Ireneusz KUBIAK, Artur PRZYBYSZ

Wojskowy Instytut Łączności, Zegrze Południowe

doi:10.15199/48.2016.01.42

Technologia druku a elektromagnetyczna ochrona informacji

Streszczenie. *Dotychczasowe badania emisji elektromagnetycznych pokazują, że na rynku dostępne są urządzenia, których rozwiązania technologiczne mogą zapewnić ochronę elektromagnetyczną przetwarzanych danych bez konieczności stosowania dodatkowych zabiegów. Urządzeniami tymi są drukarki komputerowe wykorzystujące technologię LED. Sygnały te, będące źródłami emisji ujawniających, zakłócają się wzajemnie uniemożliwiając skuteczne prowadzenie procesu infiltracji elektromagnetycznej.*

Abstract. *Previous studies of electromagnetic emissions show there are devices in the market which technological solutions can provide electromagnetic protection of data transform without the need for additional treatments. These devices are computer printers that use LED technology. The technology bases on parallel transmission of electrical signals which control the LEDs. These signals are sources of reveal emissions and they interfere with each other.* ***(A printing technology and electromagnetic protection of information).***

Słowa kluczowe: drukarka laserowa, drukarka LED, ochrona informacji, przenik informacji, proces infiltracji elektromagnetycznej
Keywords: laser printer, LED printer, protection of information, leakage information, electromagnetic infiltration process

Wprowadzenie

Stosowanie w procesie przetwarzania informacji urządzeń niebędących źródłami emisji elektromagnetycznych, nie wymagało specjalistycznych rozwiązań zapewniających ochronę takich danych (rys.1). Wystarczyły odpowiednie przedsięwzięcia organizacyjne, ograniczające liczbę osób upoważnionych do dostępu chronionych danych. Wówczas najsłabszym ogniwem całego łańcucha był człowiek. To jego słabości mogły decydować o udostępnieniu danych osobom trzecim.

Rys.1. Bezpieczne elektromagnetycznie urządzenie służące do przetwarzania danych tekstowych

Wykorzystanie w przetwarzaniu informacji urządzeń zasilanych prądem elektrycznym, znacząco wpłynęło na zmianę sposobów zabezpieczenia miejsc i urządzeń przed utratą danych. Związane to było z powstawaniem emisji elektromagnetycznych, posiadających cechy skorelowane z sygnałami elektrycznymi pod postacią, których występowały przetwarzane informacje. Odbiór takich emisji był jednoznaczny z utratą informacji na rzecz osób trzecich. Dlatego rozpoczęto prace zmierzające do znalezienia rozwiązań przeciwdziałających powstawaniu emisji ujawniających o poziomach umożliwiających odtworzenie informacji pierwotnej. Rozwiązania te polegały na stosowaniu m.in. odpowiednich stref ochrony fizycznej czy też rozwiązań technicznych w postaci ekranów elektromagnetycznych oraz filtrów sieci zasilania i obwodów sygnałowych. Nierzadko rozwiązania te wpływały na pogorszenie funkcjonalności urządzeń, a także na ich wygląd i masę.

W kolejnym etapie pojawiły się rozwiązania tzw. programowe, oparte na stosowaniu specjalnych fontów komputerowych. Nie są to jednak wyselekcjonowane fonty ze zbioru wielu fontów komercyjnych. Są to specjalnie zaprojektowane i stworzone fonty dla potrzeb ochrony informacji tekstowych przed elektromagnetycznym przenikaniem. Znaki takich fontów charakteryzują się wysokim stopniem podobieństwa przy jednoczesnym zapewnieniu odpowiedniego poziomu ich czytelności.

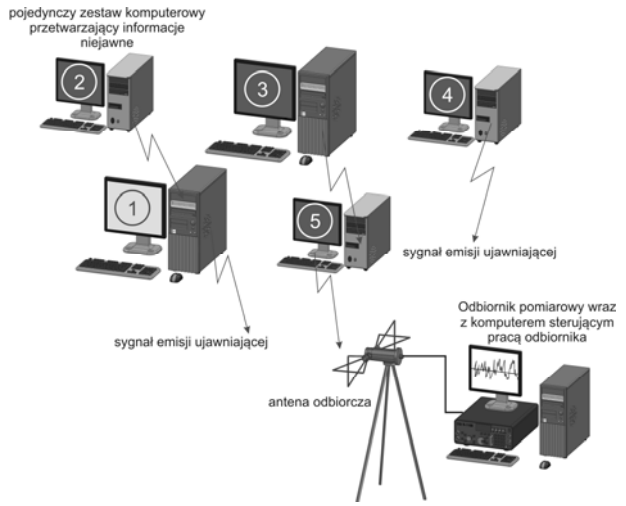
Każde z wymienionych wyżej przedsięwzięć jest rozwiązaniem dodatkowym, wymuszającym w taki czy inny sposób ochronę informacji. Jednak czy każde urządzenie w wykonaniu komercyjnym jest podatne na infiltrację elektromagnetyczną? Może stosowanie nowoczesnych rozwiązań technologicznych samo w sobie zabezpiecza przetwarzaną informację przed podsłuchem elektromagnetycznym? Przeprowadzone badania i analizy różnych scenariuszy pokazuje, że takie możliwości istnieją.

