Azərbaycan Milli Elmlər Akademiyasi
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

Rasim Əliquliyev
Yadigar İmamverdiyev
Vüqar Musayev

BİOMETRİK TEXNOLOGİYALAR

Bakı - «İnformasiya texnologiyaları» - 2009

Əliquliyev R.M., İmamverdiyev Y.N., Musayev V.Y.

Biometrik texnologiyalar

Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2009, 376 səh.

Kitabda biometrik eyniləşdirmə sistemlərində istifadə edilən ideyaların, metodların və alqoritmlərin icmalı verilmişdir. Müxtəlif biometrik texnologiyaların vəziyyəti və inkişaf meylləri analiz edilmişdir. Barmaq izləri, sifət şəkli, gözün qüzehli qişası, səs xarakteristikalarından istifadə edən biometrik sistemlər ətraflı nəzərdən keçirilmiş, müxtəlif biometrik sistemlərdə geniş istifadə edilən təsvirlərin və siqnalların rəqəmsal emalı üzrə əsas metodlar təsvir edilmişdir. Biometrik sistemlərin iş xarakteristikalarının test edilməsi, biometrik texnologiyaların təhlükəsizliyi, elektron pasportlar ətraflı analiz edilmişdir.

Müvafiq ixtisasların tələbələri və aspirantları, həmçinin biometrik sistemlərin tətbiqi ilə maraqlanan şəxslər üçün nəzərdə tutulmuşdur.

Kitab AMEA İnformasiya Texnologiyaları İnstitutu Elmi şurasının qərarı ilə çapa məsləhət görülmüşdür.

Elmi redaktor: f.-r.e.n. R.M.Alıquliyev

ISBN: 978-9952-434-20-0

MÜNDƏRİCAT

GİRİŞ

Biometrik eyniləşdirmə sistemi milli eyniləşdirmə infrastrukturunda mühüm yer tutur. Biometrik texnologiyaların tətbiqi pasport-viza və şəxsiyyəti təsdiq edən digər sənədlərin mühafizə dərəcəsinin və şəxsin başqa fərdi məlumatlarla sənəd almasına nəzarətin gücləndirilməsini, kritik infrastrukturun və digər obyektlərin mühafizə rejiminin təkmilləşdirilməsini, identifikasiya işlərinin dəqiqliyini və müxtəlif informasiya resurslarında şəxs barədə fərdi məlumatların kompleks əlaqələndirilməsini təmin edir. Azərbaycan Respublikası Prezidentinin 13 fevral 2007-ci il tarixli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı" milli biometrik eyniləşdirmə sisteminin yaradılması sahəsində hüquqi, təşkilati, texniki, iqtisadi məsələlərlə yanaşı ölkənin elmi ictimaiyyəti qarşısında mühüm elmi-nəzəri və praktiki problemlər də qoyur.

Dövlət Proqramının həyata keçirilməsi iki mərhələdə nəzərdə tutulur.

1-ci mərhələ (2007-2009-cu illər) biometrik eyniləşdirmə sahəsində qanunvericilik bazasının təkmilləşdirilməsi, biometrik texnologiyalar əsasında elektron pasport-viza və şəxsiyyəti təsdiq edən digər sənədlərin istehsalının və tətbiqinin təşkili, biometrik informasiya resurslarının formalaşdırılması və təkmilləşdirilməsi işlərini əhatə edir.

2-ci mərhələ (2010-2012-ci illər) biometrik texnologiyaların tətbiqi sahələrinin genişləndirilməsi və onların təkmilləşdirilməsini (biometrik informasiya servislərinin təşkil edilməsini) nəzərdə tutur.

Biometrik eyniləşdirmə sisteminin yaradılması üzrə Tədbirlər planında müvafiq dövlət qurumları ilə yanaşı AMEA İnformasiya Texnologiyaları İnstitutuna da bir sıra mühüm elmi-praktiki tədbirlərin icrası tapşırılmışdır. Biometrik texnologiyalar yüksək elmi tutumlu informasiya texnologiyalarıdır. Milli biometrik eyniləşdirmə sisteminin qurulması möhkəm elmi-nəzəri və praktiki bazaya, yüksək hazırlıqlı kadr potensialına əsaslanmalıdır.

Fikrimizcə bu sistemin qurulmasında ilk addım biometrik texnologiyalar sahəsində elmi-tədqiqat və tədris-metodiki fəaliyyətin təşkilidir.

AMEA İnformasiya Texnologiyaları İnstitutunda biometrik texnologiyalar sahəsində elmi tədqiqatların əsas istiqamətləri ilk növbədə hazırki təxirəsalınmaz praktiki ehtiyaclara cavab vermək prinsipindən çıxış edərək müəyyən edilmişdir. Qeyd etmək lazımdır ki, institutda milli biometrik eyniləşdirmə sisteminin tədqiqi, biometrik texnologiyaların test edilməsi, biometrik sistemlərin təhlükəsizliyinin qiymətləndirilməsi, mövcud biometrik texnologiyaların təkmilləşdirilməsi və yeni texnologiyaların işlənməsi istiqamətlərində artıq bir sıra elmi nəticələr əldə edilmişdir. İnstitutda biometrik texnologiyalar üzrə dünyanın aparıcı elmi-tədqiqat mərkəzləri ilə əməkdaşlıq əlaqələrinin qurulmasına xüsusi fikir verilir. Məsələn, San-Xose Dövlət Universiteti nəzdində ABŞ Milli Biometrik Test Mərkəzi ilə biometrik sistemlərin təhlükəsizliyinin qiymətləndirilməsi üzrə birgə elmi-tədqiqat işləri aparılır.

