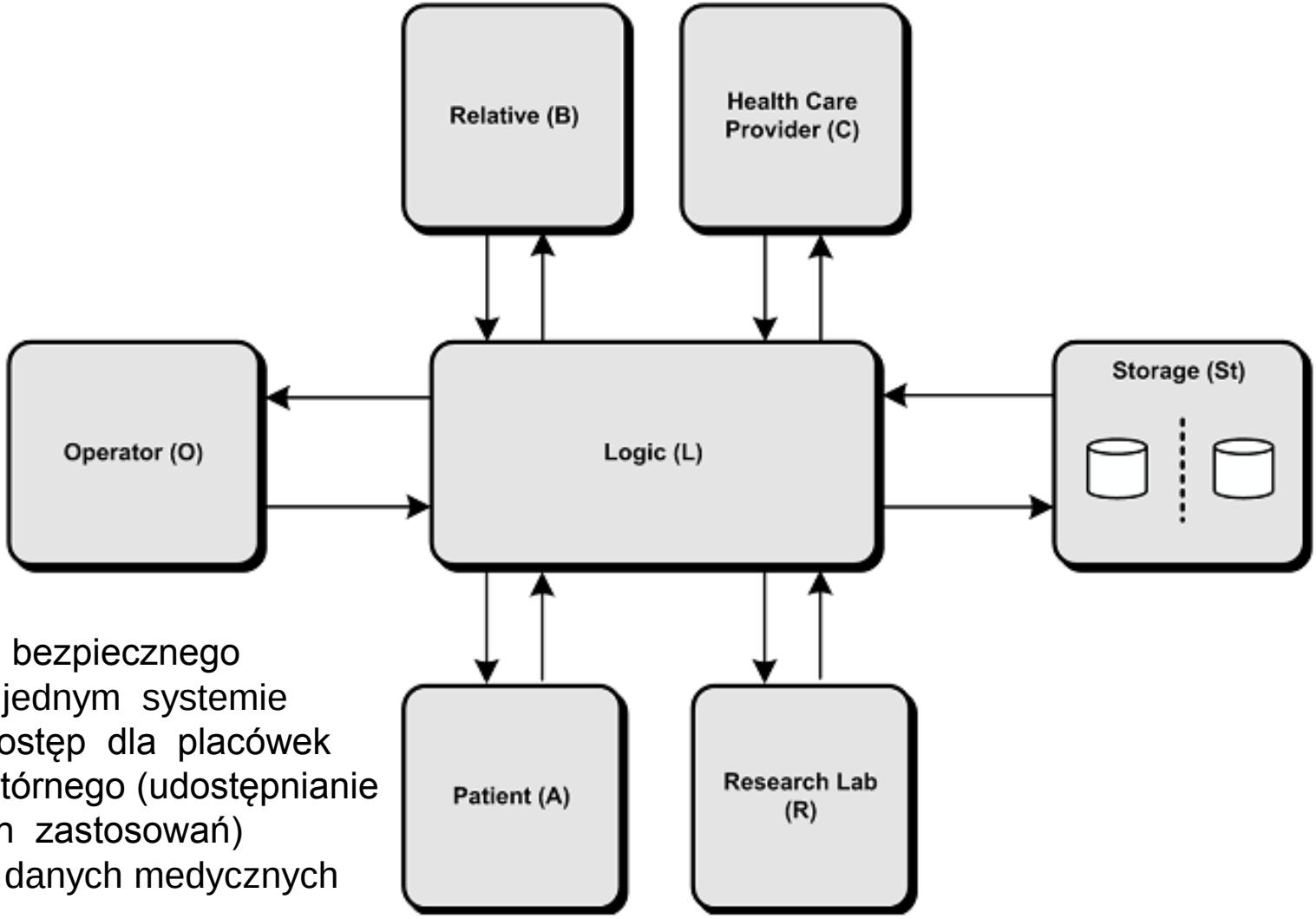

Architektura systemu




Integracja informacji chronionej

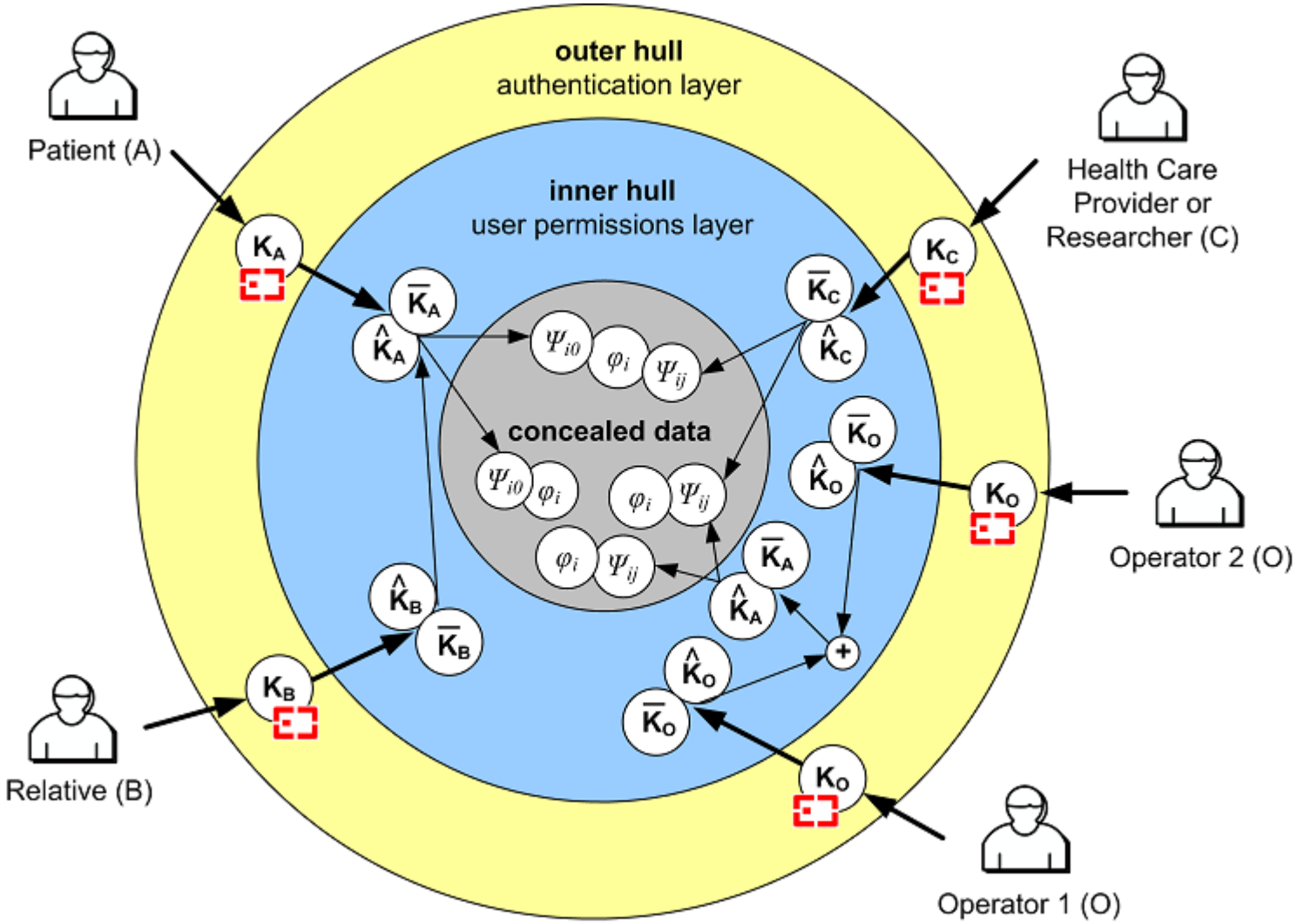
*R.Agrawal, C.Johnson (2007) Securing electronic health records without impending the flow of information, Int J Med Inf 76*

