ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 68 Nr kol. 1905

Michał SZCZEPANIK, Ireneusz J. JÓŹWIAK
Politechnika Wrocławska
Instytut Informatyki

METODY WYKRYWANIA CZŁOWIECZEŃSTWA W SYSTEMACH BIOMETRYCZNYCH

Streszczenie. W artykule autorzy analizują istniejące metody oszukiwania systemów biometrycznych i na podstawie tych badań opracowują metody zapobiegania tego typu włamaniom. Głównym celem badań jest zabezpieczenie przed oszustwem popularnych systemów rozpoznawania linii papilarnych. Badania mają także wykazać, jakie dodatkowe cechy fizyczne powinny być weryfikowane przez systemy biometryczne w celu zredukowania prawdopodobieństwa oszustwa.

Słowa kluczowe: biometria, bezpieczeństwo, niezawodność, system rozpoznawania odcisków palców.

METHODS OF DETECTING HUMANITY IN BIOMETRIC SYSTEMS

Summary. In this paper authors analyze the existing methods of cheating biometric systems and based on these studies develop methods to prevent this type of intrusion. The main goal of the research is to prevent cheating popular fingerprint recognition systems. Experiment also demonstrated that additional physical characteristics should be verified by biometric systems to reduce the possibility of not authorized access.

Keywords: biometric, security, reliability, fingerprints recognition system.

1. Wprowadzenie

W tradycyjnym ujęciu biometria to technika pobierania oraz dokonywania pomiarów cech istot żywych w celu przeprowadzenia ilościowych badań nad populacją i jej zmiennością [4]. Obecnie znaczenie tego pojęcia zostało rozszerzone i oznacza także zautomatyzowaną analizę cech fizycznych bądź behawioralnych w celu identyfikacji lub weryfikacji tożsamości osoby

żyjącej [13]. W obu przypadkach biometria ściśle korzysta z metod statystyki matematycznej związanej z indywidualnością niektórych cech.

Do cech fizycznych zalicza się między innymi geometrię twarzy, układ linii papilarnych lub żył. Cechy behawioralne obejmują sposoby mówienia, pisania odręcznego, poruszania się bądź pisania na klawiaturze i są uznawane za znacznie trudniejsze do podrobienia w porównaniu z cechami fizycznymi.

Dane biometryczne są stale powiązane z ich właścicielem i większości przypadków pozostają niezmienne. Niestety, ostatnie badania zespołu naukowców z University of Notre Dame pod kierownictwem prof. Kevina Bowyera wykazały, że nawet tęczówka oka jest wrażliwa na procesy starzenia się [7] i nawet w przeciągu 3 lat może zmienić swoją strukturę do tego stopnia, że system biometryczny nie jest w stanie jej poprawnie zidentyfikować. Systemy biometryczne zyskały popularność dzięki temu, że nie wymagają pamiętania haseł ani noszenia ze sobą dodatkowych przedmiotów, tj. tokenów czy kart chipowych. System biometryczny wymaga niewielu działań ze strony użytkownika, głównie na etapie pobierania charakterystyki, np. przyłożenia palca do skanera linii papilarnych. Zwykle proces przetwarzania danych jest w całości autonomiczny. Sklonowanie cech biometrycznych na inny organizm żywy jest procesem bardzo trudnym, często wymagającym skomplikowanych operacji chirurgicznych, dlatego wszelkie próby złamania zabezpieczeń biometrycznych opierające się na fizycznych cechach realizuje się przez odtworzenie ich w sztucznych materiałach. Jest to możliwe ze względu na luki w systemach będących najczęściej na styku człowiek-urządzenie pomiarowe, czyli np. skanerach, miernikach.

