Pomiary Automatyka Robotyka, ISSN 1427-9126, R. 25, Nr 3/2021, 65–72, DOI: 10.14313/PAR_241/65

Komunikacja skryta w termowizji – analiza możliwości i przykłady

Krzysztof Sawicki, Grzegorz Bieszczad, Tomasz Sosnowski, Mariusz Mścichowski
Wojskowa Akademia Techniczna, Instytut Optoelektroniki, Zakład Techniki Podczerwieni i Termowizji, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa 46

Streszczenie: W artykule przedstawiono nową koncepcję zastosowania techniki termowizji – steganografię w termowizji. Steganografia jest techniką ukrywania informacji w sposób nieoczywisty i należy do dziedziny nauk związanych z bezpieczeństwem informacyjnym. W artykule przeanalizowano trzy przykłady steganograficznych kanałów – kanałów komunikacji skrytej wykorzystujące urządzenia termowizyjne na trzy różne sposoby. Pierwsza proponowana metoda korzysta z możliwości kształtowania sceny obserwowanej przez kamerę termowizyjną w taki sposób, żeby w termogramie zawarta była dodatkowa informacja. Druga metoda, nazwana ThermoSteg, korzysta z modyfikacji jednego z parametrów kamery termowizyjnej (czasu integracji) jako sposobu kształtowania sygnału zawierającego informację skrytą. Trzecia metoda bazuje na cyfrowych termogramach i sposobach zastępowania w nich martwych pikseli tworząc tzw. zombie piksele przenoszące informacje skryte. Trzy metody zostały zaimplementowane w rzeczywistych warunkach i potwierdzono ich działanie w praktyce.

Słowa kluczowe: termowizja, steganografia, kanały skryte, promieniowanie podczerwone, mikrobolometry

1. Wprowadzenie

Informacja jest obecnie jednym z podstawowych dóbr, a mechanizmy bezpieczeństwa informacji rozwijają się bardzo szybko. W przypadku większości scenariuszy użytkowania, najlepszym sposobem zabezpieczenia danych jest użycie kryptografii. Jednak w niektórych, szczególnych przypadkach stosuje się podejście alternatywne – steganografię [1, 2]. Steganografia to technika umożliwiająca transmisję danych w sposób skryty. W przypadku steganografii kluczowym czynnikiem jest uczynienie danych „ukrytymi", aby nikt, kto nie jest uprawniony (poinformowany), nie był w stanie odebrać przekazywanej informacji. To podejście różni się od celu kryptografii, gdzie dane mogą być odbierane przez dowolnego odbiorcę, ale nie mogą być odszyfrowane bez znajomości klucza.

Steganografia tworzy tak zwane kanały skryte (ang. *covert channels*) – kanały komunikacyjne, w których dane są przesyłane w sposób skryty. Kluczowym elementem tych skrytych kanałów jest metoda ukrywania danych. Metoda ta powinna być utrzymywana w tajemnicy, analogicznie jak w metodach kryptograficznych, gdzie tajemnicę stanowi klucz szyfrujący. Skryte kanały komunikacyjne można projektować na różne sposoby: zagospodarowując nieużywane bity w nagłówkach protokołów sieciowych, modyfikując parametry czasowe protokołów lub wykorzystując zjawiska, które w większości przypadków są traktowane jako niepożądane lub nieistotne. Większość skrytych kanałów zapewnia przepływność mniejszą niż dziesiątki bitów na sekundę. Istnieją wyrafinowane skryte kanały, które zapewniają przepływność rzędu dziesiątych części bitu na sekundę [2]. Tak niskie wartości przepływności uniemożliwiają korzystanie z ukrytych kanałów do transmisji sygnałów audio lub wideo, ale są wystarczające do sygnalizacji lub podstawowego sterowania urządzeniami. Z punktu widzenia bezpieczeństwa informacyjnego, tak niewielka przepływność nadal stanowi wystarczające parametry do przekazania lub wycieku klucza szyfrującego, prywatnej części podpisu elektronicznego itp. Ponadto niewielka przepływność jest czynnikiem utrudniającym wykrycie kanału skrytego [3].

Skryte kanały mogą być stosowane, gdy fakt obecności komunikacji powinien pozostać tajny np., gdy czujniki poszerzające wiedzę o otoczeniu są umieszczone na wrogim terytorium. Komunikacja steganograficzna między czujnikami utrudni ich wykrycie. Innym, typowym zastosowaniem steganografii może być komunikacja implementowana w tzw. trojanach sprzętowych, czyli ukrytych, nieudokumentowanych funkcjach urządzeń, często służących do zapewnienia możliwości sterowania urządzeniami poza wiedzą jego uprawnionego użytkownika.

Skryte kanały i ich zastosowanie to popularny temat badawczy. Zasady tworzenia kanałów skrytych zostały opisane w 1989 r. [4]. Od tego czasu opublikowano wiele nowych i bardziej wyrafinowanych rodzajów kanałów skrytych. Jedną z najbardziej eksploatowanych tematyk jest steganografia w sieciach teleinformatycznych, która wyróżnia dwa rodzaje skrytych kanałów:

Autor korespondujący:
Krzysztof Sawicki, krzysztof.sawicki@wat.edu.pl

Artykuł recenzowany
nadesłany 12.06.2021 r., przyjęty do druku 18.08.2021 r.

kanały czasowe i kanały pojemnościowe. Pierwszy typ używa modulacji odstępu między dwoma zdarzeniami sieciowymi, np. początkami transmisji pakietów w kanałach bezprzewodowych [5]. Drugi typ, kanały pojemnościowe, wykorzystuje nieużywane lub modyfikuje częściowo używane pola w protokołach sieciowych. Przykładowy pojemnościowy kanał skryty tworzy metoda Stego-Beacon, która eksploatuje pola Timestamp w ramkach Beacon sieci IEEE 802.11 do transmisji informacji [6]. Skryte kanały mogą być również zaimplementowane w innych typach mediów, takich jak dźwięk [7] i obrazy statyczne oraz dynamiczne [8].

Duży wybór różnych typów skrytych kanałów sprawia, że jest to interesujący temat dla zespołów zajmujących się bezpieczeństwem teleinformatycznym w szerokim zakresie. Skryte kanały mogą stanowić narzędzie potencjalnych naruszeń bezpieczeństwa i mogą być użyte do wycieku danych z systemów komputerowych izolowanych od sieci. Przeprowadzono wiele eksperymentów potwierdzających tę możliwość. Przykładowo możliwe jest zastosowanie obrazów o bardzo niskim kontraście lub szybko migoczących, niewidocznych dla ludzi, do przesyłania danych za pomocą wyświetlacza komputera [9]. Innym sposobem jest użycie stosunkowo taniego sprzętu do wykrywania emisji elektromagnetycznej z USB [10].