Zwróćmy uwagę na fakt, z którym najprawdopodobniej każdy z nas miał do czynienia. Dotyczy on np. odbioru wybranej stacji radiowej czy też telewizyjnej. Bardzo często słuchanie spektaklu, wiadomości, transmisji sportowych było zakłócane dodatkowymi sygnałami, które utrudniały zrozumienie tego podstawowego sygnału. To samo było zauważalne podczas oglądania ulubionych stacji telewizyjnych. Pojawiały się dodatkowe efekty graficzne w najmniej oczekiwanych momentach. Powodowane to było tym, że przez tor odbiorczy przechodziły sygnały niepożądane, które równolegle z sygnałem użytecznym podlegały procesowi przetwarzania i docierały do naszych zmysłów w postaci różnorodnych zakłóceń. Podobne rozwiązania, mające na celu ochronę elektromagnetyczną informacji niejawnych, były stosowane jeszcze kilkanaście lat temu. Wówczas brak odpowiednio zaawansowanych technologicznie metod inżynierii kompatybilności elektromagnetycznej, uniemożliwiał obniżanie poziomów lub całkowitą eliminację emisji elektromagnetycznych. W urządzeniach montowano więc dodatkowe generatory sygnałów szumopodobnych dla bardzo szerokiego zakresu częstotliwości. Odbiorowi sygnałów skorelowanych z przetwarzaną informacją towarzyszyły więc sygnały niepożądane. W takich przypadkach próby odtworzenia informacji kończyły się brakiem sukcesu. Jednakże, z biegiem lat dodatkowe, wzbogacanie widma elektromagnetycznego zostało wyeliminowane poprzez wprowadzanie rygorystycznych wymagań normatywnych związanych z dopuszczalnymi poziomami zaburzeń elektromagnetycznych.

Równoległe i szeregowe przetwarzanie informacji

Przyjrzyjmy się bliżej zjawisku zakłóconego odbioru sygnałów użytecznych (stacja radiowa lub telewizyjna), czy też sygnałów emisji ujawniających w towarzystwie silnych sygnałów z generatora sygnałów szumopodobnych. Jak wspomniano wcześniej, równolegle z sygnałem użytecznym lub sygnałem emisji ujawniającej dokonywany jest odbiór sygnałów zaburzających. Przeanalizujmy to zjawisko z punktu widzenia występowania w jednym miejscu kilku urządzeń przetwarzających informacje niejawne (rys.2).

Urządzeniami tymi niech będą typowe stacje komputerowe będące źródłem sygnałów emisji tzw. wrażliwych.

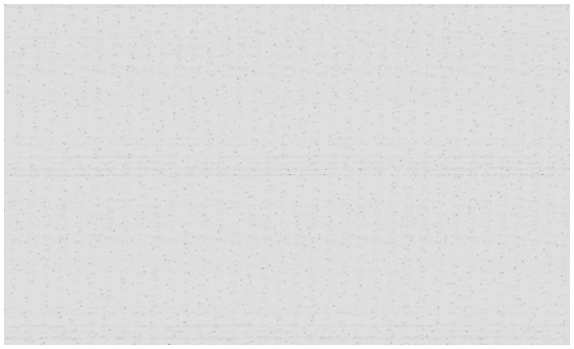


Rys.2. Układ odbioru równoległego emisji ujawniających

„Podsłuchiwanym" urządzeniem jest zestaw oznaczony cyfrą „1". Na pozostałych zestawach komputerowych nie musi być wyświetlany ten sam obraz co na zestawie oznaczonym jako „1". Ponadto, każdy z monitorów może pracować w innym trybie graficznym. Znajomość tego parametru ma ogromne znaczenie w procesie odtwarzania obrazów z zarejestrowanych wcześniej sygnałów emisji ujawniających.

a)

