DOI: 10.5604/01.3001.0009.5188

CHARAKTERYSTYKA WYBRANYCH TECHNIK UKRYWANIA OBRAZU

Agnieszka Świerkosz
AGH w Krakowie, Katedra Automatyki i Inżynierii Biomedycznej

Streszczenie. *Zważywszy, że różne techniki utajniania obrazów są znane od dawna, lecz nie znalazły szerszego zastosowania, być może ze względu na ich mankamenty, w tej publikacji zostaną opisane niektóre rodzaje technik sekretnego podziału obrazów, które już są. Autor ma na celu przeglądnięcie tych technik i ich podsumowanie.*

Słowa kluczowe: kodowanie obrazu, rekonstrukcja obrazu, ochrona danych, autentykacja

CHARACTERISTIC OF SELECTED IMAGE HIDING TECHNIQUES

Abstract. *Considering that different techniques of hiding images are known for a long time, but have not found wider application, perhaps because of their shortcomings. In this publication are described some types of techniques secret sharing images that are already in use. The author aims to review these techniques and summarizes their features.*

Keywords: image coding, image reconstruction, data privacy, authentication

Wstęp

Z techniką utajniania informacji ludzkość ma do czynienia od bardzo dawna. Niekiedy zachodzi potrzeba przekazania informacji tak, aby osoby niepowołane nie miały dostępu do ich treści. Uwagę należy zwrócić na to, iż utajnianiu nie podlegają tylko informacje zawierające treści pisane ale również obrazy. Taki stan rzeczy mógłby być nieoceniony np. w medycynie, wojsku, astrofizyce etc.

W tej publikacji zostaną scharakteryzowane mechanizmy sekretnego podziału obrazów, a także przybliżone i porównane cztery techniki progowego ich podziału. Na początku wyjaśniona jest charakterystyka progowego podziału obrazu. W drugiej części artykułu został przedstawiony przykład sekretnego podziału obrazu z odwracalną steganografią. Natomiast trzeci rozdział poświęcony jest utajnianiu obrazu ze zdolnością wstępnego przeglądnięcia. W czwartym został opisany sekretny podział i sposób ukrywania z autentykacją. Rozdział piąty poświęcony jest czwartemu schematowi progowego podziału obrazu, z losowym podziałem. Przedostatnia część dotyczy zastosowania tych technik w medycynie. Ostatni rozdział stanowi podsumowanie całej pracy.

1. Charakterystyka (*t*, *n*)-progowego podziału obrazu

Sekretnemu podziałowi (ang. *Secret Sharing* – SS) obrazów [5, 32, 34] towarzyszy potrzeba zastosowania odpowiedniego klucza, dzięki któremu obraz zostaje utajniony i podzielony na kilka nieczytelnych części. W taki sposób każdy uczestnik otrzymuje jedną z *n* części zaszyfrowanego obrazu. Oryginalnego obrazu nie może odtworzyć jedna osoba posiadająca jeden element sekretu. Aby odtworzyć jego oryginał, każdy uczestniczy przy jego rekonstrukcji stosując się do metody odzyskiwania informacji przy pomocy tajnego klucza. Przy odzyskiwaniu sekretnego obrazu potrzebnych jest określonych *t* uczestników będących w posiadaniu *t*-części z wszystkich możliwych *n*. W takim przypadku $t \leq n$. Metoda ta jest zalecana jako jedno z zabezpieczeń przed złośliwymi intruzami [36].

Wynalezieniu (*t, n*) – progowej koncepcji Noara i Shamira [9] towarzyszyło wynalezienie techniki sekretnego podziału obrazu znane jako wizualny podział obrazu (ang. *Visual Secret Sharing* – VSS) [5], które posiadają następujące cechy [9]:

- każdych *t* z *n* upoważnionych uczestników może współdziałać aby odtworzyć sekretne dane,
- żaden z *t* - 1 uczestników eksperymentu nie wie nic o sekretnym obrazie,
- kamuflaż nie może zdradzać utajnionego obrazu,
- jakość cząstkowych obrazów musi być dobra,
- ujawniony obraz musi być wolny od zniekształceń.

2. Sekretny podział obrazu z odwracalną steganografią

Wobec rozpowszechnienia cyfryzacji, audio wizualizacji i transmisji danych niezbędne są techniki utajniania informacji. Z pomocą przychodzi sekretny podział obrazów z odwracalną steganografią. Metoda ta jest użyteczna, gdyż maskuje ukryty obraz tworząc nieczytelny tzw. stegoobraz. Wizualnie nie można dostrzec sekretnego obrazu, gdyż jest on schowany pod inny. Ważna jest również jakość utajnionych danych. Po zakodowaniu obraz ujawniony musi być czytelny i jednoznaczny. W przypadku obrazów artystycznych i medycznych nietolerowane jest nawet nieznaczne zniekształcenie treści. Poniżej zostanie opisana koncepcja Shamira (*t*, *n*) progowego podziału [9, 34]. Mając podzielny sekret s, użytkownik wyznacza pierwszą wartość *m* i wytwarza wielomian (*t* - 1)-stopnia:

$$F(x) = (s + a_1 x + ... + a_{t-1} x^{t-1}) \bmod m \qquad (1)$$

gdzie składowe a_1, a_2, a_{t-1}, są przypadkowo określone z liczb całkowitych przedziału [0, *m*-1]. Użytkownik oblicza składowe sekretu:

$$y_1 = F(1), y_2 = F(2), ..., y_n = F(n) \qquad (2)$$

i rozdziela składowe y_i wtajemniczonym uczestnikom. Właściwie obraz zostaje nieczytelny dla każdego posiadacza. Żaden z nich nie może zrekonstruować ukrytego obrazu, nawet używając wielomianu Lagrange'a. Nieczytelny obraz zachowuje dobrą jakość jeśli liczba uczestników jest większa lub równa *t*. Posiadający składowe sekretu mogą współdziałać rekonstruując $F(x)$ [9].

Mając podzielony sekretny obraz *S*, można utajnić i utworzyć *n* stegoobrazów (steganografię). Posiadając dowolne *t* z *n* stegoobrazów, wtajemniczeni uczestnicy eksperymentu mogą otrzymać wolny od zniekształceń sekret *S* .

2.1. Odwracalna procedura (*t*, *n*) podziału

Na wstępie, można wybrać pierwszy numer *m* i wyznaczyć unikalny klucz K_i dla każdego posiadacza jednego elementu tajemnicy, gdzie *i* = 1, 2, …, *n*. Aby podzielić sekretny obraz *S*, użytkownik zmienia *S* w *m* system znaków. Na przykład można przyjąć, że wybrane *m* wynosi 7. Jeśli dwa odpowiednie piksele *S* są równe 83 i 110, wtedy przemienione cyfry wynoszą $(1,4,6)_7$ oraz $(2,1,5)_7$.