Promieniowanie cieplne można również wykorzystać jako podstawę dla utworzenia kanału skrytego. Dwa odizolowane sieciowo komputery, mogą komunikować się za pośrednictwem skrytego kanału termicznego. Jeden z komputerów – komputer nadawczy – moduluje obciążeniem procesora, co powoduje zmiany ilości wydzielanego przez ten komputer ciepła. Odczytując czujniki temperatury na drugim komputerze – komputerze odbiorczym [11] otrzymywany jest sygnał, w którym detekowalny jest wpływ ciepła wydzielanego przez sąsiadujący komputer nadawczy. Stworzony w ten sposób kanał skryty umożliwia transmisję steganograficzną z przepływnością 8 bitów na godzinę na odległość do 40 cm.

W niniejszym artykule przedstawione zostały możliwości nieoczywistego użycia kamer termowizyjnych do transmisji danych w sposób skryty. Analizom poddano trzy koncepcje, których działanie zostało potwierdzone eksperymentalnie.

2. Analiza proponowanych metod transmisji skrytych z użyciem kamer termowizyjnych

Oczywistym faktem jest, że kamery termowizyjne nie służą do realizacji klasycznych kanałów komunikacyjnych. Ich podstawowy cel jest klarowny. Jednak modyfikując bądź analizując scenę lub różne parametry kamery w trakcie jej działania, istnieje możliwość uzyskania dodatkowego efektu ubocznego – transmisji dodatkowej informacji. W analizie tej skupimy się na trzech sposobach: ukryciu informacji w obserwowanym termogramie, ukryciu informacji przez modyfikację parametrów konfiguracyjnych kamery oraz ukryciu informacji w cyfrowym termogramie.

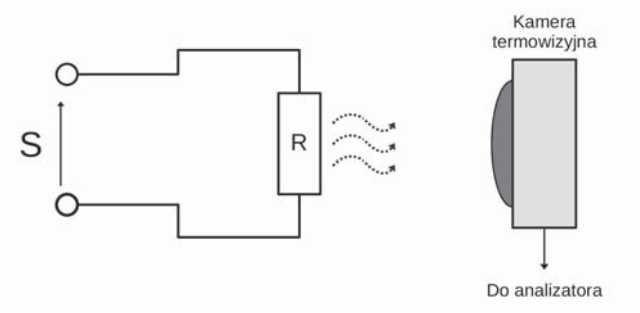
2.1. Termogram jako sygnał niosący informację skrytą

W zarejestrowanym przez kamerę termowizyjną obrazie – termogramie – uzyskujemy informację, w dużym uproszczeniu, o rozkładzie natężenia promieniowania podczerwonego emitowanego przez obserwowaną scenę. Zakładając, że istnieje możliwość wpływu na natężenie promieniowania elementów sceny, możemy wyobrazić sobie, że modyfikując natężenie promieniowania wybranych punktów obserwowanej sceny, jesteśmy w stanie zakodować w tym natężeniu informację. Analizując zmiany natężenia promieniowania przy pomocy kamery termowizyjnej (lub w najprostszym przypadku przy pomocy pirometru), istnieje możliwość rozróżnienia dwóch podstawowych stanów – niskiego natężenia promieniowania lub wysokiego natężenia promieniowania. Te dwa stany można interpretować wprost jako dwie różne wartości pojedynczego bitu informacji. Ponieważ zmiany natężenia promieniowania cieplnego nie są widoczne dla ludzkiego oka oraz niewielkie zmiany natężenia promieniowania cieplnego mogą nie być zauważone w termogramie przez obserwatora, możemy mówić o takiej metodzie transmisji, jako o metodzie steganograficznej. Podobna koncepcja, stosująca aktywne oświetlanie laserem została przedstawiona w [12].

Wyobraźmy sobie sytuację, w której kamera termowizyjna obserwuje scenę zawierającą rezystor – najprostszy pasywny element elektroniczny (Rys. 1). Rezystor zasilony jest napięciem przenoszącym sygnał S, którego charakter jest binarny – pojawia się prąd lub prądu nie ma. Przepływ prądu powoduje nagrzanie rezystora zgodnie z prawem Joule'a. Rezystor emituje zmienne natężenie promieniowania, które jest następnie odbierane przez kamerę termowizyjną. Analiza danych z kamery termowizyjnej pozwala na wyselekcjonowanie z całego termogramu obszaru P, w którym analizowany jest sygnał jedynie z interesującego obiektu, będącego nadajnikiem informacji skrytej. Dla obszaru P należy wyznaczyć sygnał $\overline{S}_P(n)$ złożony ze średnich wartości obszaru w czasie obserwacji:

$$\overline{S}_P(n) = \frac{\sum_{x=0}^{X}\sum_{y=0}^{Y} P_{xy}(n)}{X \cdot Y} \tag{1}$$

gdzie X to szerokość wyznaczonego obszaru P, Y to jego wysokość, natomiast $P_{xy}(n)$ to wartość piksela na pozycji (x, y) -tego termogramu.



Rys. 1. Najprostszy układ do nadawania i odbioru danych przez modulację natężenia promieniowania
Fig. 1. The simplest system for transmitting and receiving data by modulating the intensity of radiation

Sygnał $\overline{S}_P(n)$ będzie zmieniał się w takt nagrzewania oraz schładzania obserwowanego obiektu, a zatem będzie odwzorowywał takt zmian sygnału wejściowego S. Dokonując prostej klasyfikacji progowej sygnału $S_P(n)$ uzyskamy sygnał $S_{Pb}(n)$:

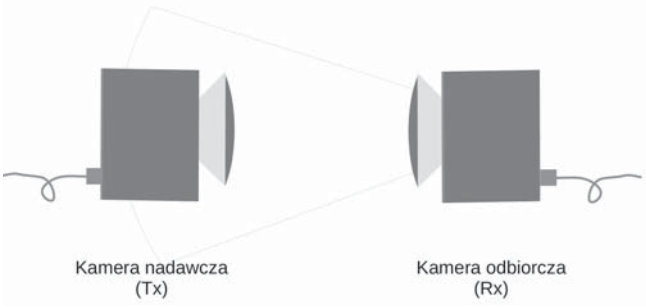
$$S_{Pb}(n) = \begin{cases} 0 & \text{gdy } \overline{S}_P(n) < P_t \\ 1 & \text{w pozostalych przypadkach} \end{cases} \tag{2}$$

gdzie P_t jest eksperymentalnie dobraną wartością progową. Próbkując sygnał $S_{Pb}(n)$ z częstością zmian sygnału S otrzymywany jest sygnał binarny zawierający informację, która modulowała sygnał S.

Taki kanał skryty można opisać dwoma podstawowymi parametrami: bitową stopą błędów (BER) oraz przepływnością binarną B_d. Wartości tych parametrów zależą od wielu czynników, które mają wpływ na ilość energii rejestrowaną przez kamerę. Tymi czynnikami są: stała czasowa układu nadawczego, jego emisyjność, NETD kamery, stała czasowa detektora kamery, transmisyjność atmosfery itp.

