

Wykład dotyczący Biometrycznych metod
identyfikacji z wykorzystaniem kodu DNA
człowieka

Copyright © Wojciech Bogucki

Rozdział 1 Podstawowe wiadomości dotyczące biometrii

1.1 Co to jest biometria?

Termin 'biometria' wywodzi się z greckich słów bio (życie, żywy, procesy życiowe) i metrics (mierzyć). Jest nauką zajmującą się identyfikowaniem i weryfikowaniem tożsamości osoby na podstawie jej cech fizjologicznych lub behawioralnych zwanych biometrykami. Takie cechy fizjologiczne są całkowicie niepowtarzalne, ponieważ żadne dwie osoby – nawet bliźnięta jednojajowe – nie otrzymują identycznych wyników pomiarów biometrycznych. Mówiąc ogólnie w biometrii człowiek jest kluczem.

Fizjologiczne	Behawioralne
Geometria twarzy	Barwa Głosu
Odciski palców	Podpis
Geometria dłoni	Chód
Obraz tęczówki	Ruch ust
Obraz siatkówki	Pisanie na klawiaturze
Kształt ucha	
Kod DNA	

Tabela 1.1 Popularne biometryki

Niestety metody biometryczne nie są idealne – bazują one na konieczności porównania pobranej wcześniej próbki, np. odcisku palca, z pomiarem podczas próby weryfikacji. Powoduje to, że są one wprawdzie wysoce skuteczne, lecz nie stuprocentowo pewne lub unikalne. W przeciwieństwie do np. stałego numeru dowodu osobistego przypisanego danemu obywatelowi próbki biometryczne pobrane w różnym czasie mogą się od siebie nieznacznie różnić. Przykładowo pracownik firmy, która zainstalowała u siebie system bezpieczeństwa bazujący na rozpoznawaniu głosu może mieć problem, jeżeli ma chrypkę. Aby sobie z tym problemem jakoś poradzić systemy biometryczne posiadają algorytmy aproksymacji, których zadaniem jest „dopasować” otrzymaną próbkę do wzorca danej osoby.

Możliwe zdarzenia występujące w takim systemie można podzielić następująco:

1. Prawidłowa akceptacja – dana osoba pracująca w firmie znajduje się w bazie i zostaje poprawnie w niej odnaleziona (identyfikacja) lub system prawidłowo rozpoznaje właściciela danego PIN-u (weryfikacja).
2. Fałszywa akceptacja – człowiek, który nie jest pracownikiem firmy (brak rejestracji w bazie) zostaje pozytywnie zidentyfikowany przez system (otrzymuje więc dostęp do zasobów chronionych).
3. Fałszywe odrzucenie – występuje wtedy, gdy osoba zarejestrowana w bazie i posiadająca właściwą akredytację zostaje mimo to odrzucona.
4. Prawidłowe odrzucenie – potencjalny oszust, człowiek niezarejestrowany w bazie wzorców nie otrzymuje dostępu do zasobów systemu (zachowanie jak najbardziej pożądane).

W praktyce najczęściej stosujemy dwa współczynniki oceny systemu biometrycznego:

1. False acceptance ratio (współczynnik błędnej akceptacji) – określa procentowo, jaką ilość pomiarów błędnie uznano za zgodną ze wzorcem.
2. False rejection ratio (współczynnik błędnego odrzucenia) – określa procentowo, jaką ilość pomiarów błędnie uznano za niezgodną ze wzorcem.

Budowa typowego systemu biometrycznego pociąga za sobą konieczność balansowania pomiędzy tymi danymi, ponieważ próby zmniejszenia jednego współczynnika prowadzą często do zwiększenia drugiego.

1.2 Jak działa system biometryczny?

Systemy Biometryczne działają na zasadzie rejestracji użytkowników przy pomocy pobierania oraz dalszego przechowywania konkretnego biometryka danej osoby. Następnie podczas próby uzyskania dostępu do danego zasobu lub lokacji taki unikalny wyznacznik jest porównywany z próbką pobraną od jeszcze niezidentyfikowanego osobnika.

Cały proces wygląda następująco:

1. Rejestracja użytkowników

Zanim dany człowiek będzie mógł skorzystać z dobrodziejstw systemu biometrycznego musi ukończyć proces rejestracji. W zależności od rodzaju systemu proces ten może być automatyczny lub wymagać ingerencji osób trzecich. Przyszły użytkownik podaje swoje dane oraz poddany zostaje

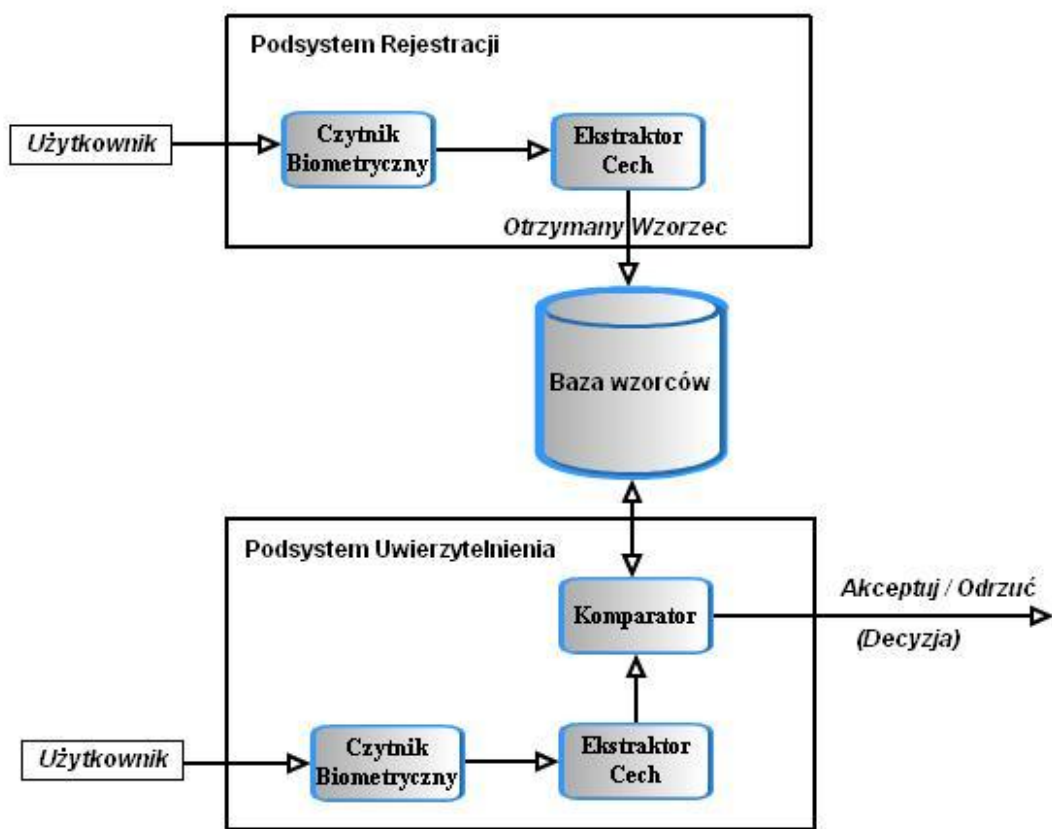
procesowi poboru próbki (np. skan siatkówki oka). W większości systemów wymagane jest kilka początkowych próbek, aby system mógł „uśrednić” wynik, biorąc pod uwagę możliwe przyszłe wahania.