Zamiast osadzać jeden sekretny piksel w wielomianie *F(x)*, można osadzić (*t* - 1) sekretne liczby w *F(x)*. Ta odwracalna procedura składa się z podpunktów 2.2. i 2.3.

2.2. Faza tworzenia nieczytelnych obrazów

Przyjmijmy, że podzielone (t - 1) liczby S są odpowiednie s_1, s_2, …, s_{t-1}. Przypuśćmy, iż O jest szarą skalą pokrytego obrazu z H × W pikselami, a p jest pikselem z O. Celem procesu podziału inwersji jest nie tylko odzyskanie sekretnych liczb s_1, s_2, …, s_{t-1}, , ale również zachowanie jakości p. Aby to osiągnąć trzeba obliczyć wartość d jako:

$$d = p \bmod m \tag{3}$$

Mając d i s_1, s_2, …, s_{t-1}, odwrócony wielomian $F(x)$ można sformułować jako:

$$F(x) = s_1 + s_2 x^1 + ... + s_{t-1} x^{t-2} + dx^{t-1} \bmod m \tag{4}$$

Można przez to wytworzyć n nieczytelnych obrazów y_i wypełnionych sekretnym kluczem K_i w $F(x)$.

$$y_i = F(K_i),\ y_2 = F(K_2),\ y_n = F(K_n) \tag{5}$$

Dla przykładu, w (3, 3)-progowym systemie, można podzielić dwie liczby $(s_1, s_2) = (1,4)_7$ z S w przykryty pikselami, którego wartość wynosi 157. Wartość d może być obliczona jako $d = 3 = 157 mod 7$. W ten sposób $F(x)$ może być sformułowana jako

$$F(x) = s_1 + s_2 x^1 + dx^2 \bmod m = 1 + 4x^1 + 3x^2 \bmod 7 \tag{6}$$

2.3. Faza ukrywania

Aby osiągnąć cel steganografii, większość cieni bazuje na zamianie bitów [2, 9, 24, 33], które polegają na przekręceniu oryginalnego obrazu. Wiele metod jest niezdolnych do rekonstrukcji stegoobrazów do sekretnego obrazu.

Nowy schemat posiada różnice wartości d (równanie 4), które mogą być użyte do odzyskania oryginalnego przykrytego pikselami obrazu, dzięki czemu możemy otrzymać wartość p. Uzyskując wartości p z utajnionych pikseli, trzeba dodać wartość p i ukryć dane y_i jako formę utajnienia pikseli:

$$Q = \lfloor p / m \rfloor \times m \tag{7}$$

$$\mathrm{p_i} = \mathrm{Q} + \mathrm{y_i} \tag{8}$$

gdzie Q jest skwantyzowaną wartością p, i p_i reprezentuje i-ty utajniony piksel. Można zobaczyć, że skwantyzowana wartość piksela p oryginalnego ukrytego sekretu jest taka sama co utajnionego piksela p_i. Przez powtarzanie faz pochodzenia cieni i utajnienia można ujawniać i maskować całe części sekretu w pokryty pikselami, w porządku do otrzymania stegoobrazu O_i. Wtedy można rozdzielić znaczące stegoobrazy O_i i klucz K_i wtajemniczonym uczestnikom eksperymentu.

2.4. Procedura odzyskiwania sekretnego obrazu

Mając t z n stegoobrazów O_j' i klucz K_j od wtajemniczonych uczestników, sekretny obraz S i wolny od zniekształceń ukryty obraz O może być zrekonstruowany. Na początku trzeba zauważyć, że p_j' odpowiada pikselowej wartości O_j'. Aby uzyskać sekret cyfrowy i oryginalne piksele p, upoważnieni uczestnicy muszą wyprowadzić wielomian $F(x)$ od p_j'. W ten sposób mogą użytkować operacje modułową aby otrzymać cienie y_j' przez obliczenie:

$$y_j' = p_j' \bmod m \tag{9}$$

Z cieniami y_j' i sekretnym kluczem K_j, wielomian $F(x)$ może być zrekonstruowany przez formułę interpolacji Lagrange'a w równaniu (4).

Upoważnieni uczestnicy eksperymentu przez wyciągnięcie (t - 1) składowych $F(x)$ mogą otrzymać sekretne liczby liczb s_1, s_2, …, s_{t-1}. Mogą uzyskać różne wartości d z ostatnich składowych $F(x)$. Do odbudowy oryginalnych ukrytych pikseli p, uczestnicy muszą obliczyć ilościową wartość Q jako:

$$Q = \lfloor p' / m \rfloor \times m \tag{10}$$

Zgodnie z tym ukryte piksele p mogą być odbudowane jako

$$p = Q + d. \tag{11}$$

Powtarzając powyższy proces, upoważnieni uczestnicy eksperymentu mogą przywrócić ukryty obraz O bez zniekształceń i wyciągnąć sekretne liczby. W końcu następuje możliwość odsłonięcia sekretnego obrazu S przez transformatę wszystkich sekretnych liczb do dziesiętnej reprezentacji.

3. Sekretny podział obrazu ze zdolnością wstępnego przeglądnięcia

W pracy [12] została przedstawiona nowa metoda sekretnego podziału ze zdolnością do wcześniejszego podglądu sekretu. Niektóre (t, n) –obrazy podczas progowego podziału mogą być podzielone na n nieczytelnych o rozmiarach t-krotnie mniejszych od tego oryginalnego, sekretnego. Małe rozmiary tych obrazów powodują, że sposób ten jest odpowiedni do szybkiej transmisji w sieci multimedialnych systemów, gdzie każda składowa sekretu jest rozdzielona, gromadzona i wiązana. Jednak każda część obrazu jest trudna do zidentyfikowania i zarządzania nią [12]. Zgodnie z tym, można nazwać przyjacielskim schemat ze składowymi pokazanymi jako skurczona wersja sekretnego obrazu, ale również proponowana lokalizacja do zarządzania problemami, takimi jak portrety składowych obrazów. Ten schemat nie jest jednak ściśle mówiąc schematem sekretnego podziału. W związku z tym zostanie przedstawiony nowy sposób sprawdzający ważności składowych obrazu.