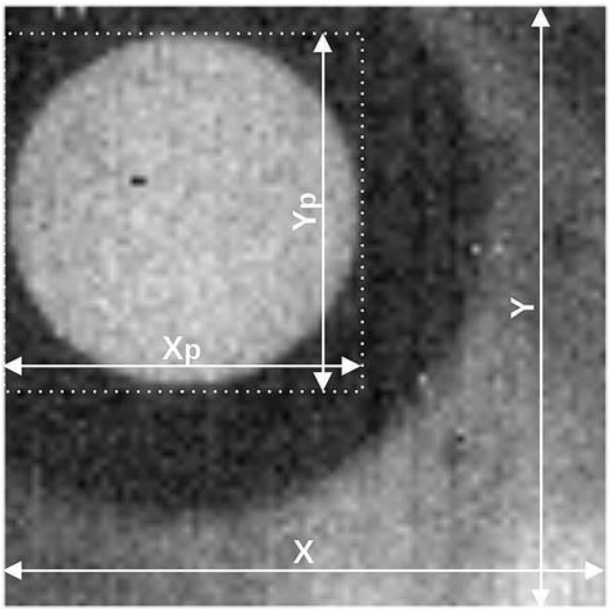
2.2. Modyfikacja parametrów kamery termowizyjnej jako nośnik informacji skrytej – metoda ThermoSteg

W proponowanym rozwiązaniu dwie mikrobolometryczne kamery termowizyjne są zwrócone obiektywami ku sobie (Rys. 2). Jedna z kamer funkcjonuje jako nadajnik informacji skrytych (Tx) natomiast druga jako ich odbiornik (Rx).



Rys. 2. Kamera nadająca informacje skryte (Tx) oraz kamera odbierająca (Rx)
Fig. 2. The transmitting covert information camera (Tx) and the receiving camera (Rx)

W obszarze obserwowanym przez kamerę Rx można wyróżnić obszar, w którym widoczna jest soczewka kamery Tx ROI (ang. *Region of Interest*). Obszar ten o wymiarach $X_p \cdot Y_p$ pikseli jest zaznaczony na Rys. 3. Należy dodać, że obie kamery pracują w normalnym trybie umożliwiającym rejestrację termogramów i tworzony kanał komunikacji skrytej nie powoduje ograniczenia możliwości zasadniczej pracy kamery.



Rys. 3. Obraz rejestrowany przez kamerę Rx po korekcji niejednorodności. W wyróżnionym kwadracie widoczny obiektyw kamery Tx. Widoczny wokół obiektywu ciemny okrąg to jego metalowa obudowa
Fig. 3. The image recorded by the Rx camera after the non-uniformity correction. The Tx camera lens is visible in the highlighted square. The dark circle around the lens is its metal housing

Kamera Tx korzysta z matrycy mikrobolometrów. Metoda odczytu danych z takiej matrycy polega na odczycie wartości z kolejnych wierszy sensorów. W trakcie odczytu wiersza sensorów w matrycy, przez odczytywany wiersz sensorów przepływa prąd, co powoduje chwilowe zwiększenie temperatury bolometrów umieszczonych w tym wierszu. Zmiana temperatury wiersza jest widoczna w termogramie rejestrowanym przez kamerę Rx jako linia o większej jasności.

2.2.1. Kodowanie danych

Kodowanie danych skrytych jest realizowane przy pomocy zmiany jednego z parametrów matrycy mikrobolometrów – czasu integracji (t_i). Zmniejszenie tego czasu powoduje, że przez wiersz w matrycy bolometrów prąd płynie krócej, czego efektem jest słabsze samonagrzewanie się elementów z odczytywanego aktualnie wiersza. Analogicznie, zwiększenie t_i spowoduje większe nagrzanie się elementów aktualnie odczytywanego wiersza. Różnice te można zdetekować za pomocą kamery odbiorczej. Szczegółowy opis działania układu odczytującego w matrycy mikrobolometrów oraz jego właściwości termodynamiczne przedstawione zostały w [13]. Dane skryte są kodowane dwuwartościowo za pomocą dwóch różnych czasów integracji t_{i1} oraz t_{i2}.

2.2.2. Odbiór danych

W obszarze obserwowanym (ROI) znajduje się $X_p \cdot Y_p$ pikseli. Dla zwiększenia stosunku mocy sygnału do szumu, wyliczana jest średnia wartość wszystkich obserwowanych pikseli F_n dla każdego termogramu:

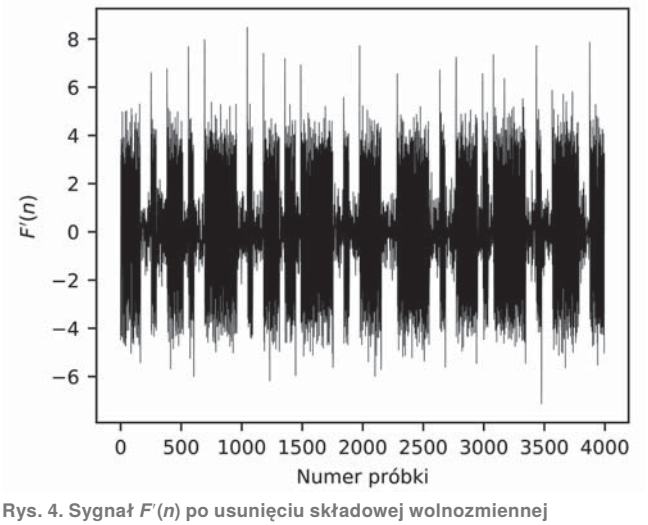
$$F(n) = \frac{\sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} p_{xy}(n)}{(x_2 - x_1)(y_2 - y_1)} \tag{3}$$

gdzie $p_{xy}(n)$ to wartość piksela o współrzędnych (x, y) w n-tym termogramie, x_1 oraz x_2 to numery pierwszej i ostatniej kolumny analizowanego obszaru, natomiast y_1 oraz y_2 to numery pierwszego i ostatniego wiersza analizowanego obszaru. Powstaje w ten sposób zbiór $F = \{F(0), F(1), \ldots, F(N)\}$, który jest sygnałem próbkowanym z częstotliwością pracy kamery f_p. Konieczność uśredniania w operacji (3) pozwala wyeliminować dryft temperaturowy kamery.

W przebiegu sygnału F są zauważalne zmiany o niskiej częstotliwości wynikające z oddziaływania czynników zewnętrznych, tj. zmiany temperatury otoczenia kamery. Do dalszej analizy należy odfiltrować jedynie zmiany o wyższej częstotliwości:

$$F'(n) = F(n) - \frac{\sum_{i=n-w}^{n} F(i)}{w} \text{ dla } n = \{w, w+1, \ldots, N\} \tag{4}$$

gdzie $F'(n)$ to n-ta próbka sygnału F', to długość sygnału F, w to szerokość zastosowanego okna. Szerokość okna w należy dobrać eksperymentalnie do charakteru zmian obserwowanych w sygnale. Wynikowy przykładowy sygnał $F'(n)$ jest przedstawiony na rys. 4.