2. Użytkowanie

W momencie, kiedy dana osoba chce uzyskać dostęp do danego chronionego zasobu następuje proces autentykacji zgodnie z procedurą (np. użycie skanera). Niezależnie od tego jak jest to przeprowadzane system porównuje pobrane dane biometryczne z tymi zapisanymi w bazie użytkowników i podejmuje decyzję dotyczącą danej osoby (odrzuć lub zaakceptować).

3. Aktualizacja

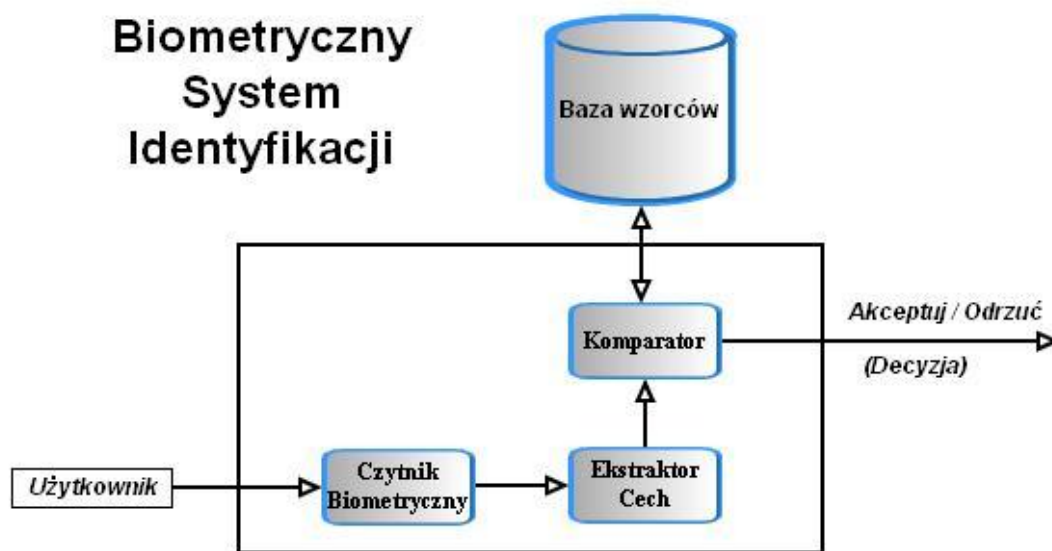
Niektóre typy biometryków (np. pismo lub geometria twarzy) z czasem mogą ulec zmianie u danej osoby. W takiej sytuacji system biometryczny wymaga aktualizacji, w przeciwnym wypadku może dochodzić do fałszywego odrzucenia uprawnionej osoby. Taka aktualizacja może się odbywać w trakcie normalnego użytkowania systemu (wykorzystywane są próbki pobierane podczas kolejnych prób identyfikacji) lub może to być osobny proces.



Rys 1.1 Architektura przykładowego systemu bezpieczeństwa

Użytkowanie systemu biometrycznego wiąże się zazwyczaj z koniecznością wyboru pomiędzy dwoma podstawowymi sposobami jego działania – identyfikacją oraz weryfikacją.

1. Identyfikacja – jest procesem porównywania przez system biometryczny pobranej próby do całego zestawu wzorców zapisanych w bazie danych (porównanie 1 do N). Pozytywna identyfikacja następuje jeżeli znajdzie się odpowiednik. Jako przykład identyfikacji można tu przytoczyć policyjne bazy odcisków palców. Aktualnie taki system funkcjonuje chociażby w FBI (IAFIS).

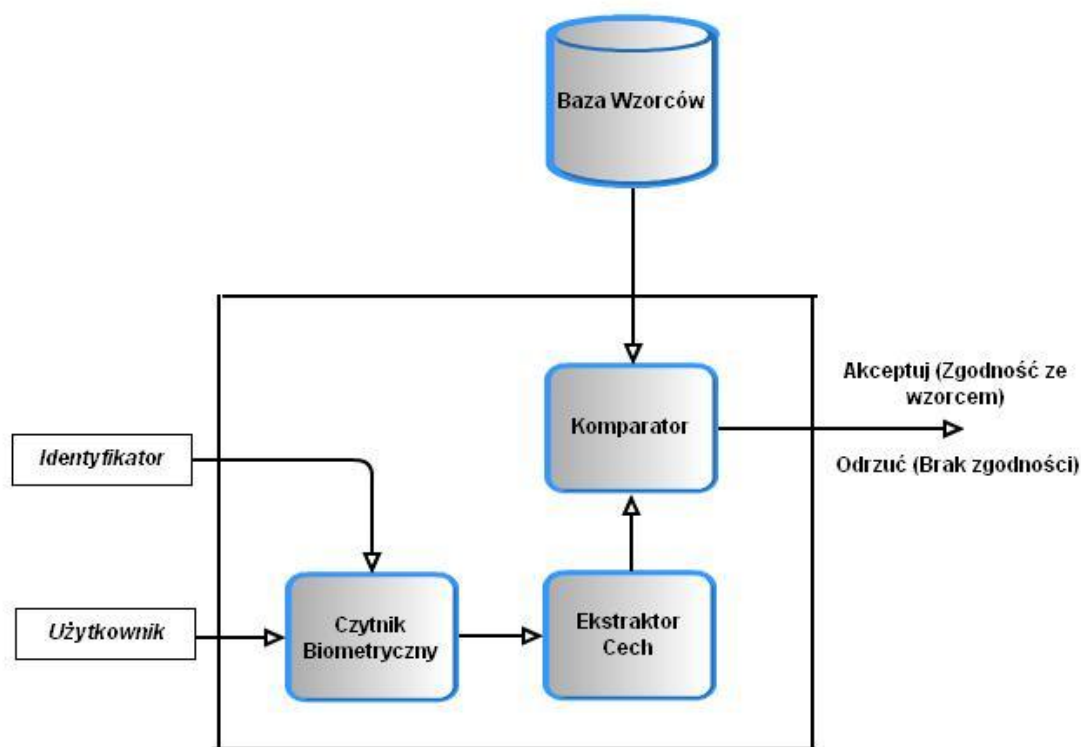


Rys 1.2 Przykład biometrycznego systemu identyfikacji

2. Weryfikacja – operacja systemu polegająca na porównaniu próbki biometrycznej oraz identyfikatora, np. PIN-u lub karty dostępu, którą dana osoba posiada ze konkretnym wzorcem znajdującym się w bazie (porównanie 1 do 1). Użycie identyfikatora w systemie biometrycznym znacznie skraca czas uzyskania wyniku, ponieważ wymaga tylko sprawdzenia zgodności z pojedynczym rekordem bazy.