Każdy (t, n)-progowy schemat sekretnego podziału obrazu [12, 30], gdzie $t \le n$, podzielony na n składowych nieczytelnych w sposób wymagający przynajmniej t części sekretu może odtworzyć obraz. Można osadzić sekretne piksele jako mnożniki wielomianu (t - 1)-stopnia, aby zakodować sekretny obraz w składowe o rozmiarze 1/t oryginalnego sekretnego obrazu. Tylko t odgałęzień potrzeba do transmisji ich własnych cieni do odbiorcy, aby zrekonstruować i całkowicie przesłać oryginalny, sekretny obraz. Progowa własność polega na tym, iż zaniedbanie (n – t) części składowych podczas transmisji nie będzie zakłócało fazy rekonstrukcji tak, że sekretny obraz będzie perfekcyjnie odbudowany przy użyciu t części [12].

Dla rekonstrukcji w przyjacielskim schemacie, odbiorca może poznać czy ten powszechnie przyjęty składowy obraz jest poprawny lub nie przez skurczoną wersję cienia. Jakkolwiek, portret na cieniu obrazu przepuszcza sekretną informację przed rekonstrukcją i dlatego w/w schemat nie jest w rzeczywistości sekretnym podziałem obrazu. Chociaż schematy te [12, 30, 35] są sekretnymi podziałami, odbiorca może wykonać szereg bezużytecznych obliczeń wielomianu Lagrange'a i wreszcie finalnie uznać uzyskany cień za błędny.

Można się zastanawiać nad tym jak zatrzymać nieczytelne obrazy i jednocześnie nie spędzać za dużo czasu na obliczeniach dla sprawdzenia ważności składowych obrazów. Można to uzyskać łącząc dwie sekretne strategie podziału: bazujący na wielomianie sekretny podział i wizualny sekretny podział (VSS) [12, 13, 17, 18, 27, 29, 33, 34]. Unikalną korzyścią płynącą ze schematu VSS jest łatwe odkodowanie wizualnych znaków. Przysposabiając te własności techniki wizualnego, sekretnego podziału w bazujący schemat wielomianu, można z sukcesem otrzymać wcześniejszy podgląd. Odbiorca może łatwo sprawdzić część składową bezpośrednio nie dokonując obliczeń. Po sprawdzeniu przez wcześniejsze podglądnięcie, może użyć obliczeń interpolacji Lagrange'a do odzyskania sekretnego obrazu. W takim razie nowy schemat może zachować obliczenia dla otrzymania poprawności nieczytelnych obrazów w chwili gdy porównuje się schematy. Zakłócone obrazy zachowują cechy schematów sekretnego podziału [12, 30].

3.1. Sekretny podział obrazu bazujący na wielomianie

(t, n)-progowy schemat [12, 30] tworzący n zakłóconych obrazów przy podzieleniu sekretnego obrazu na τ niezachodzących na siebie t– pikselowych bloków, w którym każdy z nich przedstawia równoważny nieczytelny obraz jak poniżej:

$$S_j(x) = (P_{jt} + P_{jt+1} x + P_{jt+2} x + ... + P_{jt+t-1} x^{t-1}) \bmod 251 \tag{12}$$

gdzie $S_j(x)$ przedstawia nieczytelny obraz pikseli łączących się z j-tym blokiem i r-tym nieczytelnym obrazem, dla $0 \le j \le \tau$-1 i $1 \le x \le n$. Wartość $S_j(x)$ powstaje w wyniku użycia oryginalnego piksela wartości $P_{jt}+P_{jt+1}+...+P_{jt+t-1}$ włącznie w j-tym bloku. Główny numer 251 wybiera się z własności takiej, że $S_j(x)$ jest ograniczony pomiędzy 0 a 250 i odpowiednio reprezentuje umowny 8-bit szarej skali obrazu. Osadzanie t pikseli za każdym razem, powoduje, że rozmiar nieczytelnego obrazu jest równy $1/t$ sekretnego obrazu. Aby odwrócić kodowanie, wielomian (12) może być zrekonstruowany przez interpolację Lagrange'a i w ten sposób bloki mogą być niezawodnie odzyskane. Powtarzając tę procedurę dla każdych składowych pikseli można odbudować sekretny obraz [12].

3.2. Wizualny podział sekretu (VSS)

Dla (t, n)-progowego wizualnego podziału sekretu, sekretny obraz jest kodowany na n nieczytelnych obrazów przez rozszerzenie każdego piksela (nazwanego jako piksel-ekspansywny) na m podpikseli. Jeżeli t uczestników posiadających nieczytelne obrazy może wizualnie odszyfrować sekretny obraz, to t - 1 mniej składowych nie ukaże żadnej informacji [12].

Obraz sekretny jest kodowany w n nieczytelnych obrazach (cieniach) poprzez podział (ekspansję) każdego z jego pikseli na m podpikseli. Pierwsze schematy wizualnego podziału sekretu były przeznaczone do utajniania czarnobiałych obrazów w postaci obrazów nieczytelnych. W pracy [30] autorzy użyli bieli do uwydatnienia czerni, gdzie np.:

$$''m-h''B''W \text{ (odpowiednio } ''m-l''B''l''W) \quad (13)$$

reprezentuje biel (odpowiednio czerń), przy czym $h > l$. Bardziej złożone schematy wizualnego podziału sekretu umożliwiają zakodowanie sekretnego obrazu w skali szarości lub barwnego, wyznaczenie minimalnej wartości m, oraz zachowanie proporcji w stosunku niezmiennym. Czarno-białe (t, n)-schematy progowego, wizualnego podziału obrazów mogą być wyznaczone przez dwie bazowe macierze B_1 i B_0 o rozmiarach $n \times m$ z elementami „1" i „0"oznaczającymi odpowiednio czarne i białe podpiksele. Przy podziale czarnego sekretnego piksela, wybiera się przypadkowo jeden wiersz macierzy C_1 włączając całą macierz otrzymaną poprzez przestawienie kolumn w B_1 (odpowiednio B_0) do związanych nieczytelnych obrazów. Można oznaczyć $OR(B_i|r)$, $i = 0, 1$, jako wypadkowy wektor z r wierszami w B_i, a H(·) może być wagą Hamminga wektora. Wówczas macierze bazowe (t, n)-wizualnego schematu podziału sekretu spełniają następujące warunki kontrastu i bezpieczeństwa [14]:

$$H(OR(B_0|r)) \ge (m-l), \quad (14)$$

$$H(OR(B_1|r)) \le (m-h) \quad (15)$$

dla $r \ge t$, gdzie $0 \le l \le h \le m$;

$$H(OR(B_1|r)) = H(OR(B_0|r))| \quad (16)$$

dla $r \le (t-1)$.

