Biometria,
system bezpieczeństwa,
uwierzytelnianie

KRYSOWATY Ireneusz[1]
NIEDZIEJKO Paweł[2]
OSTROWSKI Piotr[3]

WYBRANE PROBLEMY WSPÓŁCZESNEJ BIOMETRII W SYSTEMACH BEZPIECZEŃSTWA

Artykuł porusza ważne problemy związane z wdrażaniem biometrycznego uwierzytelniania w systemach bezpieczeństwa in corporre. W artykule podnosi się aspekty uwarunkowań społeczno-prawnych stosowania biometrii oraz znaczenie wykorzystania cech osobniczych w systemach bezpieczeństwa. Autorzy szczególną uwagę zwracają na istnienie podatności i słabych punktów biometrycznych systemów uwierzytelniania, które mogą w istotny sposób kompromitować skuteczność systemów bezpieczeństwa. W artykule autorzy opisują także wybrane metody i sposoby przeciwdziałania atakom uwypuklając rolę multibiometrii jako ważnego elementu zwiększającego bezpieczeństwo.

SELECTED PROBLEMS OF MODERN BIOMETRICS IN SECURITY SYSTEMS

The article addresses important issues related to implementation of biometric authentication security systems in corporre. The article raises the aspects of socio-legal use of biometrics and the importance of using the characteristics between individuals in security systems. The authors pay special attention to the existence of vulnerabilities and weaknesses of biometric authentication systems, which can significantly compromise the effectiveness of security systems. In the article the authors describe the selection of methods and ways to prevent attacks, highlighting the role multimodal biometric as an important part of increasing safety.

1. WSTĘP

Jesteśmy świadkami niezwykle szybkiego rozwoju nowoczesnych technologii. Permanentna informatyzacja społeczeństw zmienia Świat w globalną wioskę McLuhan-a. Wraz z tymi dynamicznymi zmianami powstają nowe szanse i zagrożenia, które z kolei stymulują potrzebę wysoce wiarygodnego uwierzytelniania tożsamości. Papierowy dokument tożsamości wyparła plastikowa karta, wzbogacona nieco później o elektroniczny

[1] Wojskowa Akademia Techniczna, Wydział Elektroniki; 00-908 Warszawa; ul. Gen. Sylwestra Kaliskiego 2. Tel: + 48 22 683-98-72, E-mail: ikrysowaty@wat.edu.pl
[2] Wojskowa Akademia Techniczna, Zespół Analiz i Ekspertyz Wojskowych. E-mail: pniedziejko@wat.edu.pl
[3] Wojskowa Akademia Techniczna, Instytut Optoelektroniki. E-mail: postrowski@wat.edu.pl

procesor. Lecz i ten atrybut ludzkiej tożsamości m.in. w wyniku historycznych, tragicznych wydarzeń szybko rozpoczął przeobrażanie, podążając ku biometrycznej identyfikacji.

Lecz z tym szybkim rozwojem nauki podążają wątpliwości, obawa o zachwianie statusu prywatności i ograniczeń wolności, swobód. Rodzi się pytanie czy tak samo szybko podąża natura prawa czy wszystkie obecne zastosowania biometrii są de lege artis.

Interesującym jest i niezwykle ważnym zagadnieniem, czy system „mocnego" uwierzytelniania, biometrycznej autentykacji jest bezpieczny? Czy systemy biometryczne mogą być podatne na różnorodne ataki w celu jego oszukania, destabilizacji, unieszkodliwienia etc.

Biometria niesie ze sobą np. to niebezpieczeństwo, że w wyniku ataku na system trudno podważyć fakt weryfikacji tożsamości osoby, która temu procesowi autentykacji, w danym momencie, się nie poddała.

2. WYJĄTKOWOŚĆ CECHY A PRAKTYKA

Cechy brane pod uwagę do identyfikacji mają wyjątkowy charakter – są unikalnym identyfikatorem dla każdego osobnika, ale przede wszystkim można dokonać ich ekstrakcji, czyli można je pomierzyć. Cechy te wykazują niezmienność i niezniszczalność, stanowią trudne do podrobienia dane, których teoretycznie nie można ukraść, nie można ich zgubić i nie należy ich pamiętać. Cechę (biometrykę) powinna charakteryzować akceptowalność ze względów społecznych, kulturowych, religijnych i zdrowotnych. Jednakże w różnych grupach społecznych jest różnorodny poziom W procesie automatyzacji analizy cechy to szybkość przetwarzania ma decydujące znaczenie. By z kolei mówić o szybkości przetwarzania, dana cecha musi zapewniać mocne uwierzytelnienie, czyli potwierdzenie autentyczności tożsamości osobniczej.