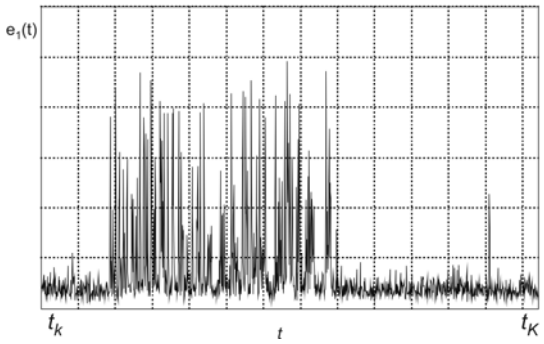
b)



Rys.3. Odtworzony obraz (inwersja) dla parametrów rastrowania zgodnych (a) i niezgodnych (b) z parametrami obrazu pierwotnego

Potwierdzeniem tego są przykładowe obrazy przedstawione na rysunku 3, odtworzone dla parametrów rastrowania, odpowiadających trybowi 800 x 600 x 60 Hz (rys.3a, częstotliwość próbkowania 62,5 MHz) i trybowi 1024 x 768 x 60 Hz (rys.3b, częstotliwość próbkowania 125 MHz). Obraz pierwotny wyświetlany był w trybie 800 x 600 x 60 Hz.

Prześledźmy proces tworzenia obrazu zwany rasteryzacją. Na początek rozważmy szeregową transmisję sygnału wideo dla pojedynczego zestawu komputerowego, który decyduje o wyświetlaniu na monitorze zadanego obrazu. Rejestrowanym sygnałem niech będzie sygnał $e_1(t)$, którego fragment realizacji przedstawiono na rysunku 4.

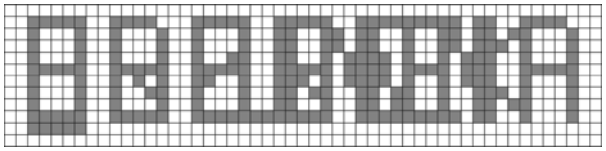


Rys.4. Fragment zarejestrowanego sygnału emisji ujawniającej dla źródła w postaci szeregowego sygnału wideo

Każda z próbek sygnału decyduje o wyświetleniu pojedynczego piksela odtwarzanego obrazu. Jeżeli zarejestrowana odpowiednio długa realizacja $e_1(t)$, zostanie podzielona na odcinki o długości odpowiadającej długości pojedynczej linii obrazu, możliwe jest odtworzenie obrazu pierwotnego, linia po linii. Spójrzmy na powyższe zagadnienie, gdy sygnał wideo przetwarzany jest w sposób szeregowy, ale przez kilka stacji w tym samym czasie, usytuowanych w jednym miejscu, jak to pokazano na rysunku 2 (ograniczmy się do trzech stacji). Każda stacja może przetwarzać inny obraz (rys.5).

Rys.5. Przykładowe obrazy przetwarzane w tym samym czasie na trzech różnych stacjach komputerowych

Rejestrowana realizacja $e_{MNT}(t)$, dla zadanej chwili czasu, jest sumą wartości amplitud sygnałów decydujących o odtworzeniu obrazu. Interesujący nas sygnał zaburzany jest sygnałami wideo pochodzącymi z innych stacji. Rejestracja realizacji $e_{MNT}(t)$ pozwala zatem odtworzyć obraz linia po linii, które jednak mogą nie odpowiadać żadnej linii obrazu pierwotnego „podsłuchiwanej" stacji komputerowej (rys.6).



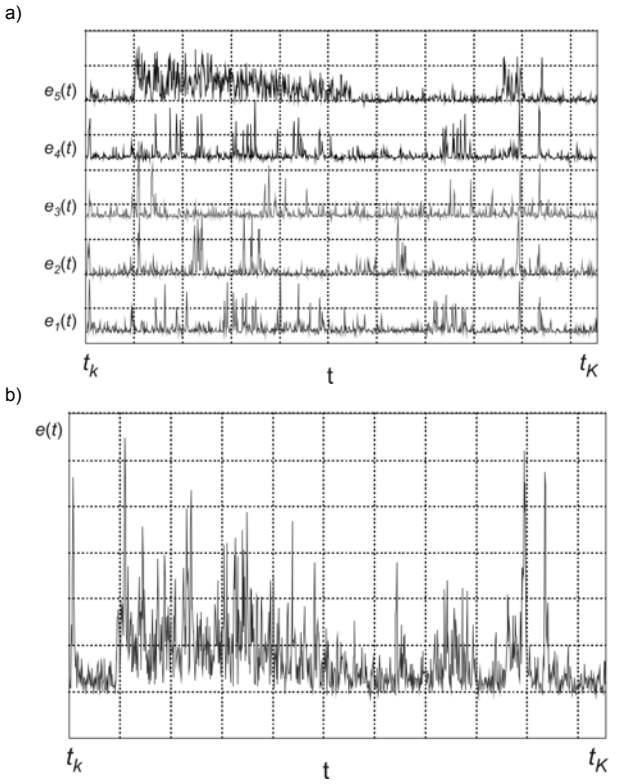
Rys.6. Możliwa postać obrazu odtworzonego