Przykładowy schemat [12] został opisany poniżej.

Oczywiste jest to, że kiedy podpiksel jest ułożony w stertę przez biały podpiksel, jego intensywność jest niezmienna. Podczas gdy sterta zawiera dwa szare podpiksele otrzymujemy jeszcze jeden szary kolor. Jeśli zamieniamy szary piksel zamiast czarnego podpiksela w nieczytelnym obrazie schematu wizualnego podziału sekretu, można użyć bieli w każdych m podpikselach aby uwydatnić czarny kolor z białego koloru. W tym czasie szary podpiksel może być użyty do reprezentacji $S_j(r)$ w (12). Dla rekonstrukcji, sekretny obraz może być wizualnie podglądnięty przez prostą stertę cieni jak w schemacie wizualnego podziału sekretu. Następnie, sekretny obraz może być perfekcyjnie zrekonstruowany z wartości $S_j(r)$ używając wielomianu Lagrange'a. Formalne procedury kodowania i dekodowania zostały opisane poniżej [12] z zastosowaniem następujących oznaczeń:

I – sekretny obraz z określonym rozmiarem.

$E(\cdot)$ – schemat (t, n) sekretnego podziału obrazu.

S_i – wydobycie nieczytelnych obrazów z E(I), $i = 1, \ldots, n$, gdzie rozmiar wynosi (|I |/t).

I' – zmieniony rozmiar i barwa I na binarny obraz w rozmiarze (| I |/(t×w)), gdzie w jest tłumieniem wagi w bazie macierzy.

$V(\cdot)$ – czarny i biały (t, n) schemat wizualnego podziału sekretu w pikselowej ekspansji m.

O_i – czarny i biały cień z V(I'), $i = 1, \ldots, n$, gdzie rozmiar wynosi (|I|×m/(t×w)).

O_i' – szary i biały cień tego schematu, $i = 1, \ldots, n$, gdzie rozmiar wynosi (|I|×m/(t×w)).

$T(\cdot,\cdot)$ – operacja zamiany miejsc pikseli. Przekształcenie cieni O_i na O_i', gdzie, $T(O_i, S_i) = O_i'$, gdzie czarny piksel O_i jest zastąpiony przez piksel S_i piksel po pikselu. Przy czym uporządkowane numery czarnych pikseli w O_i są (|I|/t) są takiego samego rozmiaru jak S_i.

3.3. Procedura kodowania

1) Szyfrowanie sekretu przez E(I) = S_i, $i = 1, \ldots, n$.
2) Otrzymanie I'z I.
3) Zastosowanie V(I') = O_i, $i = 1, \ldots, n$.
4) Generowanie O_i' używając $T(O_i, S_i) = O_i'$, $i = 1, \ldots, n$

3.4. Procedura odkodowania

Składa się z dwóch faz. Pierwsza, wstępnego przeglądnięcia, to podpunkty 1) i 2). Druga to całkowita rekonstrukcja składa się z procedur 3) i 4).

1) Sterta t cieni $O_{i_1}', \ldots, O_{i_t}'$, do wizualnego wstępnego przeglądnięcia binarnego sekretu I'.
2) Identyfikacja i weryfikacja obrazu I' przez ludzki wzrok.
3) Otrzymanie ($S_{i_1}', \ldots, S_{i_t}'$) z ($O_{i_1}', \ldots, O_{i_t}'$).
4) Używanie wielomianu Lagrange'a do rekonstrukcji I z ($S_{i_1}', \ldots, S_{i_t}'$).

4. Sekretny podział obrazu i ukrywanie z autentykacją

Lin-Tsai, Yang i Chang proponują sekretny podział obrazu i ukrywanie schematu z autentykacją [28]. Sekretny obraz jest dzielony i ukrywany pod stegoobrazy w sposób taki, aby transmisja była bezpieczna. Niestety istnieje wada tej techniki, polegająca na tym, że każdy stegoobraz musi być zredukowany wielokrotnie, w stosunku do sekretnego obrazu. Jako przykład zostanie przytoczony (t, n)-progowy schemat z obrazem zredukowanym do 3,5/t-krotności sekretnego obrazu z jakością obrazu lepszą niż po przedni schemat [28].

W tej pracy będzie zaprezentowany schemat z mniejszym rozmiarem stegoobrazu. Dwa cienie pikseli zostają osadzone w siedmiopikselowym bloku przykrywającym obraz. W ten sposób, ekspansja rozmiaru pokrywającego obrazu jest redukowana 3,5-krotnie.W rezultacie proponowany schemat może osiągać lepszą wizualną jakość. W dodatku integracja stegoobrazu może być sprawdzana efektywnie [28].

Poniżej został opisany przykładowy schemat [28], który zawiera dwie czynności: procedurę podziału i ukrycia, autentykację i procedurę ujawnienia.

4.1. Procedura podziału i ukrycia

Przed podziałem, sekretny obraz powinien być zaszyfrowany przy użyciu sekretnego klucza K, podzielonego na n podkluczy dla n osób, używając do tego wielomianu:

$$f_i(x)=(d_0+d_1x+...+d_{t-1}x^{t-1}) \bmod p \quad (17)$$

gdzie moduł p w wielomianie jest ustalany do 251. Wszystkie szare wartości pikseli są ustawiane w rząd od 0 do 250. Każdy

piksel o wartości większej lub równej 250 jest reprezentowany jako dwie wartości: 250 i różnicy pomiędzy wartością piksela a 250. Następnie, zmodyfikowany sekretny obraz jest podzielony na *n* nieczytelnych obrazów w (*t*, *n*)– progowy sposób [28].

Dla bezpiecznej transmisji, każdy nieczytelny obraz powinien być osadzany w nakryciu z obrazu. W przykładowym schemacie są równocześnie osadzane dwa nieczytelne piksele i wstrzymujący bit w siedmiopikselowy, okrywający blok B_i. Siedem pikseli z każdego bloku B_i jest oznaczone jako X_i, W_i, V_i, Z_i, T_i, Y_i, *i* U_i. Parametry x_i, w_i, v_i, z_i, t_i, y_i, *i* u_i są odpowiednio ich binarnymi wartościami. Można założyć, że s_1, s_2, …, s_{16} są binarną reprezentacją dwóch nieczytelnych pikseli i *p* jest wstrzymującym bitem. Stegoblok $B_i^{'}$ wytworzony przez zastąpienie 17 bitów $x_1x_2w_1w_2v_1v_2z_1z_2t_1t_2t_3y_1y_2y_3u_1u_2u_3$ z $s_1s_2s_3...s_{16}$. W celu poprawy jakości stegoobrazu zastosowane jest podstawienie najmniejszego mającego znaczenie bitu [28].