Producenci i dostawcy rozwiązań biometrycznych, gdy tylko zauważyli ogólne zaniepokojenie poziomem bezpieczeństwa – głównie po wydarzeniach z 11 września 2001 roku – rozpoczęli walkę o rynek [3], prezentując coraz to doskonalsze urządzenia. W wyniku wzrostu zainteresowania często wprowadzane na rynek rozwiązania nie miały dostatecznej jakości. Wynikało to z presji czasu i popytu rynku na nowe rozwiązania, które zaburzały proces planowania oraz projektu urządzenia. Walka o klienta sprowadzała się głównie do chwytów marketingowych, często zawierających niezgodne z prawdą stwierdzenia. Urządzenia są coraz częściej tworzone pod testy akceptacyjne oraz bazy próbek biometrycznych w nich stosowanych [1] tylko po to, by urządzenie zyskało lepsze od konkurencji parametry FAR i FRR [2]. Niedoskonałości urządzeń biometrycznych w połączeniu z ich niefachowym wykorzystaniem sprawiają, że systemy te nie zapewniają odpowiedniego poziomu bezpieczeństwa. Wynikiem tego jest testowanie żywotności w systemach biometrycznych, które od lat pozostaje ważnym i wciąż nie w pełni rozwiązanym zagadnieniem. Na problematykę testu żywotności zwrócono szczególną uwagę w 2002 roku po publikacji wyników [10, 12] pozytywnej akceptacji sztucznych obiektów z wykorzystaniem uznanych na rynku systemów biometrii twarzy, odcisku palca i tęczówki. Badania obrazujące skalę problemu wykonano w Instytucie Fraunhofera w Darmstadt przy

współpracy z Niemieckim Federalnym Instytutem do spraw Bezpieczeństwa w Systemach IT (BSI) [6].

2. Zabezpieczenia systemów biometrycznych

Obecnie skuteczność systemów biometrycznych najczęściej mierzy się dwoma parametrami: FAR i FRR [2]. Im niższe są ich wartości, tym system jest odpowiednio bezpieczniejszy lub użyteczny.

Bezpieczeństwo określone jest przez parametr FAR (ang. False Acceptance Rate). Jest to prawdopodobieństwo zakwalifikowania wzorca do danej klasy, mimo iż przynależy on do innej. W biometrii natomiast oznacza prawdopodobieństwo przyznania dostępu do systemu mimo braku stosowanych uprawnień.

Użyteczność określa parametr FRR (ang. False Rejection Rate). Jest to prawdopodobieństwo niezakwalifikowania wzorca do danej klasy, mimo iż do niej należy. W biometrii natomiast oznacza prawdopodobieństwo nieprzyznania dostępu do systemu mimo posiadania uprawnień. Tabela 1 prezentuje skuteczność popularnych systemów biometrycznych.

Tabela 1

Porównanie popularnych metod biometrycznych

	FAR (%)	FRR (%)
Linie papilarne	0.2000	0.0100
Geometria dłoni	0.2000	0.2000
Siatkówka oka	10.0000	0.0010
Tęczówka oka	0.0005	0.0005
Geometria Twarzy	1.0000	0.5000

Źródło: G. Błoński: Hardware hacking – oszukiwanie zabezpieczeń biometrycznych. Hakin9 PL, 7/2007.

Jednym z głównych zabezpieczeń systemów biometrycznych jest wykrywanie człowieczeństwa, czyli weryfikacja, czy badany obiekt jest naprawdę człowiekiem. Większość systemów w wersji podstawowej analizuje tylko obraz i dają się one łatwo oszukać przez sztuczne (nie żywe) kopie cechy biometrycznej. Coraz częściej stosują one dodatkowe analizatory, które weryfikują cechy charakterystyczne dla żywej części ciała, np. zmienność wielkości źrenicy pod wpływem światła, temperaturę, pH, wilgotność.