Prawdopodobieństwo wystąpienia powtarzających się dwóch takich samych wzorców linii papilarnych jest jak 1 do 10^{12} (1 do 1 biliona). Do dnia dzisiejszego nie stwierdzono, aby u 2 osób wystąpiły identyczne wzorce. Są to dane wciąż potwierdzane codzienne przez registratury daktyloskopijne na całym świecie przy obecnej około 7 miliardowej populacji (szacuje się, że ilość mieszkańców Ziemi oscylować będzie maksymalnie przy wartości ok. 9 miliardów). Wzór linii papilarnych kształtuje się już u noworodków i jest niezniszczalny przez całe życie, a każda blizna staje się dodatkowym elementem wspomagającym identyfikację. Pozostaje jednak problem rozpoznania, czy urządzenie skanuje prawdziwy palec, czy też ma ono do czynienia z atrapą, fantomem, a może z palcem, obciętym (odnotowano przypadek kradzieży samochodu z użyciem odciętego palca). Największym problemem urządzeń do automatycznego czytania odcisków palców jest jakość odwzorowania - praktycznie wszystkie mają kłopoty z niektórymi typami palców. Producentom tych urządzeń udało się, co prawda, zdobyć do dzisiaj dość spore doświadczenia i pokonać wiele trudności, ale do doskonałości jeszcze daleko i np. przy wyrabianiu polskiego paszportu biometrycznego pojawiają się przypadki niemożności pobrania wzorca odcisku palca. Dodatkowym problemem, który muszą pokonać producenci wielu urządzeń, są tłuszczowe odciski palców, pozostawione na powierzchni czujnika. Wiele z nich reaguje na takie odciski jak na prawdziwe. Najlepszą jakość obrazu dają urządzenia ultradźwiękowe, które nie mają problemów z kontrastem i z żadnymi typami palców (w sensie jakości i pokrycia powierzchni). Są też jedynymi, które mogą sprawdzić, czy przedłożony im do weryfikacji odcisk jest częścią prawdziwego i żywego palca.

Ze względu na możliwość różnego ułożenia palca na czytniku, czy różną siłę nacisku, za każdym razem kod tworzony na podstawie odcisku palca jest inny. Kluczowym elementem systemu biometrycznego jest algorytm pozwalający na porównanie odcisku palca ze wzorcem. Wczytany obraz linii papilarnych jest przetwarzany w celu wykluczenia szumu informacyjnego. Następnie „czysty" obraz jest analizowany w celu odnalezienia punktów charakterystycznych, które są porównywane z zapamiętanymi wzorcami. Algorytmy analizujące powinny być w stanie przetwarzać obrazy silnie zaburzone (na przykład odcisk brudnego palca) i umieć rozpoznać linie papilarne niezależne od ułożenia palca na sensorze. Szacuje się, że prawdopodobieństwo znalezienia dwóch osób o takim samym kształcie linii papilarnych wynosi około 1 : 64 miliardów. Przy opisie linii stosuje się około 30 - 40 punktów charakterystycznych (rożna ilość punktów w różnych krajach jest brana pod uwagę przy wiarygodność identyfikacji). Opis odcisku palca ma objętość kilkuset bajtów (tym większą, im dokładniejszy jest pomiar). Istnieją poglądy, że taka ilość punktów charakterystycznych może być niewystarczająca.