Aby przeszkodzić złośliwym uczestnikom modyfikacji stegoobrazów, w każdym stegoobrazie osadza się strumień bitów wstrzymujących. W przykładzie [28] autorzy użyli funkcji skrótu MD5, aby wytworzyć ciąg bitów autentykacyjnych. Wstrzymujące bity zostały obliczone jako alternatywa rozłączna (XOR) bitów autentykacyjnych i strumienia znaków wodnych. Najpierw stegoobraz jest dzielony na oddzielne sekcje, przy czym każda z nich zawiera 128 stegobloków. Autentykacyjne bity każdej sekcji są szacowane jak poniżej:

$$h_1h_2...h_{128} = MD5((B_1^{'} - p_1)\|(B_2^{'} - p_2)\|...\|(B_{128}^{'} - p_{128})\|K) \tag{18}$$

gdzie $B_i^{'} - p_i$ reprezentuje 55 zastrzeżonych wstrzymujących bitów p_i z *i*-tego stegobloku $B_i^{'}$ bieżącej sekcji i *K* jest sekretnym kluczem. '||' reprezentuje powiązane operacje [28].

Bieżące 128 znaków wodnych bitów wytwarzanych przez *K* jest oznaczanych jako $w_1w_2...w_{128}$, wstrzymujące bity $p_1p_2...p_{128}$ są obliczane jak poniżej:

$$(v_1v_2\ldots v_{128}) = (w_1w_2\ldots w_{128}) \oplus (h_1h_2...h_{128}) \tag{19}$$

Na końcu $p_1p_2...p_{128}$ są osadzane w 128 stegoblokach bieżącej sekcji, odpowiednio. Powstały proces blokujących bitów jest powtarzany, dopóki wszystkie bloki stegoobrazów zakończą proces. Powstałe stegoobrazy są przesyłane do upoważnionych uczestników eksperymentu. Zauważyć trzeba, że dwa bity (s_1 i *p*) są osadzane w stegopikselach $X_i^{'}$ używając prostego podstawienia LSB (ang. *least significant bit*) zamiast optymalnego podstawienia LSB. Inaczej mówiąc, sprawdzające bity obliczane z stegoobrazów mogą być zamienione a jakość stegoobrazu może nie przejść procesu autentykacji [28].

4.2. Procedura autentykacji i odkrywania

Aby ujawnić sekretny obraz każde *t* lub więcej stegoobrazów powinno być gromadzone razem. Najpierw sekretny klucz *K* może być ujawniony przez interpolacje Lagrange'a z *t* podkluczami. Następnie bity znaków wodnych są wyznaczane w oparciu o klucz *K*. Później, każdy stegoobraz jest dzielony na odrębne sekcje, z których każda posiada 128 siedmiopikselowe bloki. Następnie są obliczane bity kontrolne $\left(p_1^{'}p_2^{'}\ldots p_{128}^{'}\right)$ bieżącej sekcji. Jeśli są one równe tym osadzonym bitom $\left(p_1p_2\ldots p_{128}\right)$, wtedy bieżąca sekcja jest weryfikowana pomyślnie i odpowiadające nieczytelne piksele są odzyskiwane. Proces autentykacji i ujawniania jest powtarzany dopóki *t* nieczytelnych obrazów mogą być odzyskane z *t* stegoobrazów. Ostatecznie sekretny obraz jest ujawniony z *t* nieczytelnych obrazów przy użyciu interpolacji Lagrenge'a [28].

5. Sekretny podział obrazu z ulepszonym losowym podziałem

W tym podrozdziale została krótko omówiona metoda utajniania obrazu z ulepszonym losowym podziałem, która jest szczegółowo zaprezentowana w [31] i bazuje na schemacie Chen i Wu [14].

Ukrywanie sekretnych danych pomiędzy innymi częściami jest jednym z ważniejszych problemów w zastosowaniu różnych aplikacji [6]. Aktualnie jest kilka metod utajniania informacji. Steganografia i znaki wodne są przykładowymi takimi technikami [15, 26, 27]. Istniej również tzw. progowy podział (ang. *Secret Sharing* SS), a także ten bazujący na wielomianie (ang. *Polynomial-Style Sharing* – PSS) [12, 30]. Wizualna kryptografia (ang. *Visual Cryptography* – VC), która była przedmiotem analizy w [19] bazuje na wizualnym ludzkim systemie (ang. *Human Visual System* – HVS) [10, 30]. Metoda ta została już zaproponowana przez Naora i Shamira jako *k* z *n* wizualny progowy schemat, w którym każdy *k* z *n* uczestników może odtworzyć tajny obraz [16]. Prowadzono już prace naukowe w zakresie wizualnej kryptografii. Między innymi aby rozwiązać problem kontrastu przy rekonstrukcji [3, 7, 16, 21, 36, 38], lub przenieść na zewnątrz wizualny schemat podziału w kolorowy lub szary poziom obrazu [22, 29, 35]. Były także badania nad metodami podziału więcej niż jednego sekretnego obrazu [11, 14, 23].

Wizualny podział sekretu (VSS) jest metodą, która rozprasza sekretny obraz w losowo podzielone kawałki tak, aby po złączeniu ich razem zrekonstruować oryginalny obraz. Każda część tajemnicy jest to losowy wzór czarno-białych pikseli i nie można odtworzyć sekretnego obrazu z tylko jednego kawałka.

Muszą być ułożone razem, aby zrekonstruować tajemnicę. Stos dwóch części może zrekonstruować pierwszy sekret podczas obracania pierwszej części o 90° przeciwnie do kierunku wskazówek zegara rekonstruując drugą część sekretu.

Nowość algorytmu, zaproponowana w niniejszej pracy, polegająca na utworzeniu obydwu części z dwóch sekretów jest ulepszona losowością. Dzielący algorytm tworzy się przez wybieranie rozszerzonych wzory przypadkowych pikseli w celu poprawnego kontrastu wymaganego od obu tajemnic zrekonstruowanych przez normalne i obracane układanie w stos. Proponowana metoda zawiera cechy właściwości bezpieczeństwa ze względu na lepszą losowości części tajemnicy [31].