Dövlət Proqramında nəzərdə tutulmuş elmi-tədqiqat işlərinin yerinə yetirilməsi gedişində əldə edilmiş elmi-praktiki təcrübəni, həmçinin biometrik texnologiyaların təhlükəsizliyinin test edilməsi üzrə alınmış elmi nəticələri nəzərə alaraq ABŞ tərəfdaşlarının tövsiyəsi və dəstəyi ilə biometrik texnologiyalar üzrə kitabın yazılması qərara alınmışdı.

Kitabın əsas məqsədi mümkün qədər geniş oxucu kütləsini biometrik texnologiyaların əsas problemləri ilə tanış etməkdir. Kitabda biometrik texnologiyaların əksər problemlərinə baxılır və analiz edilir. Kitab on bir fəsildən və əlavələrdən ibarətdir.

Kitabın birinci fəslində biometrik texnologiyaların əsas anlayışları təqdim olunur və həm geniş istifadə edilən, həm də elmi-tədqiqat və laborator sınaq mərhələlərində olan biometrik texnologiyaların geniş icmalı verilir. Geniş mənada biometriya dedikdə fərdin unikal fiziki və/və ya davranış xarakteristikalarının ölçülməsi başa düşülür. Dar mənada (hazırda əsasən bu istifadə edilir) bu anlayışa insanın unikal biometrik parametrlərinin analizi

əsasında şəxsiyyətin avtomatik identifikasiyası texnologiyaları və sistemləri daxil edilir.

İkinci fəsildə biometrik autentifikasiya sistemlərinin praktik tətbiqlərinin bir çox aspektləri öyrənilir, konkret tətbiqlər üçün biometrik parametrlərin seçilməsi prinsipləri və seçimə təsir edən amillər ətraflı analiz edilir. Biometrik sistemlərin dəqiqliyinin qiymətləndirilməsi, iş keyfiyyətlərinin ölçülməsi və müqayisəsi metodlarına baxılır. Biometrik texnologiyalar haqqında insanlarda formalaşan miflərin dağıdılması və biometrik texnologiyaların problemlərinin açıq müzakirəsinə cəhd edilir.

Üçüncü fəsildə artıq bir əsrdən çox tətbiq edilən barmaq izləri üzrə identifikasiya texnologiyasına baxılır. Barmaq izlərinin quruluşu, xarakterik nöqtələri, barmaq izlərinin sinifləri haqqında geniş məlumat verilir. Barmaq izlərinin ilkin emalı və müqayisəsi metodları ətraflı analiz edilir.

Dördüncü fəsildə aparıcı biometrik texnologiyalardan biri olan sifət şəkli üzrə tanıma texnologiyasının əsas metodları – sifətin həndəsi əlamətlərə görə tanınması, baş komponentlər metodu, xətti diskriminant analizi, sifətin kontur modelləri, elastiki qrafların müqayisəsi metodu, gizli Markov modelləri, üçölçülü sifət tanıma metodları nəzərdən keçirilir.

Beşinci fəsildə insanların da gündəlik həyatda geniş istifadə etdikləri səsə görə tanıma texnologiyası müzakirə edilir. Səsin fiziki xarakteristikaları, nitq siqnalının ilkin emalı, nitq əlamətlərinin parametrləşdirilməsi üsulları, diktor modelləri və qərar qəbul etmə qaydaları haqqında ətraflı məlumat verilir.

Altıncı fəsildə yaxın gələcəkdə geniş istifadə ediləcəyi gözlənilən texnologiyalar – gözün torlu qişası, DNT üzrə identifikasiya və multibiometrik texnologiyalar analiz edilir. Gözün torlu qişasının əlavə biometrik parametr kimi elektron pasportlara daxil edilməsi gündəmdədir. DNT üzrə identifikasiya isə ən dəqiq tanıma texnologiyası hesab olunur. Bəzi biometrik xüsusiyyətlər müəyyən şəxslərdə olmur və ya əlverişsiz vəziyyətdə olur. Bundan başqa multibiometrik sistemlər hücumlara qarşı daha dözümlü və etibarlıdır. Bir sıra başqa

üstünlüklərinə görə də multibiometrik sistemlərin yaradılması və tətbiqi – perspektivli inkişaf istiqamətidir.

Yeddinci fəsildə biometrik texnologiyaların test edilməsi metodologiyalarına baxılır, bir sıra biometrik texnologiyalar üzrə beynəlxalq testlərin təcrübəsi və nəticələri analiz edilir. Biometrik texnologiyalara tələbatın çox sürətlə artmasına baxmayaraq əsas məsələyə obyektiv və əsaslandırılmış cavab vermək lazımdır. Başqa sözlə, hələ lap cavan olan texnologiyalar onların üzərinə qoyulan məsələlərin öhdəsindən gəlməyə nə dərəcədə hazırdırlar? Biometrik sistemlərin test edilməsi bu suala müəyyən dərəcədə cavab verməyə xidmət edir.

Səkkizinci fəsildə biometrik texnologiyaların təhlükəsizliyi məsələləri araşdırılır. Autentifikasiya metodlarına tələbat artdıqca biometrik texnologiyalar daha geniş tətbiq edilməyə başlayır. Lakin avtomatik biometrik identifikasiyanın nailiyyətlərinə ictimaiyyətin artan diqqəti sayəsində insanların çoxuna elə gəlir ki, bu sahədə bütün problemlər həll edilib. Lakin əsil həqiqətdə bu belə deyil, çünki, biometrik sistemlərə bir sıra real təhlükələr mövcuddur və bunlar haqqında istifadəçilərin məlumatlı olmaları zəruridir.

Doqquzuncu fəsildə biometrik texnologiyalar üzrə normativ texniki və hüquqi baza analiz edilir. Biometrik texnologiyalar üzrə standartlaşdırma təşkilatlarının fəaliyyəti, biometrik standartların əsas sinifləri, biometrik məlumatların istifadəsi, mübadiləsi və saxlanması üzrə konkret beynəlxalq standartlar analiz edilir, yeni nəsil pasport-viza sənədlərinin istifadəsi üçün zəruri biometrik standartlar barədə tövsiyələr verilir.