Czujniki odcisku palca to najpowszechniej implementowane czujniki biometryczne. Znane są przypadki nie w pełni sprawnego funkcjonowania biometrycznych systemów rejestracji czasu pracy oraz kontroli dostępu na podstawie weryfikacji wzoru odcisku palca (Siemianowice Śląskie – US). Zdarza się, że z chwilą uruchomienia systemów niektórym pracownikom nie udaje się pobrać wzorców biometrycznych odcisku palca, a firmy instalujące (a nawet firmy produkujące) nie są w stanie wyjaśnić, dlaczego. Sprawność takich „konwencjonalnych" systemów zależy w dużej mierze od dokładności kontaktu palca z czujnikiem. Coś, co przeszkadza w tym kontakcie wpływa na jakość pobieranego obrazu. Przykładowo, jeżeli opuszki palca osobnika są zniszczone (sławny w biometrii przykład stolarza), to odróżnienie odcisku palca może być niemożliwe. Jeżeli palce są spocone, pot zaciemni wzorzec. Palec może też zostać niedokładnie przyłożony do czujnika. Jeżeli osoba wysiada z transatlantyckiego lotu, jej skóra może być zbyt sucha dla czujnika. Może zdarzyć się również, że osoba nieuprawniona użyje np. lateksowego fantomu palca i tradycyjny czujnik nie wykryje oszustwa. Te i dużo innych banalnych sytuacji może przeszkodzić „konwencjonalnemu" systemowi biometrycznemu w poprawnej weryfikacji tożsamości. Jednak odcisk palca wykorzystywany powszechnie w systemach bezpieczeństwa, m.in. paszportach biometrycznych staje się biometryką, którą można ukraść. Na różnego rodzaju forach oraz filmach popularno naukowych (Pogromcy Mitów - ang. MythBusters) prezentowane są różnego rodzaju przepisy jak „ukraść" odcisk palca i wykonać fantom by oszukać system biometryczny.

W przypadku rozpoznawania tęczówki oka metoda analizy polega na wykonaniu w podczerwieni fotografii tęczówki jednego lub obojga oczu. Ignorowane są przy tym rzęsy, refleksy światła, szkła kontaktowe i okulary przeciwsłoneczne. Odległość kamery od oka może wynosić do l metra - w rezultacie pomiar nie powinien być uciążliwy dla użytkownika lecz wymaga dobrej woli i niestety zaangażowania. Uzyskany w ten sposób obraz jest przetwarzany przez wyspecjalizowane oprogramowanie. Określane są granice tęczówki, obraz jest dzielony na strefy, które są analizowane pod kątem odnalezienia cech charakterystycznych. Proces ten nosi nazwę demodulacji, a jego rezultatem jest 256÷512-bitowy kod tęczówki (IrisCode), który jest porównywany z zapisem w bazie danych. Wyszukanie wzorca tęczówki w dużej bazie danych zajmuje jedynie kilka sekund. Przetwarzany obraz jest czarno-biały dzięki temu system jest niewrażliwy na zmiany koloru oka. Jest to o tyle istotne, że ten z biegiem czasu nieznacznie się zmienia i zjawisko to

mogłoby mieć wpływ na pracę systemu. Głównym czynnikiem, który decyduje o tak wysokiej dokładności metody, jest budowa tęczówki. Powstaje ona w procesie morfogenezy chaotycznej (kształtowanie organów bez wpływu DNA), co oznacza, że nawet dysponując kodem genetycznym danej osoby, nie jesteśmy w stanie jej odtworzyć. Tęczówka nie zmienia się od ok. 18-ego miesiąca życia (zakończenie procesu morfogenezy), aż do momentu śmierci. Może zostać opisana przez 400 różnych punktów charakterystycznych (system wykorzystuje ich ok. 260), zwanych stopniami swobody. O tym, jak są one niepowtarzalne, może świadczyć fakt, że różnią się one u bliźniąt jednojajowych, a także w obojgu oczu tej samej osoby. Według Byometrictm GmbH, prawdopodobieństwo wystąpienia identycznych tęczówek wynosi jak 1 do 10^{78}.

Z kolei przy uwzględnieniu systemu rozpoznawania twarzy pojawiają się statystyki i głosy, że gdyby na lotnisku pojawił się nieprzebrany Osama bin Laden to mielibyśmy tylko 40% szans by zidentyfikować Go przez twarzowy systemem rozpoznający, a około 1 osoba na 100 ludzi mogłaby zostać niesłusznie uznana właśnie za Osamę bin Ladena. Należy przy tym pamiętać, że pomijając fakt niewystępowania dwóch identycznych twarzy nawet u bliźniaków, każda twarz jest dodatkowo asymetryczna, co stanowi kolejną istotną cechę w twarzowym rozpoznawaniu.