W tej części pracy zostanie zaprezentowany (2, 2)-progowy schemat podziału obrazu. Części są prostokątnego kształtu i utworzone w całkowicie losowy sposób. Rozszerzone wzory losowych pikseli eliminują jednolitość pikseli przez podział. Pierwsza część tajemnicy jest wygenerowana całkowicie przypadkowo, następnie drugą tworzy się zależnie od tej pierwszej. Ułożone w stertę dwie części tajemnicy mogą zrekonstruować utajniony obraz. Obracając pierwszą sekretną część o 90° odwrotnie do wskazówek zegara i ułożenie na stos z tą drugą można odtworzyć drugi sekret.

Proponowana metoda [31] składa się z dwóch procesów. Pierwszy to generowanie części S_1 i S_2. Zaprezentowany poniżej algorytm wytworzenia S_1 bazuje na specjalnej macierzy i zwie się procesem tablicowym (ang. *Process Table* – PT). Rozszerzone bloki utworzone podczas kreowania części są wytworzone zgodnie z procesem tablicowym. Proces ten ma te same rozmiary co oryginalny obraz i zainicjalizowany jest do wszystkich jedynek (kolor biały) na początku. Dla uproszczenia wszystkie 2×2 rozszerzone bloki zakamuflowanych części są reprezentowane przez pojedynczą komórkę.

Proces tablicowy jest skanowany zstępująco poprzez kolumny zaczynając od pierwszej z lewej. Pierwszą rzeczą tego procesu, używając owego algorytmu jest pierwszy biały piksel w napotkanej kolumnie. Wartość piksela w PT jest zgodna z procesem rozszerzonego bloku i jest przydzielana do czarnego po każdym kroku. Po tych czterech krokach, proces badania zaczyna się od przeszukania w celu znalezienia następnego białego piksela w procesie tablicowym od punktu, gdzie ostatni biały piksel został umieszczony dopóki żaden biały piksel nie został pozostawiony.

- Krok 1: Od momentu, kiedy proces tablicowy – PT (1, 1) jest pierwszym białym pikselem podczas sprawdzania, algorytm będzie działał odpowiednio z rozszerzonym blokiem przy S_1.

2×2 rozszerzony blok przy (1, 1) jest reprezentowany przy a_1. Odpowiednia pozycja a_1 przy $S_1^{90°}$ jest użyta do konstrukcji drugiego piksela w rysunku względem położenia ale jeszcze pusta. A_1 rozszerzony blok z pierwszego podziału jest losowo sprawdzany od jednego z 2×2 wzorów. Potem obracając wartość a_1 przeciwnie do wskazówek zegara o 90° umieszcza się tą właściwą pozycję w $S_1^{90°}$, nazywając $a_1^{90°}$.

- Krok 2: Odpowiednia pozycja rozszerzonego bloku $a_1^{90°}$ w S_1 zostaje zastosowana do konstrukcji pierwszego piksela w rysunku na tej samej pozycji ale $a_1^{90°}$ w $S_1^{90°}$ jest przydzielona w pierwszym kroku. Ta wartość jest stosowana do konstrukcji drugiego piksela w rysunku na tej samej pozycji. Rozszerzony blok reprezentowany przez a_1 w S_1 jest ustalany przez wzięcie z raportu pierwszego rysunku, drugiego rysunku i $a_1^{90°}$. 2×2 rozszerzony blok reprezentowany przez a_1 w S_1 jest wybrany zależnie do zasady podanej w pseudokodzie [31]. Wartość a_2 jest obracana odwrotnie do wskazówek zegara o 90° i w rezultacie jest umieszczana w a_2 przy $S_1^{90°}$ oraz nazwana $a_2^{90°}$.
- Krok 3: Odpowiednia pozycja $a_2^{90°}$ to a_3 przy S_1. a_3 jest ustalana przez piksele rysunków przy zależnych pozycjach i wartość $a_2^{90°}$ przy $S_1^{90°}$. Następnie rezultat obrotu a_3 obracany odwrotnie do ruchu wskazówek zegara o 90° jest umieszczany na odpowiedniej pozycji w $S_1^{90°}$ i nazwany $a_3^{90°}$. Ta wartość w $S_1^{90°}$ daje klucz dotyczący drugiego piksela w rysunku na tej samej pozycji.
- Krok 4: Odpowiednie grupy pikseli a_4 w S_1nie są ustalone tylko przez wartość $a_3^{90°}$, ale w dodatku do tego a_1 w S_1 może być wzięte w tym rozrachunku. Ponieważ wartość będzie umiejscowiona przy a_4 z S_1, to będzie umieszczona w (1, 1) w $S_1^{90°}$. Ta wartość będzie użyta do ustanowienia pierwszego piksela dwóch rysunków.

Pseudokodu używa się do wybierania kandydatów dla pozycji a_4, którzy będą obracani i w rezultacie stertowani z rozszerzonym blokiem reprezentowanym przez a_1. Jeden zrekonstruowany, kiedy ułożone w stóg razem zgodne wartości (czarne lub białe) dla obu rysunków będą wybrane dla miejsca a_4 w S_1.

Każdy krok w tym schemacie przełącza wartość procesu tablicowego od jeden do zera (białego do czarnego). Te cztery kroki są powtarzane dopóki wszystkie piksele PT nie staną się zerami (czarne).

Drugi podział jest generowany na bazie pierwszego i obu sekretnych obrazów. Rozszerzony 2×2 blok w drugim podziale musi być zdefiniowany zgodnie z odpowiadającymi 2×2 rozszerzonymi blokami w S_1, $S_1^{90°}$ i wartościami pikseli dwóch poufnych rysunków na zależnych pozycjach. Każdy rozszerzony blok w drugim podziale ma dwa piksele i dwa czarne piksele. Jest sześć możliwych kombinacji.

Rozdzielczość w drugim podziale rozszerzonych bloków składa się z trzech etapów. Kombinatorycznie wzrost wszystkich możliwych przypadków jest wielce przytłaczający, dlatego ogólna procedura jest opisana poniżej.

- Krok 1: Rozszerzony blok S_1 jest ułożony w stóg z wszystkimi sześcioma możliwościami S_2 wzorów. Bloki, których wydajność poprawnej wartości piksela p_1 są wybrane.
- Krok 2: Rozszerzony blok z $S_1^{90°}$ jest ułożony w stertę z sześcioma możliwościami S_2 wzorów. Bloki, których wydajność poprawnej wartości piksela p_2 są wybrane.
- Krok 3: Wypadkowe wyniki z kroku 1 i 2 są kandydatem/ kandydatami dla S_2. Jednym z nich jest losowo wybrany do umieszczenia w odpowiednim miejscu w S_2.