Generalnie biometryczne zabezpieczenia zasobów można uznać za łatwe w obsłudze. Zarówno proces rejestracji jak i aktualizacji trwają relatywnie krótko. Dlatego

można uznać tego typu systemy za porównywalne z tradycyjnymi, a często bezpieczniejsze.



Rys 1.3 Przykład biometrycznego systemu weryfikacji

1.3 Cechy systemów biometrycznych

Każdy typ danych biometrycznych posiada pewne określone cechy, które należałoby wziąć pod uwagę podczas procesu wyboru. Do tych cech zaliczyć możemy:

1. Uniwersalność – cecha określająca jak duża jest grupa ludzi, od których dany biometryk da się pobrać. Przykładowo wszyscy pracownicy firmy mają co najmniej jeden palec z którego można pobrać odcisk, ale niektórzy jeżdżą na wózkach inwalidzkich – więc system bazujący na rozpoznawaniu chodu nie może być zaimplementowany.
2. Unikalność - cecha ta określa jak duże jest prawdopodobieństwo rozróżnienia dwóch osobników na podstawie danego biometryka. Pod tym względem prym wiodzie kod DNA.

3. Trwałość – dobry system biometryczny powinien mierzyć coś co nie zmienia się w trakcie upływu czasu. Także w tej kwestii najlepszy jest kod DNA oraz odcisk palca.
4. Inwazyjność – polega na określeniu tego jak łatwo można pobrać próbkę danego biometryka od danej osoby. Przykładowo w miarę łatwo można zeskanować dłoń przy pomocy odpowiedniego sprzętu podczas gdy kod DNA wymaga pobrania próbki genetycznej.
5. Wydajność – cecha określająca ogólne wymogi technologiczne i czasowe danego typu biometryka. Podczas gdy systemy poboru odcisków palców są niewielkie i efektywne, zdobycie wzorca DNA jest powolne i kosztowne.
6. Dokładność – określa jak dobrze system biometryczny potrafi rozróżnić pomiędzy dwojgiem ludzi i jakie są współczynniki fałszywej akceptacji i fałszywego odrzucenia.
7. Akceptowalność – cecha określająca poziom niechęci przeciętnego człowieka do używania danego systemu. Przykładowo system bazujący na DNA może budzić kontrowersje dotyczące prywatności, podczas gdy prosty czytnik linii papilarnych zostanie zaakceptowany bez większych problemów.
8. Bezpieczeństwo – cecha określająca jak łatwo dany system da się oszukać, jak dobrze radzi sobie z różnymi możliwymi metodami ataków.

1.4 Korzyści płynące z użytkowania systemu biometrycznego

Przeciwnicy rozbudowanych systemów bezpieczeństwa widzą jakiegokolwiek nowe formy ochrony jako niepotrzebne komplikacje, a często nawet problem związany z ochroną prywatności. Jednakże systemy bazujące na biometryce rozwijają się ostatnimi czasy w bardzo szybkim tempie. Ma to związek z wieloma korzyściami wynikającymi z wyboru tego typu ochrony:

1. Bardziej niezawodna identyfikacja – w przypadku identyfikacji biometrycznej prawdopodobieństwo tego, że osoba mająca dostęp do naszego systemu jest tym za kogo się podaje jest znacznie wyższe niż przy użyciu tradycyjnych metod bezpieczeństwa. Ryzyko zgubienia np. karty identyfikacyjnej w

momencie, kiedy uzyskanie dostępu wymaga także próbki biometrycznej znacznie obniża szansę infiltracji.

2. Całkowite wyeliminowanie „pożyczania” hasła – cechy biometryczne są nierozdzielnie związane z daną osobą, w związku z czym możliwości przykładowo wyludzenia hasła od współpracownika praktycznie nie istnieją.
3. Bardziej dogodne identyfikowanie – w zależności od sposobu w jaki dany system biometryczny został zaimplementowany może on okazać się bardziej przyjazny dla użytkowników od rozwiązań standardowych. Przykładowo osoba może zalogować się do systemu jedynie przykładając palec do czytnika co nie wymaga pieczołowitego wpisywania ID i hasła.

Rozdział 2 Najpopularniejsze typy biometryków

2.1 Bazujące na cechach fizycznych człowieka

Cechy fizyczne człowieka pozwalają nam na co dzień rozróżnić naszego sąsiada od całkowitego nieznajomego. Do najczęściej używanych w biometrii należą obraz tęczówki, geometria twarzy, geometria dłoni a także odciski palców. Fizyczne biometryki są ogólnie uważane za bardziej dokładne, w związku z czym są najpopularniejsze.

1. Obraz tęczówki

Systemy bezpieczeństwa bazujące na skanowaniu tęczówki oka stanowią około dziesięć procent rynku technologii biometrycznych. Skany tego typu są uznawane za najbardziej dokładne i godne zaufania. W rezultacie wykorzystywane są często do ochrony stref o zastrzonym poziomie bezpieczeństwa. Charakteryzują się średnim poziomem inwazyjności – użytkownik jest jedynie zmuszony do przyłożenia oka do odpowiedniego skanera.



Rys 2.1 Skaner tęczówki firmy Jiris

Źródło: <http://digitalcameras.techfresh.net/iris-scan-camera-jiris-jpc1000-from-jiristech/>

2. Geometria twarzy

Systemy bezpieczeństwa bazujące na rozpoznawaniu twarzy stanowią kolejne dziesięć procent rynku biometrycznego. Poziom inwazyjności tego typu systemów jest bardzo niewielki – kolokwialnie mówiąc wystarczy znaleźć się w „oku kamery”, czyli w jej polu widzenia. W razie wystąpienia problemów można także potwierdzić tożsamość osobnika wizualnie – może tego dokonać na przykład strażnik. Niestety do cech takich systemów można także zaliczyć problemy z niezawodnością – są one uzależnione od zewnętrznych czynników typu kąt widzenia twarzy lub jakość kamery.

