

**Azərbaycan Respublikası Təhsil Nazirliyi
Azərbaycan Dövlət İqtisad Universiteti**

MAGİSTRATURA MƏRKƏZİ

Əl yazması hüququnda

Mehdizadə Gündüz Fazil oğlu

***“Kompüter sistemlərində informasiya təhlükəsizliyinin biometrik
vasitələrindən istifadə” mövzusunda***

MAGİSTR DISSERTASIYASI

İxtisasın şifri və adı:	060632- "İnformasiya texnologiyaları və sistemləri mühəndisliyi"
İxtisaslaşma:	"İnformasiya mühafizəsi və təhlükəsizliyi"
Elmi rəhbər:	tex.e.n.,dos. H. İ. Mənsimov
Magistr proqramının rəhbəri:	akademik Ə. M. Abbasov
Kafedra müdiri:	akademik Ə. M. Abbasov

Bakı-2020

MÜNDƏRİCAT

GİRİŞ	3
FƏSİL I. KOMPÜTERİN NƏZƏRİ METODOLOJİ ƏSASLARI	6
1.1. İnformasiya təhlükəsizliyi.....	6
1.2. İnformasiya təhlükəsizliyinin aktual problemləri	8
FƏSİL II. BİOMETRİK PARAMETRLƏR	13
2.1. Biometrik sistemlər və biometrikanın tarixi	13
2.2. Biometrikanın məqsədi və biometrik sistemlərin üstünlüyü	18
2.3. Biometrik sistemlərin növləri.....	20
2.4. Biometrik sistemlərin işləmə mexanizmi və istifadə sahələri	37
2.5. Barmaq-damar tanıma sistemi	40
FƏSİL III. BİOMETRİK TEXNOLOGİYALARIN İSTİFADƏ MEXANİZMİ	49
3.1. Milli biometrik eyniləşdirmə sistemlərinin tədqiqi	49
3.1.1. Avtomatik barmaq izi tanıma sistemi- AFİS	49
3.1.2. IAFIS, IDENT(HART) və EURODAC.....	53
3.2. Biometrik texnologiyanın test edilməsi	54
3.3. Biometrik eyniləşdirmə sistemlərinin təhlükəsizliyinin qiymətləndirilməsi.....	59
3.4. Biometrik eyniləşdirmə texnologiyalarının standartlaşdırılması üsulları.....	59
NƏTİCƏ VƏ TƏKLİFLƏR	69
ƏDƏBİYYAT	71
SUMMARY	74
PE3IOME	75

GİRİŞ

Məxfilik və bununla da hər hansı bir məlumatın təhlükəsizliyi barədə danışmaq üçün identifikasiya anlayışı çox vacibdir. Məlumat göndərilmək üçün nəzərdə tutulan şəxsə və ya müəssisəyə deyil, başqa bir şəxsə və ya müəssisəyə göndərilirsə, arzuolunmaz nəticələr yarana bilər. Xüsusilə tibb və ya müdafiə sənayesi kimi sektorlarda əhəmiyyətli ölçülərin itirilməsini qeyd etmək lazım ola bilər.

Mövzunun aktuallığı: İnformasiya təhlükəsizliyi üçün istifadə edilən autentifikasiya prosesi üç fərqli şəkildə təhlil edilə bilər: məlumat əsaslı, mənşəli əsaslı və biometrik əsaslı. Bu işin mövzusu biometrik əsaslı təhlükəsizlik sistemləridir.

İnformasiya əsaslı eyniləşdirmə istifadəçilərdən və həmin sistemi idarə edən şəxsdən və ya şəxslərdən müəyyən məlumatların olmasını tələb edir. Bu məlumat bir istifadəçi adı və bir şifrə və ya bir pin şəklində ifadə edilən nömrələr xətti ola bilər. Belə sistemlərdə istifadəçilər və onların müvafiq məlumatları (şifrə, pin və s.) Verilənlər bazasında saxlanılır. İstifadəçilər məlumatlarını sistemə daxil etdikdə verilənlər bazasında bir müqayisə aparılır. Müqayisə nəticələri bir-birinə uyğundursa, bunun düzgün istifadəçi olduğu başa düşülür və istifadəçiyə sistemə daxil olmaq və sistem daxilində əməliyyatları həyata keçirmək icazəsi verilir. Bu cür sistemlərin əsas çatışmazlığı, istifadəçinin şifrə məlumatlarını unutması və ya bu məlumatı başqası tərəfindən əldə etməsinin asan olmasıdır.

Şəxsiyyət əsaslı identifikasiyanın başqa bir identifikasiya növündə istifadəçilərdə onlara uyğun bir obyekt var. Bu obyekt ümumiyyətlə bir maqnit kartı, rozet və ya açardır. Sözügedən sistemə giriş bu obyektlərdən istifadə edən istifadəçilər tərəfindən edilir. Obyektdə sistemə kimin daxil olduğunu və kimliyini təsdiqləyəcək məlumatlar var. Bu cür sistemlərdə bir insanın sual altındakı obyektə unutması, itirməsi, oğurlaya bilməsi bir mənfi cəhətdir.

Biometrik əsaslı eyniləşdirmə sistemlərində istifadəçi barmaq izi, səs, əl həndəsəsi, üz və ya imza atma, davranış kimi davranış xüsusiyyəti kimi fizioloji xüsusiyyətlərdən istifadə edərək sistemə daxil olur. İstifadəçi belə bir sistemə daxil

olmaq istədikdə sistem tərəfindən müvafiq biometrik məlumat (barmaq izi, retina, səs retina) sistem tərəfindən əldə edilir. Bu məlumatlar eyni şəxsdən götürülən və verilənlər bazasında qeyd olunan biometrik məlumatlarla müqayisə edilir. Müqayisə nəticəsi düzgün olarsa, şəxs təsdiqlənəcəkdir.

Tədqiqat işinin məqsədi: Bu tədqiqat işində əsas məqsəd məlumat təhlükəsizliyi üçün istifadə edilən autentifikasiya üsullarından biri olan biometrik sistemlər araşdırılır. Ədəbiyyatda aparılan araşdırmalar nəticəsində insanlarda bəzi bioloji xüsusiyyətlərin unikal olduğu ortaya çıxdı. Bu xüsusiyyətlər DNT, retina, iris, barmaq izləri, damar görüntüləri, üz formasıdır. Barmaq damarlarının tanınması sistemi təhlükəsizlik sistemlərində ayrı-ayrı şəxslərin barmaq damar şəkillərinin bir-birlərindən fərqli olmasına əsaslanan identifikasiya üsullarından biri kimi də istifadə olunur.

Tədqiqatın predmeti: Tədqiqat işinin predmeti olaraq insana xas olan biometrik parametrlərlə informasiyanın mühafizə olunmasının xüsusiyyətləri göstərilmişdir.

Tədqiqatın metodoloji bazası: Tədqiqatı aparılan mövzunun obyektini öyrənmək üçün mövcud vəziyyəti araşdıraraq müqayisəli təhlil metodikası və bu sahədə tədqiqat aparan tanınmış professor, alim və mütəxəssislərin elmi işləri və praktiki təklifləri əsas götürülmüşdür.

Tədqiqatın mənbəyi: Tədqiqat işində “Barmaq damar tanıma texnologiyası” adlı tezisdən, “Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə Dövlət Proqramı” əsasında yazılmış məqalələrdən, türk, ingilis və digər xarici dilli ədəbiyyatlardan və internet resurslarından istifadə olunmuşdur.

Elmi yenilik: Tədqiqat işində informasiya təhlükəsizliyinin təmin olunmasında biometrik parametrlərdən istifadənin bizlərə təqdim etdiyi imkanlarla bağlı praktiki və təcrübi əhəmiyyət kəsb edən təkliflər və nəticələr müəyyən edilmişdir ki, bunlar da öz növbəsində dissertasiya işinin sonunda öz əksini tapmışdır.

İşin praktiki əhəmiyyəti: Tədqiqat işi informasiyanın mühafizəsi və təhlükəsizliyi üçün lazım olan əsas vasitələrdən biometrik parametrlərdən istifadənin səmərəsi ilə bağlı praktiki təkliflərin müəyyən olunması istiqamətində aparılmışdır.

İşin strukturu və həcmi: Tədqiqat işi girişdən, üç fəsildən, nəticə və təkliflərdən ibarətdir. Birinci fəsil iki, ikinci fəsil beş və üçüncü fəsil isə dörd paraqraftan ibarətdir. Tədqiqat işinin sonunda istifadə olunan nəticə və elmi mənbələrin siyahısı verilmişdir.

İşin girişində mövzunun aktuallığı, problem haqqında qısa məlumat, tədqiqat işinin məqsədi və qarşıya çıxan problemlər müəyyənləşdirilib.

Dissertasiya işinin ***birinci fəslində*** informasiya təhlükəsizliyinə ümumi baxış həyata keçirilir. Bu fəsil iki paraqraftan ibarətdir. Birinci paraqraf informasiya təhlükəsizliyinə giriş, informasiya təhlükəsizliyi nədir və informasiya təhlükəsizliyi haqqında ümumi baza bilikləri əks olunmuşdur. İkinci paraqrafta informasiya təhlükəsizliyinin aktual problemləri olan iqtisadi və hüquqi problemlər barədə danışılmışdır.

İkinci fəsildə tədqiqat işinin əsas mövzusu olan biometrik sistemlər və parametrlərdən bəhs olunur. Bu fəsil beş paraqraftan ibarətdir. Birinci paraqrafta biometrik sistemlər və onların tarixi haqqında, biometrik sistemlər nədir kimi mövzulara toxunulmuşdur. İkinci paraqrafta biometrik sistemlərin məqsədi və üstünlüklərindən bəhs olunur. Üçüncü paraqrafta biometrik parametrlərdən- barmaq izi tanınması, gözün qüzehli qıyası, səs tanınması, üz tanınması, imza tanınması, DNT, əlin həndəsəsi kimi parametrlərdən danışılmışdır. Dördüncü paraqrafta biometrik sistemlərin işləmə mexanizmi və istifadə sahələri verilmişdir. Beşinci paraqrafta müasir dövrdə ən çox istifadə olunan biometrik tanıma sistemi olan barmaq damar tanıma texnologiyasından danışılır.