Schemat ten, bazujący na pracy Chen i Wu [14], wykorzystuje podział rotacyjny (0° i 90°) do osadzenia dwóch zestawów sekretnych wiadomości w dwie części. Odkąd ilość losowych wymaganych dla tworzonych części jest ważną kwestią w zaimplementowaniu schematu sekretnego obrazu [31], proponowana metoda tworzy S_1 poza faktycznie losowymi wzorami jako przeciwstawne ¼ losowych wzorów. Jej efektywność można sprawdzić w środowisku MATLAB.

6. Zastosowanie technik progowego podziału obrazu w medycynie

W ostatnich latach nastąpił rozwój telemedycyny. Dane pacjentów i ich historie choroby są archiwizowane w bazach komputerowych. Zdjęcia np. tomografii komputerowej są wykonywane cyfrowo.

To przejście z systemu analogowego na ten bardziej aktualny wymagający zaawansowanego sprzętu komputerowego wymaga zmian w systemie zabezpieczeń. Tu właśnie mogą mieć zastosowanie techniki utajniania obrazów.

Przy przesyłaniu obrazów medycznych wraz z towarzyszącym opisem (np. MRI, PET, ...) drogą bezprzewodową ważne jest aby dotarły one do odbiorcy bez zniekształceń [19]. W medycynie możemy kodować nie tylko obrazy, ale również sygnały (np. EEG, EKG,...) [1, 25]. Bardzo ważna rzeczą jest możliwość zakodowania treści obrazu. Jest to element zabezpieczający, stanowiący ochronę danych przed odczytaniem przez kogoś, kto nie jest do tego celu upoważniony [4]. W ustalonym zakresie informacji tylko odbiorca mający wiedzę i klucz mógłby odkodować obraz wraz z danymi osobowymi pacjenta.

Zakodowane informacje powinny mieć cechy, takie jak [4]:

- niedostrzegalność – nikt poza upoważnionym odbiorcą nie powinien domyślać się, że w informacji obrazowej przesyłanej drogą bezprzewodową zakodowane są jeszcze dodatkowe dane. Zakodowany obraz powinien być niedostrzegalny dla osób niepożądanych,
- czytelność – po odkodowaniu obraz oryginalny powinien być bez zniekształceń,
- niska złożoność – algorytm kodujący powinien być nie za prosty, ale też nie zbyt skomplikowany. Optymalny schemat kodowania ma wpływ na transmisję danych,
- bezpieczeństwo – nikt nie powinien domyślać się, jaki algorytm został zastosowany i czy w ogóle został użyty jakikolwiek system kodowania informacji. Powinien być on sekretem.

7. Podsumowanie

W publikacji zostały przedstawione skrótowo cztery metody sekretnego podziału obrazu. Sposób działania jest dla każdego z omawianych schematów bardzo podobna. Różnią się jednak strukturą algorytmu.

Wadą schematu sekretnego podziału w pierwszym przykładzie jest to, że z zastosowaniem steganografii, przy ujawnianiu tajnego obrazu jest on zniekształcony. Jest to spowodowane obcięciem skali szarości sekretnego obrazu. Pomimo, że zniekształcenie jest nieznaczne, może to być niedopuszczalne dla znaczenia istotnego sekretu. W tej przeglądowej pracy został przywołany jako przykładowy schemat zaprezentowany już wcześniej w [9], który może utajnić i ujawnić sekretny obraz bezstratnie. Również podczas odtajniania schemat może dysponować dużą pojemnością osadzania w porównaniu z powiązanymi zamaskowanym częściami schematu. Przy użyciu zakodowanego sekretnego obrazu t z n części, upoważnieni uczestnicy mogą zrekonstruować oryginalny obraz ze stegoobrazów. Proces ten jest odwracalny. Schemat podziału ma praktyczne zastosowanie zachowując cenny, ukryty obraz. Ma to istotne znaczenie dla obrazów wojskowych lub medycznych.

Przeszkodą w drugim przykładzie utajniania obrazu ze zdolnością wstępnego przeglądnięcia, jest to, iż schemat z prostymi nieczytelnymi obrazami może być nieodpowiedni do identyfikacji i nie być przykładem sekretnego podziału. Opisany przykładowy schemat jest hybrydą. W połowie bazuje na schemacie wielomianu i w połowie na wizualnym podziale sekretu (VSS). Te dwa progowe schematy są odpowiednio połączone tak, aby wzmocnić ich właściwości i wyeliminować mankamenty związane z procedurą utajniania obrazów.

Trzecim przykładem jest sekretny podział obrazu i ukrywanie z autentykacją, co cechuje się rozmiarem każdego stegoobrazu tylko 3.5/*t* razy sekretnego obrazu. Mały rozmiar stegoobrazu jest nie tylko wygodny do gromadzenia, ale również wydajny podczas transmisji. Przykładowy schemat ma również lepszą jakość stegoobrazu. W dodatku integracja i kompetentność stegoobrazów zostały efektywnie zweryfikowane.

W czwartym podrozdziale został opisany algorytm ukrywania tajnego obrazu z ulepszonym losowym podziałem. Jest to modyfikacja (2, 2)-wizualnego schematu progowego podziału zaproponowanego przez Chen i Wu [14]. Techniki heurystyczne są wykorzystywane do określenia odpowiednich wartości dla pierwszego podziału. Potem drugi podział stanowi rozszerzony blok wartości, które mogą zostać wybrane z sześciu możliwych kombinacji, podczas gdy tylko cztery mogły zostać wykorzystane w poprzedniej prace. Tajne zdjęcia wykazują niski kontrast, a ich dynamiczny zasięg jest ograniczony przez możliwe kombinacje 2×2 rozszerzonych bloków. Korzystanie z większych rozszerzonych bloków może zwiększyć zakresu dynamiki i kontrast, ale także zwiększa znacznie rozmiar podzielonych części. Losowe zdjęcia (utajnione części) przypominają schematy wizualnego sekretnego podziału. Kolejnym ulepszeniem w owym schemacie jest użycie łatwego podziału który jest podobny z wyglądu do zwykłych obrazów półtonowych. Przyszłe prace mogą bazować na prostych (2,2) schematach VSS.

Każdy przykładowy schemat ma jakieś słabości, ale zostały one pomniejszone lub nawet wyeliminowane przez połączenie kilku różnych technik. Poszczególne metody posiadają inne, szczególne, specyficzne właściwości. Każda z nich posiada unikalne cechy, które właściwie dobrze utworzone, mogą zostać poprawnie zastosowane według uznania.

Literatura

[1] Ahuja B.S., Frooq O., Kaur S., Singhal R., Digital watermarking of ECG data for secure wireless communication, International Conference on Recent Trends in Information. Telecommunication and Computing, IEEE Computer Society, 2010.