Rys. 4. Sygnał $F'(n)$ po usunięciu składowej wolnozmiennej
Fig. 4. $F'(n)$ signal after removal of low frequency components

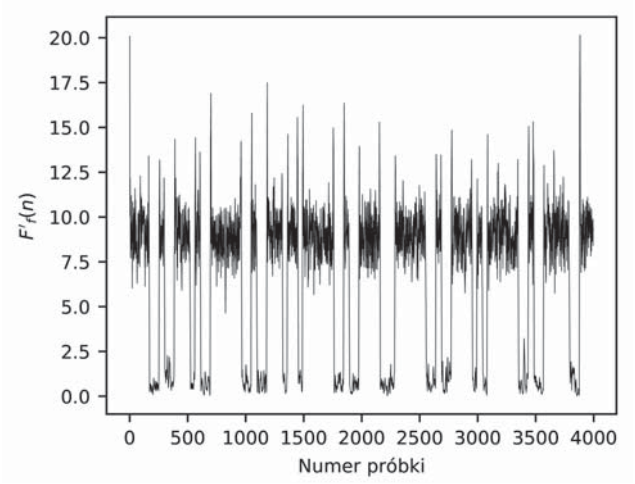
Na rys. 4 wyraźnie widać momenty większej oraz mniejszej amplitudy sygnału. Z punktu widzenia pomiaru zmienności sygnału istotną informację niesie moc sygnału:

$$F'_p(n) = \left[F'(n)\right]^2 \tag{5}$$

Sygnał $F'_p(n)$ jest następnie uśredniany w oknie czasowym o szerokości w'. Wynikiem tego uśrednienia jest sygnał $F'_f(n)$ obliczony z (6). Przykładowy sygnał uzyskany w ten sposób przedstawiono na Rys. 5:

$$F'_f(n) = \frac{\sum_{i=n-w'}^{n} F'_p(i)}{w'} \tag{6}$$

Wartość w' została dobrana eksperymentalnie z uwzględnieniem charakteru otrzymanego sygnału.



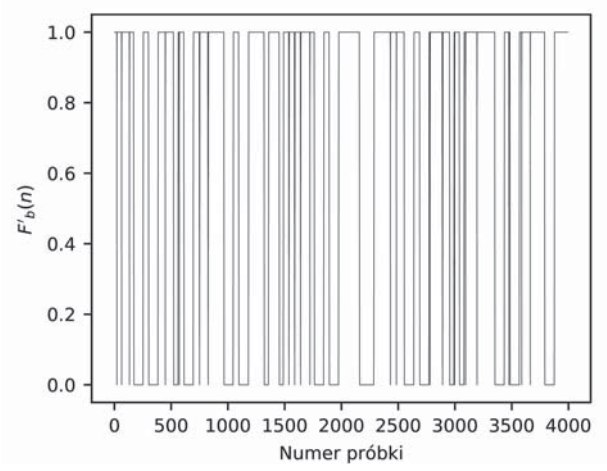
Rys. 5. Sygnał $F'_f(n)$
Fig. 5. $F'_f(n)$ signal

W sygnale $F'_f(n)$ wyraźnie widać przebieg o charakterze binarnym. Aby utworzyć binarny sygnał $F'_b(n)$ należy dokonać progowej klasyfikacji próbek:

$$F'_b(n) = \begin{cases} 1 & \text{gdy } F'_f(n) \geq \overline{F}'_f \\ 0 & \text{gdy } F'_{fn} < \overline{F}'_f \end{cases} \tag{7}$$

gdzie F'_f to średnia wartość wszystkich próbek sygnału $\overline{F}'_f$.

Przykład sygnału F'_b jest przedstawiony na Rys. 6. Charakter sygnału F'_b odpowiada sygnałowi wymuszenia sygnałem odpowiadającym danym skrytym po stronie kamery Tx.



Rys. 6. Binarny sygnał $F'_b(n)$
Fig. 6. $F'_b(n)$ binary signal

Istnieje zatem możliwość wydobycia sygnału F'_b, czyli binarnej informacji skrytej odpowiadającej informacji osadzonej pierwotnie w sygnale F.

2.2.3. Dekodowanie danych

Sygnał binarny F'_b to sygnał próbkowany z częstotliwością pracy kamery f_p. Natomiast jeden bit informacji skrytej jest zapisany w ciągu jednakowych wartości próbek sygnału F'_b o określonej liczbie próbek sygnału na jeden bit skryty W:

$$W = \frac{f_p}{B} \tag{8}$$

gdzie B to założona skryta przepływność binarna (np. 2 b/s). Na podstawie tej informacji realizowany jest proces dekodowania ciągu binarnego. Algorytm dekodowania znajduje moment wystąpienia pierwszej zmiany wartości próbki wejściowego sygnału F'_b, uznając to za początek bitu skrytego. Następnie algorytm uśrednia wartość W próbek liczonych od początku bitu skrytego. Jeśli średnia wartość tych próbek jest większa od 0,5, to jest to klasyfikowane jako skryty bit . W przeciwnym przypadku jest to skryty bit .

2.3. Zombie piksele – cyfrowa manipulacja termogramem

Trzecia proponowana metoda steganografii w termowizji korzysta z niepożądanej cechy matryc stosowanych w kamerach termowizyjnych – relatywnie dużej (większej niż w matrycach kamer widzialnych) liczby uszkodzonych pikseli. W matrycach kamer termowizyjnych występują sensory, z których odczytana wartość nie zmienia się w zależności od obserwowanej sceny. Mogą to być tzw. martwe piksele (ang. *dead pixels*) lub gorące piksele (ang. *hot pixels*). Dla lepszego zobrazowania, stosowane są metody zastępowania wartości odpowiadających tym pikselom w termogramie wartościami, które nie pogarszają parametrów statystycznych termogramu. Metody zastępowania wartości martwych i gorących pikseli są dobrze opisane w literaturze [14, 15].

Jednym z najprostszych sposobów zastępowania wartości uszkodzonych pikseli jest zastąpienie go wartością średnią obliczoną z wartości jego najbliższych sąsiadów z tego samego wiersza termogramu:

$$\overline{v}(n) = \frac{v(n-1) + v(n+1)}{2} \tag{9}$$

gdzie $v(n)$ to wartość piksela w pozycji n.

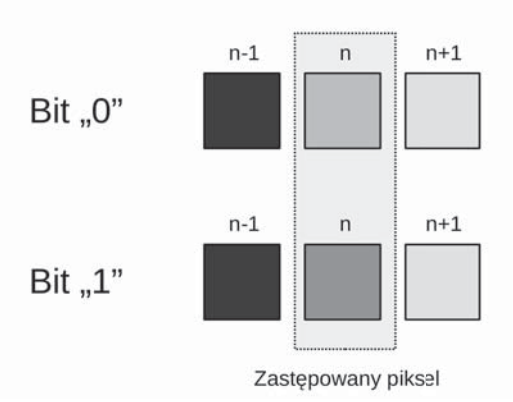
Wartość zastąpionego piksela nie wnosi do termogramu dodatkowej informacji o scenie – jest redundantna. Charakterystyką uszkodzonych pikseli jest to, że występują w każdej, rejestrowanej przez kamerę ramce termogramu. Oznacza to, że w cyfrowym strumieniu danych przychodzącym z kamery mamy wewnętrzny strumień redundantnych danych o przepływności:

$$B_d = f_p \cdot L \cdot bpp \tag{10}$$

gdzie f_p to liczba ramek generowanych przez kamerę w ciągu sekundy, L to liczba uszkodzonych pikseli w termogramie, natomiast bpp to liczba bitów przypadających na jedną próbkę (piksel). Przykładowo, jeśli w termogramie jest tylko jeden uszkodzony piksel, kamera rejestruje 30 klatek w ciągu sekundy a każdy piksel zapisywany jest za pomocą 16-bitowej liczby, to redundantny strumień danych ma przepływność $B_d = 480\ b/s$.