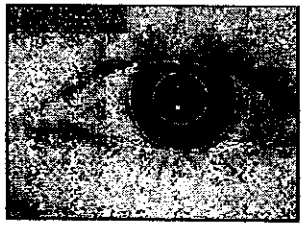
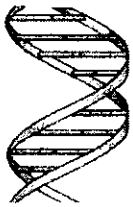
Onuncu fəsildə biometrik texnologiyaların ən geniş yayılmış tətbiqinə – yeni nəsil pasport-viza sənədlərinə baxılır. Elektron pasportların komponentləri, təhlükəsizlik mexanizmləri, e-pasportlar üçün Açıq Açarlar İnfrastrukturu (AAİ) ətraflı analiz edilir.

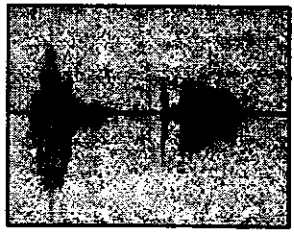
Nəhayət, on birinci fəsildə biometrik texnologiyaların inkişaf tarixi haqqında qısa məlumat verilir. İlk biometrik tanıma sistemi olan Bertilyon sistemi və onu əvəz etmiş daktiloskopiya sistemləri nəzərdən keçirilir.

Müəlliflər kitabın biometrik sistemləri layihələndirənlər və istismar edənlər, informasiya təhlükəsizliyi sahəsində fəaliyyət göstərən mütəxəssislər, müvafiq ixtisaslar üzrə təhsil alan tələbələr və aspirantlar üçün faydalı olacağına ümid bəsləyirlər.

Müəlliflər təşəkkür hissi ilə qeyd etmək istərdilər ki, kitabın yazılmasına Amerika Mülki Tədqiqatlar Fondu (U.S. Civilian Research & Development Foundation, CRDF) ilə Azərbaycan Milli Elm Fondu birlikdə qismən maliyyə dəstəyi göstərmişdir (qrant № AZM1-3112-BA-08). Müəlliflər həmçinin San-Xose Dövlət Universiteti nəzdində ABŞ Milli Biometrik Test Mərkəzinin direktoru doktor Ceyms Luis Veymana bu kitabın hazırlanmasında faydalı olmuş səmərəli müzakirələri və dəyərli məsləhətləri üçün dərin təşəkkürlərini bildirirlər.





FƏSİL 1

BİOMETRİK TEXNOLOGİYALARIN İCMALI

BİOMETRİK TEXNOLOGİYALARIN İCMALI

- **Autentifikasiya vasitələrinin növləri**
- **Biometrik sistemin komponentləri**
- **Biometrik məlumatın emalı**
- **Biometrik qeydiyyat**
- **Biometrik identifikasiya**
- **Biometrik verifikasiya**
- **Biometrik parametrlərin icmalı**

FƏSİL 1 BİOMETRİK TEXNOLOGİYALARIN İCMALI

Gündəlik həyatda insanlar bir-birini səs, yeriş, üz quruluşu kimi xüsusiyyətlərə görə tanıyır və fərqləndirirlər. Kiçik və dəyişməz qruplarda hər kəs bir-birini tanısa da, mürəkkəb, dinamik, dəyişən və qloballaşan informasiya cəmiyyətində şəxsiyyətin dəqiq müəyyən edilməsi olduqca çətinləşir və xüsusi əhəmiyyət kəsb edir. İnternetin və kağızsız texnologiyaların inkişafı ilə əlaqədar istifadəçilərin həqiqiliyinin yoxlanmasını (autentifikasiyasını) tələb edən tətbiqi proqramların sayı daim artır. İnformasiya təhlükəsizliyi risqləri artdıqca şəxslərin təhlükəsiz autentifikasiyası texnologiyalarına ehtiyac da kəskin artır. Çox zaman müəyyən resurslara müraciətin autentifikasiyası məsələsi konfidensiallığın təmin olunması məsələsindən daha vacib olur. Şəxsiyyətin dəqiq müəyyən edilməsində milyardlarla ölçülən maddi vəsaitlərin qorunması, beynəlxalq terrorizmlə mübarizə, mütəşəkkil cinayətkarlığın qarşısının alınması, qeyri-qanuni miqrasiya probleminin ciddi ölçüdə azaldılması, ticarət proseslərin sürətləndirilməsi, fərdi məlumatların qorunması kimi problemlər öz həllini tapır.

1.1. Autentifikasiya vasitələrinin növləri

Şəxsiyyətin kimliyinin düzgün müəyyən edilməsi üsullarını hansı faktora əsaslanmalarından asılı olaraq üç böyük kateqoriyaya bölmək olar:

- *nəyə isə malik olma*ya əsaslanan üsullar: bunlara adətən şəxsiyyəti təsdiq edən müxtəlif sənədlər (pasport, şəxsiyyət vəsiqəsi, sürücü vəsiqəsi, tələbə bileti), həmçinin maqnit kartlar, smart-kartlar, Touch Memory və birdəfəlik parolların

generasiyası üçün istifadə edilən fərdi generatorlar aid edilir.

- *gizli nəyisə bilməyə* əsaslanan üsullar: misal olaraq adi parolları, *fərdi identifikasiya nömrələrini* (Personal Identification Number, PIN), həmçinin gizli və açıq açarları göstərmək olar.
- *hansısa ayrılmaz xüsusiyyətlərə əsaslanan* üsullar: bu kateqoriyaya istifadəçinin biometrik xarakteristikalarının (barmaq izləri, sifət, səsin xarakteristikaları, əlin həndəsəsi, əl imzaları, gözün qüzehli qişası və s.) yoxlanmasına əsaslanan üsullar daxildir.