# Schemat budowy systemu PIPE (*Pseudonymization of Information for Privacy in e-Health*)



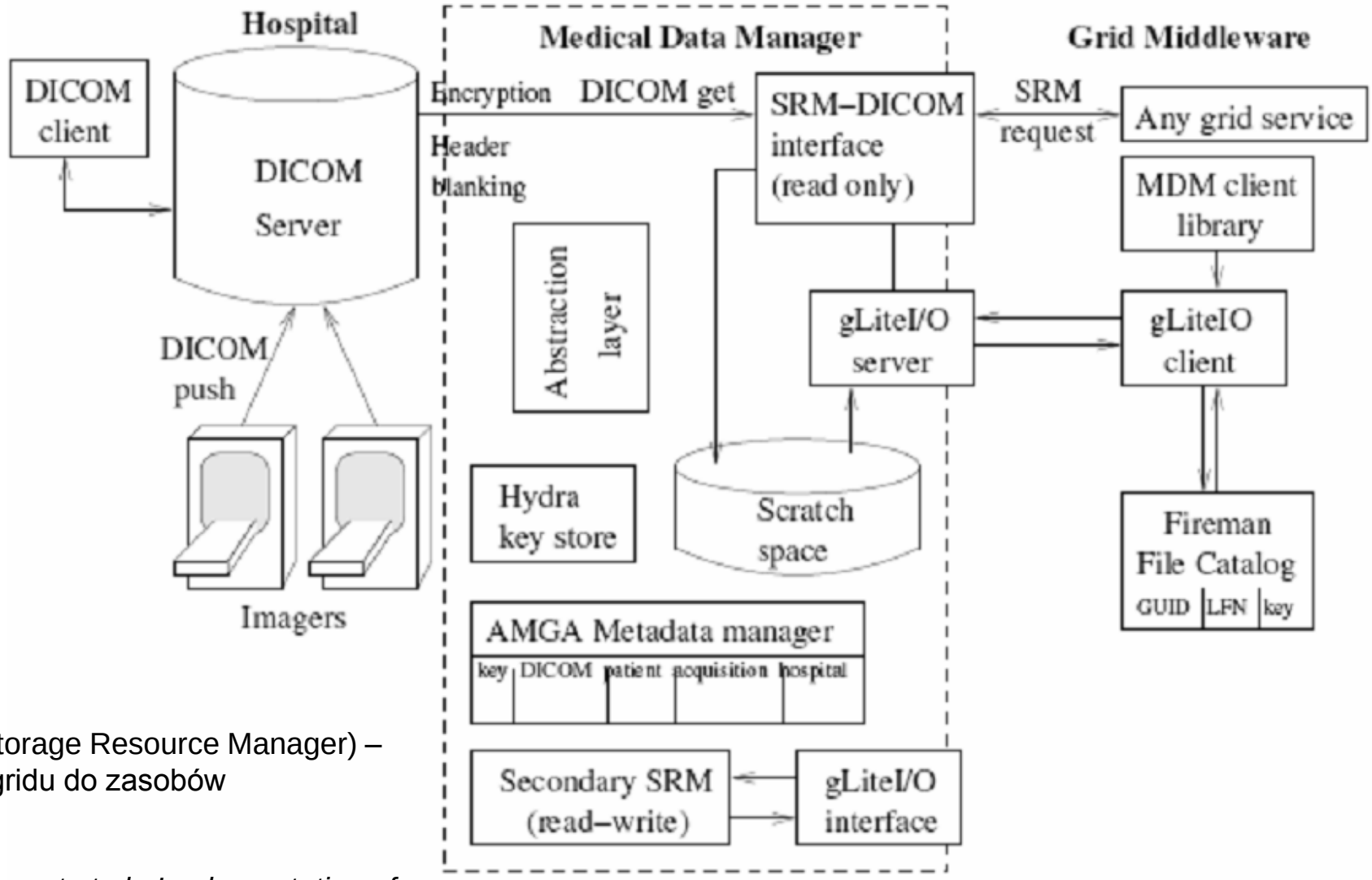

Daje możliwością bezpiecznego zintegrowania w jednym systemie podstawowego (dostęp dla placówek medycznych) i wtórnego (udostępnianie danych do innych zastosowań) wykorzystywania danych medycznych

# Architektura warstw bezpieczeństwa systemu PIPE




warstwowa polityka bezpieczeństwa

# Przykład: struktura usługi Medical Data Manager - system zarządzania danymi medycznymi z wykorzystaniem infrastruktury gridowej