Üçüncü fəsil tədqiqat işinin praktiki xarakterini daşıyır. Bu fəsil dörd paraqraftan ibarətdir. Birinci paraqrafta milli biometrik identifikasiya sisteminin tədqiqi, ikinci paraqrafta biometrik texnologiyaların test edilməsi, üçüncü paraqrafta biometrik sistemlərin təhlükəsizliyinin qiymətləndirilməsi, dördüncü paraqrafta isə biometrik texnologiyaların standartlaşdırılmasından bəhs olunur.

FƏSİL I. KOMPÜTERİN NƏZƏRİ METODOLOJİ ƏSASLARI

1.1. İnformasiya təhlükəsizliyi

“İnformasiya təhlükəsizliyi” – məlumat və ona xidmət edən infrastrukturaların təbii və süni, qəsdən və təsadüfi təsirlərdən, sahibə və istifadəçilərə zərər verən məlumat və ona xidmət edən infrastrukturardan qorunması deməkdir.

İnformasiya təhlükəsizliyi məlumatların təhrif edilməməsinə, informasiya təhlükəsizliyinin təmin edilməsinə yönələn tədbirlər məcmusudur.

Təhdid - kiminsə maraqlarına mümkün bir hadisə, proses, fəaliyyət, vəziyyət, sistemə zərər verən digər şeylər və s. kimi nəzərdə tutulur.

Təhdid - məlumatların açıqlanması və dəyişdirilməsi və ya xidmətdən imtina şəklində zərər verə biləcək hər hansı bir vəziyyətləri, şəraitləri, prosesləri və ya hadisələri ifadə edir.

Təhlükələr müxtəlif qruplara bölünə bilər. Yaranma səbəblərinə görə təhlükələri süni və təbii olanlara bölürlər. Təsirinə görə üç növ təhlükə vardır:

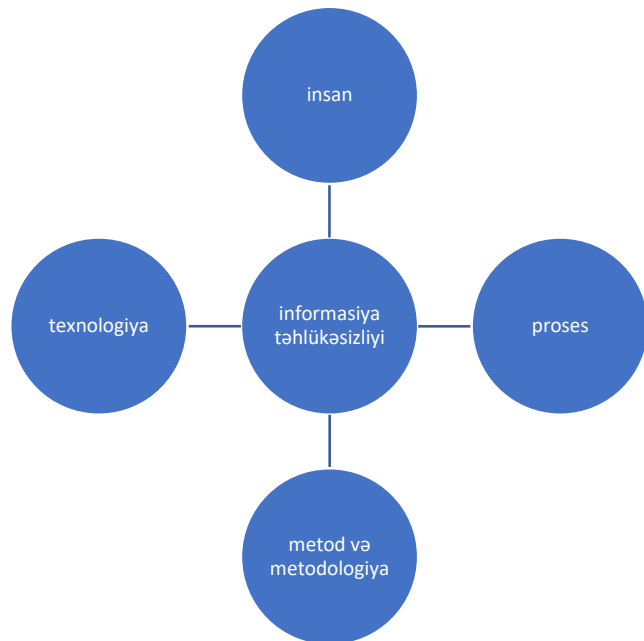
- Məlumatın məxfiliyinə yönələn təhdidlər;
- Məlumatın bütövlüyünə yönələn təhdidlər;
- Məlumatın əlçatanlığına yönələn təhdidlər

Təhdidlər digər xüsusiyyətlərə görə də təsnifləşdirilir:

- Yaranma ehtimalına görə (çox ehtimal olunan, ehtimal olunan, mümkün olmayan);
- Baş vermə səbəblərinə görə (qəsdən, təbii);
- Zərərin təbiətlərinə görə (mənəvi, maddi);
- Zərbənin təbiətinə görə (passiv, aktiv);
- Obyektə olan münasibətlərə görə (xarici, daxili)

İnformasiya təhlükəsizliyi, məlumatı icazəsiz daxil olmaqdan qorumaq, məxfiliyin təmin edilməsi, məlumatın bütöv olmasının təmin edilməsi və mövcudluğuna zəmanət etməkdir. İnformasiya təhlükəsizliyi içərisində texnologiya(aparat və proqram), insan, proses, metod və metodologiya kimi ünsürləri

birləşdirən və informatika dünyası üçün olduqca yüksək önəm daşıyan vacib bir məsələdir. Bu proses aşağıdakı şəkildə göstərilmişdir.



Şəkil 1.1. İnformasiya təhlükəsizliyinin əhatə dairəsinin təsviri

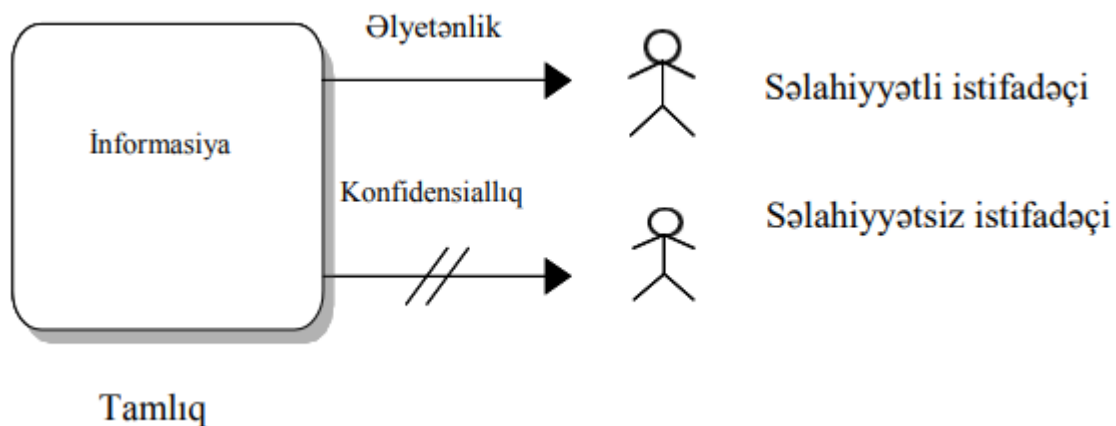
İnformasiya təhlükəsizliyi deyiləndə aşağıdakılar nəzərdə tutulur.

- Məxfilik
- Bütövlük
- Əlçatanlıq

İnformasiyanın məxfiliyi anlayışının mənası odur ki, informasiya sadəcə girişi olan şəxs və ya şəxslər üçün nəzərdə tutulmuşdur.

İnformasiyanın bütövlüyü məlumatın təhrif edilmədən, orijinal quruluşu məhv edilmədən qorunması deməkdir.

İnformasiyanın əlçatanlığı isə istənilən vaxt və məqbul bir zamanda məlumatların əldə edilməsi və istifadəsi deməkdir.



Şəkil 1.2. İnformasiya təhlükəsizliyinin əsas xassələri

İnformasiya təhlükəsizliyinin təmin edilməsi üçün məlumat aktivlərinin qorunması lazımdır. Bir təşkilatın qazanc əldə etmək, əlavə dəyər yaratmaq, rəqabətdə olmaq və korporativ dayanıqlığı təmin etmək məqsədilə sahib olduğu və ya sahib olması lazım olan bazar, texnologiya və ya təşkilata aid bütün məlumatların hamısı informasiya aktivləri kimi müəyyən edilə bilən olmalıdır. Bu informasiya aktivlərinin fiziki olaraq qorunması üçün fiziki təhlükəsizliyin, köçürülməsi lazım olan məlumatların təmin edilməsi üçün rabitə təhlükəsizliyinin, kompüter sistemlərinə girişi idarə etmək üçün kompüter və şəbəkə təhlükəsizliyinin təmin edilməsi vacib bir məsələdir.

1.2. İnformasiya təhlükəsizliyinin aktual problemləri

İnformasiya təhlükəsizliyi aşağıdakı problemlər üzrə öyrənilir:

1. İnformasiya təhlükəsizliyinin hüquqi problemləri;
2. İnformasiya təhlükəsizliyinin iqtisadi problemləri;

İnformasiya təhlükəsizliyinin hüquqi problemləri

İnformasiya cəmiyyətində insanlar öz ölkələrinin vətəndaşları olmaqla, mənsub olduqları dövlətin qanunları qarşısında məsuliyyət daşımaqla, hüquqları və vəzifələrini reallaşdırmaqla yanaşı, yeni bir dünyanın – virtual məkanın virtual vətəndaşına da çevrilirlər. Bu yeni dünyada hələlik hamılıqla qəbul edilən hüquq sistemi

formalaşmayıb. O cümlədən, virtual mühitdə informasiya təhlükəsizliyinin hüquqi tənzimlənməsi ilə bağlı bir sıra problemlər mövcuddur.

İnformasiya təhlükəsizliyinin hüquqi tənzimlənməsinin əsas vəzifəsi informasiya sahəsində milli maraq obyektlərinə qarşı olan təhdidlərin aradan qaldırılması, təhdidlərdən yaranan itkilərin minimallaşdırılmasına nail olmaqdır.

İnformasiya təhlükəsizliyinin hüquqi təminatının mühüm istiqamətlərindən biri müvafiq elmi tədqiqatların aparılmasıdır. Həmin elmi tədqiqatlar informasiya sahəsində milli maraq obyektlərinin hüquqi xüsusiyyətlərinin, həmin təhdidlərə qarşı effektiv mübarizəni təmin edən hüquqi vasitə və mexanizmlərin, müvafiq predmet sahəsində tənzimləmə prosesini həyata keçirmək üçün hüququn müxtəlif sahələrinin əməkdaşlıq imkanlarının, müvafiq sahədə beynəlxalq təcrübənin, həmçinin müvafiq tənzimlənmə ilə bağlı milli və beynəlxalq qanunvericilik arasındakı münasibətlərin öyrənilməsinə əhatə etməlidir.

Məlum olduğu kimi, informasiya sahəsi üzrə qanunvericiliyin tarixdə analoqu yoxdur. Ona görə də müvafiq qanunvericiliyin işlənməsində hüquqşünaslarla yanaşı, informasiya texnologiyaları mütəxəssisləri, psixoloqlar, sosioloqlar, pedaqoqlar və s. sahə təmsilçiləri iştirak etməlidirlər.