Jak to wygląda w praktyce? Odbiór emisji ujawniających, dla zadanego częstotliwościowego okna

pomiarowego (pasma pomiarowego BW) odbywa się w sposób równoległy od każdej stacji. Oznacza to, że w tym samym czasie do anteny odbiorczej docierają sygnały z pięciu pracujących stanowisk komputerowych (rys.7):

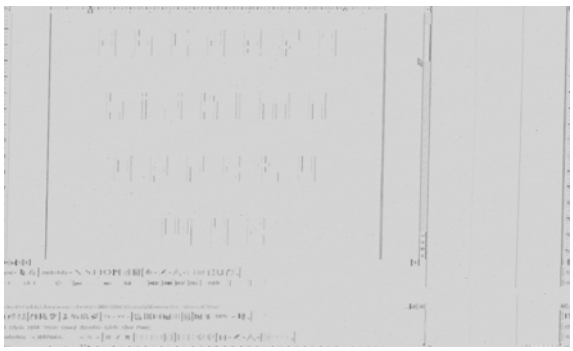
$$e_{MNT}(t) = (e_{MNT})_1(t) + (e_{MNT})_2(t) + (e_{MNT})_3(t) + \\ + (e_{MNT})_4(t) + (e_{MNT})_5(t) \tag{1}$$

gdzie: $e_{MNT}(t)$ – sumaryczny sygnał emisji ujawniającej, $(e_{MNT})_n(t)$– pojedynczy sygnał emisji ujawniającej, którego źródłem jest pojedyncza stacja pracy.

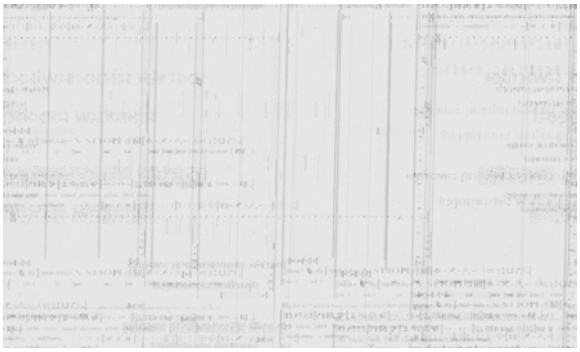


Rys.7. Przykładowe przebiegi czasowego sygnałów emisji ujawniających (a) pochodzących od pięciu zestawów komputerowych i ich suma jako sygnał zbiorczy $e(t)$ (b)

Dla sygnału $e_1(t)$ pozostałe sygnały są sygnałami zakłócającymi, utrudniającymi identyfikację i odtworzenie interesującej informacji. W idealnych warunkach, dla powodzenia procesu infiltracji elektromagnetycznej, powinna występować tylko jedna stacja pracy i tylko ona powinna być źródłem sygnałów emisji ujawniających (rys.8). Stosowanie anteny kierunkowej nie przynosi oczekiwanego efektu. W przeciwnym przypadku możemy otrzymać obraz (rys.9), który z punktu widzenia procesu infiltracji elektromagnetycznej jest bezużyteczny.



Rys.8. Odtworzony obraz (inwersja) z sygnału emisji ujawniającej zarejestrowanego od jednego źródła tej emisji