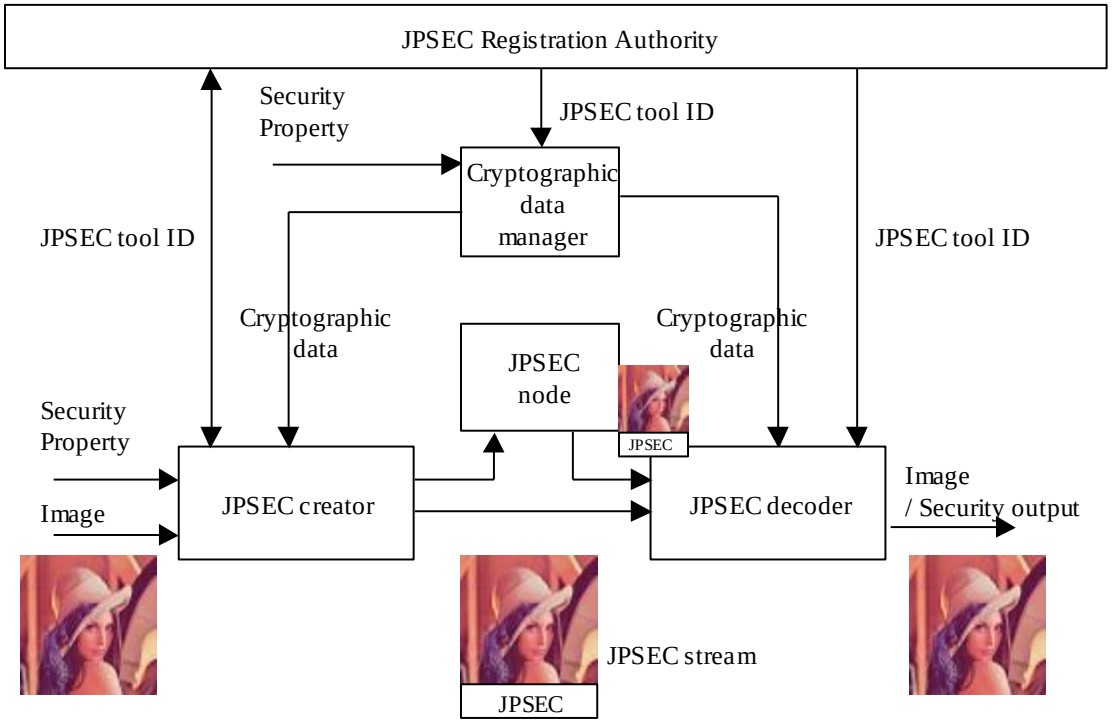


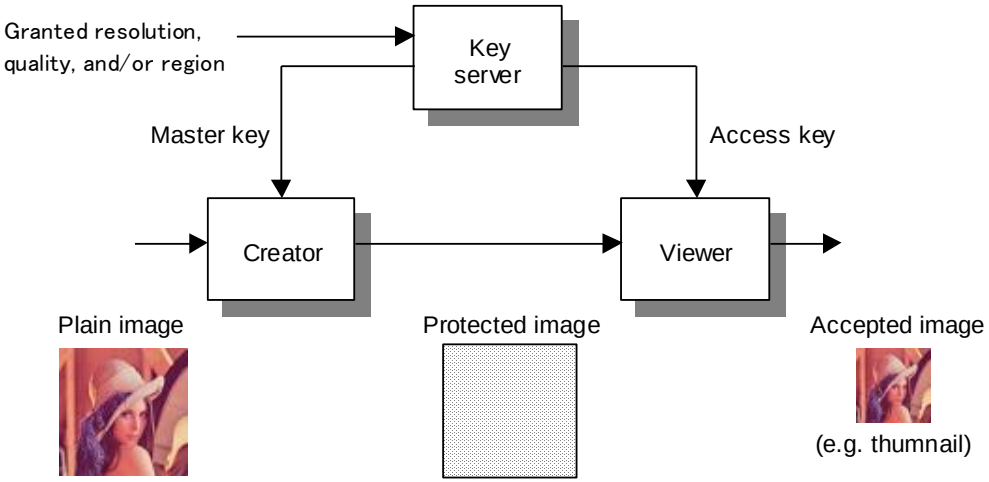

*SRM* (Storage Resource Manager) – dostęp gridu do zasobów

*J. Montagnat et al., Implementation of a Medical Data Manager on top of gLite services, EGEE Technical Report, EGEE-TR-2006-002, 2006*

# SCHEMATY ZABEZPIECZEŃ W STANDARDZIE JPEG (JPEGSEC)

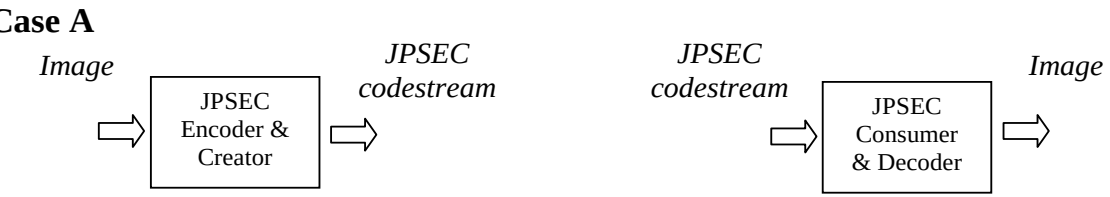
# JPSEC (*security aspects)* – schemat rozwiązań

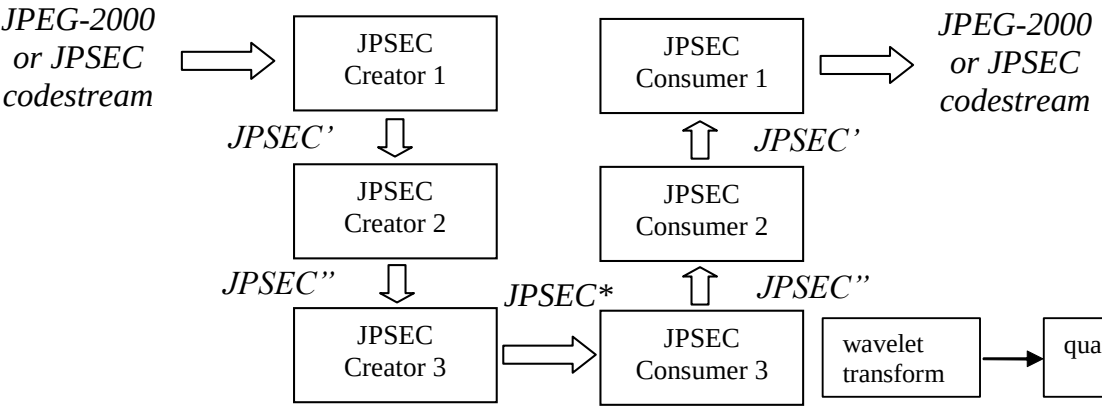



*dokumentacja standardu*

# JPSEC

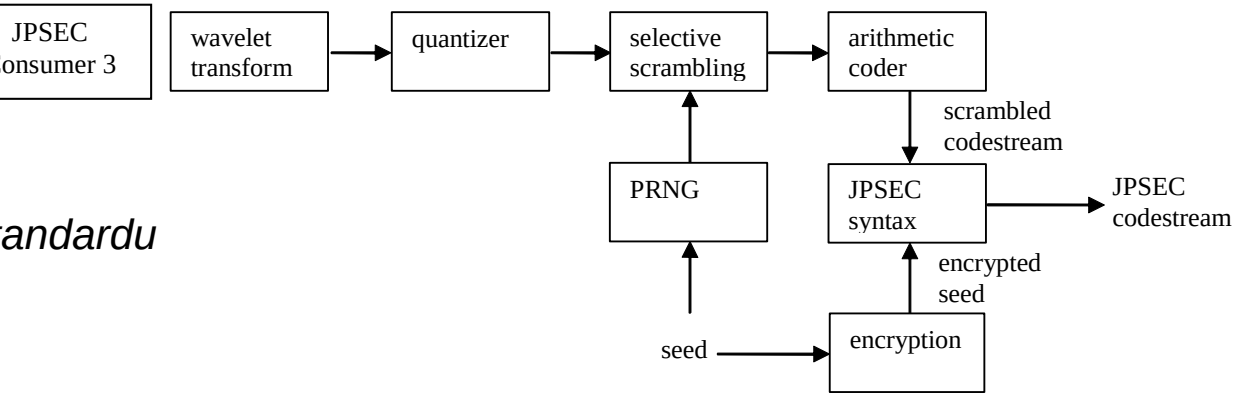



Formy:

- Podpis cyfrowy
- Znaki wodne
- Kryptografia, szyfrowanie
- Generacja kluczy i zarządzanie kluczami
- Identyfikacja i rejestracja

*dokumentacja standardu*




*Schemat szyfrowania w dziedzinie falkowej*

# Wymagania stawiane steganografii

- Percepcja - niedostrzeganie modyfikacji stego-nośnika przez typowego odbiorcę; wykorzystuje się tu głównie właściwości ludzkiego systemu widzenia (efekt maskowania, ograniczonej czułości, itp.)
- Pojemność - zdolność upakowania możliwie dużej ilości sekretnej informacji; często wymagane jest przesłanie dużej ilości tajnych danych, zatem tym więcej bitów uda się konspiracyjnie osadzić, tym lepszy jest system steganograficzny
- Bezpieczeństwo - wbudowane informację nie powinny być wykrywalne; głównym zadaniem metod steganograficznych jest utajnienie samej transmisji - po jej wykryciu, za pomocą technik stegoanalizy będzie można wyodrębnić wiadomość
- Odporność - osadzona informacja powinna być wytrzymała na różnego typu przekształcenia niszczące, sprawdzające itp.; w razie wykrycia tajnej wiadomości przez osobę niepowołaną, powinna być chroniona przed modyfikacją, czy też usunięciem; osoba atakująca może znać metody osadzania sekretnych danych dążąc do jej odczytania, zniszczenia, przekłamania