İnformasiya təhlükəsizliyi sahəsində normativ-hüquqi bazanın yaradılması çox çətin və mürəkkəb prosesdir. Bu da onunla bağlıdır ki, müvafiq normativ-hüquqi baza hələ formalaşmaqda olan, formalaşması ziddiyyətlərlə müşayiət olunan ictimai münasibətlərin tənzimlənməsi üçün yaradılır. Praktiki olaraq, hazırda nəhəng yeni informasiya vasitələri massivi hüquqi tənzimləmədən kənardadır. Bu sahədəki problemlərin kompleks şəkildə öyrənilməsinə, onların həlli üçün məqsədyönlü strategiyaların işlənməsinə və real şəraitə uyğun olaraq həyata keçirilməsinə ehtiyac vardır.

Beynəlxalq informasiya təhlükəsizliyi sahəsində hüquqi bazanın formalaşdırılması olduqca ləng və mürəkkəb bir prosesdir. Digər məsələlərdə olduğu

kimi, burada da beynəlxalq ictimaiyyət tipik problemlə üzləşir – ölkələrin maraqları üst-üstə düşür.

Beynəlxalq hüquqda da informasiya təhlükəsizliyinin təmin olunması məsələləri ilə bağlı bir sıra problemlər mövcuddur. İlk növbədə, qeyd etmək lazımdır ki, beynəlxalq hüquqda informasiya sferasında beynəlxalq təhlükəsizliyin mahiyyətinin hamılıqla qəbul edilməsi ilə bağlı yetərincə boşluqlar var. Hazırda ölkələr arasında aparılan danışıqlar bu problemi aradan qaldırmağa imkan vermir. Məsələn, bir ölkənin İKT-dən, yaxud KİV-dən silah qismində istifadə etməklə digər ölkəyə qarşı həyata keçirdiyi aqressiya aktının qiymətləndirilməsi ilə bağlı ümumi baxışlar mövcud deyil. Yaxud bu cür aqressiya aktına görə dövlətin yurisdiksiyasının hansı anda özünümüdafiə üçün tətbiq edilməsi ilə bağlı məsələlərə baxışlar da ziddiyyətlidir.

İnformasiya təhlükəsizliyinin hüquqi təminatı sahəsində mühüm problemlərdən biri də vahid terminologiyanın formalaşdırılması ilə bağlıdır. Beynəlxalq hüquqda informasiya təhlükəsizliyinin təmin olunması sahəsində baş verən prosesləri izah edə bilən kifayət qədər sabit terminlər yoxdur. Həmçinin informasiya sferasında beynəlxalq təhlükəsizliyə qarşı təhdid yarada biləcək subyektlərin sayı əhəmiyyətli dərəcədə artsa da, onların heç də hamısını mövcud hüquqi təminlərlə izah etmək mümkün deyil.

Ən mürəkkəb məsələ isə informasiya təhlükəsizliyinin təmin olunması ilə bağlı fəaliyyətin bir ölkənin yurisdiksiyası çərçivəsində həyata keçirilməsinin mümkün olmamasıdır.

Doğrudur, İKT-nin cinayətkar məqsədlərlə istifadəsi BMT Nizamnaməsində nəzərdə tutulan beynəlxalq hüququn xarakteristikası altına düşür. Belə ki, güc tətbiqi təhdidləri, güc tətbiqi, ərazi bütövlüyü, dövlət suverenliy və s. bu kimi dəyərlər BMT-nin həmin sənədində öz əksini tapıb. Amma beynəlxalq hüquq İKT-ni güc tətbiqi təhdidləri və ya güc tətbiqinin alətləri, yaxud vasitələri kimi nəzərdə tutmur.

KİV-in dövlətin daxili siyasətinə təsir etmək, onun ərazi bütövlüyünü dəyişdirmək, yaxud dövlət suverenliyini pozmaq kimi cinayətkar məqsədlərlə istifadəsi məsələsi isə, ümumiyyətlə, beynəlxalq hüququn müzakirə predmeti deyil.

İnformasiya təhlükəsizliyinin iqtisadi problemləri

İnformasiya təhlükəsizliyi texnoloji fəaliyyət sahəsi kimi qavranılsa da, bu sahədə bir sıra problemlər daha çox iqtisadi amillərlə bağlı olur. İstənilən sahədə olduğu kimi, informasiya təhlükəsizliyi iqtisadiyyatının da özünəməxsus xüsusiyyətləri mövcuddur. İnformasiya təhlükəsizliyi iqtisadiyyatı – bir sıra ümumi iqtisadi qanunlara və metodlara bağlı olsa da, iqtisadiyyatın müstəqil sahəsi kimi çıxış edir.

Cəmiyyətdə, o cümlədən iqtisadiyyatda informasiyanın artan rolu iqtisadi elmlərdə informasiya təhlükəsizliyinə marağı artırır. İqtisadi elmi istiqamətlərdə informasiya təhlükəsizliyinə, ilk növbədə, müəssisənin və dövlətin iqtisadi maraqları baxımından yanaşılır. Ən mühüm istiqamətlərdən biri informasiya təhlükəsizliyi vasitələrinin tətbiqinin iqtisadi dəyərinin qiymətləndirilməsi ilə bağlıdır. Burada əsas tədqiqat obyektı kimi müəssisənin informasiya təhlükəsizliyinin təmin edilməsinə çəkilən xərclərin iqtisadi səmərəliliyinin analizi çıxış edir [4].

Digər bir istiqamət kimi informasiya təhlükəsizliyi riskləri və təhdidlərinin qiymətləndirilməsi ilə bağlı tədqiqatları göstərmək olar. Bu istiqamət informasiya təhlükəsizliyinin iqtisadi təhdidlərinin təsnifatını, informasiya risklərinin sistemləşdirilməsini özündə birləşdirir. Həmçinin informasiya risklərinin qiymətləndirilməsi və analizi metodologiyalarının işlənməsini bu tədqiqat istiqamətinə aid etmək olar.

İnformasiya təhlükəsizliyi iqtisadiyyatının perspektiv istiqamətləri olaraq fiziki və hüquqi şəxslərin informasiya təhlükəsizliyi risklərinin sığortalanması sisteminin yaradılmasını və informasiya təhlükəsizliyi təhdidləri ilə mübarizənin iqtisadi metodlarının işlənməsini göstərmək olar.

Bütövlükdə, informasiya təhlükəsizliyinin iqtisadi problemləri istiqamətində aşağıdakı sahələr üzrə elmi tədqiqatların aparılması aktualıq kəsb edir [3]:

- müasir sosial-iqtisadi sistemlərin informasiya təhlükəsizliyi;
- informasiya təhlükəsizliyi risklərinin (o cümlədən, informasiyanın, informasiya resurslarının dəyərinin və vurulan ziyanın) qiymətləndirilməsi;

- informasiya təhlükəsizliyi risklərinin sığortalanması modelləri;
- informasiya təhlükəsizliyinə yatırılan investisiyaların modelləşdirilməsi;
- iqtisadiyyatın müəyyən sektorlarının kiber-hücumlara həssaslığının qiymətləndirilməsi;
- e-xidmətlərin, o cümlədən e-kommersiyanın informasiya təhlükəsizliyi;
- informasiya təhlükəsizliyinin təmin edilməsi üçün resursların paylanması modelləri;
- informasiya resurslarına mülkiyyət münasibətlərinin iqtisadi tənzimlənməsi məsələləri və s.

FƏSİL II. BIOMETRİK PARAMETRLƏR

2.1. Biometrik sistemlər və biometrikanın tarixi

Biometrika, bioloji məlumatları, yəni bir insanın fərdi xüsusiyyətlərini və ya davranışlarını təhlil edərək şəxsiyyəti təsdiqləyən bir elmdir. Həyatımızda böyük əhəmiyyət daşıyan biometrik əsaslı yoxlama etibarlı identifikasiya üçün güclü bir üsuldur. Bu gün biometriya getdikcə populyarlaşır. Biometrik sistem bir insanın təbiətini və ya davranışını araşdırır və əvvəllər yaradılan qeydlə müqayisə edir. Bu sistem fərdin barmaq izini, əlini, ovucunu, retinasını və ya səsini araşdırdığı üçün son dərəcə həssas olmalıdır. Fərdin anatomik və ya fizioloji xüsusiyyətlərini ölçərkən dəqiq və təkrar ölçülər edilməlidir .

Biometriya termini yunan dilində bio (həyat) və ölçü (ölçmək) sözlərindən yaranmışdır. Avtomatlaşdırılmış biometrik sistemlər yalnız son bir neçə onillikdə kompüter işlənməsində əhəmiyyətli irəliləyişlər sayəsində mövcud olmuşdur. Bu yeni avtomatlaşdırılmış texnikaların bir çoxu yüzlərlə və hətta minlərlə il əvvəl hazırlanmış fikirlərə əsaslanır .

İnsanlar tərəfindən tanınmaq üçün istifadə edilən ən qədim və əsas nümunələrdən biri də üzdür. Sivilizasiyanın başlanğıcından bəri insanlar məlum (tanış) və naməlum (tanımadığı) şəxsləri tanımaq üçün üzlərdən istifadə etmişlər. Bu sadə tapşırıq getdikcə çətinləşir və əhali artdıqca və çox sayda yeni insanı bir dəfə kiçik icmalara tanıtdırır. Şəxsdən şəxsə tanıma anlayışı dinamik və yerləş tanıma kimi davranış dominant biometriklərdə də görülür. Şəxslər bu xüsusiyyətlərdən bilinmədən gündəlik olaraq tanınan şəxsləri tanımaq üçün istifadə edirlər.

Digər xüsusiyyətlər sivilizasiya tarixi boyunca daha rəsmi tanıma vasitəsi olaraq istifadə edilmişdir. Bəzi nümunələr:

- Ən azı 31.000 il yaşı olduğu təxmin edilən bir mağarada divarları orada yaşayan kişilər tərəfindən yaradıldığına inandığı rəsmlərlə bəzədilmişdir. Bu rəsmlərin ətrafında yaradıcısının "unudulmaz bir imza kimi hərəkət etdiyi" düşünülməli bir çox əl izi var.