3. Odciski palców

Zgodnie z danymi International Biometrics Group urządzenia bazujące na pobieraniu odcisków palców stanowią połowę wszystkich systemów biometrycznych. Rozpowszechniły się w instytucjach państwowych ze względu na swą relatywną prostotę oraz niski koszt. Nie są one jednak pozbawione wad, z których główną jest problem z prawidłowym pobraniem odcisków (rejestracją). Ma to związek z tym, że skóra na palcach, która zużywa się bez przerwy, degraduje się z wiekiem i uzyskanie akceptowalnego skanu jest często niemożliwe. Z drugiej strony systemy oparte na poborze odcisków palców są mało inwazyjne – wystarczy przyłożyć palec we wskazane miejsce.



Rys 2.2 Przykładowy czytnik linii papilarnych

Źródło: <http://www.itechnews.net/tag/fingerprint-reader/>

2.2 Bazujące na ludzkich zachowaniach

Systemy biometryczne, których podstawą są ludzkie zachowania należą do najbardziej skomplikowanych. Wzorce, zawierające w sobie takie czynniki jak czas (z jakim np. piszesz na klawiaturze) są często oparte na skomplikowanych algorytmach. Do tej kategorii biometryków możemy zaliczyć rozpoznawanie człowieka na podstawie głosu, pisma oraz tego jak pisze na klawiaturze.

1. Rozpoznawanie głosu

Rzadziej używany rodzaj biometryka, bazujący na unikalności ludzkiego głosu. Zazwyczaj podczas rejestracji w systemie użytkownik jest zobowiązany do wypowiedzenia konkretnych słów, które system analizuje pod kątem zawartych w głosie wzorów i tonacji. Następnie podczas próby uzyskania dostępu osoba musi powtórzyć niektóre z tych słów aby być rozpoznaną. Wadą tego typu rozwiązań jest niska odporność systemu na odgłosy w tle czy chorobę danego osobnika.

2. Rozpoznawanie na podstawie podpisu

Związane z podpisem systemy biometryczne starają się identyfikować ludzi poprzez dogłębną analizę unikalności składanych przez nich podpisów. Nie wykonują one tylko ich porównywania, ale także biorą pod uwagę jak dany podpis został utworzony – testują szybkość, poziom nacisku, powstałe kształty itd.



Rys 2.3 Klawiatura z wbudowaną analizą podpisu

Źródło: <http://www.getusb.info/usb-keyboard-with-built-in-touch-screen-for-handwriting-recognition/>

3. Rozpoznawanie na podstawie sposobu pisania na klawiaturze

Badania wykazują, że sposób w jaki ludzie „uderzają” po klawiszach jest jak najbardziej unikalny dla danego człowieka. Rejestracja w takim systemie polega na wpisaniu na klawiaturze konkretnego słowa lub słów kilka razy – co spowoduje utworzenie odpowiedniego wzorca. Po tej operacji system będzie rozpoznawał użytkownika po jego indywidualnym rytmie, jakiego używa podczas pisania.

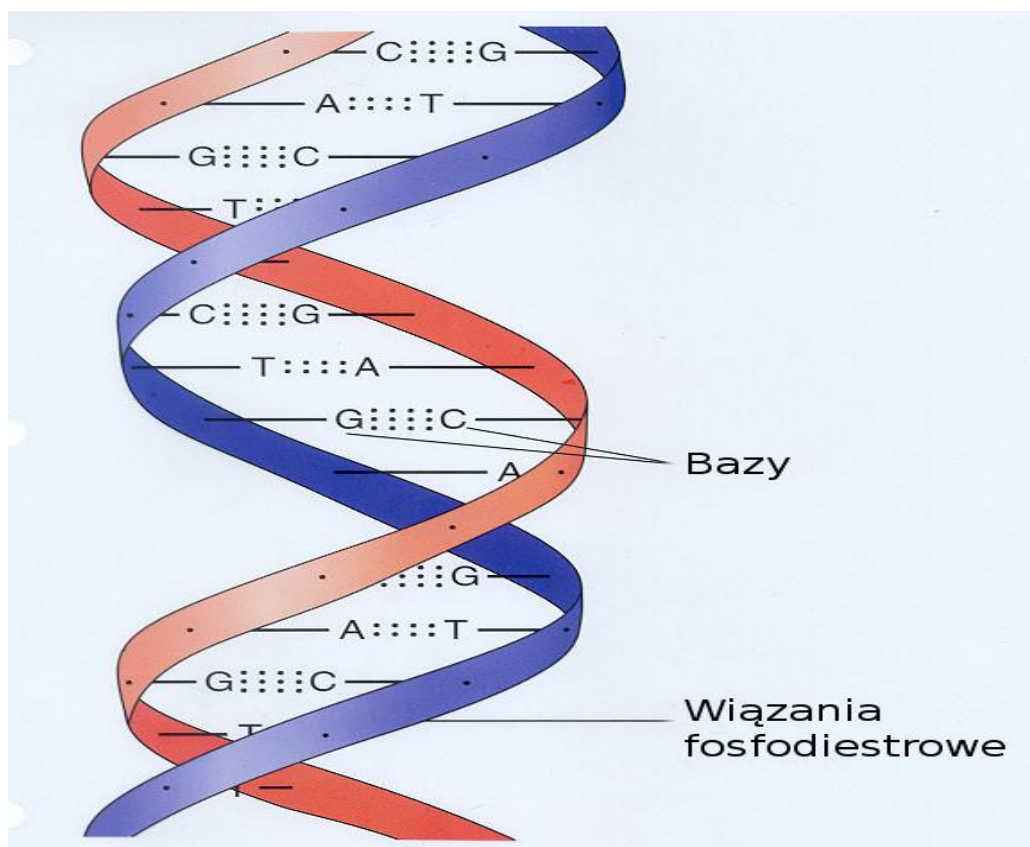
Rozdział 3 Techniki biometryczne z wykorzystaniem kodu DNA

3.1 Informacje podstawowe

Biometryka bazująca na kodzie DNA znalazła uznanie w środowisku naukowców, rządowym a także opinii publicznej jako stabilny biometryk, o teoretycznie większych możliwościach od najbardziej rozpowszechnionego do tej pory odcisku palca. Identyfikacja na podstawie unikalnej, mierzalnej a jednocześnie stabilnej charakterystyki genetycznej osobnika rozwijała się szybko w ciągu ostatnich dwóch dekad. Kod DNA (który można pobrać w bardzo różny sposób) wydaje się również być bardzo dokładnym biometrykiem, jeżeli badanie zostanie przeprowadzone prawidłowo (główne problemy to możliwe zanieczyszczenie próbki oraz ich zastępowanie).