3. MODEL ROZPOZNAWANIA OSOBNICZEGO A ATAKI NA SYSTEM

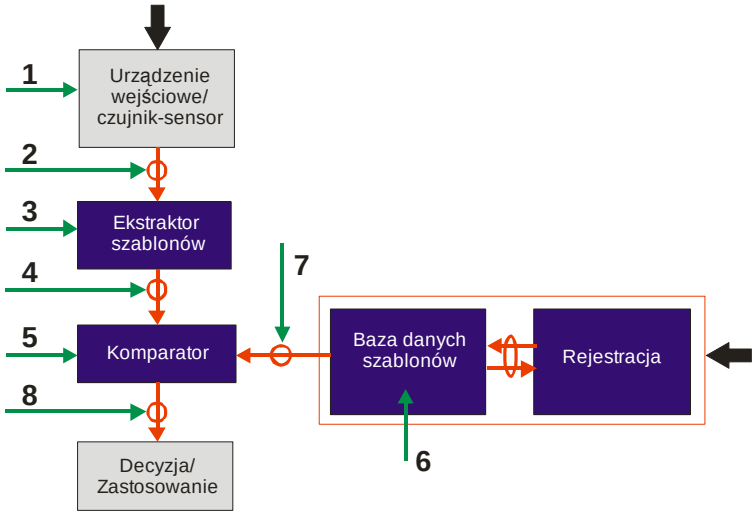
Liczba instalacji, aplikacji biometrycznych zarówno w sektorze komercyjnym jak i państwowych stale rośnie. Rośnie także liczba użytkowników tych systemów (w samym programie US VISIT - program Department of Homeland Security obejmujący paszport biometryczny - są to dziesiątki milionów). Dodatkowo powstają nowe aplikacje. Zagospodarowuje się nowe obszary zastosowania dla systemów biometrycznych m.in. w ramach programów wizowych, kontroli granic – portów lotniczych i morskich, elektronicznych dokumentów tożsamości, ochrony zdrowia, rozrywki i imprez masowych, polityki zakładów pracy - rejestracja czasu pracy, zakładów karnych, centrów informatycznych, banków i bankomatów, służb mundurowych, szkół i szpitali, instytucji rządowych oraz etc.). Zatem adekwatnie do wielkości rynku biometrycznego zwiększa się ilość potencjalnych zagrożeń – ataków. Analizy bezpieczeństwa w zakresie systemów biometrycznych wykazują, że jest to sfera niezwykle krytyczna.

Zautomatyzowane systemy biometrycznego uwierzytelniania rozwijają się by eliminować problemy związane z istniejącymi dotychczas metodami weryfikacji tożsamości użytkowników. Biometria to szansa by zwiększyć zarówno wygodę (w aspekcie procesów autentykacji) jak i poprawić bezpieczeństwo (jako element mocnego, niepodważalnego uwierzytelniania). Jednakże wydaje się, że słabe punkty są nieodzownym elementem każdego systemu bezpieczeństwa. Istnieją lub pojawiają się także w każdym urządzeniu biometrycznym, choć oczywiście w sposób niezamierzony przez projektantów systemu. Najprawdopodobniej wszelkie słabe punkty są odkrywane przede wszystkim w trakcie działania systemów, gdy np. jest on atakowany. A atak ten będzie prowadzony najskuteczniej w słabo zabezpieczonych elementach systemów.

Inaczej niż w przypadku systemów opartych np. na haśle („coś co wiesz”), podatnych np. na ataki słownikowe lub techniki psychomanipulacyjne itp., systemy biometryczne mogą wymagać od atakującego znacznie więcej inwencji, trudu i wysiłku.

Wyróżnić możemy 6 podstawowych typów zagrożeń:

1. Atakujący uzyskuje dostęp do systemu zabezpieczonego przy pomocy biometrycznego uwierzytelniania:
   - Atak na prywatność (ang. privacy attack): atakujący uzyskuje dostęp do danych nie będąc upoważnionym (np. uzyskując dostęp do dokumentacji medycznej innej osoby);
   - Atak wywrotowy (ang. subversive attack): atakujący manipuluje system (np. złożenie fałszywych oświadczeń ubezpieczeniowych).
2. Atak przez negowanie (ang. repudiation attack): osoba atakująca odmawia dostępu do systemu – np. urzędnik bankowy modyfikuje dokumentację finansową, a później twierdzi, że jej dane biometryczne został skradziony i ktoś inny dokonał zmiany danych.
3. Atak przez podstawienie (ang. contamination attack): osoba atakująca nielegalnie pobiera dane biometryczne prawdziwego użytkownika i używa go do dostępu do systemu - np. fantom palca.
4. Atak zmowy (ang. collusion): użytkownik z szerokimi uprawnieniami np. administratora systemu, nielegalnie modyfikuje system.
5. Atak pod przymusem (ang. coercion): atakujący siłą (broń, szantaż) przymusza uprawnionego użytkownika do dostępu do systemu.
6. Atak typu Denial of Service (DoS): osoba atakująca modyfikuje system informatyczny tak by uprawnieni użytkownicy nie mogli z niego korzystać – np. z serwera, który przetwarza żądania dostępu jest bombardowany wieloma fałszywymi danymi, zapytaniami aż do momentu zablokowania, przeciążenia systemu.