Istnieje prosta możliwość wykorzystania tego faktu do transmisji dodatkowej, skrytej informacji. Do kodowania informacji należy zastosować prostą zależność: jeśli kodowany bit informacji skrytej ma wartość 0, to wartość zastępująca wartość uszkodzonego piksela powinna być mniejsza od wartości średniej $\overline{v}(n)$.

W przypadku skrytego bitu 1, wartość zastępująca powinna być wyższa od średniej. Dzięki temu istnieje możliwość wprowadzenia jednego bitu informacji skrytej na każdy uszkodzony piksel termogramu. Różnice między zastępującą wartością, a wartością średnią $\overline{v}(n)$ powinny być możliwie najmniejsze, np. {–1, +1} – wartości te tworzą zbiór wprowadzanych różnic. Przykładowo, jeśli uszkodzony jest piksel na pozycji 9., piksel na pozycji 8. ma wartość cyfrową 23 921, a piksel na pozycji 10. ma wartość cyfrową 23 893, to wartość $\overline{v}(10)$ wynosi 23 907. Aby zakodować skryty bit 0, piksel na pozycji 10. zastąpiony zostanie wartością 23 906, a w przypadku bitu skrytego 1 wartością 23 908. Przykład takiego kodowania przedstawiono na Rys. 7. W przypadku kodowania wartości piksela na 16 bitach, zmiana cyfrowej wartości o ±1 oznacza zmianę wartości piksela o 0,0015 % w stosunku do całego zakresu możliwych wartości.



Rys. 7. Przykład kodowania bitu informacji skrytej w zombie pikselu
Fig. 7. The example of covert bit coding in the zombie pixel

Jeśli powiększymy zbiór wprowadzanych różnic, np. {–2, –1, +1, +2}, uzyskamy możliwość przesłania więcej niż jednego bitu informacji skrytej w każdym uszkodzonym pikselu. Rozmiar zbioru wprowadzanych różnic należy dobrać eksperymentalnie mając na uwadze charakterystykę strumienia termogramów.

Wykorzystując sygnał uszkodzonych pikseli w ten sposób istnieje możliwość przesłania dodatkowego strumienia danych skrytych o przepływności:

$$B_s = f_p \cdot L \cdot \log_2(n) \tag{11}$$

gdzie N to rozmiar zbioru wprowadzanych różnic. Przykładowo, jeśli kamera rejestruje 30 klatek na sekundę, w termogramie jest tylko jeden uszkodzony piksel, a rozmiar zbioru wprowadzanych różnic wynosi 2, to w ten sposób stworzony kanał komunikacji skrytej pozwala na przesłanie 30 b/s. W zastosowaniach steganograficznych jest to duża wartość.

Uszkodzony piksel, który do tej pory był martwym lub gorącym pikselem, zaczyna przenosić pewną informację skrytą – staje się tzw. zombie pikselem.

Metoda eksploatująca zombie piksele jest tzw. nieślepą metodą steganograficzną (ang. *non-blind steganographic method*). Odbiornik danych skrytych musi mieć *a priori* wiedzę o pozycjach zombie pikseli w termogramie. Odczytaną wartość zombie piksela porównuje się z odpowiadają mu wartością $\overline{v}(n)$ i na tej podstawie dokonuje klasyfikacji bitu skrytego.

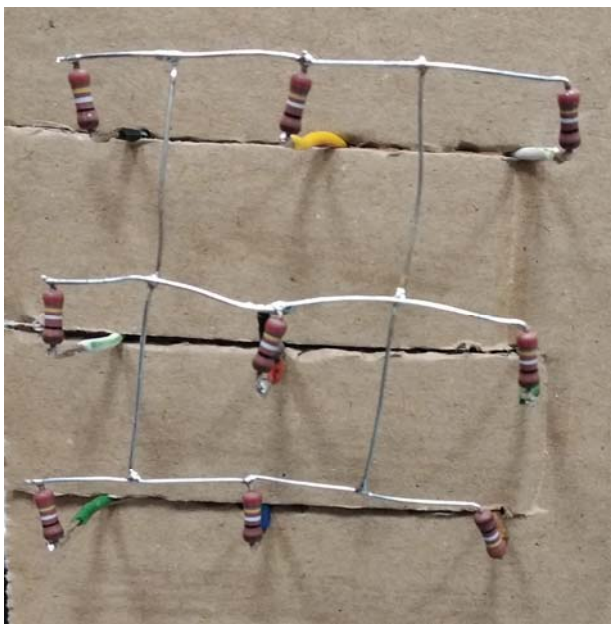
Dane skryte, które zostały zakodowane tym sposobem, nie zostaną zmodyfikowane ani utracone jeśli strumień termogramów nie zostanie poddany np. kompresji stratnej. Wynika to z faktu, że dane skryte są wprowadzane już w cyfrowej reprezentacji termogramów. Ponieważ zastępowanie wartości uszkodzonych pikseli najczęściej ma miejsce już w samej kamerze, to koderem informacji skrytej staje się właśnie ta kamera. Zombie piksele mogą zatem być użyte jako kanał komunikacji dla sprzętowego trojana wbudowanego w kamerę termowizyjną lub do celów cyfrowego znakowania obrazów (watermarking), dodawania znaczników czasu (timestamping) lub skrytego podpisu elektronicznego termogramu, na przykład do celów dowodowych.

3. Badania eksperymentalne

W celu potwierdzenia praktycznej możliwości transmisji danych skrytych w termogramie wykonane zostały eksperymenty, które potwierdziły skuteczność działania tych metod.

3.1. Badanie możliwości transmisji informacji skrytej przez modyfikację sceny

Do eksperymentu została użyta prosta matryca złożona z dziewięciu rezystorów o nominalnej mocy 0,25 W (rys. 8).



