Praktyczne aspekty wdrażania systemów biometrycznych

Część 1: Wartości współczynnika fałszywego odrzucenia dla różnych technologii biometrycznych

mgr inż. ELŻBIETA GOMULSKA, Instytut Maszyn Matematycznych, Warszawa

Każdy z nas chce czuć się bezpiecznie, pracować w godziwych warunkach, załatwiać szybko niezbędne formalności w bankach i urzędach itp. Oczekujemy, że rozwój naukowo-techniczny ułatwi realizację naszych wymagań. Coraz częściej osiągnięcie zamierzonych celów jest łatwiejsze dzięki stosowaniu innowacyjnych rozwiązań informatycznych. Niektóre systemy informatyczne dla poprawności działania wymagają uwierzytelnienia użytkownika – np. systemy kontroli dostępu, systemy bankowe itp. Można tego dokonać stosując technologie biometryczne. Jest to bezpieczniejsze niż stosowanie haseł, które można przechwycić, ujawnić lub zapomnieć.

Biometria to dziedzina wiedzy zajmująca się pomiarem cech fizycznych człowieka, ze szczególnych uwzględnieniem cech różnicujących poszczególne osoby. Każdy z nas posiada pewne unikalne cechy fizyczne (np. kształt twarzy, linie papilarne, tęczówkę oka) pozwalające jednoznacznie nas zidentyfikować. Celem stosowania technologii biometrycznych jest potwierdzenie tożsamości osoby za pomocą środków technicznych bez konieczności angażowania do tego procesu personelu pomocniczego. Istnieją dwie metody postępowania: weryfikacja tzn. sprawdzenie na podstawie cech fizycznych czy osoba jest tą, za którą się podaje i identyfikacja – odszukanie w bazie danych osoby na podstawie jej cech biometrycznych. w praktyce – z uwagi na mniejsze koszty – najczęściej korzysta się z weryfikacji tożsamości.

Biometria dostarcza środków technicznych do wspomagania procesu identyfikacji lub weryfikacji człowieka jednak paradoksalnie skuteczność tego procesu zależy od samego zainteresowanego. Informacje biometryczne pobierane są za pomocą specjalnych czytników. O jakości tych urządzeń świadczą parametry deklarowane przez producentów. Parametry te nie są jednak wartościami mierzalnymi za pomocą aparatury, a jedynie współczynnikami statystycznymi możliwymi do osiągnięcia w optymalnych warunkach – wymaga się, aby użytkownik systemu umożliwił odczyt cechy biometrycznej ściśle zgodnie z procedurą – np. przyłożył palec centralnie w okienku pomiarowym, ułożył dłoń dokładnie w wymaganej strefie itp. Tylko zastosowanie się człowieka do takich żądań gwarantuje sukces.

Na potrzeby systemów informatycznych, na podstawie obrazu cechy (np. linii papilarnych palca) jest tworzony tzw. wzorzec biometryczny, który opisuje w sposób zakodowany tylko pewne właściwości cechy niezbędne w procesie rozpoznawania człowieka. Wzorzec to ciąg bajtów informacji powstałych w skutek przetworzenia według specjalnego algorytmu z bardzo dużą redukcją obrazu wybranej cechy fizycznej człowieka. Na podstawie wzorca nie jest możliwa operacja odwrotna tzn. na podstawie wzorca nie można odtworzyć obrazu cechy biometrycznej (np. obrazu linii papilarnych palca).

Dwie podstawowe wartości charakteryzujące czytniki biometryczne to współczynnik fałszywej akceptacji i współczynnik fałszywego odrzucenia. Współczynnik fałszywej akceptacji opisuje prawdopodobieństwo uznania fałszywego wzorca za poprawny (próba oszukania systemu), a współczynnik fałszywego odrzucenia – niezaakceptowania wzorca poprawnego.