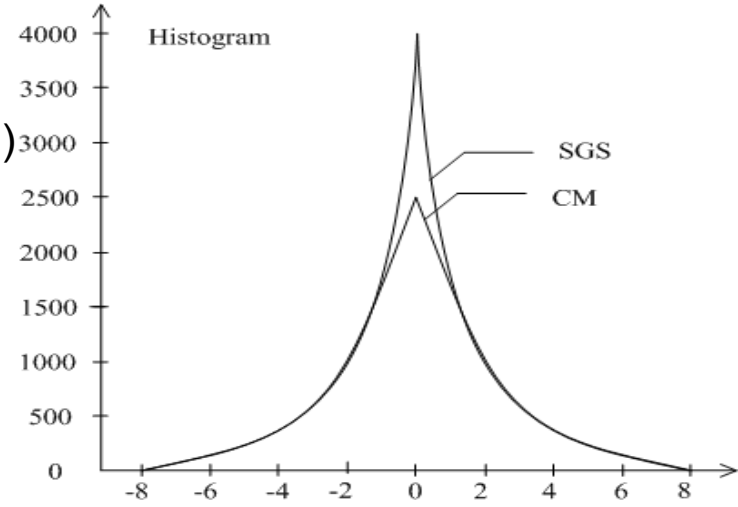
Wymagania są czasami sprzeczne lub też wzajemnie się uzupełniają

# Charakterystyka steganografii

- Nośniki ukrytej informacji:
  - Obrazy, wideo, dźwięk, zapis mowy, sygnały pomiarowe (np. EEG, EKG), teksty, dokumenty, protokoły internetowe, kody źródłowe
- Formy ukrytej informacji:
  - teksty, obraz, mowa
- Zwykle ukrywane informacje są szyfrowane
- Rodzaje
  - Ze znanym nośnikiem i bez znanego nośnika w dekoderze
  - Z istotnym lub nieistotnym nośnikiem
- Reguła
  - Znaleźć komponenty szumowe nośnika i zastąpić je zaszyfrowaną informacją ukrytą
  - Wykorzystać nieistotne komponenty nośnika

# Podstawy

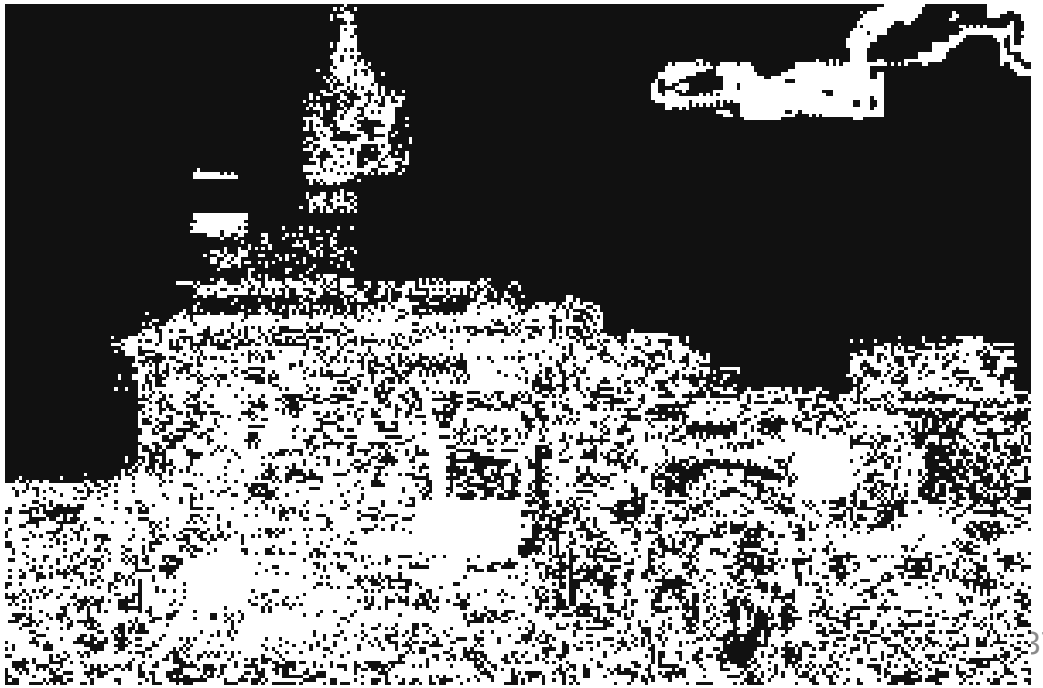
- Historia Herodota: ściąć włosy niewolnika, zrobić tatuaż z sekretną wiadomością, odczekać aż urosną włosy, wysłać niewolnika do obcego kraju, do własnego agenta, który zetnie włosy niewolnikowi i odczyta wiadomość
- Najmłodszego bitu LSB
  - Zapis ukrytej informacji na najmłodszych bitach wybieranych według ustalonego porządku pikseli
  - Stosunkowo duża pojemność, łatwa implementacja, niedostrzegalna zmiana nośnika, ale mała odporność na przetwarzanie, stegoanalizę czy aplikacje zabezpieczające
- Metody bitowo-segmentacyjne
  - BCPS (Bit Plane Complexity Segmentation) – dzielimy obraz na mapy bitowe i ukrywamy informację w obszarach odpowiednio ‘zaszumionych’, co nie wpływa na percepcję treści obrazowych
- Metody transformacyjne
  - Zmiana LSB współczynników DCT (na bazie JPEG)
- Metody lingwistyczne, graficzne, internetowe (nośnik)