Rys. 8. Matryca rezystorów użyta w eksperymencie
Fig. 8. Resistor matrix used in the experiment

Rezystory były podłączone do wyjść cyfrowych układu Arduino Nano, dzięki czemu istniała możliwość swobodnego sterowania każdym z nich z osobna. W trakcie eksperymentu rejestrowane były termogramy przy pomocy kamery termowizyjnej wyposażonej w matrycę mikrobolometryczną firmy Lynred o rozdzielczości 640 × 480 pikseli. Kamera była oddalona od matrycy rezystorów o około 1,5 m, a obszar obrazu zawierający matrycę rezystorów zajmował około 10 % całej powierzchni termogramu. Przez wybrane rezystory płynął prąd o natężeniu 20 mA. Efektem przepływu prądu było wydzielanie się ciepła na rezystorach. W ramach sprawdzenia możliwości przesłane zostały dwa wzory za pomocą matrycy rezystorów odpowiadające dziewięciobitowym ciągom binarnym 1010101 oraz 010101010. Wzory zostały przedstawione na rys. 9a) oraz 9b). Czas trwania każdego wzoru wynosił $t_s = 20$ s, między wzorami była przerwa $t_p = 20$ s, w trakcie której nie płynął prąd przez żaden z rezystorów. Kamera rejestrowała dane z częstością $f_p = 5$ Hz.

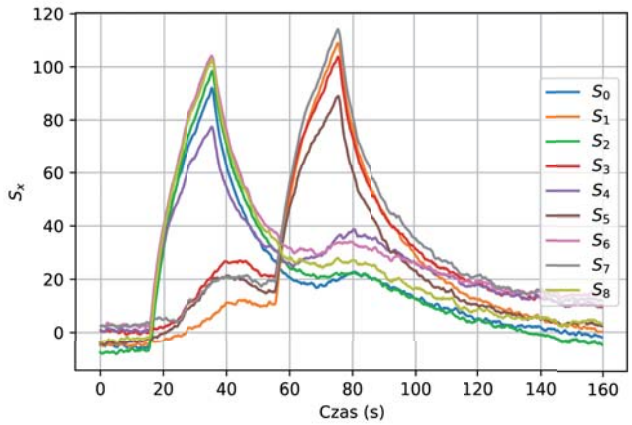
Po zarejestrowaniu termogramów dokonano prostej analizy obrazu polegającej na wyznaczeniu obszarów termogramu, które odpowiadają poszczególnym rezystorom. Dla każdego z wyznaczonych obszarów wyliczono wartość średnią pikseli w obszarze, a następnie od tej wartości odjęto wartość średnią całego termogramu w celu zlikwidowania wpływu dryftu kamery i temperatury otoczenia:

$$S_x(n) = \overline{S}(n) - \overline{F}(n) \tag{12}$$

gdzie $\overline{S}(n)$ to średnia wartość obszaru w n-tej ramce a $\overline{F}(n)$ to wartość średnia n-tej ramki całego termogramu. Wyniki analizy zostały przedstawione na Rys. 10.

a) b)

Rys. 9. Termogramy z zarejestrowanymi wzorami na matrycy rezystorów: a) sygnał binarny 101010101, b) sygnał binarny 010101010
Fig. 9. Thermograms with patterns registered on a matrix of resistors: a) binary signal 101010101, b) binary signal 010101010



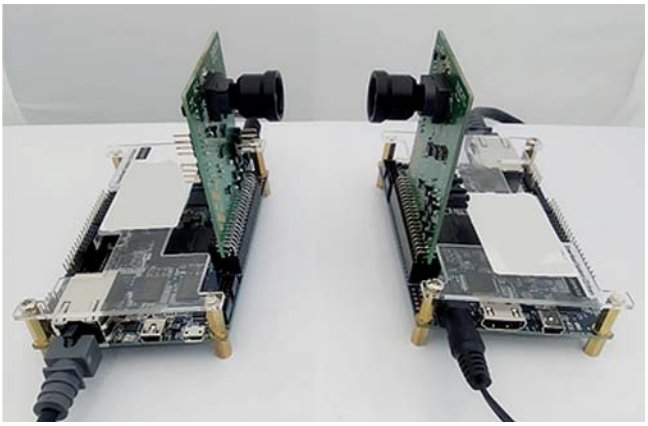
Rys. 10. Wartości sygnałów wyznaczone w eksperymencie
Fig. 10. Values of signals determined in the experiment

Na wykresie (Rys. 10) wyraźnie widać momenty, w których prąd płynął przez rezystory. Tym samym łatwo można zdetekować czy rezystor przekazywał bit "1" lub "0" skrytej informacji. Pierwszy wzór (Rys. 9a) złożony z pięciu włączonych rezystorów widać wyraźnie w czasie $t_1 = 20$ s do $t_2 = 40$ s. Drugi wzór złożony z czterech włączonych rezystorów jest natomiast widoczny w czasie $t_3 = 60$ s do $t_4 = 80$ s. Przebadany kanał skryty, w zastosowanej konfiguracji, pozwolił na przesłanie 9 bitów informacji skrytej w ciągu 20 sekund, czyli przepływność binarna kanału wyniosła $B_d = 0{,}45$ b/s. Tę wartość można poprawić skracając czas nagrzewania rezystorów oraz dodając nowe rezystory do matrycy, jednak nie było celem tego artykułu badanie granicznej wartości przepływności binarnej metody, a jedynie zasygnalizowanie możliwości metody.

3.2. Badanie możliwości transmisji skrytej przez modyfikację parametrów pracy kamery termowizyjnej – metoda ThermoSteg

W trakcie eksperymentów korzystano z dwóch kamer termowizyjnych używających układów FPGA Cyclone V oraz matryc Lynred Micro80 (o rozdzielczości 80 × 80 pikseli) [1]. Matryce kamer ustawione były na przeciwko siebie w odległości 14 cm (Rys. 11). Kamery pracowały pod kontrolą systemu GNU/Linux i transmitowały dane z użyciem dedykowanego protokołu opartego o UDP przez sieć pracującą w standardzie Gigabit Ethernet. Kamery generowały termogramy z częstością $f_p = 45$ Hz. Analiza odbywała się w oprogramowaniu napisanym w języku Python na komputerze typu PC.

W celu wyznaczenia parametrów metody, dokonano prób transmisji 100 pakietów danych o długości 32 bitów każdy. Pakiety danych poprzedzane były ośmiobitową preambułą, która służyła jako znacznik ich początku. Eksperyment powtórzono dla trzech różnych zakładanych przepływności binarnych $W = \{1, 2, 4\}$ b/s oraz trzech zestawów czasów integracji: t_{i1} = (82,05 µs; 328,21 µs), t_{i2} = (123,08 µs; 287,18 µs), oraz t_{i3} = (164,10 µs; 246,15 µs). Podczas wyznaczania bitowej stopy błędów nie były uwzględniane ewentualne błędy w preambułach.