Şəxsiyyətin müəyyən edilməsi (autentifikasiya) üsullarının əsaslandığı faktorların müqayisəsi cədvəl 1.1-də ümumiləşdirilir.

Cədvəl 1.1. Autentifikasiya üsullarının müqayisəsi

Nöqsanlar	Nəyisə bilmək	Nəyəsə malik olmaq	Biometrik xarakteristika
İtirilə bilər	Hə	Hə	Yox
Oğurlana bilər	Hə	Hə	Yox
Unudula bilər	Hə	Hə	Yox
Saxtalaşdırıla bilər	Hə	Hə	Yox
Zədələnə bilər	Yox	Hə	Hə
"Dosta" verilə bilər	Hə	Hə	Yox

Cədvəldən də görünür ki, autentifikasiya vasitəsi kimi biometrik xarakteristikaların aşkar üstünlükləri var.

İlk iki üsulun çatışmayan cəhətləri ondan ibarətdir ki, insanların kredit kartı kimi malik olduğu maddi əşyaların itirilməsi və başqası tərəfindən asanlıqla istifadəsi hər zaman mümkündür. Parol, PIN-kod kimi yadda saxlanılan məlumatlar tez-tez unudulur, bir çox halda düzgün seçilmədiyi üçün etibarsız olur, bəzən də kifayət qədər etibarlı saxlanmadığı üçün qanunsuz istifadə edilir. Aparılan sorğular göstərir ki, insanların dörddə biri ATM kartlarının kodunu unutmamaq üçün kartın üzərinə yazırlar. Belə kart itirildikdə qanunsuz istifadəçi asanlıqla ondan istifadə edir. Asan yadda saxlamaq üçün seçilən parolların bir çoxu şəxslərin öz adları, soyadları, film qəhrəmanlarının adları, telefon nömrələri, doğum tarixləri kimi etibarsız parollardır. Seçilən parolun lüğətdən ixtiyari söz olması belə onun etibarını dəfələrlə

azaldır. Düzgün seçilməmiş belə bir parolun şəxsə və ya təşkilata vura biləcəyi ziyanı izah etməyə ehtiyac yoxdur. Plastik kartların, mobil telefonların və internetin istifadəsi bəzən onlarla müxtəlif parolu yadda saxlamağı tələb edir ki, bu da başqa bir çətinlikdir. Qeyd etmək lazımdır ki, inkişaf etmiş ölkələrdə "şəxsiyyətin oğurlanması" (**ID-theft**) – şəxsiyyəti müəyyən edən müxtəlif identifikatorların qeyri-qanuni ələ keçirilməsi çox geniş yayılmışdır və böyük maddi ziyan vuran ən ciddi təhdid hesab olunur.

Biometrik məlumatların autentifikasiya vasitəsi kimi şəksiz üstünlükləri var: xüsusi, mürəkkəb vasitələr olmadan biometrik məlumatların oğurlanması, saxtalaşdırılması və paylanması çox çətindir, onların itirilməsi və ya unudulması isə qeyri-mümkündür. İlk iki üsul gündəlik həyatda geniş tətbiq olunur. Şəxsiyyətin düzgün müəyyən edilməsi üçün bu yanaşmalardan birgə istifadə edilməsi daha etibarlıdır. Biometrik məlumatların onlara əlavəsi isə xüsusi əhəmiyyət kəsb edir.

1.2. Biometrik sistemlər

Biometrik sistem şəxsin biometrik xüsusiyyətlərini qeydə alan, şəxsin təqdim etdiyi biometrik məlumatla qeydə alınmış əvvəlki məlumatı müqayisə edərək şəxsin tanınması haqqında mənfi və ya müsbət qərar verən sistemdir.

Daha ümumi yanaşmada biometrik sistem aşağıdakıları yerinə yetirə bilən avtomatik sistemdir:

- insandan biometrik nümunə götürmək (məsələn, barmaq izi);
- biometrik nümunədən biometrik verilənləri (məsələn, barmaq izindən xüsusi nöqtələri və onların parametrlərini) çıxarmaq;
- biomertik verilənləri məlumat bazasında saxlanılan və onlarla eyni növdən olan bir və ya bir neçə verilənlə müqayisə etmək;

– təqdim olunan biometrik verilənlərin məlumat bazasındakı hər hansı verilənlərlə nə dərəcədə üst-üstə düşdüyünü müəyyən etmək;

– təqdim olunan biometrik verilənlərə görə şəxsin identifikasiya edilə bilməsi haqqında nəticə çıxarmaq və ya onun özünü qələmə verdiyi şəxs olmasını təsdiqləmək.

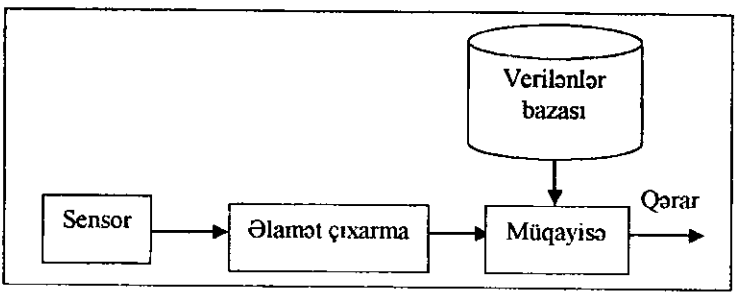
Biometrik sistem obrazların tanınması sistemidir və sadə biometrik sistemin dörd vacib komponenti var (şəkil 1.1):

(1) *Sensor modulu* – fərdin biometrik verilənlərini qəbul edir. Məsələn, barmaq izi sensoru istifadəçinin barmaq izlərini götürür.