Współczynnik fałszywej akceptacji zależy przede wszystkim od jakości algorytmu weryfikacji oraz ilości cech wzorca biometrycznego, które są w algorytmie wykorzystane i określa odporność urządzenia na świadome próby oszustwa. Niestaranna obsługa czytnika w czasie próby weryfikacji nie spowoduje z pewnością zwiększenia liczby osób uznanych za poprawnie zweryfikowane mimo dostarczenia fałszywej próbki biometrycznej

Współczynnik fałszywego odrzucenia pokazuje, jaki procent prób weryfikacji uprawnionej osoby nie zakończył się sukcesem. Aby zrozumieć, jak istotny wpływ na ten parametr mają działania człowieka trzeba poznać mechanizm działania systemów biometrycznych. Otóż najpierw pobiera się od każdego użytkownika systemu za pomocą specjalnego czytnika wzorzec biometryczny np. linii papilarnych czy tęczówki oka, który jest zapisywany w bazie danych lub na karcie identyfikacyjnej. Następnie przy każdej próbie weryfikacji tożsamości ten wzorzec jest porównywany z wzorcem pobranym w danej chwili w czytniku. Jeśli wzorzec bieżący i zapisany w bazie zostaną uznane za zgodne, tożsamość użytkownika jest potwierdzana.

Współczynnik fałszywego odrzucenia

Współczynnik fałszywego odrzucenia FRR (*ang. False Rejection Rate*) uważany jest często za kryterium komfortu korzystania z systemu, ponieważ fałszywe odrzucenie jest przede wszystkim irytujące dla użytkownika.

FRR jest daną statystyczną, której wartość zależy nie tylko od fizycznych cech urządzenia ale i od działań człowieka. Natomiast dokładność FRR zależy od liczby pomiarów.

Współczynnik fałszywego odrzucenia dla jednej (n-tej) osoby jest określany jako:

$$FRR(n) = \frac{\text{Liczba odrzuconych prób weryfikacji wykonanych przez 1 osobę}}{\text{Liczba wszystkich prób weryfikacji wykonanych przez 1 osobę}}$$

a dla N osób:

$$FRR = \frac{1}{N} \sum_{n=1}^{N} FRR(n)$$

Wpływ wyboru technologii biometrycznej na współczynnik fałszywego odrzucenia

W Polsce do najczęściej wykorzystywanych urządzeń biometrycznych należą czytniki linii papilarnych i geometrii dłoni. w końcu dziewiętnastego wieku brytyjski uczony Sir Francis Galton sformułował (1892, monografia "Fingerprints") trzy prawa głoszące, że linie papilarne są: niepowtarzalne, niezmienne, nieusuwalne. Linie papilarne opisuje się za pomocą tzw. minucji – charakterystycznych cech, takich jak początki, zakończenia, rozwidlenia, haczyki itp. Wzajemny układ minucji jednoznacznie identyfikuje daną osobę. Na tej podstawie tworzy się algorytmy tworzenia i porównywania wzorca biometrycznego. Istnieje kilka różnych technologii pobierania wzorca linii papilarnych. Najczęściej stosowane są czytniki z sensorami: optycznym, pojemnościowym lub termicznym. Do najstarszych należy metoda optyczna, obecnie coraz popularniejszą jest metoda pojemnościowa.

Czytniki geometrii dłoni wykorzystując kamerę CCD oraz dokonując pomiarów palców i części dłoni, tworzą trójwymiarowy obraz ręki, który następnie – korzystając z technologii mikroprocesorowych – jest przetwarzany na wzorzec biometryczny.

Aby móc wyrobić sobie zdanie na efektywność wykorzystania różnych technologii biometrycznych, a co za tym idzie poznać osiąganą w praktyce – z uwzględnieniem spotykanych nieprawidłowych zachowań użytkowników systemu – wartość współczynnika fałszywego odrzucenia, poddano analizie dane uzyskane w systemach działających w różnych firmach. Na wykresie (*rys. 1*) zaprezentowano wartości współczynnika fałszywego odrzucenia dla wyżej opisanych technologii osiągane w czasie eksploatacji wdrożonych systemów, a w ***tabeli 1*** – porównanie wartości katalogowych z osiągniętymi w praktyce (testowano po dwa czytniki każdego typu z ustawionym średnim poziomem ufności).