Rys. 11. Kamery użyte w eksperymencie
Fig. 11. Cameras used in the experiment

Tabela 1. Bitowa stopa błędów
Table 1. Bit Error Rate

	t_{i1}	t_{i2}	t_{i3}
1 b/s	0,00 %	0,03 %	4,28 %
2 b/s	5,87 %	12,09 %	9,06 %
4 b/s	18,94 %	18,78 %	18,74 %

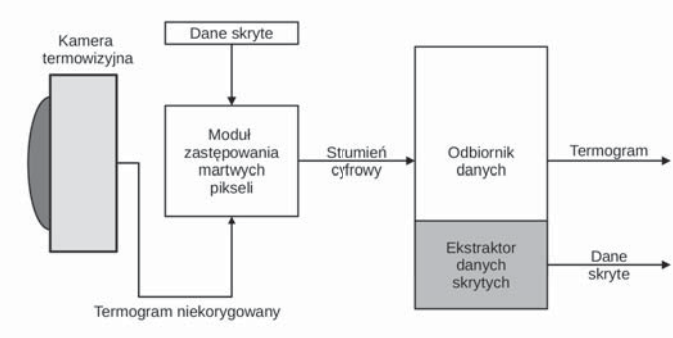
Dla przepływności 1 b/s i dwóch zestawów czasów integracji udało się zdekodować informacje bezbłędnie lub niemal bezbłędnie. Dla zastosowanej przepływności 2 b/s uzyskane stopy błędów w zakresie ok. 6 % stwarzają szanse na bezbłędną transmisję przy zastosowaniu kodów korekcyjno-detekcyjnych w warstwie informacyjnej. Uzyskane wyniki potwierdziły praktyczną możliwość utworzenia kanału skrytego metodą ThermoSteg. Wartości bitowej stopy błędów dla przepływności większych niż 2 b/s mogą stanowić istotną przeszkodę w realizacji komunikacji.

3.3. Badanie możliwości transmisji skrytej z użyciem zombie pikseli

Eksperyment przeprowadzono z użyciem kamery mikrobolometrycznej wyposażonej w matrycę 80 × 80 pikseli firmy Lynred. Matryca miała dwa martwe piksele, które stały się nośnikiem informacji skrytej — zombie pikselami. Kamera rejestrowała ramki z częstością $f_p = 45$ Hz. Strumień danych generowany przez kamerę miał przepływność $B_j = 80 \cdot 80 \cdot 45$ Hz $\cdot 16$ $bpp = 4\ 608\ 000$ b/s.

W kamerze uruchomiono programowy moduł zastępowania martwych pikseli, a cały układ transmisyjny był zbudowany jak przedstawiono na Rys. 12. Do transmisji zastosowano dwuelementowy zestaw wprowadzanych różnic, co pozwoliło na przesłanie jednego bita skrytego w każdym martwym pikselu w każdej ramce. Przepływność takiego skrytego kanału wyniosła $B_s = 45$ Hz $\cdot\ 2 \cdot \log_2(2) = 90$ b/s.

Dane rejestrowane były przez odbiornik danych wyposażony w ekstraktor danych skrytych. Po przetransmitowaniu 1000



Rys. 12. Schemat eksperymentu z transmisją skrytą korzystającą z zombie pikseli
Fig. 12. The idea of experiment with zombie pixels

ramek, w których osadzonych zostało 2000 bitów udało się po stronie odbiorczej, w sposób bezbłędny, odzyskać 2000 bitów skrytych. Potwierdziło to skuteczność proponowanego kanału skrytego. Zerowa stopa błędów w tej metodzie wynika z realizacji metody już w cyfrowym strumieniu danych, wolnym od zakłóceń.

4. Podsumowanie

Przedstawione w artykule przykłady metod ukrywania informacji w termowizji udowadniają, że nieoczywiste zastosowanie tej techniki do transmisji może być z sukcesem zaimplementowane w praktyce. Przepływności binarne danych skrytych w utworzonych kanałach komunikacji są niewielkie w porównaniu do przepływności uzyskiwanych w nowoczesnych jawnych łączach teleinformatycznych, jednak wystarczające do realizacji zarówno celów nieporządnych jak i uzyskania dodatkowych funkcjonalności. Kanały steganograficzne, ze swej natury, muszą cechować się niewielkimi przepływnościami, aby zachować odporność transmisji na czynniki degradujące oraz pozostać trudnymi do wykrycia [17].

Uzyskane przepływności kanałów skrytych są odpowiednie dla typowych zastosowań steganografii. Przykładowo, korzystając z prezentowanej metody ThermoSteg, możliwe jest ujawnienie 256-bitowego klucza kryptograficznego dowolnej kamerze termowizyjnej obserwującej kamerę nadawczą, w czasie ok. 4 minut. Taka transmisja dużo szybciej dokona się przy użyciu zombie pikseli, nawet jeśli będzie to tylko jeden zombie piksel w termogramie. Demonstracja takiego kanału komunikacji może przyczynić się do szerszych badań potencjalnych mechanizmów nadużyć bezpieczeństwa w sprzęcie dotychczasowo uznawanym za sprzęt o niskim ryzyku wycieku informacji. Instytucje zajmujące się audytami bezpieczeństwa powinny być zainteresowane opracowaniem obszerniejszych metod badania tego typu sprzętu. Ze względu na stale rosnącą liczbę urządzeń działających w tak zwanej technologii „Internet of Things", również takich, które zawierają tanie kamery termowizyjne, przedstawiony temat jest ważny w kontekście bezpieczeństwa. Większość z tych urządzeń ma oprogramowanie układowe o zamkniętym kodzie źródłowym, w którym można wdrożyć podobne metody steganograficzne i ujawniać poufne lub prywatne informacje. W trosce o bezpieczeństwo powinno wzrosnąć znaczenie oprogramowania typu open source i urządzeń z otwartym sprzętem. Artykuł pokazuje, że stosunkowo szybki kanał ukryty może być łatwo opracowany i zaimplementowany w ogólnie dostępnych urządzeniach.

Steganografia w termowizji tworzy również zupełnie nowe, do tej pory nie rozważane, rozwiązanie problemu transmisji w warunkach tzw. ciszy radiowej, podczas której nie mogą być używane klasyczne środki łączności bezprzewodowej. Mogą być do tego celu wykorzystane dwie metody: metoda modyfikacji sceny oraz metoda ThermoSteg. Ich działanie, z punktu widzenia odbiorników łączności bezprzewodowej, jest niezauważalne, a informacja nie jest ukrywana w zwykłych transmisjach radiowych. Wykrycie takiej transmisji skrytej wymaga zastosowania bardzo trudno dostępnych analizatorów widma dla wysokich częstotliwości oraz nieszablonowego sposobu analizy sygnałów. Ta cecha pozwala na zastosowanie metod steganografii w termowizji np. na polu walki do przekazywania komunikatów awaryjnych lub niestandardowego sposobu uwierzytelniania korespondencji radiowej.

Podziękowania i informacje

Projekt był częściowo finansowany w ramach pracy naukowej finansowanej przez Narodowe Centrum Badań i Rozwoju, projekt nr DOB-2P/02/09/2018 oraz częściowo z funduszy badawczych Instytutu Optoelektroniki WAT.

Metoda ThermoSteg jest przedmiotem zgłoszenia patentowego nr WIPO ST 10/C PL437673.