(2) *Əlamət çıxarma modulu* – əlamətin qiymətlərini hesablamaq üçün qəbul edilmiş biometrik verilənlər emal edilir. Məsələn, barmaq izi sisteminin əlamət çıxarma modulunda barmaq izi təsvirindəki minusiya nöqtələrinin koordinatları və istiqamətləri əldə edilir.

(3) *Müqayisə modulu* – əlamət qiymətləri şablonda olan qiymətlərlə müqayisə edilir və müqayisə qiyməti hesablanır. Məsələn, bu modulda təqdim edilən barmaq izində və şablonda üst-ütə düşən minusiyaların sayı hesablanır və müqayisə qiyməti kimi qəbul edilir.

(4) *Qərar qəbuletmə modulu* – müqayisə modulunda hesablanmış müqayisə qiyməti əsasında istifadəçinin şəxsiyyəti müəyyən edilir və ya iddia edilən şəxsiyyət qəbul/rədd edilir.



Şəkil 1.1. Biometrik sistemin sadə sxemi

Qeyd etmək lazımdır ki, bəzi müəlliflər biometrik sistemlərdə daha çox komponent ayırmağı təklif edirlər. Məsələn, C.Veymana (J.Wayman) görə biometrik sistem beş altsistemdən ibarətdir:

- verilənlərin toplanması;
- verilənlərin ötürülməsi;
- siqnalların emalı;
- qərar qəbuletmə alqoritmi;
- verilənlər bazası.

1.3. Biometrik məlumatların emalı

Bütün biometrik xüsusiyyətlər biometrik sistemdə aşağıdakı emal mərhələlərinə uyğun olaraq istifadə edilir.

Qəbul. Biometrik məlumatlar mikrofon, barmaq izi sensoru, fotokamera kimi vasitələrlə rəqəmsal olaraq qəbul edilir və yaddaşda saxlanılır.

İlkin emal. İlkin emal sonrakı əlamət çıxarışı mərhələsinə hazırlıq məqsədi daşıyır. Məsələn, səsin identifikasiyasında siqnalın bəzi hissələrinin çıxarılması, əl imzasında imzanın koordinat sisteminin başlanğıc nöqtəsindən başlaması, barmaq izi üçün dönmənin normallaşdırılması və naziltmə prosesi ilkin emal mərhələsinə aiddir.

Əlamət çıxarışı. İlkin emaldan sonra fərqləndirici xüsusiyyətlərin müəyyən edilməsi nəzərdə tutulur. Əlamət çıxarışı alqoritmləri biometrik xüsusiyyətlər üçün fərqli olsa da, əsas məqsəd odur ki, obrazların tanınması prosesində istifadə üçün daxil olan obrazların əlamətlərinin təsvirini əldə etmək üçün məlumatın ölçüsü azaldılsın. Ümumiyyətlə, əlamət çıxarışı biristiqamətli funksiya hesab edilir və bu əlamətlərdən biometrik nümunənin ilkin qəbul edilmiş təsvirinin bərpa edilməsi mümkün deyildir. Barmaq izindəki minusiyaların yerlərinin müəyyənləşdirilməsi, əl imzası üçün bucağın və sürətin müəyyənləşdirilməsi əlamət çıxarışına aid işlərdəndir.

Biometrik şablonun hazırlanması. Bu mərhələdə istifadəçinin sistemə təqdim etdiyi bir və ya bir neçə biometrik xüsusiyyətin çıxarılmış əlamətləri əsasında biometrik şablon formalaşdırılır. Bu şablon sonrakı müqayisələr üçün saxlanılır.

Ümumi şablonun hazırlanması. Bəzi biometrik alqoritmlər üçün zəruri olan bu şablon sistemdəki bütün istifadəçilərin ümumi təsviridir.

Biometrik şablonun saxlanılması. Parametrləri müəyyən edilmiş biometrik şablonlar sonrakı biometrik əməliyyatlar üçün təhlükəsiz şəkildə saxlanılır.

Şablonların müqayisəsi. Təqdim edilən biometrik nümunənin bazadakı biometrik şablonlarla müqayisəsi nəticəsində aşkarlanan oxşarlıq kəmiyyətlə ifadə edilir.

Keçid qiymətinin hesablanması. İstifadəçiyə aid olan və olmayan biometrik məlumatlar sistemdəki şablonlarla müqayisə edilərək minimum keçid qiyməti müəyyən edilir ki, bu keçid qiymətindən aşağı nəticə verən müqayisələrin nəticəsi qeyri-məqbul sayılsın. Bu keçid qiyməti istifadəçilərdən asılı olaraq və ya bütün sistem üçün vahid şəkildə seçmək mümkündür.

1.4. Biometrik qeydiyyat

Biometrik sistem üç rejimdə işləyə bilər:

1. Qeydiyyat. Bu əməliyyatla sistemə yeni istifadəçi daxil edilir. İstifadəçinin müəyyən sayda biometrik nümunəsi qəbul edilir, ilkin emal, əlamət çıxarışı mərhələlərindən sonra biometrik şablon hazırlanır və keyfiyyət göstəricisi ilə birgə yadda saxlanır.

2. Verifikasiya. İddia edilən şəxsiyyətin yoxlanılması üçün təqdim edilən biometrik nümunənin əlamət çıxarışından sonra hazırlanmış şablonu bazada saxlanılan şablonla müqayisə edilərək uyğunluq qiyməti müəyyən edilir. Uyğunluq qiyməti keçid qiyməti ilə müqayisə edilərək müsbət və ya mənfi qərar verilir.

3. İdentifikasiya. Təqdim edilən biometrik nümunə bazadakı nümunələrlə müqayisə olunur və ən yaxın nümunələr seçilir. Ən

yüksək uyğunluq qiymətinə malik şablon təqdim edilən nümunə ilə eyni qəbul edilir.