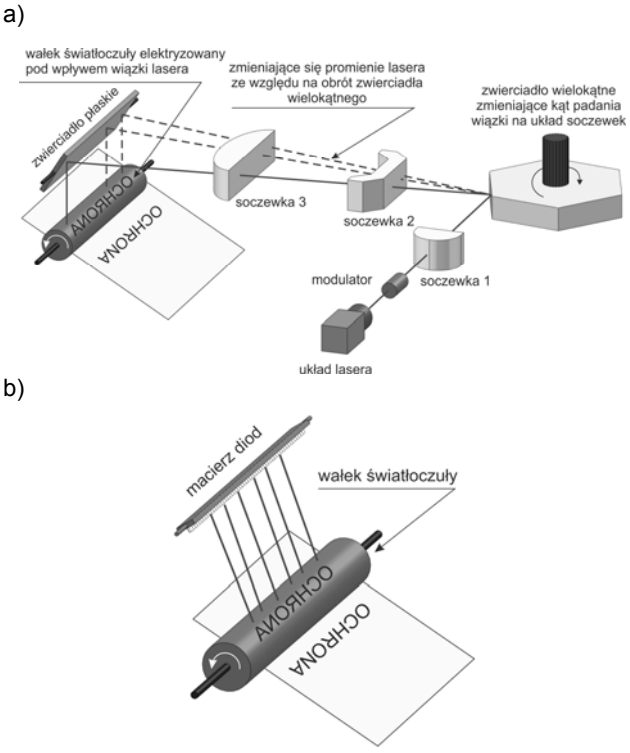


Rys.9. Obraz odtworzony (inwersja) z sygnału zbiorczego $e_{MNT}(t)$

Można zatem przypuszczać, że w przypadku występowania wielu sygnałów równoległych zamiast jednego sygnału szeregowego, odtworzenie informacji pierwotnej nie będzie możliwe.

Budowa drukarek komputerowych

Najbardziej popularnymi drukarkami komputerowymi, poza drukarkami atramentowymi, są drukarki wykorzystujące technologię laserową i LED (diody półprzewodnikowe). Pierwsza z nich wykorzystuje lasery do naświetlania wzorca obrazu na światłoczułym bębnie drukującym, druga do tego celu wykorzystuje diody półprzewodnikowe LED. Mimo, że zasada tworzenia i przenoszenia na papier obrazów jest taka sama, konstrukcja obu typów urządzeń istotnie się różni (rys.10). Wpływa to jednocześnie na możliwości prowadzenia infiltracji elektromagnetycznej obydwu typu drukarek.



Rys.10. Różnice w konstrukcji urządzeń drukujących: a) drukarka laserowa, b) drukarka LED

Drukarki laserowe, jak zostało to pokazane na rysunku 10a, charakteryzują się dość mocno skomplikowanym mechanizmem sterowania wiązką laserową, która naświetla bęben światłoczuły. W układzie możemy wyróżnić układ lesera, zwierciadło wielokątne, soczewki oraz zwierciadło płaskie, kierujące promień lasera bezpośrednio na bęben światłoczuły. Sygnał sterujący laserem do wydruku jednej

linii, podawany jest szeregowo, linia po linii. Zmienność rozdzielczości wydruku zależy od układu optycznego, parametrów tonera (wielkość drobin) oraz własności materiałowych bębna światłoczułego. Dostępne powszechnie drukarki laserowe umożliwiają wydruk o rozdzielczości do 1200 dpi.

W drukarkach LED występuje zgoła odmienna technologia druku (rys.10b). Wiąże się z tym mniejsza niż w przypadku drukarek laserowych liczba części ruchomych i prostsza konstrukcja. Drukarki te posiadają jednak i wady. Do nich możemy zaliczyć niższą rozdzielczość i jakość druku (przede wszystkim jednorodność pokrycia nośnika przez toner). Wynika to wprost z faktu, że drukarki LED wykorzystują liniową matrycę z diodami emitującymi światło. Fizyczna rozdzielczość zależy od gęstości ich upakowania, a jednorodność naświetlania – od jednolitości parametrów indywidualnych elementów półprzewodnikowych. Każdemu punktowi w linii odpowiada jedna dioda. Łącznie może ich być 2500 w dwóch szeregach dla rozdzielczości 300 dpi (lub 5000 dla 600 dpi). Drukarki z diodami są w porównaniu z klasycznymi drukarkami laserowymi mniejsze, tańsze, bardziej odporne na uszkodzenia i zużywają mniej energii. Naświetlenie jednej linii wydruku w drukarce LED odbywa się poprzez równoległą (w tym samym czasie) transmisję sygnału elektrycznego. Dlatego każdy z tych sygnałów może być traktowany jako źródło wzajemnie zakłócających się sygnałów emisji ujawniających, uniemożliwiających ich wykorzystanie w procesie infiltracji elektromagnetycznej.

Jest to zasadnicza różnica, w porównaniu z typową drukarką laserową, wpływająca na bezpieczeństwo elektromagnetyczne drukowanych danych.

Czy drukarka LED z natury rzeczy jest bezpieczna elektromagnetycznie?