Rys.1. Punkty ataków umiejscowione w ogólnym modelu biometrycznego systemu uwierzytelniania

Rysunek powyżej ilustruje punkty, w których potencjalnie mogą być dokonywane ataki na system.

- Atak 1: fałszowanie biometryk (np. fantom palca). Sensor biometryczny pobiera biometrykę z sfałszowanego wzorca.
- Atak 2: nielegalne przechwycenie danych podczas transmisji i ponowne ich użycie.
- Attack 3: funkcja ekstraktora cech zostaje zmieniony wirusem – koń trojański.
- Atak 4: rzeczywista cecha zostaje zastąpiona zmodyfikowanym wzorcem cech – ingerencja w transmisję.
- Atak 5: zmiana algorytmu porównującego zbiór cech za pomocą wirusa - konia trojańskiego.
- Atak 6: modyfikowanie rekordów w bazie danych, usuwanie lub dodawanie nowych szablonów.
- Atak 7: dane z bazy danych są modyfikowane podczas transmisji w kanale komunikacyjnym.
- Atak 8: wpływanie na decyzję systemu – modyfikacja rezultatu (np. akceptacja/odrzucenie).

Poniżej zaprezentujemy kilka sposobów przeciwdziałania atakom.

W odniesieniu do **Ataku 1**. Stosuje się techniki wykrywania „żywotności cechy" bazujące na specjalnych czujnikach wykrywających m.in.:

- **Temperaturę**: Temperatura naskórka ma wartość około 8-10 ^{0}C powyżej temperatury panującej w pomieszczeniu. Za pomocą kamery podczerwieni (mikrobolometrycznej 320x240, 7-8nm) przechwytywany jest obraz cieplny np. palca, ucha i dokonywane jest porównanie tzw. „map" poziomów energetycznych.
- **Przewodność** (konduktywność): Typowa przewodność skóry to około 200kOhm. Metoda nazywana jest również metodą oporności elektrycznej.
- **Stałą dielektryczną** (ε - przenikalność dielektryczna): relatywna stała dielektryczna ludzkiej skóry (w zakresie 20-50) jest różna od silikonu. Stała opisuje właściwości ciała dielektrycznego w polu elektrycznym.
- **Ton serca**: sprawdzanie bicia serca może być wykorzystywane by eliminować użycie martwych biometryk – odcięty palec, głowa, wyrwana gałka oczna oraz jednocześnie może stanowić odrębną unikalną biometrykę.
- **Układ naczyń krwionośnych** (dłoni, palca, napięstka, nadgarstka): Rozpoznawanie układu żył należy do technologii biometrycznych, z którymi wiąże się najwięcej nadziei. Wzorzec biometryczny żył znajduje się pod skórą co czyni technologię skuteczniejszą jeżeli chodzi o bezpieczeństwo jej stosowania i jak podkreślają producenci urządzeń, technologia ta poprzez brak kontaktu ze skanerem zapewnia absolutną higienę. Sprawdzanie tożsamości osoby odbywa się przez rozpoznanie i przyporządkowanie wzoru układu żył np. dłoni. Wzór naczyń krwionośnych w dłoni, palcu a nawet w całym ciele jest unikalny do każdego osobnika (nawet pośród bliźniąt jednojajowych oraz np. pomiędzy prawą i lewą dłonią) i oprócz rozmiaru, wzór ten nie zmieni się w ciągu życia danej osoby.
- **Strukturę fizjologii skóry**: Skóra ma budowę warstwową i wykazuje złożoną interakcję ze światłem. Światło, przechodząc przez skórę, ulega rozproszeniu i absorpcji. Użyty algorytm analizujący fakturę powierzchni twarzy, analizuje losowe cechy faktury skóry tworząc unikalny wzór osobnika.