Bibliografia

1. Mishra R., Bhanodiya P., *A Review on Steganography and Cryptography*. [In:] 2015 International Conference on Advances in Computer Engineering and Applications, 119–122. DOI: 10.1109/ICACEA.2015.7164679.
2. Lubacz J., Mazurczyk W., Szczypiorski K., *Principles and Overview of Network Steganography*. "*IEEE Communications Magazine"*, Vol. 52, no. 5, 2014, 225–229, DOI: 10.1109/MCOM.2014.6815916.
3. Griberman D., 2013. *Development of Requirements Specification for Steganographic Systems*.
4. Wolf M., *Covert Channels in LAN Protocols*. [In:] *Local Area Network Security Workshop*, 89–101, 1989. Springer, DOI: 10.1007/3-540-51754-5_33.
5. Tahmasbi F., Moghim N., Mahdavi M., *Adaptive Ternary Timing Covert Channel in IEEE 802.11*. "Security and Communication Networks", Vol. 9 (16). Wiley Online Library: 3388–3400, DOI: 10.1002/sec.1545.
6. Sawicki K., Piotrowski Z., *The Proposal of IEEE 802.11 Network Access Point Authentication Mechanism Using a Covert Channel*. [In:] 2012 19th International Conference on Microwaves, Radar & Wireless Communications, Vol. 2, 656–59, DOI: 10.1109/MIKON.2012.6233587.
7. Tabara B., Wojtuń J., Piotrowski Z., *Data Hiding Method in Speech Using Echo Embedding and Voicing Correction*. [In:] 2017 Signal Processing Symposium (Spsympo), 1–6, DOI: 10.1109/SPS.2017.8053697.
8. Lenarczyk P., Piotrowski Z., *Novel Hybrid Blind Digital Image Watermarking in Cepstrum and Dct Domain*. [In:] 2010 International Conference on Multimedia Information Networking and Security, 356–61, DOI: 10.1109/MINES.2010.81.
9. Guri M., Hasson O., Kedma G., Elovici Y., *An Optical Covert-Channel to Leak Data Through an Air-Gap*. [In:] 14th Annual Conference on Privacy, Security and Trust (Pst), 2016, 642–649. IEEE.
10. Guri M., Monitz M., Elovici Y., *USBee: Air-Gap Covert--Channel via Electromagnetic Emission from USB*. [In:] 14th Annual Conference on Privacy, Security and Trust (Pst), 2016, 264–268. IEEE.
11. Guri M., Monitz M., Mirski Y., Elovici Y., *BitWhisper: Covert Signaling Channel Between Air-Gapped Computers Using Thermal Manipulations*. [In:] IEEE 28th Computer Security Foundations Symposium, 2015, 276–89, DOI: 10.1109/CSF.2015.26.
12. Uzun C., Kahler N., de Peralta L.G., Kumar G., Bernussi A.A., *Programmable Infrared Steganography Using Photoinduced Heating of Nanostructured Metallic Glasses*. [In:] 2017 Conference on Lasers and Electro-Optics (Cleo), 1–2. IEEE.
13. Bieszczad G., Kastek M., *Measurement of Thermal Behavior of Detector Array Surface with the Use of Microscopic*

Thermal Camera. "Metrology and Measurement Systems". Polish Academy of Sciences Committee on Metrology; Scientific Instrumentation, Vol. 18, No. 4, 2011, 679–690, DOI: 10.2478/v10178-011-0064-6.
14. Ratliff B.M., Tyo J.S., Boger J.K., Black W.T., Bowers D.L., Fetrow M.P., 2007. *Dead Pixel Replacement in LWIR Microgrid Polarimeters*. "Optics Express", Vol. 15, No. 12, 2007, 7596–7609, DOI: 10.1364/OE.15.007596.
15. Nguyen, Chuong T, Mould N., Regens J.L., *Dead Pixel Correction Techniques for Dual-Band Infrared Imagery*. "Infrared Physics and Technology", Vol. 71, 227–35, 2015, 10.1016/j.infrared.2015.04.006.
16. Bieszczad G., Gogler S., Krupiński M., Ligienza A., Sawicki K., *The Concept of Thermovision Sensor Supporting the Navigation of Unmanned Aerial Platforms*. "Measurement Automation Monitoring", Vol. 65, No. 1, 15–18, 2019.
17. Cox I.J., Miller M., Bloom J., Fridrich J., Kalker Ton., *Digital Watermarking and Steganography*. Morgan Kaufmann, DOI: 10.1016/B978-0-12-372585-1.X5001-3.

Covert Communication in Thermography – Analysis of Possibilities and Examples

Abstract: The article presents a new concept of using thermography – steganography in thermography. Steganography is a technique of hiding information in a non-obvious way and belongs to the field of science related to information security. This article examines three examples of steganographic channels – covert communication channels that use thermal imaging devices in three different ways. The first proposed method uses the possibility of alternating the scene observed by the infrared camera in a way that additional information is included in the thermogram. The second method, called ThermoSteg, uses modification of one of the parameters of the thermal imaging camera (integration time) to embed the signal containing hidden information. The third method is based on digital thermograms and the methods of replacing dead pixels in them by creating the so-called zombie pixels carrying secretive information. Three methods have been implemented under real conditions and proven to work in practice.

Słowa kluczowe: thermography, steganography, covert channels, infrared radiation, microbolometers

dr inż. Krzysztof Sawicki
krzysztof.sawicki@wat.edu.pl
ORCID: 0000-0002-1368-3854

Ukończył Wydział Elektroniki Wojskowej Akademii Technicznej w 2009 r.; rozprawa doktorska z tematyki steganografii w sieciach bezprzewodowych obroniona w WAT w 2019 r.; jego zainteresowania skupiają się na sieciach bezprzewodowych, bezpieczeństwie teleinformatycznym, steganografii i systemach wbudowanych.

dr inż. Grzegorz Bieszczad
grzegorz.bieszczad@wat.edu.pl
ORCID: 0000-0001-8048-2609

Ukończył w 2008 r. Wojskową Akademię Techniczną na Wydziale Elektroniki. Stopień doktora otrzymał w 2012 r. Obecnie zajmuje się zagadnieniami związanymi z projektowaniem systemów cyfrowych, programowaniem mikroprocesorów i układów FPGA związanych z cyfrowym przetwarzaniem obrazu, w tym obrazów termicznych.

dr inż. Tomasz Sosnowski
tsosnowski@wat.edu.pl
ORCID: 0000-0003-4082-8366

Absolwent Wydziału Elektroniki Wojskowej Akademii Technicznej (1993). Tytuł doktora nauk technicznych uzyskał w 2003 r. Zajmuje się problematyką związaną z projektowaniem i programowaniem systemów cyfrowych, cyfrową analizą sygnału, analizą obrazu termograficznego, a także zastosowaniem układów mikroprocesorowych i programowalnych w technice podczerwieni.

Mariusz Mścichowski
mariusz.mscichowski@student.wat.edu.pl
ORCID: 0000-0002-0079-1960

Student Wydziału Elektroniki Wojskowej Akademii Technicznej. Jego zawodowe zainteresowania skupiają się na cyfrowych pomiarowych układach elektronicznych oraz szybkim prototypowaniu FDM.