W przypadku czytników linii papilarnych rozróżniamy kilka rodzajów takich rozwiązań: optyczne, pojemnościowe, termiczne. Czytnik optyczny porównuje zapisane cyfrowo odciski palców, czytnik pojemnościowy mierzy pojemność kondensatora utworzonego z powierzchni palca i powierzchni sensora, a czytnik termiczny porównuje różnice temperatur pomiędzy punktami linii papilarnych [5]. Najpopularniejszymi czytnikami są optyczny oraz

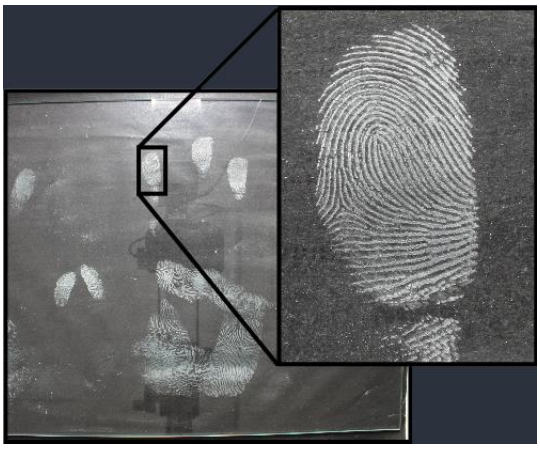
pojemnościowy. Niestety, tego typu czytniki nie są odporne na oszukiwanie za pomocą sztucznych odlewów odcisku, np. w żelu [7].

Podobnego rodzaju czytniki są stosowane w przypadku geometrii dłoni, jednak ze względów bezpieczeństwa często używa się dodatkowo kilku kamer wykonujących zdjęcia pod różnym kątem. Również ze standardowych kamer lub aparatów korzystają systemy identyfikujące geometrię twarzy [13].

Czytniki siatkówki oka wykorzystują kamery wysokiej rozdzielczości dodatkowo analizujące żywotność oka przez zmianę oświetlenia, które powoduje zmiany rozmiaru źrenicy.

3. Oszukiwanie systemów rozpoznawania odcisków palców

Skaner linii papilarnych jest najbardziej ekonomicznym rozwiązaniem identyfikującym pod względem ceny oraz wartości parametrów FAR i FRR. Niestety, jest on też najbardziej podatny na oszukiwanie. Większość obecnych skanerów ma dodatkowe czujniki temperatury oraz pojemności, jednak nie zapewniają one odpowiedniego poziomu bezpieczeństwa i nadal dają się oszukać przez popularne rozwiązania.



Rys. 1. Odcisk palca na szklance uwydatniony za pomocą cyjanoakrylu
Fig. 1. A fingerprint on a glass enhanced by cyanoacrylate
Źródło: http://www.appliedbiometrics.co.uk.

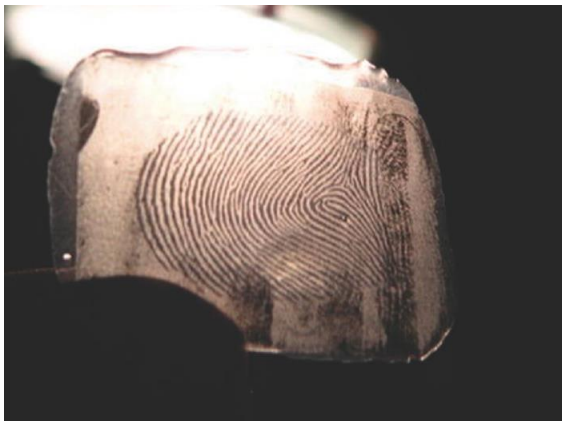
Praktycznie proces oszukania takiego systemu dzielimy na dwa główne etapy: pobranie próbki odcisku palca ofiary oraz preparację sztucznego odcisku. W pierwszym etapie najistotniejsze jest znalezienie odpowiedniej jakości próbki, jaką zostawi osoba, pod którą chcemy się podszyć. Najlepiej w tym celu podłożyć ofierze szklane naczynie, płytę CD lub inny przedmiot o gładkiej strukturze, bez nadruków oraz wzorów. Następnie na odcisk należy nanieść pył, np. grafit, który spowoduje jego uwydatnienie. Innym dość dobrym sposobem