# Obraz źródłowy

Foundations of Information Hiding
prof. dr Valery Korzhik

# Obraz po binaryzacji

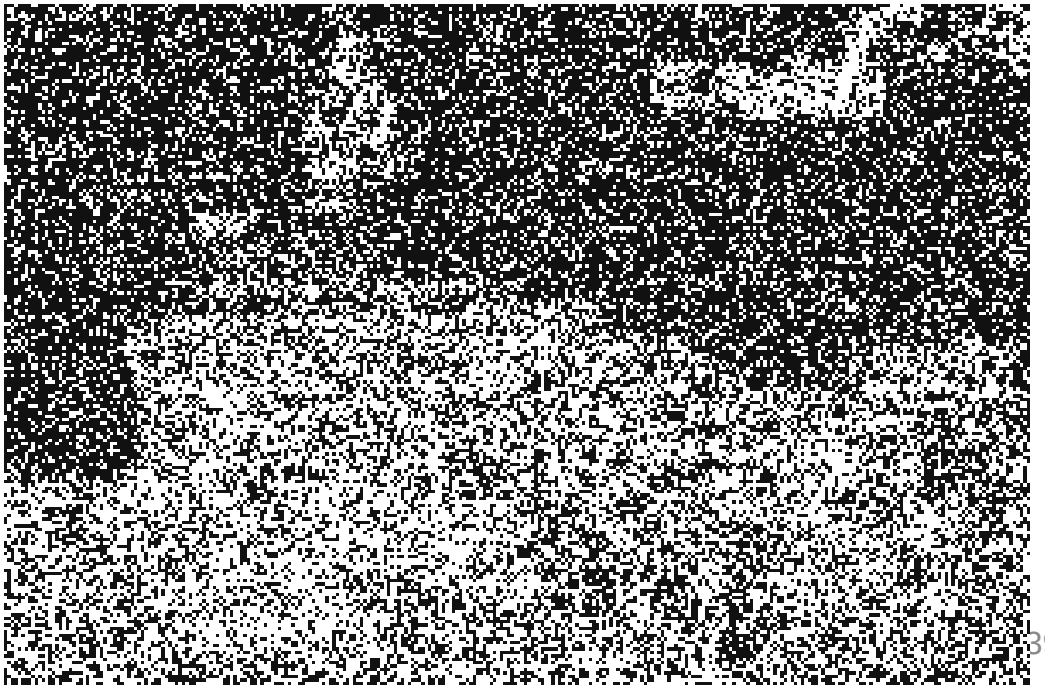


Obraz źródłowy z 5% wkładem ukrytej informacji

Obraz po binaryzacji

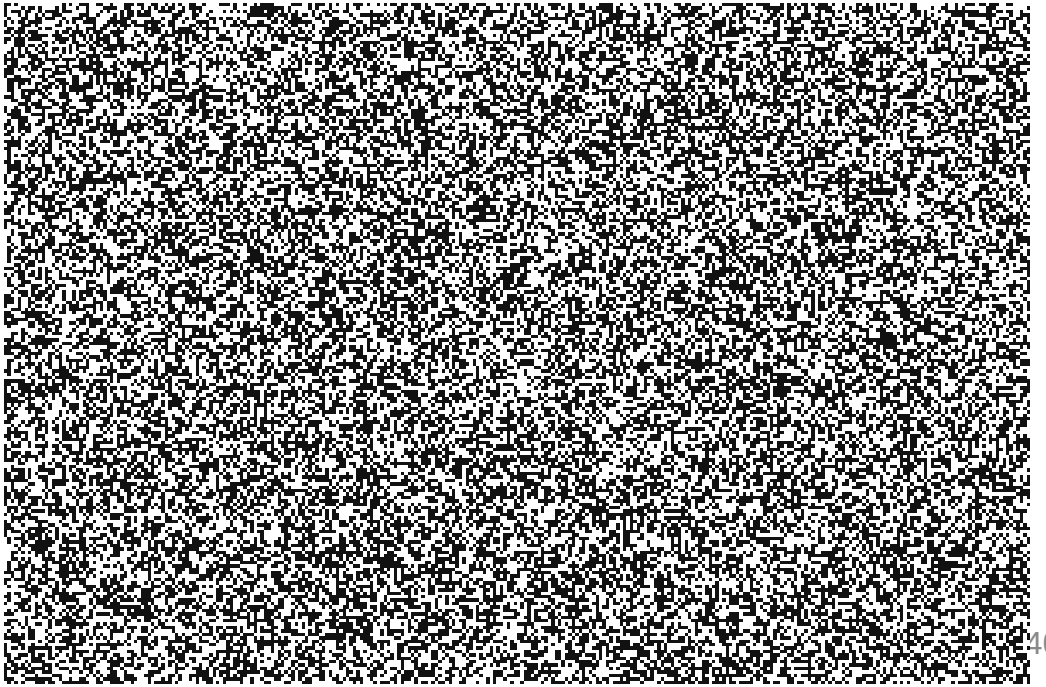
Obraz źródłowy z 50% wkładem ukrytej informacji

Obraz po binaryzacji

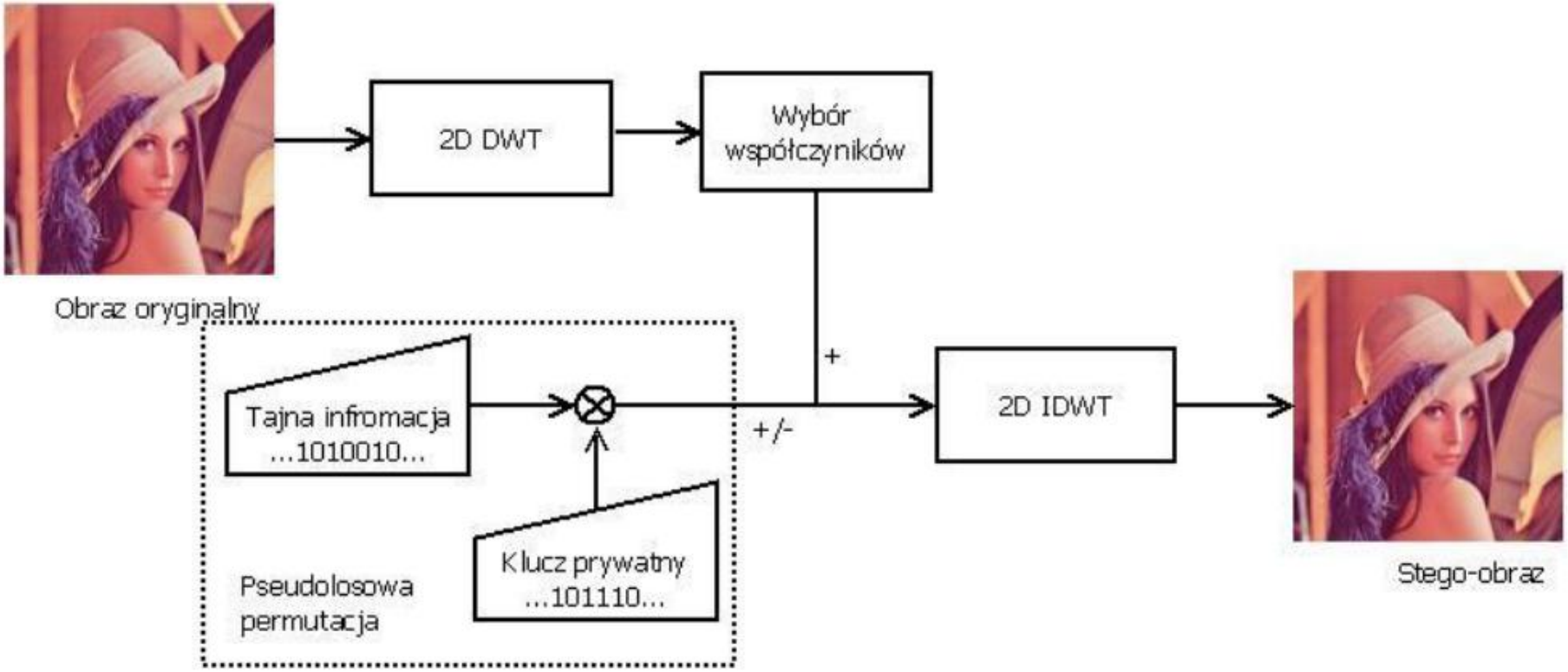


Obraz źródłowy ze 100% wkładem ukrytej informacji

Obraz po binaryzacji



# Osadzanie tajnej wiadomości za pomocą modyfikacji współczynników DWT




*ukrywanie*

$$I_m(x) = I(x) - \alpha \quad ,dla \quad m(x) = 0$$
$$I_m(x) = I(x) + \alpha \quad ,dla \quad m(x) = 1$$