[2] Ansair N., Ni Z., Lin X., Shi Y. Q., Su W., Sun Q., Robust lossless image data hiding designed for semi-fragile image authentication, IEEE Transactions on Circuits and Systems for Video Technology 18(4)/2008,497–509.

[3] Ateniese G., Blundo C., De Santis A., Stinson D. R., Visual cryptography for general access structures, Information and Computation 129(2)/1996, 86–106.

[4] Banerjee A., Gupta S. K. S., Venkatasubramanian K. K., PSKA: Usable and secure key agreement scheme for Body Area Network, IEEE Transactions on Information Technology in Biomedicine 14(1)/2010.

[5] Blakley G. R., Safeguarding cryptographic keys, Proceedings of AFIPS National Computer Conference 48/1979, 313–317.

[6] Blundo C., Naor, M., De Santis A., Visual cryptography for grey level images, Information Processing Letters 75/2000, 255–259.

[7] Blundo C., De Santis A., Stinson D. R., On the Contrast in Visual Cryptography Schemes, Journal of Cryptology 12/1999, 261–289.

[8] De Bonis A., De Santis A., Randomnees in visual cryptography, Theoretical Computer Science 314(3)/2004, 351–374.

[9] Chang C. C., Chan C. S., Lin P. Y., Secret Image Sharing with Reversible Steganography, 2009 International Conference on Computational Intelligence and Natural Computing, IEEE 2009.

[10] Chang C.C, Chen T.S., Tsai C. S., Sharing multiple secrets in digital images , Journal of Systems and SoftwareCIP99 64(2)/2002, 163–170.

[11] Chang C. C., Wu H. C., Sharing visual multi-secrets using circle shares, Computer Standards & Interfaces 28(1)/2005, 123–135.

[12] Chen T. S., Yang C. N., An image secret sharing scheme with the capability of previewing the secret image, IEEE 2007.

[13] Chen T. S., Yang C. N., Reduce Shadow Size in Aspect Ratio Invariant Visual Secret Sharing Schemes using a Square Block-wise Operation, Patter Recognition 39(7)/2006, 1300–1314.

[14] Chen L. H., Wu C. C., A study on visual cryptography. Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.

[15] Cox I. J., Bloom J. A., Miller M. L., Digital Watermarking, Morgan Kaufmann Publishers Inc., San Francisco, CA, 2001.

[16] Cimato S., De Prisco R., De Santis A., Colored visual cryptography without color darkening, Theoretical Computer Science 374(1–3)/2007, 261–276.

[17] Cimato S., Prisco R., Santis A., Probabilistic visual cryptography schemes, The computer Journal 49/2006, 97–107.

[18] Eisen P. A., Stinson D. R., Threshold visual cryptography schemes with specified whiteness, Designs, Codes and Cryptography 25(1)/2002, 15–61.

[19] Fang W.P., Friendly progressive visual secret sharing, Pattern Recognition 41(4)/2008, 1410–1414.

[20] Giakoumaki A., Koutsouris D., Pavlopoulos S., Secure and efficient health data management through multiple watermarking on medical images, Med. Bio. Eng. Comput. 44/2006, 619–631.

[21] Hofmeister T., Krause M., Simon, H., Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography, In Proceedings of the Third Annual international Conference on Computing and Combinatorics 1276/1997, 176–185.

[22] Hou Y.C., Visual cryptography for color images, Pattern Recognition 36/2003, 1619–1629.

[23] Huang S. Y., Lee Y. K., Shyu S. J., Wang R.Z., Sharing multiple secrets in visual cryptography, Pattern Recognition 40(12)/2007, 3633–3657.

[24] Hsueh N. L., Lin C. C., A lossless data hiding scheme based on three-pixel block differences, Pattern Recognition 41(4)/2008, 1415–1425.

[25] Ibaida A., Khalil I., van Schyndel R., A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system, Computing in Cardiology 38/2011, 393–396.

[26] Katzenbeisser S., Petitcolas F.A.P., Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Inc., Boston, 2000.

[27] Laih C. S., Yang C. N., New colored visual secret sharing schemes, Designs, Codes and Cryptography 20(3)/2000, 325–335.

[28] Li P., Ma P., Su X., Image secret sharing and hiding with authentication, 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, IEEE 2010.

[29] Lin C. C., Tsai W. H., Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters 2003, 349–358.

[30] Lin J. C., Thien C. C., Secret image sharing, Computers & Graphics, 26/2002, 765–770.

[31] Nabiyev V. V., Ulutas G., Ulutas M., Yazici R., (2, 2)-Secret Sharing Scheme with Improved Share Randomnes, IEEE 2008.

[32] Noar M., Shamir A., Visual cryptography, Advances in Cryptology: Eurocrypt'94, Spring-Verlag, Berlin 1995,1–12.

[33] Rodriguez J. J., Thodi D. M., Expansion embedding techniques for reversible watermarking, IEEE Transactions on Image Processing 16(3)/2007, 721–730.

[34] Shamir A., How to share a secret, Communications of the ACM 22(11)/1979, 612–613.

[35] Shyu S. J., Efficient visual secret sharing scheme for color images, Patter Recognition 39(5)/2006, 866–880.

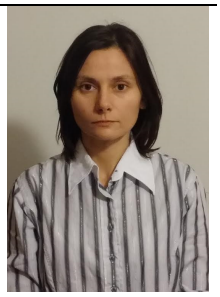
[36] Stinson D. R., An introduction to visual cryptography, Public Key Solutions'97, Canada, April 11997.

[37] Su C. H., Wang R. Z., Secret image sharing with smaller shadow images, Pattern Recognition Letters 27(6)/2006, 551–555.

[38] Van Tilborg H. C. A., Verheul E. R., Constructions and Properties of k out of n Visual Secret Sharing Schemes, Designs, Codes and Cryptography 11(2)/1997, 179–196.

Mgr inż. Agnieszka Świerkosz
e-mail: aswierk@agh.edu.pl

Doktorantka na wydziale Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej w Akademii Górniczo-Hutniczej w Krakowie. Ukończyła studia na Uniwersytecie Pedagogicznym w Krakowie z tytułem magistra inżyniera na Wydziale Matematyczno-Fizyczno-Technicznym ze specjalizacji Edukacja Techniczno-Informatyczna. Autorka kilku publikacji z dziedziny Biocybernetyki i Inżynierii Biomedycznej.



otrzymano/received: 28.07.2016 *przyjęto do druku/accepted: 30.10.2016*