Stosuje się także metody i techniki:

- **Metody ultradźwiękowe**: Lokalne różnice w impedancji akustycznej. Za pomocą tej metody rozpoznaje się zabrudzone odciski palców. Odczyt może być dokonywany przez cienkie rękawiczki gumowe. Metoda odróżnia odciski pozostawione na powierzchni czujnika od prawdziwych (żywych) palców. Potwierdza, że odcisk jest częścią żywego palca.
- **Analizy wielospektralne**: Technologia, w której płat skóry o niewielkiej powierzchni (ok. 1 cm średnicy) jest oświetlany różnej długości fali światła widzialnego i bliskiej podczerwieni. Światło to jest odbite po rozproszeniu się w skórze i wtedy dokonywany jest pomiar dla każdej długości fali. Zmiany światła podczas jego przechodzenia przez skórę są analizowane i przetwarzane celem uzyskania charakterystycznego wzoru biometrycznego, który jest porównany z wcześniej zapisanym wzorcem. Ponieważ sygnał optyczny jest odzwierciedleniem chemicznych struktur skóry i jej innych własności, dostarcza on wiarygodnej informacji o tym, że próbka nie jest martwa i pochodzi od człowieka. Materiał syntetyczny – albo inny niepochodzący od człowieka – posiada zdecydowanie inne własności niż żywa skóra ludzka. Usunięty albo amputowany płat skóry przechodzi szybkie zmiany biochemiczne; zachodzą oczywiście zmiany temperatury i dystrybucji płynów w granicach różnych przedziałów fizjologicznych, które też zmieniają jakość sygnału.
- **Analizy siatkówki oka**: (technika sama w sobie wysoce bezpieczna): Zdjęcie oka wykonuje się jedynie w obrębie małego, okrągłego obszaru siatkówki przy użyciu specjalnej kamery z bardzo małej odległości od oka, przy jednoczesnym oświetlaniu jego dna. Zdjęcie jest efektem odbicia światła od układu naczyń krwionośnych znajdującego się tuż pod siatkówką ‑ w ukrwionej warstwie naczyniówki. Uzyskany obraz nie jest zatem zdjęciem siatkówki, (sama siatkówka jest przezroczysta dla światła podczerwonego używanego w tej metodzie), a jedynie układem naczyń krwionośnych w siatkówce. Jest to cecha równie unikalna jak wzorzec tęczówki.
- **Rozpoznawanie mechaniki chodu** (linii kierunku chodu, linii chodu, długości kroku, szerokości kroku, linii stopy, kąta stopy, rozkładu siły nacisku stopy na podłoże, ciężaru osoby): Metoda ta oferuje możliwość identyfikacji na odległość, a więc jest bezinwazyjna i bezkontaktowa (nie ma interakcji z urządzeniem biometrycznym).
- **Analiza ruchu gałki ocznej**: Kilku uczonych z Uniwersytetu Joensuu w Finlandi (Roman Bednarik, Tomi Kinnunen, Andrei Mihaila oraz Pasi Fränti) zaproponowało wykorzystanie w biometrii unikalnych cech ruchu gałki ocznej.
- **Biometria wielomodalna** (Metody multibiometrii): Łączy się kilka technik biometrycznych różnymi technikami.

Ataku 2. Eliminacja powtórek (Eliminate Replay): W celu eliminacji ataku nr 2. Stosuje się systemy typu challenge-response, które gwarantują, że obraz jest naprawdę pochodzący z linii papilarnych i że atakujący nie ominął czujnika. Jest to swoistego rodzaju podpis cyfrowy. Generowany jest ciąg pseudolosowy, zainicjowany przez klienta, przesyłany wraz ze wzorcem do serwera i sprawdzana jego zgodność.

Ataku 2 – 4. – wykorzystuje się metodę eliminacji możliwości wykorzystania przez atakującego algorytmu wspinaczki na szczyt (Hill-Climbing Algorithm), który umożliwia zastąpienie rzeczywistej cechy zmodyfikowanym wzorcem cech

Ataku 6 i 7. Ochrona wzorca, szablonu biometrycznego poprzez Watermarking Cyfrowy: Technologia służąca do zabezpieczania obrazów. Polega na osadzeniu w przesyłanym pliku unikalnej kombinacji bitów – dodatkowych informacji np. o pochodzeniu, poziomie dostępu, przeznaczeniu etc. Znak wodny można oczywiście wyodrębnić z pliku i odczytać jego zawartość za pomocą specjalizowanego programu a plik (obraz) poddać dalszej analizie biometrycznej.