jest naniesienie bardzo cienkiej warstwy cyjanoakrylu (rys. 1), który jest składnikiem klejów szybkoschnących (np. kropelka, superglue), i spowodowanie jej zaschnięcia. Wysychająca warstwa kleju spowoduje związanie się tłuszczu zawartego w odcisku z klejem. Następnie taki odcisk musi zostać sfotografowany w wysokiej rozdzielczości. Najlepsze efekty dają aparaty fotograficzne do zdjęć makro.

Po usunięciu z cyfrowego obrazu zniekształceń oraz szumów należy wydrukować go za pomocą drukarki laserowej na folii używanej do drukowania prezentacji wyświetlanych na projektorach. Wydrukowany odcisk niestety nie ma takiej faktury, jaką ma skóra palca pokryta liniami papilarnymi, choć i tak ponad połowa czytników palców stosowanych w urządzeniach przenośnych zidentyfikuje go jako odcisk poprawny. Nałożenie bardzo cienkiej (<0,3 mm) warstwy kleju (wikolu) mającego wilgotność zbliżoną do skóry człowieka dodatkowo zwiększy stopień zgodności preparowanego odcisku w pozostałych czytnikach.

Innymi metodami utworzenia odlewu odcisku jest użycie masy lateksowej lub ciastoliny, czyli masy podobnej do plasteliny sprzedawanej pod marką Play-Doh. Główne zalety ciastoliny to niebrudzenie i niewysychanie. Evana Blass [7] przeprowadził testy wykazujące, że ok. 90% obecnych na rynku czytników linii papilarnych jest podatnych na oszukiwanie przy użyciu odcisku wykonanego w ciastolinie. Bardzo zbliżoną metodę opracował Tsutomu Matsumoto, który wykonywał odlew w rozgrzanej masie plastikowej, a następnie zalewał taką formę żelatyną pochodzącą z rozpuszczonych cukierków żelowych, nazywanych popularnie „miśkami".

Każda z zaprezentowanych metod podrobienia odcisku palca jest bardzo prosta w realizacji i możliwa do wykonania w domu bez zastosowania specjalistycznego sprzętu.



Rys. 2. Gotowa do użycia kopia odcisku palca
Fig. 2. Copy of the fingerprint which is ready to use
Źródło: http://www.appliedbiometrics.co.uk.

4. Oszukiwanie innych systemów biometrycznych

W przypadku systemów rozpoznających twarz użytkownika najprostszym sposobem jest użycie zdjęcia ofiary. Metoda ta działa tylko, gdy twarz jest analizowana z jednej kamery, tak jak w telefonach z systemem Android v 4.x. Jeśli chodzi o obraz z wielu kamer, metodą umożliwiającą oszukanie jest użycie maski bezpośrednio przylegającej do twarzy. Systemy opierające się na tęczówce oka dają się oszukać przez wydruk zdjęcia oka w dużej rozdzielczości. Większość systemów opracowanych po 2005 roku zawiera system weryfikacji żywotności oka przez zmianę oświetlenia [8]. Rozwiązanie to nie jest jednak w pełni skuteczne, gdyż algorytmy analizują tylko pewien pierścień z tęczówką, więc wycięcie w zdjęciu dziury na źrenicę i przyłożenie wydruku do naszego oka rozwiązuje ten problem. W 2003 roku opracowano metodę umożliwiającą wykrycie sztucznych regularności powstałych wskutek wydruków rastrowych, np. za pośrednictwem drukarki [8]. Dobór parametrów metody odbywa się przez optymalną selekcję odpowiedniego zakresu częstotliwości, w ramach którego widmo amplitudowe wykazuje największe różnice dla obrazów żywych oczu i ich wydruków.