- Barmaq izlərinin eramızdan əvvəl 500-cü ilə qədər bir insanın əlaməti olaraq istifadə olunduğuna dair sübutlar da mövcuddur. Babil ticarət əməliyyatları barmaq izləri olan gil lövhələrdə qeyd olunur.
- İspaniyalı tədqiqatçı və yazıçı Joao de Barros yazırdı ki, ilk Çin treyderləri ticarət əməliyyatlarını həyata keçirmək üçün barmaq izlərindən istifadə edir. Çinli valideynlər uşaqları ayırd etmək üçün barmaq izlərindən və ayaq izlərindən də istifadə etdilər.
- 14-cü əsr farsca Jaamehol-Tawarikh kitabında barmaq izlərindən insanları müəyyənləşdirmək üçün tətbiq olunan şərhələr var.
- 1684-cü ildə Dr. Nehemiah Grew, London Kral Cəmiyyətinin Fəlsəfi Prosesləri məqaləsində sürtünməyə qarşı dəri müşahidələrini yayımladı.
- Hollandiyalı anatomist Govard Bidloonun 1685-ci il tarixli İnsan bədəninin anatomiyası kitabı da sürtünmənin təfərrüatlarını izah etdi.
- 1686-cı ildə Bolonya Universitetinin anatomiya professoru Marcello Malpighi, araşdırmasında barmaq izləri silsilələri, spiral və döngələri qeyd etdi.
- 1800-cü illərin ortalarına qədər, sənaye inqilabı və daha məhsuldar kənd təsərrüfatı səbəbiylə şəhərlərin sürətli böyüməsi ilə insanların müəyyənləşdirilməsinə rəsmi şəkildə ehtiyac duyuldu. Tacirlər və vəzifəli şəxslər getdikcə daha çox və daha fəal əhali ilə qarşılaşdılar və artıq yalnız öz təcrübələrinə və yerli biliklərə etibar edə bilmədilər. Jeremy Bentham və digər Utilitar müfəkkirlərin yazılarından təsirlənən bu dövr məhkəmələri bu günə qədər bizimlə qalan ədalət anlayışlarını kodlaşdırmağa başladı. Ən əsası, ədliyyə sistemləri cinayətkarlara ilk dəfə daha yumşaq davranmağa və cinayətkarları daha sərt şəkildə təkrarlamağa çalışdı. Bunun üçün cinayətin ölçülmüş şəxsiyyət xüsusiyyətləri ilə birlikdə cinayətləri qeydə alan rəsmi bir sistem tələb edildi. İki yanaşmadan birincisi, Fransadan gələn müxtəlif bədən ölçülərini ölçən Bertillon sistemi idi. Bu ölçülər boy, qol uzunluğu və ya başqa bir parametrlə sıralana

bilən kartlarda yazılmışdır. Bu sahəyə antropometriya deyilirdi. Alphonse Bertillon Bertillonage və ya antropometriyalar, bədən ölçmələrinin, fiziki təsvirlərin və fotosəkillərin detallı qeydləri əsasında fərdlərin müəyyənləşdirilməsi üsulu hazırladı. Təkrar cinayətkarlar tez-tez həbs olunduqda fərqli ləqəblər verirdilər. Bertillon, adlarını dəyişdirə bilsələr də, bədənlərinin müəyyən elementlərini dəyişdirə bilmədiklərini qeyd etdi.

- Digər bir yanaşma, polis idarələri tərəfindən barmaq izlərinin rəsmi istifadəsi idi. Bu proses Cənubi Amerika, Asiya və Avropada baş verdi. 1800-cü illərin sonlarında Bertillon metodu kimi qeydlər almaq imkanı təmin edən daha çox fərqli metrik barmaq izi nümunələri və barmaq izlərini indeksləşdirmək üçün bir metod hazırlanmışdır. Barmaq izlərini indeksləşdirən ilk belə güclü sistem Hindistandakı Bengal Baş katibi Edvard Henri üçün Əzizul Haque tərəfindən hazırlanmışdır. Henri Sistemi adlanan bu sistem və onun dəyişmələri barmaq izlərini təsnif etmək üçün hələ də istifadə olunur. Bengal Polis Müfəttişi Sir Edward Henry antropometriləri eyni vaxtda tətbiq etmək və ya dəyişdirmək üçün bir identifikasiya metodu axtarırdı. Henry, cinayətkarların müəyyənləşdirilməsi metodu kimi barmaq izi ilə bağlı ser Frensis Galtonla məsləhətləşdi. Barmaq izi sistemi tətbiq olunduqda, Henrinin işçilərindən biri Əzizul Haque məlumatların təsnifləşdirilməsi və saxlanması metodunu hazırlamışdır ki, tədqiqat asan və səmərəli aparılsın. Sir Henry daha sonra Londonda ilk İngilis barmaq izləri sənədlərini quraşdırdı. Genri Təsnifat Sistemi, məlum olduğu kimi, Federal Təhqiqat Bürosu (FBI) və on barmaq izi axtaran digər cinayət ədliyyə təşkilatları tərəfindən uzun illərdə istifadə olunan təsnifat sisteminin qabaqcılıdır.
- Həqiqi biometrik sistemlər kompüter sistemlərinin yaranması ilə üst-üstə düşən XX əsrin ikinci yarısında görünməyə başladı. Yeni yaranan sahə 1990-cı illərdə bir fəaliyyət partlayışını yaşamış və 2000-ci illərin əvvəllərində gündəlik praktikada yaranmağa başlamışdır.

- New York Dövlət Qulluğu Məsələləri üzrə Komissiya, müraciət edənlərin daha ixtisaslı insanların özləri üçün sınaqlarına mane olmaq üçün barmaq izləri tətbiqini qurdu. Bu təcrübə Nyu-York əyalətinin həbsxana sistemi tərəfindən qəbul edilmiş və 1903-cü ildə barmaq izlərinin istifadə edildiyi cinayətkarların aşkarlanması üçün istifadə edilmişdir. 1904-cü ildə Leavenworth, Kanzas və St. Sent-Luisdəki ABŞ Həbsxanası, Missuri Polis İdarəsi, hər ikisində barmaq izi idarələri qurdu. 20-ci əsrin birinci rübündə daha çox yerli polis şəxsiyyət bürosunun barmaq izi sistemləri quraşdırılmışdır. Polis zabitlərinin barmaq izi qeydiyyatı üçün milli anbar və rəsmiləşdirmə otağına artan tələbat və tələb 1921-ci il iyulun 1-də FBI İdarəetmə şöbəsinin yaradılmasına səbəb oldu.
- 1936-cı ildə oftalmoloq Frank Burch, iris modellərini fərdin tanınması üçün bir metod olaraq istifadə konsepsiyasını təklif etdi.
- 1960-cı illərdə ilk yarı avtomatik üz tanıma sistemi ABŞ hökuməti ilə müqavilə əsasında Woodrow W. Bledsoe tərəfindən hazırlanmışdır. Bu sistem administratorundan fotolarda göz, qulaq, burun və ağız kimi xüsusiyyətləri tapmasını tələb etdi. Bu sistem yalnız mövcud xüsusiyyət nöqtələrini çıxarmaq qabiliyyətinə əsaslanırdı. Məsafələri və nisbətləri istinad məlumatlarına nisbətən ümumi bir istinad nöqtəsi kimi hesabladı.
- 1960-cı illərdə İsveçli bir professor Gunnar Fant, akustik nitq istehsalının fizioloji komponentlərini izah edən bir model nəşr etdi. Onların tapıntıları müəyyən fonetik səslər verən şəxslərin rentgen analizinə əsaslanır. Bu tapıntılar natiqin tanınması üçün çox vacib bir anlayış olan nitqin bioloji komponentlərini daha yaxşı başa düşmək üçün istifadə edilmişdir.
- North American Aviation ilk imza tanıma sistemini 1965-ci ildə inkişaf etdirdi.
- 1974-cü ildə ilk kommersiya əl həndəsə tanıma sistemləri, barmaq izinin erkən implantasiyasından sonra, bəlkə də 1960-cı illərin sonlarında, bazarda ilk

biometrik cihaz oldu. Bu sistemlər üç əsas məqsəd üçün həyata keçirilmişdir: fiziki girişə nəzarət, vaxt və iştirak və şəxsiyyət.

- 1998-ci ildə FBI məhkəmə hüquq tətbiqetmə məqsədləri üçün DNT markerlərini rəqəmsal olaraq saxlamaq, axtarmaq və əldə etmək üçün Qarışıq DNT İndeksi Sistemini (CODIS) işə saldı. Ardıcılıq 40 dəqiqədən bir neçə saata qədər dəyişən bir laboratoriya prosedurudur.
- 1999-cu ildə FBI-nin geniş miqyaslı on barmaq izi (açıq dəst) identifikasiya sistemi olan IAFIS fəaliyyətə başladı. Bu sistemlə əlaqəli standartların hazırlanmasından əvvəl bir sistemdə toplanan bir barmaq izi başqa bir sistemdə barmaq izləri axtarıla ilə bilməzdi. Bu sistemin inkişafı FBI-yə barmaq izlərinin elektron ötürülməsi üçün milli şəbəkənin qurulması, ayrı-ayrı sistemlər arasında rabitə və məlumat mübadiləsi ilə bağlı problemləri həll etdi. IAFIS, cinayət hadisələrinin tarixini yoxlamaq və cinayət yerlərində gizli təzyiqləri müəyyən etmək üçün istifadə olunur. Bu sistem avtomatik və gizli axtarış xüsusiyyətləri, barmaq izlərinin və üz şəkillərinin elektron görüntü saxlanmasını və barmaq izlərinin və zəng cavablarının elektron dəyişdirilməsini təmin edir.
- 2013-cü ildə Apple istehlakçılara yönəlmiş smartfonlara barmaq izi skanerlərini əlavə etdi. Touch ID- Apple Inc iPhone 5S, iPhone 6 və iPhone 6 Plus tərəfindən hazırlanan və iPad Air 2 və iPad Mini 3-də mövcud olan barmaq izi tanıma xüsusiyyəti. Touch ID iOS cihazlarına cihazlarının kilidini açmaq və müxtəlif Apple rəqəmli media mağazalarında (iTunes Mağazası, App Store, iBookstore) və Apple Pay-da onlayn və ya tətbiqlərdə identifikasiya etməyə imkan verir[5] .

19-cu əsrdə kriminologiya tədqiqatçılarının fiziki xassələrinin və xüsusiyyətlərinin cinayət meyillərinə hər hansı bir aidiyyəti olub-olmadığı barədə araşdırma bu sahəyə marağı artırdı. Bu tədqiqatlar nəticəsində bir çox ölçü cihazı istehsal edildi və çox sayda məlumat toplandı. Nəticələr dəqiq olmasa da, şəxslərin fiziki xüsusiyyətlərinin ölçülməsi qəbul edildi və barmaq izi tətbiqi polisin şəxsiyyət üçün istifadə etdiyi beynəlxalq bir metod oldu .