Dla rozdzielczości 300 dpi w budowie drukarki LED występuje 2500 diod. Nie każda jednak dioda w procesie naświetlania jest wykorzystywana. Światło emitują jedynie te diody, które elektryzują miejsca pokrywane w następnym etapie proszkiem tonera. W jednym cyklu pracy może zostać pobudzonych elektrycznie kilkaset diod. Sygnały sterujące stają się wówczas źródłami emisji. Ze względu na równoległą ich pracę, niezależny odbiór każdego z sygnałów sterujących staje się mocno utrudniony, a nawet wręcz niemożliwy. Tym samym odtworzenie drukowanych danych przy wykorzystaniu emisji ujawniających kończy się niepowodzeniem. Odbierany sygnał możemy zapisać jako:

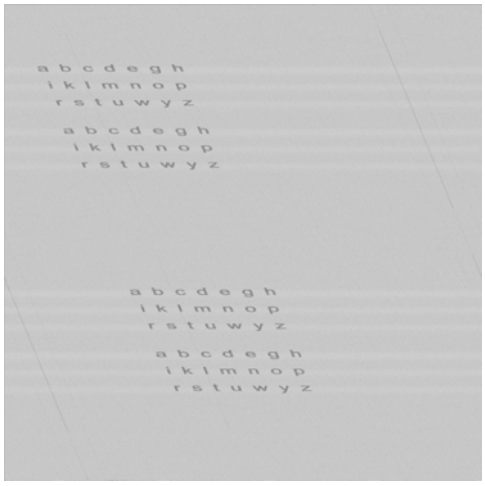
$$e_{LED}(t) = \sum_{n=1}^{N} (e_{LED})_n(t) \tag{2}$$

gdzie: n – numer kolejnego sygnału emisji ujawniającej dla źródła w postaci sygnału pobudzającego diodę LED, N – liczba równoległych sygnałów elektrycznych będących źródłami emisji ujawniających skorelowanych z przetwarzaną informacją, $(e_{LED})_n(t)$ – n-ty sygnał emisji ujawniającej, którego źródłem jest sygnał elektryczny sterujący pracą pojedynczej diody LED. Dla typowej drukarki laserowej jest to:

$$e_{LAS}(t) = (e_{LAS})_1(t) \tag{3}$$

gdzie: $(e_{LAS})_1(t)$ – sygnał emisji ujawniającej, którego źródłem jest szeregowy sygnał elektryczny sterujący pracą lasera drukarki.

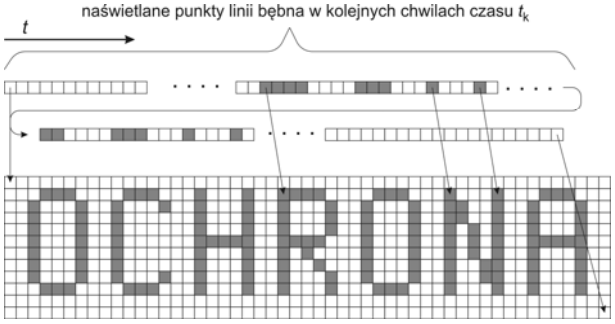
Przykładowy odtworzony obraz dla typowej drukarki laserowej zamieszczono na rysunku 11. Zawarte w nim elementy graficzne są wyraźne i czytelne. W przypadku drukarki z technologią LED niestety tak wyraźnego obrazu nie jesteśmy wstanie uzyskać.



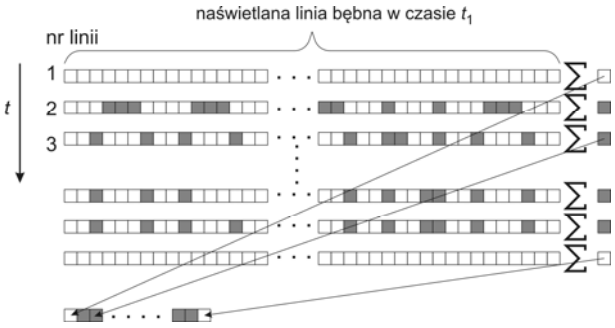
Rys.11. Obraz odtworzony (inwersja) z sygnału emisji ujawniającej mierzonego od drukarki laserowej

Spójrzmy na bardzo istotne zjawisko jakie zachodzi w trakcie drukowania dokumentu przez drukarkę LED. Dla tego typu drukarek w danej chwili np. t_1, naświetlana jest jedna linia wydruku. Dla drukarki laserowej jest to jeden punkt linii. Jakie to pociąga za sobą konsekwencje z punktu widzenia ochrony elektromagnetycznej przetwarzanych danych? Załóżmy, że czas naświetlania jednej linii (drukarka laserowa) odbywa się szeregowo w chwilach czasowych t_k, gdzie $k = 1, 2, \ldots K$. Rejestracja takiego sygnału pozwala odtworzyć taką linię (rys.12).