Skrót DNA rozwija się jako „kwas deoksyrybonukleinowy”. DNA jest unikalną i możliwą do analizy cechą ludzką, powszechnie uznawaną przez społeczeństwo za jedyny konieczny dowód identyfikacji. W rzeczywistości tego typu badanie nie jest niepodważalne, ale jest jedynym o prawie idealnej skuteczności określonej na ok. 99,999%. Struktura chemiczna DNA każdego człowieka jest taka sama. Jedyna różnica pomiędzy ludźmi leży w sekwencji podstawowych par. U każdego osobnika występują ich miliony. Na podstawie kolejności ich występowania można rozpoznać danego człowieka. Ponieważ analiza wszystkich tych par nawet u jednego osobnika byłaby bardzo pracochłonna naukowcy skupiają się na niewielkiej ilości par, co do których wiadomo, że różnią się one w znacznym stopniu pomiędzy ludźmi.

W kodzie DNA zawarte są informacje genetyczne żywych organizmów. Ma ono strukturę dwóch łańcuchów, odkrytych przez Jamesa Watsona oraz Francis Cricka w 1953 roku. Każdy łańcuch ma liniową strukturę składającą się z czterech rodzajów nukleotydów: A – adeniny, G – guaniny, C – cytozyny oraz T – tyminy. Trzeba też wziąć pod uwagę, że tylko dwa typy połączeń są tutaj możliwe mianowicie adenina(A) zawsze łączy się z tyminą(T) natomiast guanina(G) z cytozyną(C). W związku z tym oba łańcuchy wzajemnie się uzupełniają, jeśli na przykład pierwszy zawiera sekwencję CCTTAGATCA to drugi będzie wyglądał tak GGAATCTAGT. Taka sekwencja par określa wszelkie cechy genetyczne danego człowieka.



Rys 3.1 Łańcuch DNA

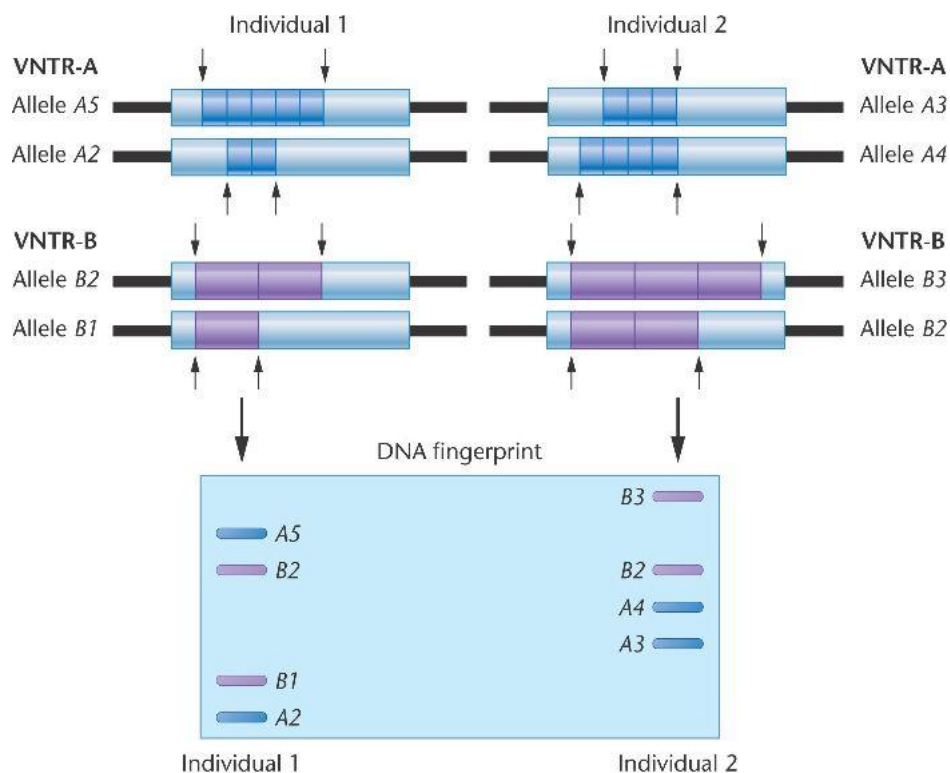
Źródło: http://coledavid.com/wonders/wonders_modern.html

W praktyce identyfikacja DNA bazuje na pewnych regionach kodu, zwanymi regionami niekodowanymi molekuly DNA (nie zawierają żadnych informacji o konkretnych cechach osobnika). Próbkę do zbadania można pobrać z bardzo różnych źródeł takich jak: ślina, krew, mocz, włos, tkanka czy kość. Żyjąc na co dzień własnym życiem mimowolnie „rozsiewamy” nasz kod genetyczny, zostawiając go w miejscach w których przebywaliśmy. Przekształcanie takiej próbki we wzorec jest procesem nieodwracalnym. Na podstawie takiego wzorca nie można poznać cech genetycznych lub medycznych danego człowieka, ponieważ technika ta skupia się na niekodowanych regionach łańcucha DNA, a konkretnie na regionach charakteryzujących się wysokim wskaźnikiem polimorfizmu (różnic u każdego człowieka).

3.2 Genetyczny odcisk palca

Technika odkryta przez Aleca Jeffreysa w 1984 na Uniwersytecie Leicester pozwala identyfikować pewne wzory DNA w loci (l. mnoga od „locus”, rodzaj „pojemników” na konkretne sekwencje kodu), które są unikalne dla każdego człowieka

za wyjątkiem bliźniąt jednojajowych. Każdy taki wzór to powtarzająca się część DNA (znana jako „zmienna liczba tandemowych powtórzeń” tzn. VNTR), której wielkość zależy od ilości powtórzeń. W granicach danego locus liczba takich powtórzeń jest różna u różnych osobników.