2.2. Biometrikanın məqsədi və biometrik sistemlərin üstünlüyü

Biometrikanın məqsədi. Biometrik praktikantların ümumi məqsədi yadda saxlamaları lazım olan hər hansı bir məlumatı və ya daşımaq, itirmək və ya unutmaq məcburiyyətində qalan kart və açarlar kimi alətləri əvəzinə kopyalamaq və ya təqlid etmək mümkün olmayan xüsusiyyətlərindən istifadə etməkdir. Biometrik sistemlərdə eyniləşdirmə şəxslərin fiziki və ya davranış xüsusiyyətləri əsasında aparıldığı üçün onu başqasına ötürmək, unutmaq və itirmək mümkün deyil. Digər metodlarla müqayisədə daha az riskə malikdir. Bununla birlikdə biometrik sistemlərin yaradılması üçün bəzi standart tədbirlərdən istifadə edilməlidir. Biometrik ölçmələr adlanan bu tədbirlərdən istifadə etmək üçün INCITS (Beynəlxalq İnformasiya Texnologiyaları Standartları üzrə Beynəlxalq Komitə) tərəfindən yaradılmış beynəlxalq standart mövcuddur .

Biometrik sistemlərin üstünlükləri. Bir çox yeni texnologiyaların inkişafında olduğu kimi, təhlükəsizlik amili də biometrikliyin inkişafına səbəb oldu. Bütün biometrik sistemlər aşağıda təsvir olunan beş xüsusiyyətə sahib olmalıdır :

- 1.Universallıq: Bütün fərdlərin biometrik xüsusiyyətləri var.
2. Unikal olmaq: hər insanda fərqli şəkildə baş verən biometrik xüsusiyyətdir.
- 3.Davamlılıq:Xarakteristikası,zamanladəyişməməsidir.
4. Mövcudluq: Biometrik xüsusiyyətlər bəzi praktik cihazlarla ölçülə bilər.
5. Qəbul edilə bilən: Şəxslər biometrikliyin ölçülməsinə və toplanmasına etiraz etməməlidirlər.

Biometrik tanıma sistemlərinin növləri ilə skan edilmiş xüsusiyyətlər cədvəl 2.1-də verilmişdir, biometrik texnologiyaların müqayisəsi cədvəl 2.2-də verilmişdir .

Biometrik parametr	Xüsusiyyətlərin təsviri
Barmaq izi	Barmaq xətləri, məsamə quruluşu
İmza tanıma	Təzyiq və sürətlə yazı fərqləri

Üz həndəsəsi	Gözlər, burun və s. arasındakı məsafə
Retina	Retina quruluşuna (naxışına) görə
Əl həndəsəsi	Barmaq və ovuc ölçülərinə görə
Barmaq həndəsəsi	Barmaq ölçmə
Əl-damar quruluşu	Əl, barmaq və ya ovuc damarının arxa quruluşu
Qulaq forması	Qulağın görkəmli ölçüləri
Səs	Ton və ya səs rəngi
DNT	İrsi daşıyıcı olan DNT
Qoxu	Qoxunun kimyəvi tərkibi
Klaviatura vuruşları	Klaviatura vuruşlarının ritmi

Cədvəl 2.1. Biometrik tanıma sistemlərinin növləri və xüsusiyyətləri

Biometrik xarakteristikalar	Universallıq	Bənzərsizlik	Davamlılıq	Mövcudluq	Performans	Məşhurluq
DNT	Yuxarı	Yuxarı	Yuxarı	Aşağı	Yuxarı	Aşağı
Qulaq forması	Orta	Orta	Yuxarı	Orta	Orta	Orta
Üz həndəsəsi	Yuxarı	Aşağı	Orta	Yuxarı	Aşağı	Yuxarı
Üz Termoqramı	Yuxarı	Yuxarı	Aşağı	Yuxarı	Orta	Aşağı
Barmaq izi	Orta	Yuxarı	Yuxarı	Orta	Yuxarı	Orta
Əl həndəsəsi	Orta	Orta	Orta	Yuxarı	Orta	Orta

Retina	Yuxarı	Yuxarı	Orta	Aşağı	Yuxarı	Aşağı
İmza	Aşağı	Aşağı	Aşağı	Yuxarı	Aşağı	Yuxarı
Səs	Orta	Aşağı	Aşağı	Orta	Aşağı	Yuxarı
Damar quruluşu	Yuxarı	Orta	Orta	Orta	Yuxarı	Aşağı

Cədvəl 2.2. Biometrik texnologiyaların müqayisəsi

2.3. Biometrik sistemlərin növləri

Biometrik metodlar insanların fiziki və ya davranış xüsusiyyətlərindən istifadə edərək şəxsiyyəti təmin edən üsullardır. Mövcud biometrik tanıma üsulları aşağıdakılardır :

Fizioloji xüsusiyyətlərə əsaslanan biometrik tanıma sistemləri:

1. Barmaq izinin tanınması
2. Əl həndəsəsinin tanınması
3. DNT-nin tanınması
4. Retinanın tanınması
5. Üzün tanınması
6. Səsin tanınması
7. Üz termoqramı
8. Damarların tanınması

Davranış xüsusiyyətlərinə əsaslanan biometrik tanıma sistemləri:

1. İmza tanıma
2. Gəzmək
3. Klaviatura vuruşu
4. Nitq

Barmaq izi tanıma

Barmaq izi yüz ildən bəri istifadə olunan təkrarolunmaz bir texnikadır. Yumurta əkizləri də daxil olmaqla illərdir dəyişməyən, istifadəsi asan və yeni texnologiyalar inkişaf etdirən hər bir insanın fərqli barmaq izləri bu texnikanın geniş yayılmasını təmin etmişdir[15]. İstifadəsinin ilk illərindən bəri həm proqram, həm də aparatda barmaq izi sistemlərində əhəmiyyətli irəliləyişlər əldə edilmişdir. Avtomatik barmaq izi tanıma sistemində (OPTS) barmaq izinin tanınması ümumiyyətlə barmaq izindəki xüsusiyyət nöqtələrini və parametrlərini müqayisə etməyə əsaslanır.

Bir OPTS-də aparılan əməliyyatlar aşağıdakı kimi sıralana bilər :

1. Barmaq izlərini götürüb nömrələrə çevirmək,
2. Barmaq izlərində məlumat olan hissənin arxa plandan ayrılması,
3. İstinad nöqtələri əldə etmək,
4. Barmaq izinin təmizlənməsi və yaxşılaşdırılması,
5. Şəklin ikili şəkilə çevrilməsi,
6. İkiqat şəkilin incəlməsi,
7. Xüsusiyyət nöqtələrini və parametrlərini tapmaq,
8. Saxta əmlak nöqtələrini aradan qaldırmaq,
9. Müqayisə prosesinin həyata keçirilməsi,
10. Sistemin müvəffəqiyyətinin qiymətləndirilməsi.

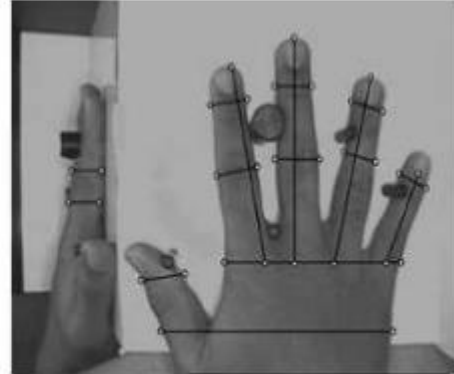


Şəkil 2.1. Barmaq izi

Bu sistemlərin ən vacib çatışmazlığı, barmaq izi təqlid edildiyi təqdirdə sistem səhv ola bilər. Digər bir dezavantaj, bəzi insanların barmaq izlərinin bir çox səbəbdən (orqan çatışmazlığı, yanma, dəri xəstəlikləri) olmamasıdır. Barmaq izi təqlid problemi, barmaq izinin alındığı barmağın canlılığını yoxlamaq üçün qabaqcıl sensorlar istifadə edərək aradan qaldırıla bilər. Şəxsin barmaq izləri yoxdursa (məsələn, baş dərisi soyulur və yangından sonra izlər yox olur), barmaq izi aşkar edilə bilməz [17].

Əl həndəsəsinin tanınması

Əl həndəsəsinin tanınması Amerikada 20 ildir istifadə olunan, xüsusilə hava limanlarında və nüvə stansiyalarında üstünlük verilən bir üsuldur. Bu üsulda, Şəkil 2.2-də göstərildiyi kimi, şəxslərin əlinin və ya iki barmağının həndəsi quruluşu təhlil edilir. Barmaqların uzunluğu, genişliyi, eni və əyilmə yerləri fərqli xüsusiyyətlər kimi istifadə olunur. Əl həndəsəsinin tanınması yüksək dəqiqliyə malik bir üsuldur, lakin böyük və ağır oxu cihazı sayəsində dəyəri və istifadəsi baxımından mənfi cəhətlərə malikdir.



Şəkil 2.2. Əl həndəsəsinin tanınması

Şəkil çəkmə müddətinin uzun olması da sistemin ləng getməsinə səbəb olan amildir. Bundan əlavə, üzüklər, bantlar, yaralanmalar və barmaqların itməsi, gut və ya kalsifikasiya kimi alətlər səbəbindən sistem performansı azalır və uşaqlarda əllərin sürətli böyüməsi və inkişafı səbəbindən sistem çətin istifadə olunur .