*ekstrakcja*

$$m'(x) = 0 \quad ,dla \quad I_m(x) - I(x) < 0$$
$$m'(x) = 1 \quad ,dla \quad I_m(x) - I(x) \geq 0$$

$I(x)$ - wartość współczynnika dyskretnej transformaty falkowej (DWT)

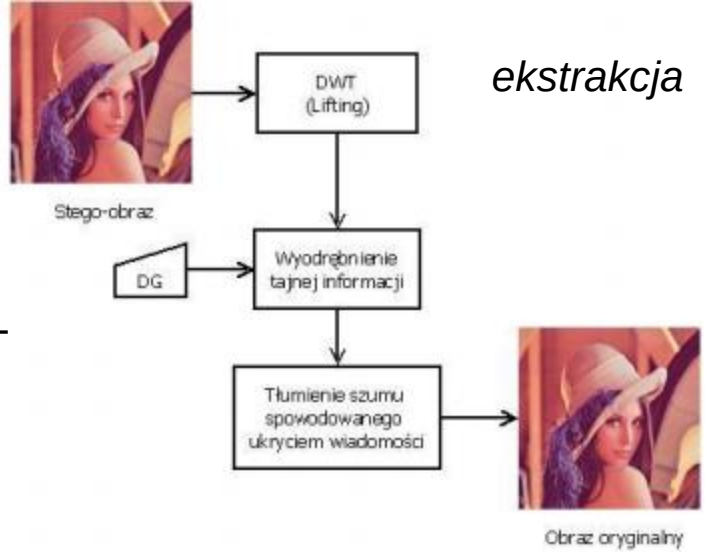
$I_m(x)$ - **zmodyfikowana** wartość współczynnika dyskretnej transformaty falkowej (DWT)

$\alpha$ - ustalona wartość rzeczywista >0, $m(x)$ – osadzany bit sekretnej informacji

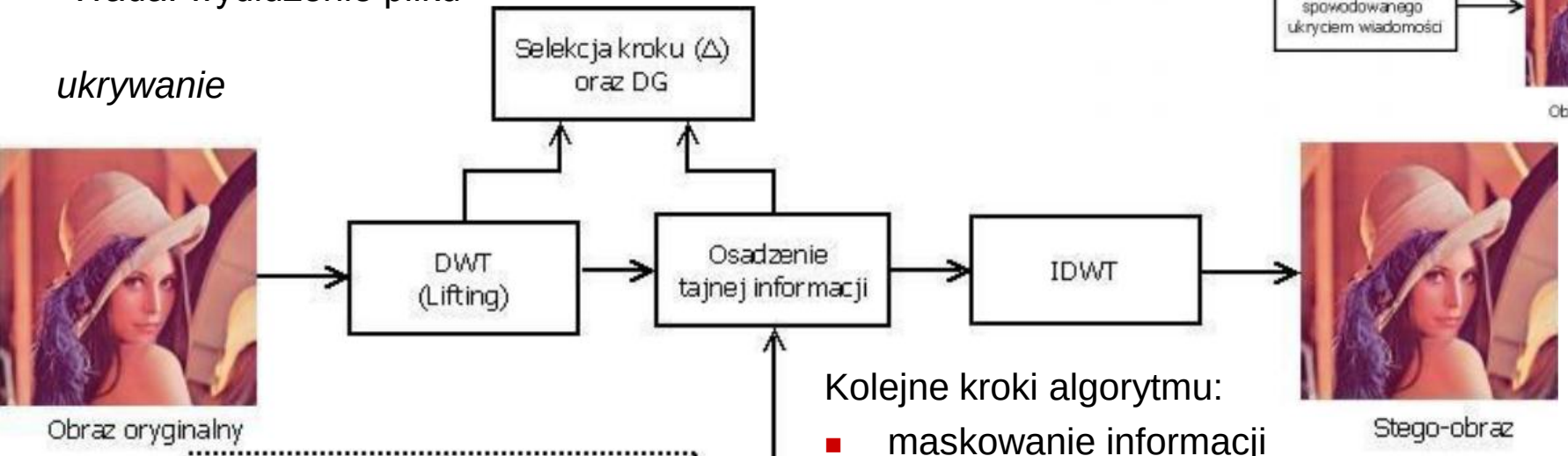
# Osadzenie tajnej informacji za mocą metody QIM-DG

QIM - quantization index modulation
Zaleta: zachować histogram kwantow. współczynników DWT
Wada: wydłużenie pliku

*ekstrakcja*



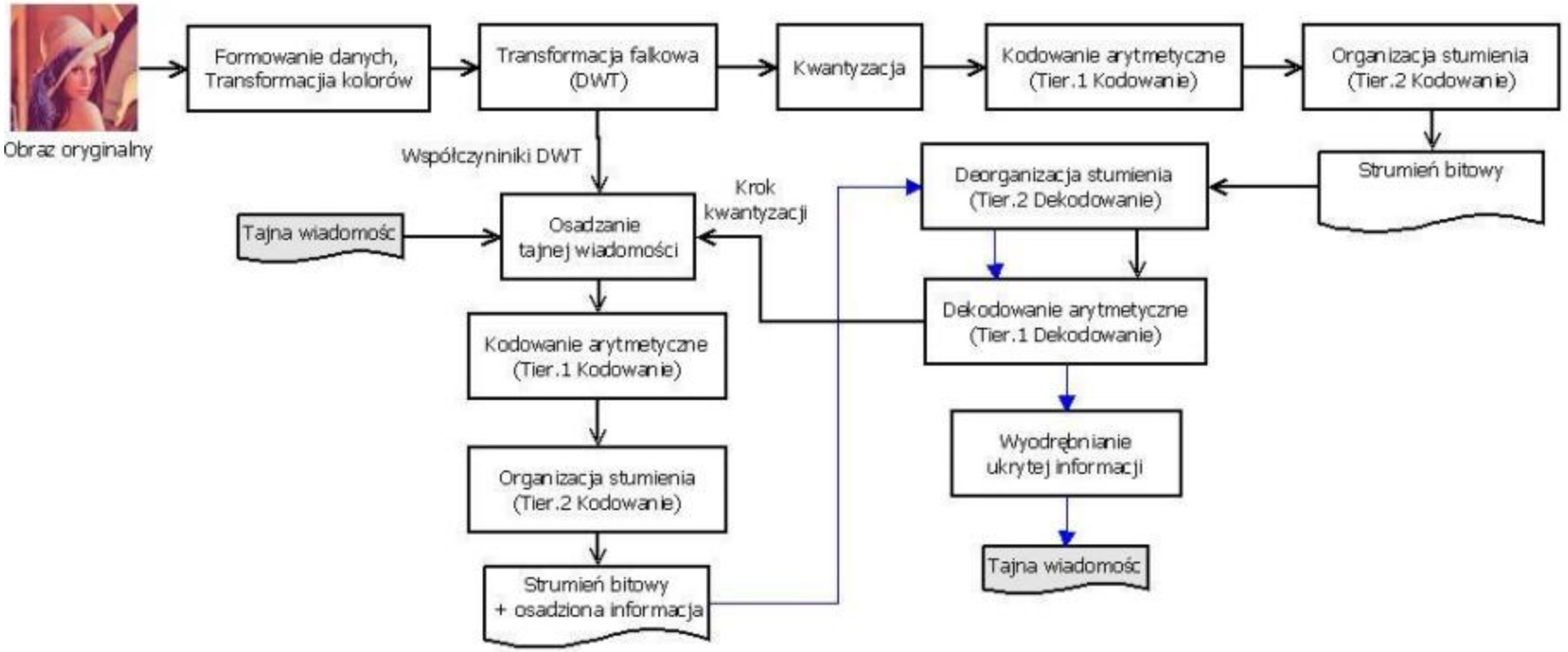

*ukrywanie*




Kolejne kroki algorytmu:

- maskowanie informacji
- transformacja obrazu
- kryteria wyboru współczynników dla jednego bitu danych
- dobieranie kategorii współczynnikom
- selekcja kroku kwantyzacji wybranego dla QIM
- przeprowadzenie binarnego zamaskowania w podpasmach
- ukrycie zamaskowanej informacji

# Metoda QIM-JPEG2000




Schemat procesu ukrywania informacji oraz ich ekstrakcji

Linie czarne oraz niebieskie różnicują odpowiednio procedury osadzania i ekstrakcji

# Osadzenie informacji na etapie kodowania płaszczyzn bitowych według JPEG2000

Obraz oryginalny

Transformacja falkowa (DWT)

Kwantyzacja

Kodowanie płaszczyzn bitowych

Optymalizacja zniekształceń

Określenie punktów służących do osadzenia informacji, określenie ich intensywności

Osadzanie tajnej wiadomości

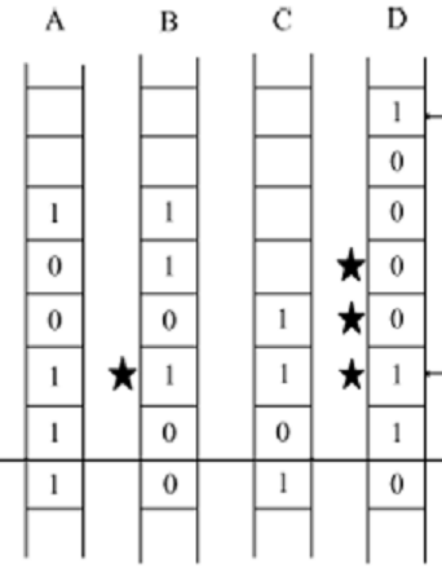
Tajna wiadomosc

Klucz prywatny

Drugie kodowanie płaszczyzn bitowych

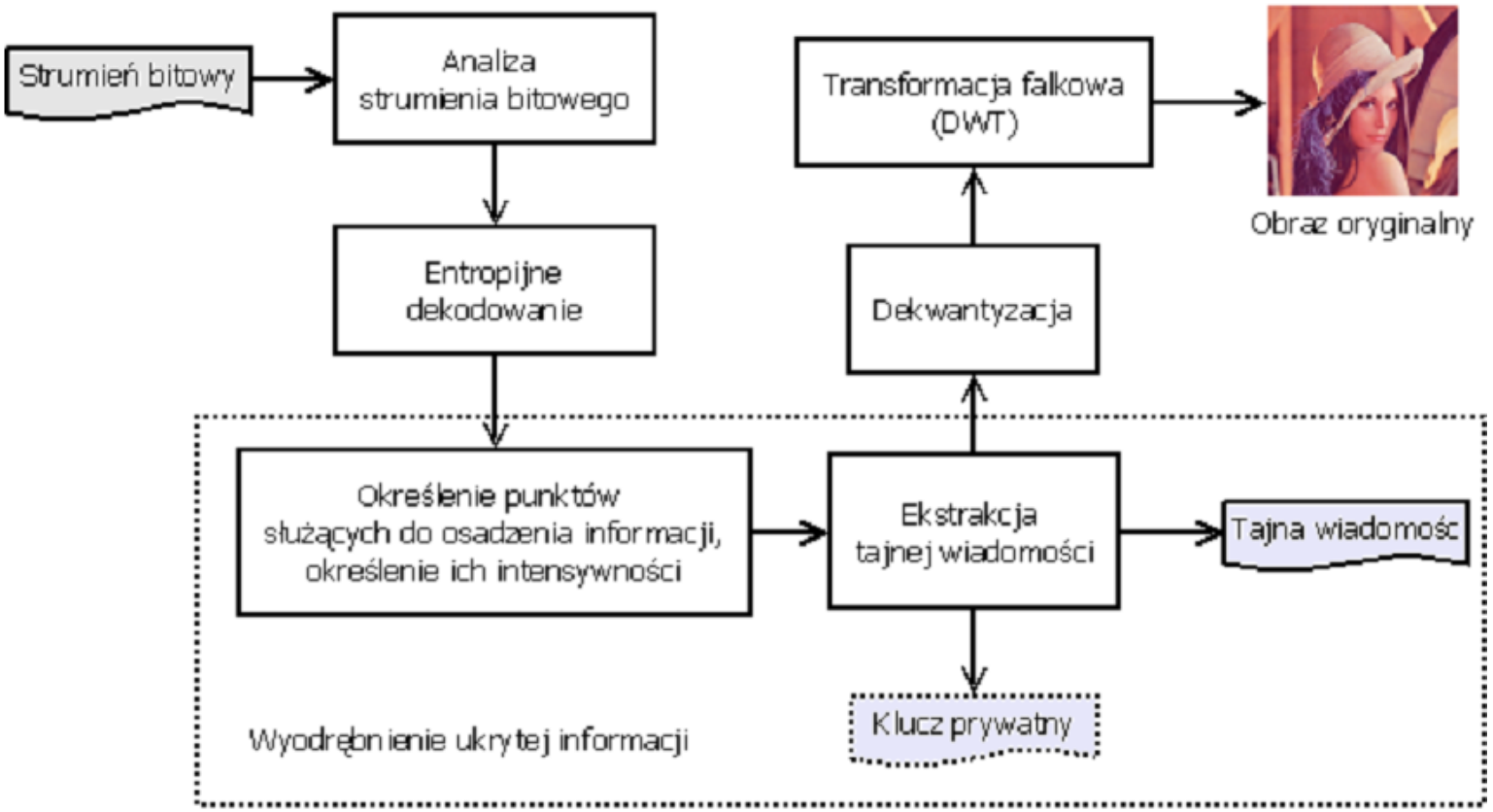
Strumień bitowy

Ukrycie sekretnej informacji



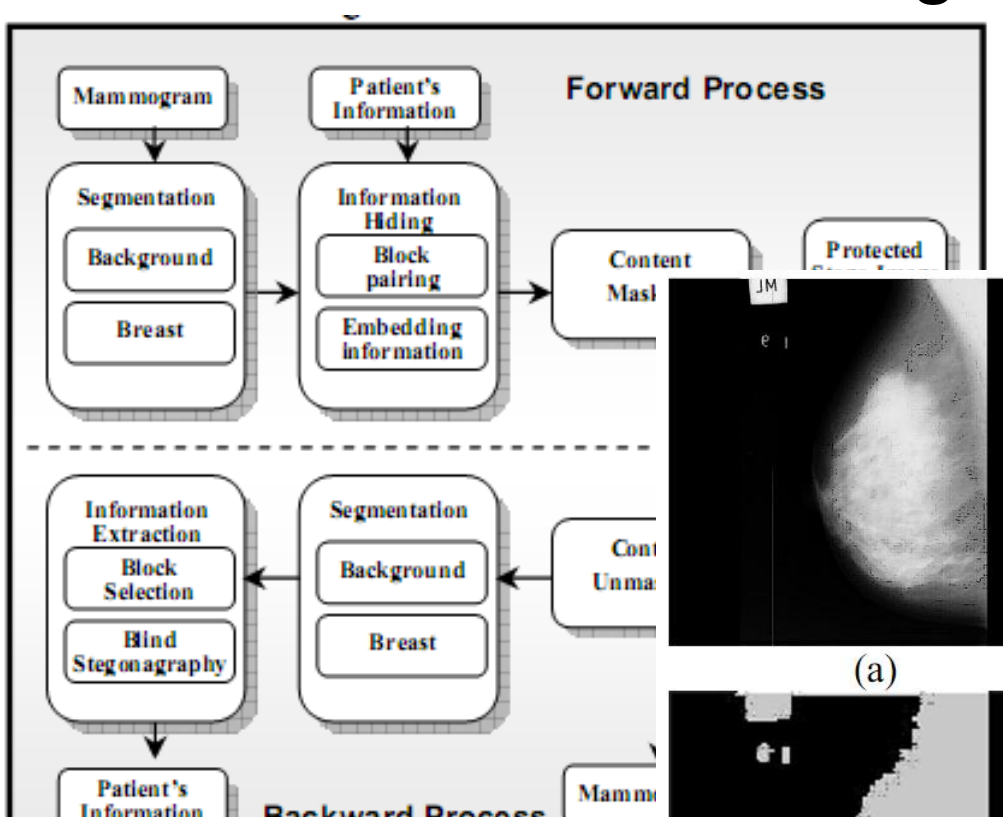

Ustalone punkty osadzenia bitów informacji ukrytej

# Ekstrakcja informacji ukrytej na etapie kodowania płaszczyzn bitowych według JPEG2000




| method | embedded data size (bytes) | compressed image size (bytes) | file size increase (bytes) | PSNR (dB) | KL divergence |
|---|---|---|---|---|---|
| (no embedding) | - | 32793 | - | 38.0 | - |
| QIM-JPEG2000 (max. amount) | 3865 | 39403 | 6610 | 35.3 | 0.0030 |
| QIM-JPEG2000 (equal amount) | 2446 | 37234 | 4441 | 36.0 | 0.0019 |