Tab. 1. Porównanie FRR według danych katalogowych i osiągniętego w praktyce
Tabl. 1. Comparison of value FRR from data sheet with value *achieved* in practice

Typ czytnika	***Technologia***	***FRR według danych katalogowych***	***FRR osiągnięty w praktyce***
FIU500 (Sony)	linie papilarne – optyczny	<1%	28,9–29,4%
MV1200 (Bioscrypt)	linie papilarne – pojemnościowy	min. <1% (skalowalny, dla zastosowanego poziomu ufności 3 – <0,1%)	9,2–9,7%
HandPunch 3000 (Recognition Systems)	geometria dłoni	<0,1%	3,4–4,5%

Z wykresu jednoznacznie wynika, że najmniej problemów z fałszywym odrzuceniem wzorców należy się spodziewać w przypadku czytników geometrii dłoni (*geometria dłoni 1,2*), a najwięcej kłopotów – przy czytnikach optycznych linii papilarnych (*linie papilarne opt1, opt2*).

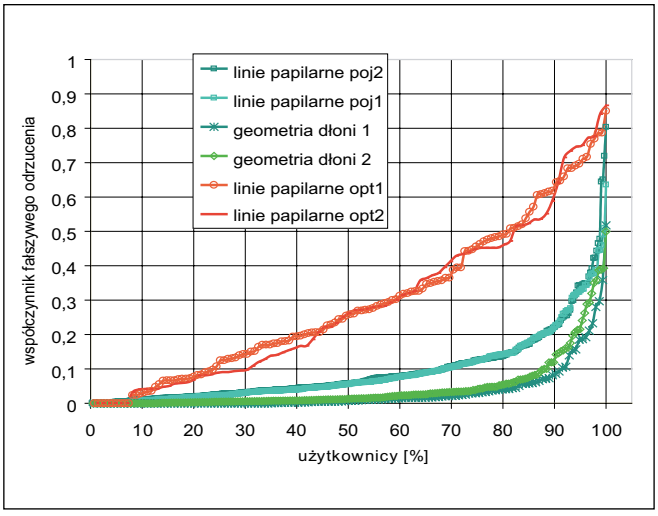
Należy jasno podkreślić, że przedstawione wyniki w żaden sposób nie podważają rzetelności danych katalogowych deklarowanych przez producentów sprzętu, a jedynie pokazują w jak niedoskonały sposób użytkownicy korzystają z najnowszych technologii. Powstaje jedynie pytanie, jakie czynniki powodują tak duże rozbieżności i czy użytkownik może wpływać na poprawę efektywności wykorzystania sprzętu.

Uwaga: Wszystkie zaprezentowane dane pochodzą z aktualnie eksploatowanych systemów. Użytkownicy nie byli w żaden szczególny sposób dobierani ani szkoleni – podlegali jedynie zwykłemu procesowi wdrażania systemów kontroli dostępu lub rejestracji czasu pracy. Korzystanie z systemu było obowiązkowe dla wszystkich pracowników w firmie.

Poniżej zamieszczono w formie tabelarycznej (*tab. 2*) informacje o danych prezentowanych na wykresie.

Tab. 2. Informacje o zakresie danych prezentowanych na *rys. 1*
Tabl. 2. Information about data presented in *Figure 1*

Czytnik	***Ilość wzorców***	***Ilość fałszywych odrzuceń***	***Ilość poprawnych rejestracji***	***Sumaryczna ilość rejestracji***	***FRR [%]***
poj1	348	98412	13033	111445	9,2
poj2	332	125786	12727	138513	9,7
dlon1	154	53134	1191	54325	3,4
dlon2	217	122696	5400	22596	4,5
opt1	135	4717	3466	8183	29,4
op2	86	2130	2982	8183	28,9
SUMA:	1581	484337	45009	426917	



Rys. 1. Współczynnik fałszywego odrzucenia dla wybranych technologii biometrycznych
Fig. 1. False rejection factor for the selected biometric technologies

Literatura

[1] Bolle R. M., Connell J.H., Pankanti S., Ratha N.K., Senior A. W.: Biometria. WNT, Warszawa, 2008.
[2] Techniki komputerowe. 1/2007, Instytut Maszyn Matematycznych, Warszawa.
[3] Recognition Systems.Inc: HandPunch 3000-4000 Operations and Users' Manual.
[4] Bioscrypt: MV 1200 MV-Lite OEM Modules. (DataSheet).
[5] Gomulska E.: Praktyczne aspekty wdrażania systemów biometrycznych – wartości współczynnika fałszywego odrzucenia. Elektronika, 2010.