DNT tanınması

İlk dəfə 1985-ci ildə kəşf edildi ki, deoksiribonuklein turşusunun quruluşu fərdi xarakterikdir. DNT tanınması bu gün ən etibarlı identifikasiya yanaşmalarından biridir və əsasən atalıq testlərində və məhkəmə proseslərində istifadə olunur. DNT tanıma zamanı saç, qan və digər bioloji materiallar müayinə olunur. Metoddə hüceyrə nüvələrində xromosomlarda saxlanılan DNT molekulaları istifadə olunur. Hər DNT molekulunda 4 kimyəvi vahid var. Bunlar Adenine (A), Guanin (G), Sitozin (C) və Timin (T) olaraq sadalana bilər. Bu quruluşlar şəkər molekulaları və fosfat qrupları ilə birlikdə mövqe və ardıcılıq baxımından genetik məlumatların kodlandığı çatı təşkil edir. Tandem təkrarları kimi tanınan A, G, C, T strukturlarının təkrarlanması və təkrar saylarının və miqdarının dəyişməsi özünəməxsusdur. Tək yumurta əkiləri istisnadır. DNT-nin tanınmasında aparılmış prosesləri aşağıdakı kimi sıralamaq olar:

1. DNT nümunəsini götürmək
2. DNT-nin izolə edilməsi
3. Polimeraz zəncirvari reaksiyasından (PCR) istifadə edərək enzimatik məhdudlaşdırma və yüksəklik
4. Parçaların ayrılması
5. Təkrar quruluşların tapılması
6. Alınan nəticələrin təhlili

Çox dəqiq bir metod olsa da, metodun dəqiqliyi digər biokimyəvi və kimyəvi analizlərdə olduğu kimi DNT analizindəki nümunə keyfiyyətindən də asılıdır. Nümunələrin qarışdırılması, çirklənmə və sümük iliyinin transplantasiyası kimi hallarda metodun uğuru azalır. DNT analizi digər biometrik üsullarla müqayisədə bəla başa gəlir. Bundan əlavə, işləmə müddətinin 24 saat tələb etməsi real vaxt şəxsiyyət nəzarəti tələb olunduqda bu metodu əlverişsiz hala gətirir. Bu metodun əlverişsiz xüsusiyyətləri son illərdə gündəmə gətirilən DNT fişləri və mikro ardıcılıqla aradan qaldırılacaqdır .

Retina tanınması

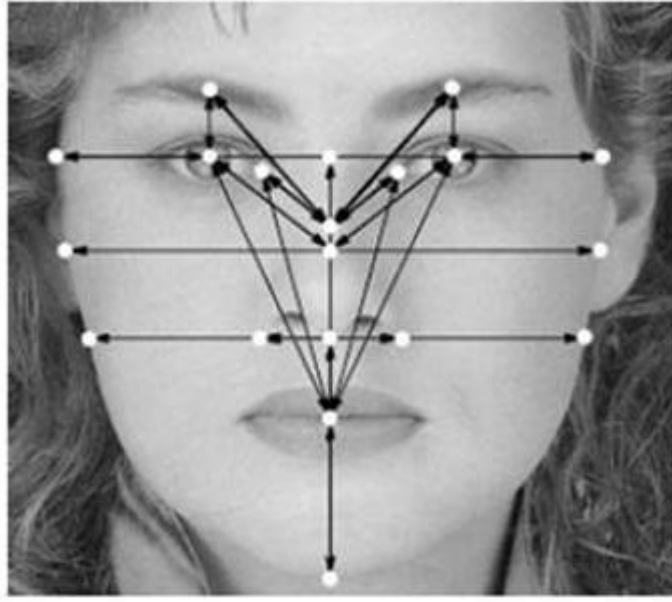
Optik bir qəbuledici vasitəsi ilə aşağı intensivlikli işıq mənbəyi olan retinanın unikal nümunələrini taramağa əsaslanan qurulmuş bir texnologiyadır. Sübut edilmiş bir texnik olsa da, istifadəçidən müəyyən bir nöqtəyə baxmağı tələb edir. Eynək taxırsa və ya oxucu ilə göz təması qurmaqdan narahat olsa, etibarlı metod deyil. Bu səbəblərə görə, retinal taramanın istifadəçilər tərəfindən qəbul edilməsi çətin olsa da, texnologiya çox səmərəli işləyir. 90-cı illərin ortalarında yenidən işlənilib hazırlanmış, təkmilləşdirilmiş əlaqə və istifadəçi interfeysi təmin edilmiş, lakin yenə də son dərəcə biometrik bir texnologiya kimi görünür [16].

Üz tanınması

Üz tanıma sistemi əslində ən təbii biometrik fərqləndirici metoddur. İnsanlar bir-birlərini ayırd etmək üçün üzlərindən istifadə edirlər. Bu səbəbdən bu metod demək olar ki, insan tarixi ilə biometrik fərqləndirmə metodudur. Buna baxmayaraq, bu metodu elmi olaraq kompüterlərdə fərqli bir xüsusiyyət kimi istifadə etmək nisbətən yeni bir mövzudur. Polisin cinayətkarı müəyyənləşdirmək üçün istifadə etdiyi üsula misal olaraq verilə bilər. İnsanlardan üz formasını təyin etməyə çalışması barədə cinayətkardan soruşmaq. Polis rəssamlarının standart olaraq əvvəllər çəkdikləri bəzi üz hissələri var. Verilən reseptə görə, bu parçalar cinayətkarın üzünə yaxın bir üz forması tapmağa çalışmaq üçün bir yerə qoyulur. Kompüterlərin həyatda sürətli istifadəsi də üz tanıma metodlarında əhəmiyyətli irəliləyişlərə səbəb oldu. Bu gün üz identifikasiyasında istifadə olunan iki üsul var. Bunlar aşağıdakılardır:

1. Üz Metrik Metodu
2. Eigenfaces metodu (Üz hissələri)

Üz Metrik Metodunda, Şəkil 2.3-də olduğu kimi, üzdə yerləşən orqanlar arasındakı məsafələri ölçməklə bir riyaziyyat ifadəsinin bunlardan alınmasına çalışılır. Məsələn, gözlər arasındakı məsafə, ağız-burun arasındakı məsafə və s.

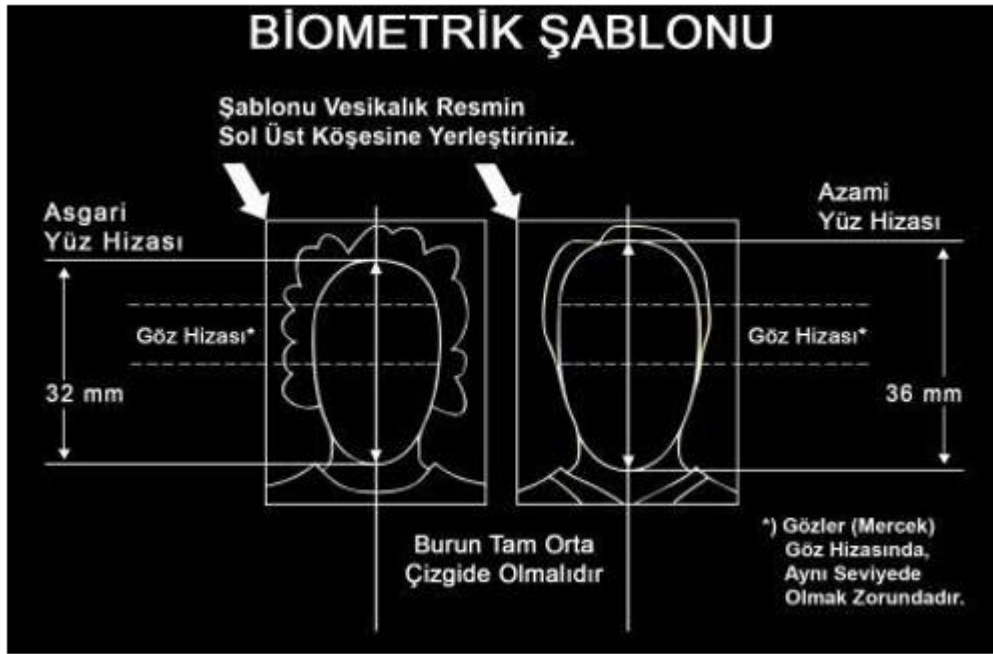


Şəkil 2.3. Üz Metrik Metodu

Eigenfaces Metodunda, polis sənətçisi tərəfindən edilənə bənzər bir üsul tətbiq olunur. Üz 150 hissəyə bölünür. Bu 150 ədədin 40-nın təyin edilməsi digər hissələrə nisbətən daha yüksəkdir. Əvvəlcə bu 40 hissədən başlayaraq, üz tanıma prosesi başlayır. Beləliklə, üzün müəyyənləşdirilməsinə çalışılır. Bu üsul üz ölçüləri metoduna görə yeni bir üsuldur və hələ də sınaq mərhələsindədir. Tədqiqatçılar tərəfindən hazırlanmışdır [10].

Biometrik şəkil

Biometrik fotosəkil, ICAO tərəfindən təyin olunan standartlar, viza müraciətləri və pasportlar üçün ölkənin səfirlikləri, konsulluqları və ya konsulluq başçıları tərəfindən tələb olunan müəyyən ölçülərə və spesifikasiyalara malik yüksək keyfiyyətli pasport şəklidir [11]. Biometrik fotosəkil Şəkil 2.4 ölçüsündə 3.5 sm x 4.5 sm olaraq təyin olunur. Demək olar ki, bütün fotoqraflarda biometrik pasport vurmaq mümkündür. Elektron pasportlarda üç növ biometrik məlumatlardan istifadə olunur: üz, barmaq izi və göz bəbəyi. Biometrik pasportlarda qan qrupundan barmaq izi və təbəssüm quruluşuna qədər bir çox məlumat çip ilə kodlanır.



Şəkil 2.4. Biometrik pasport şəkli

**ICAO standartlarında biometrik pasport fotosəkilləri üçün tələb olunan
xüsusiyyətlər
Üz cizgiləri**

Üzü tamamilə görünməlidir, saç düzüümü fotonun mərkəzində olmalıdır.



Şəkil 2.5. ICAO standartlarına görə biometrik pasport fotosəkillərinin üz cizgiləri

Şəkil keyfiyyəti

Fotoda ləkələr və bükülmələr olmamalıdır. Rənglər neytral olmalıdır və uzun təbii rənglərini əks etdirməlidir.



Şəkil 2.6. ICAO standartlarına görə biometrik fotoqrafiyanın şəkil keyfiyyəti

Kəskinlik və kontrast

Kontrast yaxşı düzəldilməlidir, detallar kifayət qədər kəskin və aydın olmalıdır.



Şəkil 2.7. ICAO Standartlarına görə Biometrik Fotoqrafiyanın Üz Zolaqları

Saç və görünüş istiqaməti

Gözlər açıq və aydın görünməlidir. Saç gözləri bağlamamalı və foto çəkilərkən birbaşa kameraya baxılmalıdır.