W przypadku systemów z analizą głosu stosuje się zwykle nagrania wypowiedzi ofiary. Zabezpieczeniem przed tego typu rozwiązaniami jest konieczność podania różnych sekwencji słów przez użytkownika. Wykorzystuje się także systemy wykrywające szum charakterystyczny dla odtwarzanego dźwięku, jednak to rozwiązanie może powodować nieprawidłowe działanie w niektórych środowiskach eksploatacji.

Obecnie systemy rozpoznawania odcisków palców analizują kilka dodatkowych parametrów, tj. temperaturę, pojemność, wilgotność. Stosuje się także systemy analizujące pH człowieka [10]. Wszystkie te parametry mają wartości charakterystyczne dla człowieka, jednak można je przekazać w bardzo prosty sposób na spreparowaną sztuczną próbkę przez poślinienie jej. Dzięki ślinie zyskujemy wszystkie parametry poza temperaturą, którą i tak przekażemy czytnikowi poprzez cienką warstwę sztucznego odcisku nałożonego na nasz palec.

Najnowocześniejsze systemy wykorzystują wielomodułowe systemy biometryczne i bardzo często analizują dodatkowo rozkład żył w palcu. Jest to metoda dość nowa, która nawet samodzielnie daje bardzo dobre wyniki. Integracja takiego systemu z czytnikiem odcisków palców znacznie skraca czas analizy, gdyż system ten służy potwierdzeniu tożsamości, która została określona przez strukturę odcisku palca.

5. Opracowany system biometryczny

Opracowany system wykorzystuje pewną charakterystykę ludzkiej skóry, która uwydatnia bruzdy pod wpływem wilgoci. Oznacza to, że wszystkie bruzdy, które tworzą odcisk palca, pogrubiają się pod wpływem wilgoci, dlatego w systemie zastosowano dwa czytniki linii papilarnych rozdzielone mechanizmem nawilżającym. Pierwszy czytnik ma za zadanie zidentyfikować skanowaną osobę, a drugi zweryfikować pojawienie się zmian strukturalnych odcisku na skutek wilgoci. Drugi czytnik porównuje uzyskany skan odcisku z czytnikiem pierwszym i weryfikuje rozszerzenie się bruzd.

System nawilżający stanowi pasek nawilżający, podobny do używanego w nowoczesnych golarkach ręcznych, pokryty dodatkowo żelem mocno nawilżającym. Najlepsze efekty uzyskano, stosując krem do rąk mocno nawilżający firmy Garnier.

6. Eksperyment

W celach badawczych pobrano 25 odcisków i opracowano sztuczne próbki na podstawie rozwiązań opisanych w rozdziale 3, czyli:

- odwzorowanie odcisku w odlewie z masy lateksowej,
- odwzorowanie odcisku w odlewie z żelatyny (cukierków żelatynowych),
- odwzorowanie odcisku w ciastolinie,
- wydruk odcisku na drukarce laserowej,
- wydruk odcisku pokryty wikolem,
- prawdziwy (żywy) odcisk palca (cele porównawcze).

Każdą próbkę starano się przeanalizować w systemie czterokrotnie. Niestety uszkodzenia spowodowane paskiem nawilżającym w masie ciastolinowej i wydruku laserowym były na tyle duże, że uniemożliwiały wykonanie więcej niż dwóch prób.

Tabela 2

Wyniki eksperymentu

	Pojedynczy czytnik		Opracowany system	
	zaakceptowane	odrzucone	zaakceptowane	odrzucone
Odlew lateksowy	99%	1%	0%	100%
Odlew żelowy	98%	2%	3%	97%
Masa ciastolinowa (1p)	94%	6%	0%	100%
Wydruk laserowy (1p)	89%	11%	2%	98%
Wydruk pokryt wikolem	99%	1%	12%	88%
Odcisk palca	99%	1%	99%	1%

Źródło: opracowanie własne.