Rys 3.2 Przykład analizy VNTR

Źródło: http://bio3400.nicerweb.com/Locked/media/ch22/22_27-VNTR.jpg

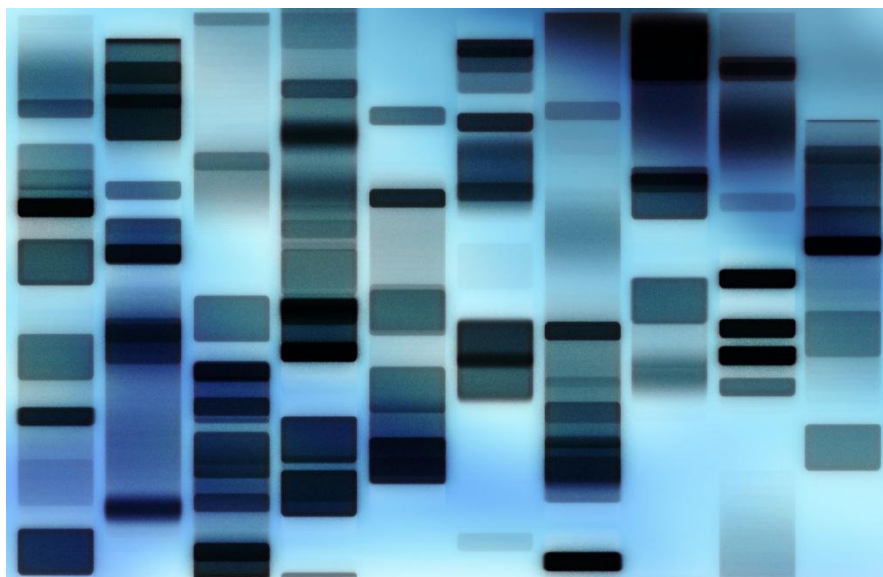
W rezultacie proces ten bazuje na analizie RFLP (polimorfizm długości fragmentów restrykcyjnych), którą to techniką wykrywa się różnice pomiędzy rozmiarami fragmentów DNA pociętych restryktazami.

Procedura utworzenia genetycznego odcisku palca składa się z następujących kroków:

1. Izolacja DNA – konieczne jest uzyskanie próbki DNA. Należy w szczególności uważać na możliwość jej zanieczyszczenia.
2. Cięcie, mierzenie oraz sortowanie – przy pomocy specjalnych enzymów zwanych restryktazami próbka DNA zostaje pocięta w konkretnych miejscach, w związku z czym powtarzalne sekcje kodu, o których była wcześniej mowa, stają się widoczne. Następnie zostają one odseparowane oraz posortowane przy pomocy procesu elektroforezy żelazowej (istotą tej

techniki jest rozdzielnie poprzez wymuszenie wędrówki cząsteczek w polu elektrycznym).

3. Przeniesienie – uzyskany w ten sposób wynik jest nanoszony na odpowiednią błonę nylonową (tzw. Blotting DNA – jest to transfer DNA na błonę/filtr najczęściej w celu hybrydyzacji z próbką znakowanego DNA).
4. Sondowanie – do otrzymanego związku dodajemy radioaktywne lub kolorujące cząsteczki znakujące w celu uzyskania genetycznego odcisku palca.
5. Faza końcowa – ostateczny wynik otrzymujemy przy pomocy ok. 5 do 10 takich cząsteczek – przypomina on pod pewnymi względami kod kreskowy.



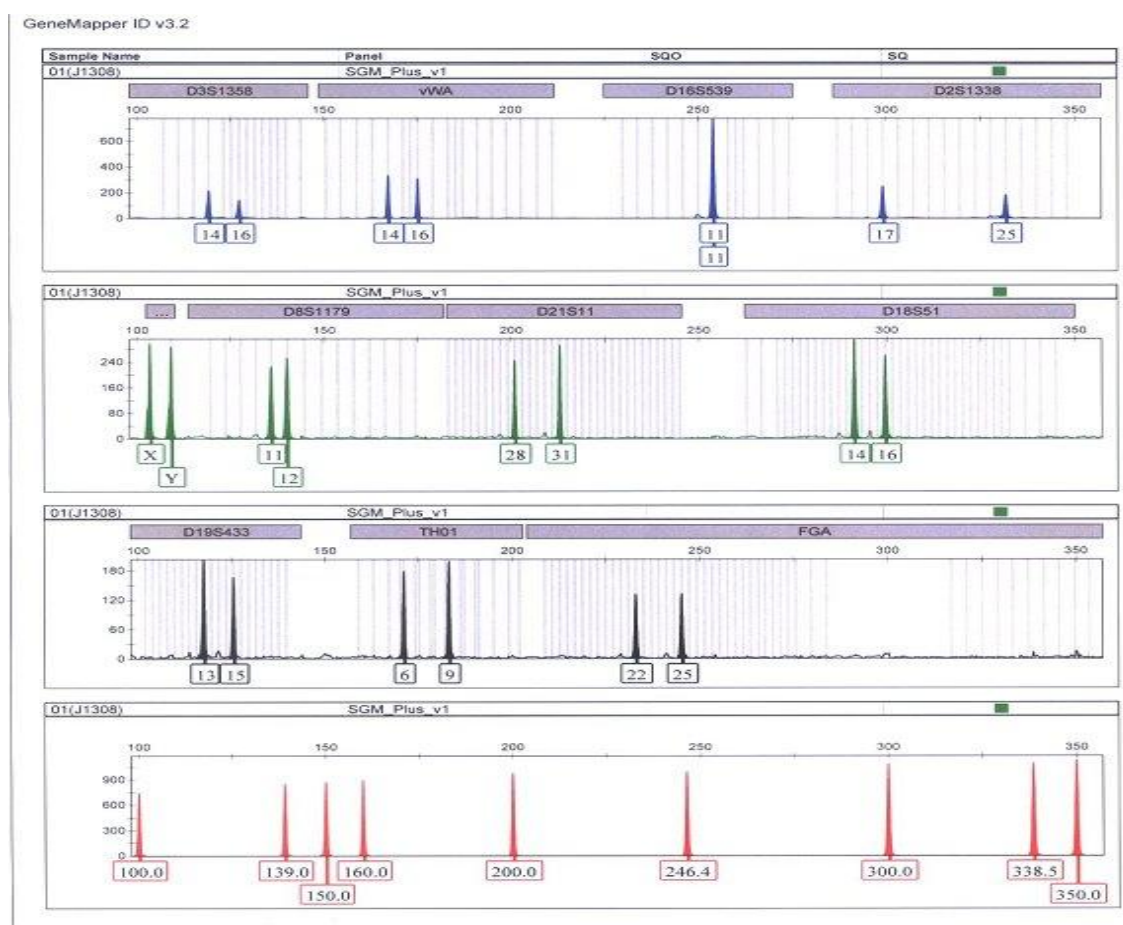
Rys 3.3 Genetyczny odcisk palca

Źródło: <http://www.nuffieldbioethics.org/bioinformation/>

3.3 Profilowanie DNA

Wykorzystując próbkę DNA jest możliwe utworzenie tzw. profilu DNA, który pozwala na reprezentowanie konkretnych wzorów będących częścią kodu w postaci numerycznej. Taka numeryczna reprezentacja może wyglądać na przykład tak: „15.313 , 12-13 , 17.5 , 9-10 ,7”. Każda para liczb w takim profilu jest związana z danym locus. Takie techniki wykorzystuje się głównie w kryminalistyce. Według danych Interpolu w Europie sytuacja systemów opartych na DNA przedstawia się następująco:

- 96% regionu Europy wykorzystuje identyfikację DNA
- 39 krajów używa jej w kryminalistyce
- 29 krajów zaimplementowało bazę danych kodów genetycznych
- 24 kraje mają oficjalne akredytowane laboratoria
- 27 krajów europejskich pozwala na wymianę profili DNA z innymi państwami



Rys 3.4 Przykładowy profil DNA utworzony przy użyciu programu GeneMapper

Źródło: <http://www.forensicscience.ie/index.asp?locID=18&docID=-1>

Tworzenie profili to świetne narzędzie, które z powodzeniem można wykorzystać do eliminacji osobników z grona podejrzanych. W większości śledztw konieczne jest kontrastowanie DNA podejrzanych z tym znalezionym na miejscu zdarzenia. W przypadku, gdy wzór DNA podejrzanego jest różny od tego zawartego w dowodach można go wykluczyć. W rezultacie genetyczny odcisk palca jest używany do udowodnienia niewinności podejrzanego. W takich przypadkach znacznie łatwiej wykluczyć danego osobnika z grona podejrzanych niż go do tej listy dodać. Takie założenia wykorzystuje się też przy ustalaniu ojcostwa. Istnieją tylko trzy realne konkluzje testu DNA:

1. Eliminacja – osobnik nie może być źródłem danej próbki.
2. Niemożność eliminacji – osobnik nie może zostać wykluczony z grona potencjalnych dawców.
3. Brak wyniku – analizy nie da się przeprowadzić.

3.4 Jak to działa w praktyce

W przeciwieństwie do pozostałych metod biometrycznych pobranie próbek DNA jest zawsze możliwe – każdy z nas posiada swój kod DNA. Poza tym DNA można pobrać w każdym wieku – praktycznie od momentu narodzin człowieka. Jednym z głównych plusów biometrii DNA jest właśnie współczynnik niemożności pobrania próbki, znany jako FTE (failure to enroll) wynoszący 0%. Z drugiej strony systemy biometryczne DNA nie są ani bezpośrednie (cały proces wymaga „fizycznej ekstrakcji” próbki oraz przeprowadzenia konkretnych reakcji biochemicznych – niestety nie da się zrobić „zdjęcia” DNA jak przykładowo podczas używania biometryka geometrii twarzy) ani automatyczne (wymaga ludzkiej ingerencji). Konsekwencją tego jest traktowanie biometryka DNA jako bardzo specyficznego typu, co wynika głównie z braku zautomatyzowanego procesu identyfikacji.

Pobieranie DNA polega na ekstrakcji komórek (jak wiadomo każda zawiera kompletny kod genetyczny) z konkretnego źródła, np. tkanki w celu uzyskania próbki DNA. Taki proces jest zazwyczaj prosty i mieści się w kilkunastu sekundach. Najczęstsze metody to ukłucie palca, pobranie śliny przy pomocy wacika czy też kawałka skóry. DNA podlega degradacji oraz zanieczyszczeniu, więc sposób przechowania próbki jest ważnym czynnikiem, aby w ostateczności uzyskać prawidłowy wynik. Degradacja może wynikać chociażby z powodu temperatury pomieszczenia, wilgotności powietrza lub nieodpowiedniego oświetlenia.

Zanieczyszczenie może mieć charakter chemiczny, biologiczny lub ludzki. W związku z powyższym konieczne jest wysuszenie oraz zamrożenie pobranego materiału. Tylko to zagwarantuje integralność oraz odpowiednią jakość próbki.

Jeśli chodzi o przekształcenie takiego materiału we wzorec to sposób uzyskania genetycznego odcisku palca został już wcześniej opisany (wynikiem jest swoisty „kod kreskowy” osobnika). Genetyczny odcisk palca reprezentuje konkretne wzory (czarne paski) znajdujące się w różnych loci (konkretnych częściach DNA). Istnieje także możliwość ich reprezentacji poprzez dane numeryczne, tworząc profil DNA co opisano w poprzednim podrozdziale. Jednakże w każdym przypadku transformacja jest procesem czasochłonnym (nawet kilka godzin) i wymaga odpowiednich umiejętności.

3.5 Cyfryzacja i przechowywanie

Aby wykonać digitalizację genetycznego odcisku palca konieczne jest uzyskanie zdjęcia np. przy użyciu kamery cyfrowej. W związku z czym typowa baza danych tutaj to zbiór zdjęć. Niektóre aspekty jak np. ilość cząsteczek (służących do wyodrębniania odcisku) oraz jakość obrazu powinna podlegać normalizacji, szczególnie jeżeli w przyszłości używane będą programy do ich porównywania.

W przypadku profili DNA baza danych przechowuje dane numeryczne, a bardziej szczegółowo ciągi liczb, które są bezpośrednią reprezentacją profilu DNA. Długość takich ciągów zależy bezpośrednio od ilości loci, które były użyte aby dany profil stworzyć. Najczęściej liczba ta nie jest w danej bazie stała. Także stopień precyzji liczb jest różnorodny. Jeżeli używa się tego rodzaju cyfryzacji konieczne wydaje się ustalenie pewnej standaryzacji, aby porównywanie w przyszłości było zasadne.

Jako przykład można podać USA gdzie uruchomiony został zintegrowany system indeksowania DNA, tzn. CODIS. Ta baza danych przechowuje wzorce DNA. Przy jej pomocy stróże prawa mogą analizować i dzielić się informacjami z innymi służbami. Z kolei w Europie istnieje system zwany European Network of Forensic Science Institute (ENFSI).

Porównywanie wzorców DNA nie jest prostym ani tanim zadaniem w związku ze skomplikowanym sposobem przekształcania próbki we wzorec. Czas potrzebny na przeprowadzenie weryfikacji nie jest krótki – wynosi nawet kilka godzin. Nawet używając specjalnych markerów DNA (na przykład program CODIS), niektóre części

tego procesu nadal są wykonywane ręcznie. Także porównywanie próbek nie przebiega w czasie rzeczywistym. Dodatkowo proces ten wymaga udziału naukowców, ponieważ jest uzależniony od konkretnej wiedzy i umiejętności. Ryzyko porównywania próbek sprowadza się do problemu bliźniąt jednojajowych – których tą metodą rozróżnić się nie da.