W przypadku drukarki LED, w dużym uproszczeniu, naświetlenie wspomnianej linii odbywa się w czasie t_k gdzie $k = 1$. W tym czasie rejestrujemy więc sygnał równoległy, niosący informacje o wszystkich naświetlanych, w jednym czasie, punktach danej linii. Rejestrowany zatem sygnał umożliwia odtworzenie jednego punktu linii, nieodpowiadającego jednak punktowi pierwotnemu (rys.13).



Rys.12. Sposób odtwarzania informacji z sygnału emisji ujawniającej dla źródła w postaci szeregowego sygnału elektrycznego (drukarka laserowa)



Rys.13. Sposób odtwarzania informacji z sygnału emisji ujawniającej dla źródła w postaci równoległego sygnału elektrycznego (drukarka LED)

Możemy zatem wnioskować, że rozwiązanie komercyjne w postaci równoległego sterowania pracą w tym samym czasie kilkuset diodami LED, może skutecznie chronić przetwarzane dane przed podsłuchem elektromagnetycznym, co potwierdzają wstępne badania tego typu urządzeń.

Podsumowanie

W obecnych czasach wysokiego stopnia komputeryzacji każdego obszaru życia, zagadnienia ochrony informacji przed elektromagnetycznym przenikaniem stanowią ogromne wyzwanie. Tym bardziej, że emisje ujawniające skorelowane z przetwarzanymi informacjami mogą propagować się w sposób niekontrolowany. Wraz z rozwojem technologicznym urządzeń przetwarzających dane niejawne następuje ciągły rozwój metod, które przeciwdziałałyby skuteczności infiltracji elektromagnetycznej. Stosowane są rozwiązania w postaci filtracji sieci zasilania, obwodów sygnałowych, ekranowania czy też uziemiania i symetryzacji obwodów elektrycznych. Powyższe bardzo często wpływa jednak na wygląd zewnętrzny, jak i masę urządzeń specjalnych. Ponadto, adaptacja do zastosowań specjalnych urządzeń komercyjnych, w których występują elementy ruchome oraz elementy będące źródłem ciepła, jest bardzo skomplikowana. Prowadzone są zatem ciągłe badania nad doskonaleniem rozwiązań skutecznie chroniących przetwarzane dane poprzez eliminację źródeł emisji skorelowanych z informacjami niejawnymi.

Jednym z interesujących rozwiązań, niewymagającym dodatkowych przedsięwzięć technicznych, a jednocześnie mogącym skutecznie przeciwdziałać infiltracji elektromagnetycznej, mogą być sygnały elektryczne powiązane z przetwarzaną informacją generowane równolegle. Przykładem takiego rozwiązania są drukarki komputerowe bazujące na technologii LED. W tym przypadku sygnał elektryczny odpowiedzialny za prawidłowe naświetlanie bębna światłoczułego, podawany jest równolegle na wszystkie diody, które w danej chwili muszą wygenerować światło. W ten sposób w jednej chwili naświetlana jest cała linia drukowanego następnie dokumentu. W przypadku typowych drukarek laserowych naświetlanie bębna światłoczułego dla każdej linii odbywa się szeregowo, punkt po punkcie.

Równoległe sterowanie pracą diod skutecznie utrudnia możliwości prowadzenia infiltracji elektromagnetycznej. Dla każdego sygnału elektrycznego wybranej diody, pozostałe sygnały, ze względu na ich równoległe występowanie, stanowią zaburzenie, zakłócające jego zdalny odbiór. Zjawisko to można porównać do przypadku występowania wielu źródeł emisji ujawniających w tym samym miejscu i w tym samym czasie. Selektywny odbiór pojedynczego sygnału z punktu widzenia skuteczności procesu infiltracji elektromagnetycznej jest niemożliwy.

Dlaczego więc drukarki LED nie są tak popularne tam, gdzie przede wszystkim powinniśmy chronić swoje dane? Tym bardziej, że mechanizm drukarek LED posiada mniej ruchomych części niż drukarek laserowych, przez co jest również mniej awaryjny. Drukarka LED jest tańsza w produkcji. W tego typu drukarkach fizyczna rozdzielczość zależy od gęstości rozmieszczenia diod LED. Ponadto jednorodność naświetlania, czyli jakość druku zależy od jednolitości parametrów indywidualnych elementów półprzewodnikowych. W efekcie drukarki LED mają małe zastosowanie w obszarach, gdzie wymagana jest jakość i wierność odwzorowania kolorów. Jak wspomniano mechanizm drukarek LED jest mało skomplikowany. Fakt ten działa na korzyść tych drukarek. Zwiększenie rozdzielczości druku nie zmniejsza nominalnej szybkości drukowania. Dla drukarek laserowych pojedyncze źródło światła musi odwzorować coraz większą liczbę punktów na cal, co wpływa na wydłużenie czasu druku. Jak widać odpowiedź na wyżej postawione pytanie jest bardzo trudna.