Tabela 2 prezentuje wyniki eksperymentu. Wyraźnie widać, że opracowany system wykrył większość prób oszustwa. Wydruk laserowy ze względu na zbyt małą wypukłość wydruku w 11% okazał się niewystarczający, by oszukać pojedynczy czytnik. W przypadku wikolu, który pod wpływem kremu rozszerzał się, nawet opracowany system został oszukany w 12%. Jest to wartość nieakceptowalna, dlatego w dalszych pracach nad systemem ten problem będzie szczegółowo analizowany; prawdopodobnie odpowiednie dobranie parametrów związanych ze stopniem rozszerzenia się bruzd umożliwi wykrywanie kopii odcisku wykonanej z wikolu.

7. Podsumowanie

Badania wykazały, że nawet proste metody wytwarzania sztucznych kopii odcisków palców umożliwiają oszukanie popularnych systemów biometrycznych, w szczególności systemów rozpoznawania odcisków palców. Opracowany system umożliwia wykrycie większości prób sforsowania systemu biometrycznego przez sztuczne próbki. W dalszych badaniach planowane jest takie dobranie parametrów systemu definiujących minimalną i maksymalną zmianę grubości bruzdy, by zniwelować błędy akceptujące odciski wykonane z wikolu.

Bibliografia

1. Alisto H. et al.: Biometric Modalities and Technology. BioSec 4th Workshop, Brussels, November 28-29, 2005.
2. Bowman E.: Everything You Need To Know About Biometrics. Identix Corporation, 2000.
3. Denning D.: Wojna informacyjna i bezpieczeństwo informacji. Wydawnictwa Naukowo-Techniczne, Warszawa 2002.
4. Dubisz Stanisław (red.): Uniwersalny słownik języka polskiego. Wydawnictwo Naukowe PWN SA, Warszawa 2003.
5. Hicklin A., Watson C., Ulery B.: How many people have fingerprints that are hard to match. NIST Interagency Report, 7271, 2005.
6. Jain A.K., Ross A., Nandakumar K.: Introducing to biometrics. Spinger, 2011.
7. Maltoni D., Maio D., Jain A.K.: Prabhakar S. Handbook of Fingerprint Recognition. 2nd Edition, Springer, 2009.

8. Pacut A., Czajka A.: Iris Aliveness Detection. BioSec 2nd Workshop, Brussels, January 20, 2005.
9. Pankanti S., Prabhakar S., Jain A.K.: On the individuality of fingerprints. Proceedings of Computer Vision and Pattern Recognition (CVPR), 2001.
10. Ratha N.K., Govindaraju V.: Advances in Biometrics: Sensors, Algorithms and Systems. Springer, 2007.
11. Ross A., Nandakumar K., Jain A.K.: Handbook of Multibiometrics (International Series on Biometrics). Springer, 2011.
12. Thalheim L., Krissler J., Ziegler P.M.: Biometric Access Protection Devices and their Programs Put to the Test, c't 11/2002, p. 114.
13. Wayman J.L., Jain A.K., Maltoni D., Maio D.: Biometric Systems. Technology, Design and Performance Evaluation. 1st Edition, Springer, 2005.
14. http://www.appliedbiometrics.co.uk [dostęp:19 czerwca 2013].

Abstract

Authors present few methods which allow cheats popular biometric systems. They focus on fingerprints recognition system and cheat it by artificial fingerprint copies created from latex cast, die-cast gel, laser print, print covered by Wikol glue. Most of these methods allow to be identify by popular systems. Authors created they own solutions which base on two fingerprints scanners and humidification system. It base on characteristics of human skin, which enhances furrows moisture. This means that all the furrows that form the fingerprint thicken when exposed to moisture. The Table 2 presents the results of an experiment and confirm that this method allow to reduce incorrectly decisions of the system when someone try cheat it using popular methods.