Biometrik qeydiyyat obyektlərin biometrik verilənlər bazasında qeydiyyatı prosesidir. Qeydiyyat müsbət və ya mənfi ola bilər.

Müsbət qeydiyyat – verifikasiya və müsbət identifikasiya üçün qeydiyyatdır. Belə qeydiyyatın məqsədi qanuni obyektlərin verilənlər bazasını yaratmaqdır. Onun üçün obyektlərin qeydiyyata yararlı olmasının hansı əsaslarla qərarlaşdırıldığını müəyyən etmək lazımdır.

Biometrik nümunələr və digər təsdiqləyici məlumatlar verilənlər bazasında saxlanır. Verifikasiya rejimində verilənlər bazası paylanmış ola bilər. Qeydiyyat zamanı obyektə identifikasiya nömrəsi və ya biometrik şablon olan hər hansı bir daşıyıcı verilir.

Mənfi qeydiyyat – mənfi identifikasiya üçün qeydiyyatdır – müəyyən tətbiqlərə buraxılmayan obyektlər haqqında verilənlərin toplanmasından ibarətdir. Belə qeydiyyat zamanı yaradılan verilənlər bazaları mərkəzləşmiş olur. Mənfi qeydiyyat zamanı da obyektin hansı əsaslarla yararsız hesab olunacağını müəyyən etmək zəruridir. Obyektə qeydiyyatdan imtina ediləcəyi konkret tətbiq sahəsindən asılıdır.

Biometrik nümunələr və digər təsdiqləyici məlumatlar mənfi identifikasiya verilənlər bazasında saxlanır. Bu məcburi və ya gizli, obyektin özünün köməyi və razılığı olmadan edilə bilər.

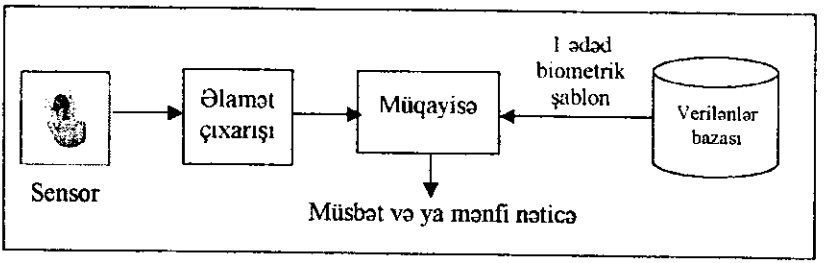
Qeydiyyat istifadəçi haqqında doğru məlumatlar formasında olan, yəni rəsmi sənədlərdən və ya digər etibarlı mənbələrdən, doğum haqqında şəhadətnamə, pasport, əvvəllər yaradılmış verilənlər bazası və cinayətkarların rəsmi verilənlər bazasından olan informasiyaya əsaslanır. Girişdəki obyekt əsas sənədlərlə və ya digər oxşar verilənlərlə müqayisə edilir. Oxşarlığın müəyyən edilməsi avtomatik sistem yox, insan tərəfindən aparılır, bu da səhvlərin potensial mənbəyidir.

1.5. Biometrik verifikasiya

Biometrik verifikasiyada biometrik sistemə biometrik parametr və unikal identifikator təqdim edilir. Təqdim edilən biometrik nümunə verilənlər bazasında bu identifikatora uyğun olan bir yazı ilə müqayisə edilir, buna görə də verifikasiya birin-birə (1:1) müqayisədir. Verilənlər bazası böyük ola bilər, lakin təqdim edilən identifikator verilənlər bazasında yalnız bir biometrik şablonu göstərir. Obyektin təqdim etdiyi unikal identifikator əsasında verilənlər bazasından seçilən biometrik şablonla biometrik nümunə müqayisə olunduqdan sonra sistem qəbul/imtina barədə qərar qəbul edir (şəkil 1.2).

Verilənlər bazasının iki konfiqurasiyası mümkündür.

Mərkəzi verilənlər bazası – qeydiyyata alınmış bütün istifadəçilərin biometrik məlumatlarını saxlayır. İstifadəçi hər hansı identifikasiya nişanı təqdim edir (kartı daxil edir, identifikasiya nömrəsini yığır), verilənlər bazasında uyğun biometrik şablonu tapmaq və sonradan obyektin biometrik nümunəsi ilə müqayisə etmək olar. Biometrik sistemlə biometrik şablon olan daşıyıcı arasında məlumat mübadiləsi təhlükəsiz protokol üzrə aparılmalıdır.



Şəkil 1.2. Biometrik verifikasiya

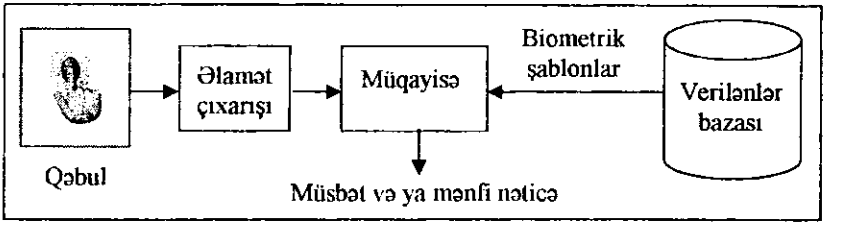
Belə verilənlər bazası bir obyekt və ya obyektlərin kiçik qrupu hər hansı qurğuların istifadəsi üçün avtorizə olunmalı olduqda istifadə edilir (məsələn, noutbuk, mobil telefon, fərdi kompüter).

Paylanmış verilənlər bazası – biometrik məlumat paylanmış şəkildə saxlanır (məsələn, smart-kartda). Bu halda şablonu bir verilənlər bazasında saxlamaq zəruri deyil.