Şəkil 2.8. ICAO standartlarına görə biometrik fotoqrafiyanın saç və görünüşü

Baş və üz ifadəsi

Başın mövqeyi dik olmalıdır, baş heç bir istiqamətə tərs tutulmamalıdır. Şəkildə gülmək və s. mimika olmadan ağız bağlı olmalıdır.



Şəkil 2.9. ICAO standartlarına görə biometrik fotoqrafiyada baş mövqeyi və üz ifadəsi

Arxa plan

Arxa plan ağ və naxışsız olmalıdır. Kölgələr arxa planda meydana gəlməməlidir.



Şəkil 2.10. ICAO standartlarına görə biometrik fotoqrafiyada arxa plan

İşıq

İşıq üzə bərabər şəkildə əks etdirilməlidir və heç bir əks və kölgə olmamalıdır. Fotoda qırmızı göz olmamalıdır.



Şəkil 2.11. ICAO standartlarına görə biometrik fotoqrafiyada işıq

Eynəklər

Gözlər aydın görünməlidir, gözlükdə əks olunmamalı, rəngli şüşə və ya eynək istifadə edilməməlidir. Lensin kənarı və ya çərçivəsi gözləri bağlamamalı və ya gözləri bağlayacaq qədər qalın olmamalıdır.



Şəkil 2.12. ICAO standartlarına görə biometrik fotoqrafiyada eynəklər

Balaca uşaqlar

Balaca uşaqların şəkillərində başqa şəxslər və ya əşyalar olmamalıdır.



Şəkil 2.13. ICAO standartlarına görə biometrik fotoqrafiyada balaca uşaqlar

Papaq və başqa aksesuarlar

Fotoşəkildə şəxsin istifadə etdiyi eynək və bənzər aksesuarlardan başqa əşyalar tapılmamalıdır.



Şəkil 2.14. ICAO standartlarına görə biometrik fotoqrafiyada papaq və başqa aksesuarlar

Baş örtüyü

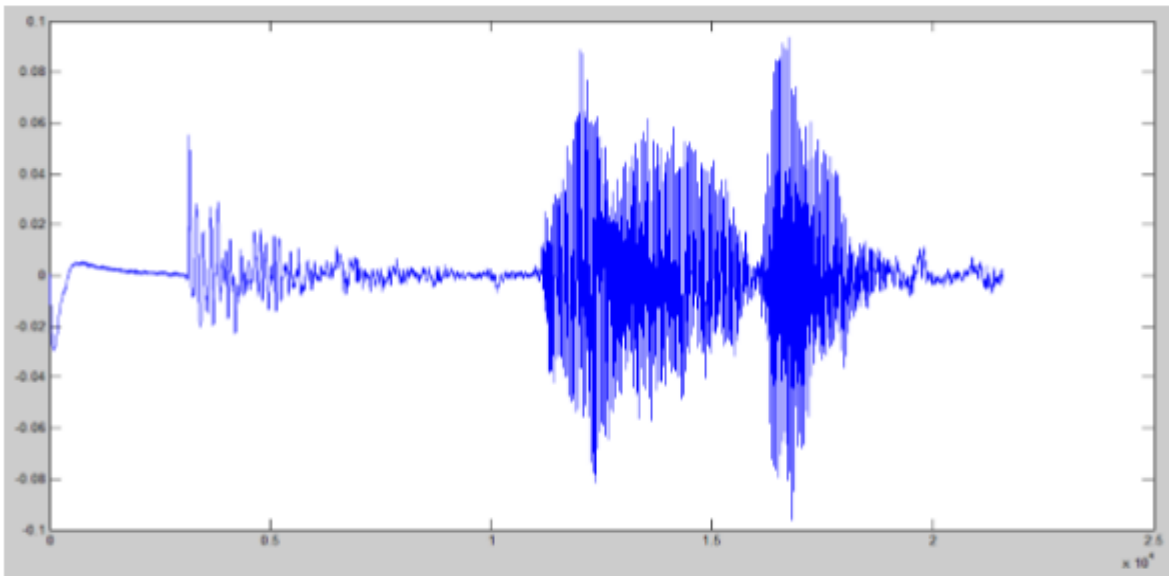
Hicablı fotoşəkillərdə üz çənənin ucundan alına qədər görünməlidir və kölgələr üzdə görünməməlidir.



Şəkil 2.15. ICAO standartlarına görə biometrik fotoqrafiyada baş örtüyü

Səs tanıma

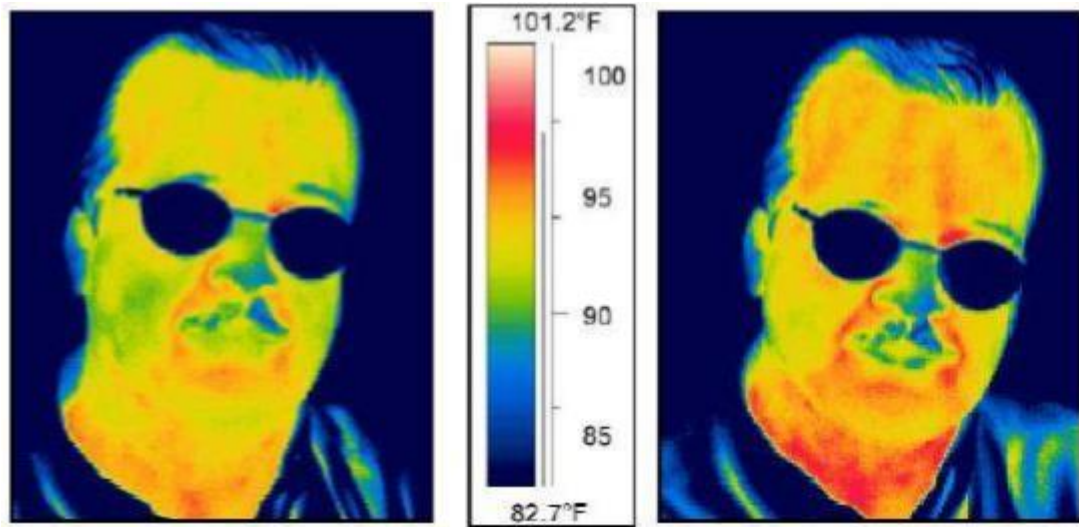
Səs tanıma tətbiqetməsində, siqnallar tanınmazdan əvvəl düzgün ifadə edilməlidir. Başqa sözlə, araşdırılan səs signalının tərkibində olan və yalnız tanınmağı hədəfləyən səs elementləri müxtəlif rəqəmsal signal emal üsullarını bir-birinin ardınca müəyyənləşdirilir. Sonra, göstərilən elementlər bir atribut vektoru ilə ifadə edilməlidir. Bu xüsusiyyətlər ilə səs tanıma məlumat bazası yaradılır. Məlumat sorğusu zamanı istifadəçi tərəfindən sistemə təqdim olunan nümunə verilənlər bazasındakı qeydlərdən biri ilə uyğunlaşdırılmasına çalışılır. Uyğunlaşma prosesinin nəticəsi sistemin son qərar mexanizminə köçürülür və icazə tələbi müsbət və ya mənfi olaraq təyin olunur [14].



Şəkil 2.16. Səs tanınması

Üz termoqramı

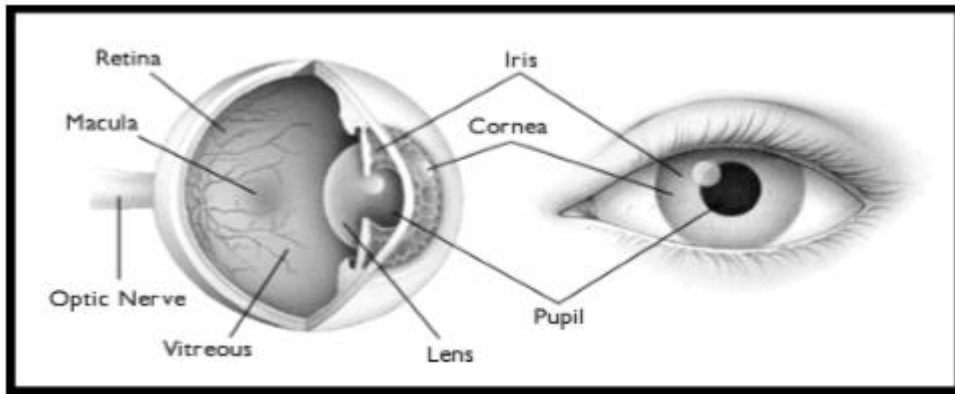
Üzün istilik xəritəsini təhlil edərək identifikasiya və doğrulama proseslərində istifadə olunan biometrik metodlardan biridir. Bu mövzuda araşdırmalar hələ davam edir.



Şəkil 2.17. Üz termogramı

İris tanıma

İris tanıması biometrik tarama arasında ən sadə biridir. Təxminən 15-20 sm məsafədən tanıma adı CCD kamera vasitəsi ilə edilə bilər. İstifadəçi və brauzer arasında fiziki təmasa ehtiyac yoxdur. Eynək ilə istifadə oluna bilməsi, sistemlərə asanlıqla birləşdirilə bilməsi və iris naxışının ən etibarlı nümunələrdən biri olması, iris tanıma sistemlərini daha üstün edir. Şəkil 2.18-də, insan gözünün anatomik quruluşu göstərilir [20].