| Modified QIM-JPEG2000 | 2446 | 33249 | 456 | 37.1 | 0.0022 |
| LSB | 2425 | 33101 | 308 | 36.6 | 0.0095 |

# Przykład ukrywania informacji w mammogramach




**PROTECTION OF MAMMOGRAMS USING BLIND STEGANOGRAPHY AND WATERMARKING**

*Yue Li, Chang-Tsun Li and Chia-Hung Wei*

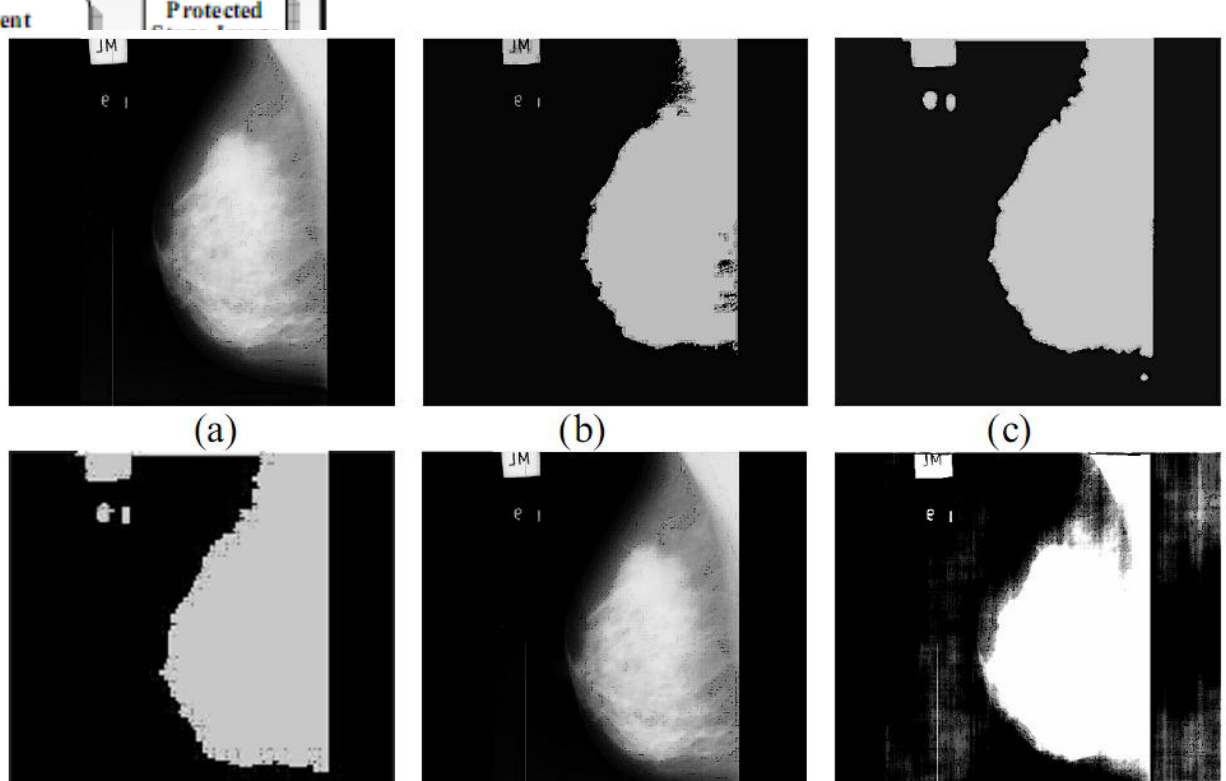



**Figure 3** (a) Original Mammogram; (b) Segmented Mammogram; (c) Dilated Mammogram; (d) Block Separation; (e) Stego-Mammogram; (f) Masked Mammogram.

# Przykład ukrywania informacji w mammogramach -algorytm

- Segmentacja mammogramu (obszar sutka, tło)
- Podział mammogramu na bloki o rozmiarach 8x8 pikseli
- Selekcja bloków tła
- Sortowanie bloków i łączenie ich w pary przy użyciu klucza prywatnego k1
- Obliczenie DCT dla pary wybranych bloków (A i B) oraz wybór rozstrzygających współczynników dla każdego bloku (a i b)
- Modulacja współczynnika b zgodnie z równaniem $b' = \gamma \cdot b$, gdzie $10<\gamma<10000$
- Znalezienie dwóch liczb pierwszych najbliższych iloczynowi $a \cdot b'$ zgodnie z zależnością $p1<a \cdot b'<p2$
- Obliczenie liczby c bitów informacji możliwej do ukrycia w danej parze bloków (na podstawie p1 i p2)
- Pobranie c bitów informacji o pacjencie w formie binarnej
- Obliczanie na podstawie tych bitów, p1 oraz a nowej wartości współczynników b w bloku B
- Przeprowadzenie odwrotnej transformaty kosinusowej (IDCT) na blokach A i B
- Ustalanie obrazu wyjściowego jako

obraz wyjściowy =stego_obraz *(1+k * znak_wodny)