Praktikada sistemlərin çoxu hər iki tip verilənlər bazasından istifadə edir – gündəlik oflayn verifikasiya üçün paylanmış bazadan, onlayn verifikasiya və ya itirilmə halında biometrik parametrləri təkrar ölçmədən yeni kart vermək üçün mərkəzi verilənlər bazası istifadə edilir.

1.6. Biometrik identifikasiya

Biometrik identifikasiya zamanı verilənlər bazasına daxil edilmiş məlumatlar əsasında qeyri-müəyyən şəxsiyyətin müəyyən edilməsi nəzərdə tutulur. Burada şəxsin verilən biometrik məlumatı bazadakı bütün məlumatlarla müqayisə edilir, yəni müqayisə *birin-çoxa* (1:N) müqayisədir. Sistem nəticədə ən yaxşı oxşarlığı və ya oxşarlıq dərəcəsinə görə sıralanmış bir neçə ehtimalı müəyyən edir. Biometrik identifikasiyada yalnız biometrik xarakteristikalar istifadə edilir (təsdiqləyici verilənlər), verifikasiya rejimindəki kimi sistemə identifikator təqdim edilmir. Şəkil 1.3-də biometrik identifikasiya sisteminin əsas blokları göstərilir. Birincisi, belə sistem biometrik şablonlar (biometrik şablonda bir neçə biometrik nümunə ola bilər) olan biometrik verilənlər bazası ilə əlaqəlidir.



Şəkil 1.3. Biometrik identifikasiya

İkincisi, biometrik identifikasiya sistemi obyektin daxil edilən biometrik nümunəsi ilə oxşarlığı olan şablonları müəyyən etmək üçün verilənlər bazasında axtarış apara bilər. Bu funksiya şəkildə

orta blokda göstərilib. Verilənlər bazasındakı şablonlar təqdim olunan nümunə ilə bir-bir yoxlanır. Prosedurun sonunda biometrik sistem daxil edilən biometrik nümunə ilə oxşarlığı yüksək olan identifikatorların siyahısını verir.

İdentifikasiya – mənfi və ya müsbət ola bilər.

Müsbət identifikasiya – biometrik sistem verilən şəxsin verilənlər bazasında olduğunu müəyyən edir. Burada məqsəd eyni bir şəxsiyyət identifikatorunun bir neçə istifadəçi tərəfindən istifadəsinin qarşısını almaqdır.

Mənfi identifikasiya – biometrik sistem verilən şəxsin müəyyən mənfi verilənlər bazasında olmadığını yoxlayır. Məsələn, bu axtarışda olan cinayətkarların siyahısı ola bilər.

Biometrik identifikasiya sistemi verilənlər bazasında obyektlə oxşarlığı olan bir neçə namizəd tapa bilər. Müsbət identifikasiya zamanı tələb olunur ki, namizədlər siyahısında bir namizəd olsun və ya ən azı namizədlərin sayını sürətlə birə qədər azaltmaq mümkün olsun. Mənfi identifikasiya zamanı operatorlar tərəfindən rahat emal olunması üçün namizədlərin sayı az olmalıdır.

1.7. Biometrik parametrlərin təsnifatı

Biometrik xüsusiyyətlər insanın fizioloji və davranış xüsusiyyətləri ilə əlaqədar olmaqla iki qrupa bölünür. Barmaq izi, əl həndəsəsi, gözün qüzehli qişası, ovucun izi kimi biometrik xüsusiyyətlər fizioloji, yeriş, əl imzası kimi biometrik xüsusiyyətlər isə davranışla bağlı hesab olunur. Səs kimi bəzi biometrik xüsusiyyətlərə fizioloji və davranışla bağlı xüsusiyyətlərin birləşməsi kimi baxmaq mümkündür. Əlavə olaraq, biometrik xüsusiyyətlər ailəsinə bioloji xüsusiyyətləri də əlavə etmək mümkündür. Əsas bioloji xüsusiyyətə misal kimi DNT (DeoksiriboNuklein Turşu) göstərilir. Texniki imkanlar nəzərə alındıqda, avtomatlaşdırılmış sistemlərdə DNT-nin biometrik xüsusiyyət kimi istifadəsi hələlik mümkün deyil.

Biometrik identifikatorun sabit (uzun müddət ərzində) və ya dəyişən olmasından asılı olaraq biometrik identifikatorları *statik* və *dinamik* olmaqla iki əsas qrupa bölürlər (cədvəl 1.2).

Statik identifikasiya metodları insanın dəyişməz fizioloji xarakteristikalarının analizinə əsaslanır (məsələn, barmaq izləri, əlin həndəsi ölçüləri, gözün qüzehli qişası).

Dinamik identifikasiya metodları şəxsin davranış xarakteristikalarının – hər hansı hərəkətin yerinə yetirilməsi prosesində hər bir insana xas xüsusiyyətlərin analizinə əsaslanır (məsələn, əl imzası, yeriş, səs).

Cədvəl 1.2. Biometrik xüsusiyyətlərin növləri

Növ	Misallar
Fizioloji	Barmaq izləri, gözün qüzeli qişası, gözün torlu qişası, əl həndəsəsi, termoqramlar, əl venaları
Davranış	Səs, əl imzası, yeriş, klaviatura xətti, dodaqların hərəkəti, ensefaloqram analizi
Bioloji	DNT, bədənin qoxusu

Davranış və fizioloji xarakteristikalar arasındakı fərq kifayət qədər sünidir. Biometrik davranış xarakteristikaları fizioloji xarakteristikalardan kifayət qədər asılıdır, məsələn, səs – səs tellərinin formasından, imza – barmaqların və biləyin cəldliyindən asılıdır. Bəzi fizioloji xarakteristikalar (məsələn, sifət) da insanın davranışından asılı olaraq dəyişə bilər. İnsanın davranışı (məsələn, barmağını skanerə necə qoyması və ya kameraya baxması) autentifikasiya sisteminin işinə təsir edə bilər.