4. WNIOSKI

Odpowiedzią na wzrost przestępczości elektronicznej, ale także ciągły wzrost terroryzmu ogólnoświatowego jest wprowadzanie nowoczesnych sposobów zabezpieczeń i ochrony tożsamości w oparciu o systemy biometryczne (identyfikatory biometryczne, urządzenia do inteligentnego monitoringu audio i wideo, systemy do ustalania tożsamości pasażerów lotniczych oraz do automatycznego śledzenia, nadzorowania więźniów etc.).

Jednakże sama biometria to nie panaceum na bolączki systemów bezpieczeństwa. Ważnym jest to, że:

- Bezpieczeństwo systemów biometrycznych jest poważnym problemem. Atak na system biometryczny może spowodować m.in. utratę prywatności, naruszenie bezpieczeństwa oraz straty finansowe bądź też może podważyć wiarygodność;
- Systemy biometryczne są narażone na wiele ataków również ze względu na prozaiczny fakt, że są systemami informatycznymi. Ataki mogą być zarówno bardzo proste w przeprowadzeniu jak i bardzo złożone wymagające wiedzy specjalistycznej.
- Istnieją rozwiązania eliminujące ataki, ale jest jeszcze wiele do zrobienia w obszarze bezpieczeństwa tych systemów.
- Dodatkowo nowe problemy bezpieczeństwa związane właśnie z systemami biometrycznymi mogą być definiowane niejednokrotnie wraz z rozwojem rynku biometrycznego.
- Wciąż brak jednoznacznych wykładni prawnych dotyczących możliwości stosowania biometrii niestwarzających nadinterpretacji przepisów.
- Wciąż rodzi się wiele kontrowersji w aspekcie społecznej akceptowalności różnorodnych technik i możliwości ich zastosowania.

5. BIBLIOGRAFIA

[1] Andrzejkowicz M.: *Administracyjnoprawne i cywilnoprawne aspekty zastosowań biometrii*, Warszawa 2004.

[2] Bolle R. M., Connell J. H., Pankanti S., Ratha K., Senior A.: *Biometria*, Wydawnictwa Naukowo-Techniczne, Warszawa 2008.

[3] Chrostowski J.: *Uważne oko biometrii*, „Wiedza i Życie" 2006, nr 4, s. 20.

[4] European Commission, Joint Research Centre, Institute for Prospective Technologies: Technical Report "Biometrics at the Frontiers: Assessing the impact on Society", 2005 - EUR 21585 EN.

[5] Kasprowski P.: *Identyfikacja osobnicza na podstawie ruchu oka* - autoreferat rozprawy doktorskiej, Instytut Informatyki Wydziału Automatyki, Elektroniki i Informatyki Politechniki Śląskiej, Gliwice 2004, s. 2.

[6] Koziczak A.: *Karnoprawne uwarunkowania biometrii*, Materiały Konferencji Naukowej Biometria 2003 - Technologia, Prawo, Społeczeństwo, Instytut Maszyn Matematycznych 2003.
[7] Krysowaty I., Niedziejko P.: Biometria - *Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie*, „Zabezpieczenia" 2006, nr 4, 5.
[8] Krysowaty I., Niedziejko P.: *Biometria w bezpieczeństwie lotnisk*, Materiały konferencyjne, Wrocław 2006.
[9] Krysowaty I., Niedziejko P.: *Standaryzacja Biometrii; Konferencja Biometrii*, Sztab Generalny 28.04.2011.
[10] Krysowaty I., Niedziejko P.: *Z biometrią w podróży*, Czasopismo Zabezpieczenia nr 2/2007, Wydawnictwo AAT Trading Company.
[11] Praca zbiorowa pod redakcją Kaszubski R.: *Biometria w bankowości i administracji publicznej*, Związek Banków Polskich, Warszawa, 16 czerwca 2009 r.

„Praca naukowa finansowana ze środków na naukę w latach 2010-2012 jako projekt rozwojowy."