W przypadku genetycznego odcisku palca wykorzystywanego w kryminalistyce porównywanie odbywa się przy pomocy wzorców DNA, pobranych z miejsca zdarzenia oraz od ewentualnych sprawców. Proces określania zgodności jest procesem wykonywanym przez człowieka, którego komputer jedynie wspomaga. Na początku egzaminujący musi stwierdzić zgodność warunków laboratoryjnych z ustalonymi standardami. Następnie egzaminujący musi określić czy wzorce są zgodne biorąc pod uwagę kryteria zgodności. Wreszcie on lub ona musi określić prawdopodobieństwo tego, że wzorce są zgodne (czyli prawdopodobieństwo tego, że ta zgodność nie jest przypadkowa), tzw. współczynnik RMP (random match probability). W przypadku amerykańskiego systemu CODIS w tym miejscu następuje automatyczne przeszukanie baz danych skazańców oraz bazy kryminalistycznej zawierającej dane z miejsc popełnienia przestępstwa.

3.6 Aktualny stan technologii oraz jej ograniczenia

Testowanie przy pomocy DNA jest bardzo efektywne. Statystyka wykazuje szansę na to, że dwoje ludzi będzie miało ten sam profil na 1-do-6 miliardów. Z kolej używając technik DNA nie da się rozróżnić identycznych bliźniaków, a także dokładność tego biometryka jest uznawana za niższą niż obrazu siatkówki czy tęczęwki oka. Istnieje także prawdopodobieństwo zanieczyszczenia oraz degradacji próbki. Jeżeli chodzi o genetyczny odcisk palca aktualnie w fazie badań i rozwoju znajdują się już technologie pozwalające na błyskawiczne otrzymanie wyniku badania. Można się w związku z tym spodziewać większej automatyzacji całego procesu.

Kod DNA człowieka nie zmienia się poprzez całe życie, w związku z czym niezmienność DNA jest niepodważalna. Sprawdza się dobrze w takich zadaniach jak kryminalistyka, badania ojcostwa, itd. , lecz nie jest równie przydatna we wszystkich typach zadań. Testy DNA są trudne do podrobienia, jeśli są wykonywane we właściwych warunkach (nadzorowane i profesjonalne), jeżeli jednak pobory próbek nie są odpowiednio nadzorowane oszust mógłby łatwo podstawić DNA kogokolwiek. W

praktyce „zostawiamy” nasze DNA wszędzie gdzie się pojawiajemy – w związku z tym teoretycznie każdy ma do nich dostęp.

Biometria z wykorzystaniem DNA ma także inne problemy. Otrzymanie genetycznego odcisku palca trwa nawet kilka godzin. Metody pobierania próbek (fizyczne) także często rodzą niechęć. Dane zawarte w kodzie DNA to nie tylko dane pozwalające na identyfikację, ale także genetyczne, co budzi społeczny niepokój. Podsumowując można powiedzieć, że do plusów DNA zaliczamy uniwersalność, niezmienność, unikalność oraz odporność na oszustwa, a do minusów należą trudność zdobycia próbek oraz poziom ogólnej akceptowalności.

3.7 Problem prywatności oraz bezpieczeństwa

Pobieranie DNA uznawane jest za proces o wysokim stopniu inwazyjności. Aczkolwiek najnowsze metody ewoluowały w kierunku jej zmniejszenia (np. pobór próbki przy użyciu plastra na przedramieniu). W związku z tym nowe metody próbkowania uznawane są za nienaruszające społecznych standardów prywatności.

Głównym problem dotyczącym kodu DNA jest to, że zawiera on osobiste dane genetyczne oraz aspekty medyczne danego osobnika. Potencjalnie można więc naruszyć przy jego pomocy sferę prywatności, np. ujawniając czynniki dziedziczne danego człowieka. Jednakże profil DNA jest reprezentowany jedynie ciągiem liczb, więc nie jest z natury niebezpieczny i uznaje się go za neutralny. W kryminalistyce wybór markerów DNA jest wykonywany głównie po to by zachować neutralność. Uporczywie wybiera się na markery te części kodu, które znajdują się pomiędzy regionami kodowanymi (genami).

Jeśli chodzi o koncepcję rasy czy pochodzenia to jest to pojęcie kulturowe a nie biologiczne czy naukowe. Pomimo tego kod DNA potrafi określić miejsce pochodzenia przynajmniej niektórych przodków danego badanego.

Problem prywatności w największym stopniu związany jest z próbkami DNA, które przed dalszą obróbką pozwalają na określenie wielu wrażliwych informacji dotyczących jej dawcy. Kwestie prywatności skupiają się więc na bezpieczeństwie pobranych próbek oraz zapewnieniu ich pełnego zniszczenia po przekształceniu we wzorzec.

Podsumowując główne problemy bezpieczeństwa takich systemów należy zwrócić więc uwagę na implementację mechanizmów bezpieczeństwa w celu osiągnięcia wysokiego poziomu poufności, a także bezpieczeństwa bazy danych DNA. Wydaje się także rzeczą podstawową zapewnienie odpowiednich mechanizmów przechowywania próbek DNA (anonimowe, zaszyfrowane przechowywanie).

3.8 Przyszłe możliwości rozwoju

Przewidywany rozwój technik testowania DNA jest dwubiegunowy – aktualnie istniejące technologie rozwijają się w kierunku większej automatyzacji, precyzji oraz szybszego czasu procesów. Rozwijają się także nowe techniki eksploatujące elektroniczne właściwości DNA. Na dzień dzisiejszy nie da się rozróżnić bliźniąt jednojajowych, w przyszłości może to być jednak możliwe przy pomocy innego podejścia do sprawy. Taką alternatywną metodą może być badanie DNA mikroorganizmów, takich jak np. wirusy czy bakterie, które człowiek w sobie posiada. Ważne jest, aby zrozumieć, że DNA bakterii, zwierząt czy człowieka posiada tę samą strukturę chemiczną i budowę – główna różnica leży w długości takich molekuł (liczba podstawowych par u bakterii to około cztery miliony podczas gdy u człowieka to co najmniej trzy miliardy) oraz ich sekwencji. W związku z tym łatwiej i szybciej zbadać DNA grupy pasożytów, jakie dany osobnik posiada niż jego własne. Rozwijana jest także idea bezinwazyjnego badania DNA przy pomocy odpowiedniego skanera bazującego na technologii Bluetooth. Adresowany jest też problem czasu potrzebnego na przeprowadzenie badania – testy systemów opartych na PCR(reakcja łańcuchowa polimerazy, polegająca na sekwencji wielokrotnego podgrzewania i oziębiania próbki) pozwoliły zredukować czas potrzebny na wykonanie testu do 14 minut.