Dinamik metodlar dəqiqlik və səmərə baxımından statik metodlardan xeyli geri qalırlar və bir qayda olaraq köməkçi biometrik xarakteristika kimi istifadə edilirlər.

Davranış və fizioloji xarakteristikalar arasındakı fərq kifayət qədər sünidir. Biometrik davranış xarakteristikaları fizioloji xarakteristikalardan kifayət qədər asılıdır, məsələn, səs – səs tellərinin formasından, imza – barmaqların və biləyin cəldliyindən asılıdır. Bəzi fizioloji xarakteristikalar (məsələn, sifət) da insanın davranışından asılı olaraq dəyişə bilər. İnsanın davranışı (məsələn, barmağını skanerə necə qoyması və ya kameraya baxması) autentifikasiya sisteminin işinə təsir edə bilər.

Dinamik metodlar dəqiqlik və səmərə baxımından statik metodlardan xeyli geri qalırlar və bir qayda olaraq köməkçi biometrik xarakteristika kimi istifadə edilirlər.

Başqa bir təsnifata görə biometrik identifikasiya metodlarını *interaktiv* və *qeyri-interaktiv* növlərə bölmək olar. İnteraktiv metodlar identifikasiya prosesində şəxsdən müəyyən hərəkətləri yerinə yetirməsini tələb edir. Məsələn, səsə görə tanıma metodunda müəyyən frazaları tələffüz etmək və ya barmaq izini götürmək üçün xüsusi qurğuya toxunmaq tələb edilir. Qeyri-interaktiv metodlar şəxs müəyyən vəziyyətə yaxınlaşdıqda avtomatik işə düşə bilərlər. Məsələn, sifətə görə tanıma metodu üçün şəxsin videoaparatın görüş dairəsinə düşməsi kifayətdir. Buna görə qeyri-interaktiv metodlar gizli rejimdə işləyə bilərlər – insanlar heç ağıllarına da gətirməyə bilərlər ki, maskalanmış qurğuların köməyi ilə onların biometrik xüsusiyyətlərini ölçürlər.

1.8. Biometrik parametrlərin icmalı

Müxtəlif tətbiqlərdə bir sıra biometrik parametrlər istifadə edilir. Hər biometrik parametrin üstün və zəif cəhətləri var və seçim adətən tətbiqdən asılı olur. Aşağıda geniş məlum olan biometrik parametrlərin qısa xülasəsi verilir.

Barmaq izləri. Barmaq izlərinə (şəkil 1.4) görə identifikasiya texnologiyası ən geniş yayılmış biometrik texnologiyadır. Bu metodun əsasında hər bir insanın əl barmaqlarında papilyar naxışların unikallığı ideyası durur.

Şəkil 1.4.

Barmaq izini papilyar xətlər əmələ gətirir, onların quruluşu dərinin şırımlarla ayrılmış qılıc çıxıntılarının sıraları ilə şərtlənir. Bu xətlər mürəkkəb naxışlar əmələ gətirirlər (qövs, ilgək və spiral), onların aşağıdakı xassələri var:

a) fərdilik və təkraredilməzlik;

b) zamana görə sabitlik (bətndaxili inkişafdan meyidin çürüməsinədək);

c) bərpa olunma (dəri qatının səthi zədələndikdə xətlərin quruluşu əvvəlki şəklində bərpa olunur).

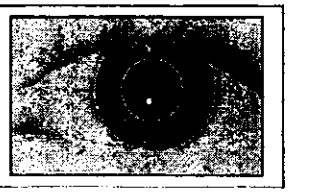
Bütün bunlar şəxsi yüksək etibarlıqla identifikasiya etməyə imkan verir. Xüsusi skanerin köməyi ilə götürülən barmaq izləri rəqəmsal koda çevrilir və əvvəl qeydiyyata alınmış şablonla müqayisə edilir.

XX əsrin ikinci yarısında yeni texniki imkanların meydana çıxması ilə əlaqədar olaraq barmaq izinə görə tanıma yalnız kriminalistikada istifadə edilmək çərçivəsindən çıxdı və informasiya texnologiyalarının ən müxtəlif sahələrində öz tətbiqlərini tapdı.

Barmaq izinə görə tanımanın üstünlükləri – istifadənin sadəliyi, rahatlığı və etibarlı olmasıdır. Bütün identifikasiya prosesi az vaxt alır. Tədqiqatlar həmçinin göstərmişdir ki, şəxsin identifikasiyası üçün barmaq izinin istifadəsi bütün biometrik metodlardan ən rahatıdır. İdentifikasiya zamanı səhv ehtimalı digər biometrik metodlarla müqayisədə xeyli kiçikdir. Bundan başqa, barmaq izinə görə identifikasiya qurğuları həcmcə kiçikdirlər.

Barmaq izinin tanınması və onun alqoritm tərəfindən düzgün emalının keyfiyyəti barmaq səthinin vəziyyətindən və skaner elementinə nəzərən onun yerləşməsindən çox asılıdır. Müxtəlif sistemlər bu iki parametrə müxtəlif tələblər irəli sürür. Tələblərin xarakteri xüsusi halda tətbiq edilən alqoritmdən asılıdır.

Gözün qüzehli qişası. İnsan gözünün qüzehli qişası (şəkil 1.5) barmaq izləri kimi onun unikal biometrik xarakteristikasıdır. Qüzehli qişanın şəklini analiz edən sistemlər kifayət qədər etibarlı tanımanı təmin edirlər. Bu xarakteristika yetərincə stabildir, insanın



Şəkil 1.5.