Pytaniem bez odpowiedzi pozostaje również jakie właściwości w tym obszarze posiadają drukarki atramentowe?

Autorzy: *dr inż. Ireneusz Kubiak, Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe, E-mail: i.kubiak@wil.waw.pl; mgr inż. Artur Przybysz, Wojskowy Instytut Łączności, ul. Warszawska 22A, 05-130 Zegrze Południowe, E-mail: a.przybysz@wil.waw.pl*

LITERATURA

[1] Kubiak I., „*Metody analizy i cyfrowego przetwarzania obrazów w procesie infiltracji elektromagnetycznej*”, Wydawnictwo Wojskowej Akademii Technicznej 2013, ISBN 978-83-62954-86-5.

[2] Kubiak I., Przybysz A., Musiał S., Grzesiak K., „*Elektromagnetyczne bezpieczeństwo informacji”*, Wydawnictwo Wojskowej Akademii Technicznej 2009, ISBN 978-83-61486-32-9.

[3] Kubiak I., Przybysz A., Musiał S., Grzesiak K., „*Generator rastra w procesie infiltracji elektromagnetycznej”*, Wydawnictwo WAT 2012, ISBN 978-83-62954-28-5.

[4] Kubiak I., „*Możliwości odtwarzania danych tekstowych z sygnałów emisji niepożądanych metodą korelacji znakowej – standard DVI*”, Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, ISSN 1230-3496, 2-3 2014.

[5] Kubiak I., „*Font komputerowy odporny na proces infiltracji elektromagnetycznej*”, Przegląd Elektrotechniczny, ISSN 0033-20972014, 2014.

[6] Kubiak I., „*Digital processing methods of images and signals in electromagnetic infiltration process*”, Image Processing and Communication, vol. 18, no. 1, pp. 5-16, DOI: 10.2478/v10248-012-0070-7, 2013, ISSN: 1425-140X.

[7] Kubiak I., „*Two-dimensional correlation as a search method of relationship between pattern image and compromising emanation*”, Journal of Basic and Applied Phisics, V 2014.

[8] Tadeusiewicz R., Korohoda P., Komputerowa analiza i przetwarzanie obrazów, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1997.

[9] Grzesiak K., Przybysz A., *Emission security of laser printers*, MCC 2010: Military Communications and Information Systems Conference, Wrocław 2010;

[10] Hebisz T.: *Algorytmy rastrowe*. Skrypt. Instytut Sterowania i Systemów Informatycznych, Wydział Elektrotechniki, Informatyki i Telekomunikacji, Uniwersytet Zielonogórski, Zielona Góra 2002.

[11] Markus G. Kuhn, Ross J. Anderson: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 124-142, ISBN 3-540-65386-4.

[12] Agus Zainal Arifin and Akira Asano, Image Thresholding by Histogram Segmentation Using Discriminant Analysis, In Proceedings of Indonesia–Japan Joint Scientific Symposium, IJJSS,pp. 169-174, 2004.

[13] Markus G. Kuhn: *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, 4th Workshop on Privacy Enhancing Technologies, 26-28 May 2004, Toronto, Canada, Proceedings, LNCS 3424, pp. 88–105, Springer-Verlag.

[14] Iwanowski M., Zastosowanie morfologii matematycznej do wykrywania obszarów o zadanych cechach na obrazach cyfrowych, V Sympozjum Naukowe “Techniki przetwarzania obrazów”, Serock, listopad 2006, materiały konferencyjne, str. 270-281.

[15] Sojka, E., 2002. In: A New and Efficient Algorithm for Detecting the Corners in Digital Images. Lecture Notes in Computer Science, vol. 2449. Springer, Berlin, pp. 125–132.

[16] Markus G. Kuhn: *Compromising emanations of LCD TV sets*. IEEE International Symposium on Electromagnetic Compatibility (EMC 2011), Long Beach, California, August 14–19, 2011, pp. 931–936, ISBN 978-1-4577-0811-4.

[17] Kuo S. M., Lee B. H., Real-Time Digital Signal Processing. Implementations, Applications and Experiments, Chichester, Wiley 2001.