Şəkil 2.18. Gözün quruluşu

- Son illərdə iris tanıma sistemi digər sistemlərə nisbətən daha etibarlıdır, tətbiq etmək daha asandır və hər gün yenilənir. Bunun səbəbləri:

- İris 3-cü aydan ana bətnində struktur olaraq formalaşmağa başlayır, 8-ci ayda meydana gəlməsini tamamlayır və doğuşdan 2-3 il sonra tam inkişafını başa çatdırır. Bundan sonra, iris bir quruluş olaraq dəyişmir.
- Son illərdə aparılan araşdırmalar, irisin barmaq izləri kimi insanları tanımaq üçün istifadə edilə bilən fərqli bir xüsusiyyətə sahib olduğunu göstərdi.
- İrisin meydana gəlməsi embrionun inkişafından asılı olduğundan, genetik quruluşdan asılı deyil. İris quruluşu tanınmaq üçün daha fərqli bir xüsusiyyətə sahibdir, belə ki, əkilər də belə eyni adamın sağ və sol gözlərindəki iris quruluşlarında fərqlənirlər. Buna görə, iris tanıma sistemlərində, sistemin işləmə prinsipinə görə insanlar ya eyni gözlə sistemə daxil edilir və ya şəxsin hər iki gözü sistemdə qeyd olunur.
- Gözdəki iris kornea, göz qapağı və göz bəbəği tərəfindən qorunur. Bu səbəbdən xarici təsirlərdən ən az təsirlənə biləcək xüsusiyyətə malikdir.
- İrisin quruluşu cərrahi müdaxilə ilə də dəyişdirilə bilməz.
- İris tanıma sistemi insana zərər vermir. Şəkil lazer və ya oxşar görüntü texnikasına ehtiyac olmadan sadə bir CCD kamera ilə çəkilə bilər [13].

Damar tanıma sistemi

Ovuc damarının tanınması texnologiyası, ovuc içindəki qan damarlarının hər bir insanda fərqli olduğuna əsaslanaraq aşkar edilmiş bir texnologiyadır. Bu texnologiyada əvvəlcə infraqırmızı işıq damar quruluşunu aşkar etmək üçün sensor tərəfindən qan damarlarına göndərilir. Damar quruluşunun ortaya çıxmasında, göndərilən infraqırmızı işığı udan qandakı hemoglobinin prinsipi qəbul edilir. Damar tanıma texnologiyasında qanda hemoglobinin istifadəsi səbəbindən, canlı olduğu müəyyən edilmiş əzanın həyatda olması vacibdir, damardakı qan əhəmiyyətli olur və texnologiyaya dəyər qatır. Sensor rolunu oynayan IR kamerası tərəfindən əldə edilən görüntü, biometrik api sayəsində sensorda ədədi dəyərə çevrilir. Bu ədədi dəyər daha sonra 256 bit AES

(Advanced Encryption Standard) algoritmi ilə şifrələnir və təhlükəsiz məlumat ötürülməsi üçün server / müştəri kompüterlərinə ötürülür.



Şəkil 2.19. Əl-damar görüntüsü

Palm (Palm) Damar tanıma texnologiyasının digər texnologiyalarla müqayisədə ən böyük üstünlüyü, əl kəsildiyi və ya yaralanması halında damar quruluşuna təsir göstərməyəcəyi üçün işləməyə davam etməsidir [17].

Ovuc damar texnologiyasının əsas istifadə olunduğu sahələr aşağıdakılardır:

- ATM cihazları
- Tibbi təsvir (SGK, xəstəxana, aptek və s.)
- Giriş nəzarəti
- İşçilərin davamiyyətinə nəzarət
- Veb əsaslı şəxsiyyət tətbiqləri
- Sistem giriş əməliyyatları
- Bank əməliyyatları

İmza tanıma sistemi

Hər zaman yazdığı, oxuduğunu və ya təsdiqləndiyini ifadə etmək üçün bir adamın hər hansı bir yazı altında eyni şəkildə yazdığı adlar və ya işarələr kimi müəyyən edilə bilən imza, ömrü boyu dəfələrlə istifadə edilmişdir. Böyük hüquqi sanksiyaların və təqlidlərin olması, şəxsin borclu qalması, bütün varlıqlarını başqa şəxsə bağışlaması, törətmədiyi cinayətləri aşmasına səbəb olması kimi səbəblərdən ötrü həyati əhəmiyyət daşıyır. Buna görə bəlkə də ən çox istifadə edilən identifikasiya üsulu olan imzanın əslində həmin şəxs tərəfindən atılıb-atılmadığını müəyyən etmək vacib bir problemdir.

Bu səbəbdən, imzanı tanıma sistemlərində imzanı tanımaq üçün iki növ məlumat istifadə olunur. Bunlardan birincisi, imza vaxtı, sürət, qələmin ciddiliyi kimi şəxsin imzalanma prosesi ilə əlaqəli xüsusiyyətlərdir, digəri isə bir nümunə olaraq imza xüsusiyyətləridir. Bir imza təqlid edən hər kəs imzanı nümunə kimi təqlid edə bilsə belə, imza atma nümunəsini (müddəti, sürətlənməsi, qələm çıxartma miqdarı və s.) təkrarlamaq çətindir.



Şəkil 2.20. Bir imza nümunəsi

İmza tanıma sistemlərinin mənfi cəhətləri, sistemin istifadəçinin sürətini və imza davranışını öyrənmək üçün lazımi sayda nümunələrə ehtiyacı olmasıdır və imza dəyişməsi istifadəçinin hazırkı əhval-ruhiyyəindən, xüsusən də tələsik olduğu vəziyyətdən asılı olaraq dəyişir [15].

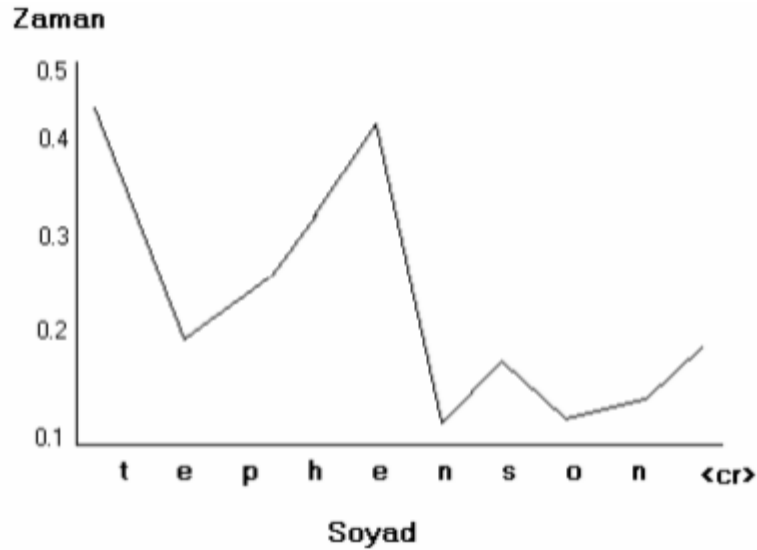
Davranış(Yeriyiş)

İnsanların gəziş tərzinə görə identifikasiya üçün istifadə olunan biometrik metodlardan biridir. Ədəbiyyatda bu mövzuda araşdırmalar yer almır.

Klaviatura vuruşu

Digər biometrik sistemlərin ən böyük çatışmazlıqlarından biri bütün terminallarda əlavə qurğuların istifadəsinə ehtiyac olması ilə yanaşı, yazı ritm sistemlərini digər biometrik sistemlərdən fərqləndirən əsas cəhət onun xüsusi aparata ehtiyacı olmamasıdır. Yazma tərzini hazırlamaq üçün lazım olan yeganə giriş cihazı yalnız klaviaturadır. Belə bir üstünlüyə sahib bir biometrik sistemin real həyatda istifadə edilməməsi üçün heç bir səbəb yoxdur. Xüsusilə universitetlər kimi bir çox yerdə bu tip sistem həm elmi, həm də texniki baxımdan istifadə edilə bilər. Çünki insanların əl yazısı kimi klaviaturaları necə yazmaları arasında böyük oxşarlıq var. Həqiqətən, bir şəxs klaviaturaya bir şey yazmağa başlayanda təbii olaraq klaviaturada

iz buraxır. Başqa sözlə, klaviaturadakı simvolları gəzən istifadəçi əslində mütəmadi olaraq etdiyi bir yazı ritm hərəkətinə uyğundur. Nəzəri olaraq, klaviaturadan istifadə edərək kompüterdəki bir redaktora bir söz yazmaq istədikdə sözdəki hərfləri yazmağa sərf olunan vaxt bir-birinə bərabərdir. Bir istifadəçidən soyad yazmağı xahiş edildi və yazı mərhələsində keçən vaxt müəyyən edildi. Stephenson sözünün keçdiyi vaxt ölçülür və onun qrafiki Şəkil 2.21-də göstərilmişdir.



Şəkil 2.21. Stephenson sözünün yazılış ritminə aid qrafik

Şəkil 2.21-də istifadəçinin yazı ritm sisteminin tapıntıları verilmişdir. İstifadəçi t və e simvolları arasında çox vaxt itirsə də, n və s və ya s və o simvolları arasında çox tez keçə bilər. Klaviaturaya daxil olan iki simvol arasındakı vaxtı ölçərək istifadəçilərin yazma ritmlərini təyin etməyə çalışılır. Əslində, bu yazı ritminə aid bir çox araşdırmada ölçülən və qiymətləndirilən dəyərdir.

Ritm sistemlərinin yazılmasının ən vacib çatışmazlıqlarından biri qərar qəbulu üçün tələb olunan məlumatların yalnız bir parametrdən, yəni iki düymənin arasındakı gecikmə vaxtından əldə edilməsidir. Yalnız açar aralıkları deyil, düymələri basmağa sərf olunan vaxtın müəyyənləşdirilməsi yazı ritminin tədqiqatlarında etibarlılıq dərəcəsini artıracaqdır [18].

2.4. Biometrik sistemlərin işləmə mexanizmi və istifadə sahələri

Bütün biometrik texnologiyalar dörd addım kimi oxşar şəkildə işləyir: məlumatların əldə edilməsi, xüsusiyyətlərin çıxarılması, müqayisə və uyğunluq-uyğunsuzluq. Məlumat əldə etmə prosesində sistem müvafiq texnika ilə bir görüntü və ya məlumat əldə edir. Məlumat və ya şəkil əldə edildikdən sonra, emal mərhələsi ilə lokallaşdırılmalıdır.

Lokallaşdırma xüsusiyyət hasilat mərhələsindədir. Xüsusiyyətin çıxarılması mərhələsində mövzu ilə əlaqəli olmayan məlumatlar atılır və müvafiq məlumatlar biometrik şablon kimi götürülür və saxlanılır. Bu tanınma prosesində yeni bir məlumat görüntü alınır və saxlanılan biometrik şablonla müqayisə olunur. Bu müqayisənin nəticəsi odur ki, yeni alınan məlumatlar şablonla eynidirsə, uyğunluq var, əgər yoxsa uyğunluq yoxdur [13].

Biometriyaya əsaslanan metodlar ilə digər metodların müqayisəsi

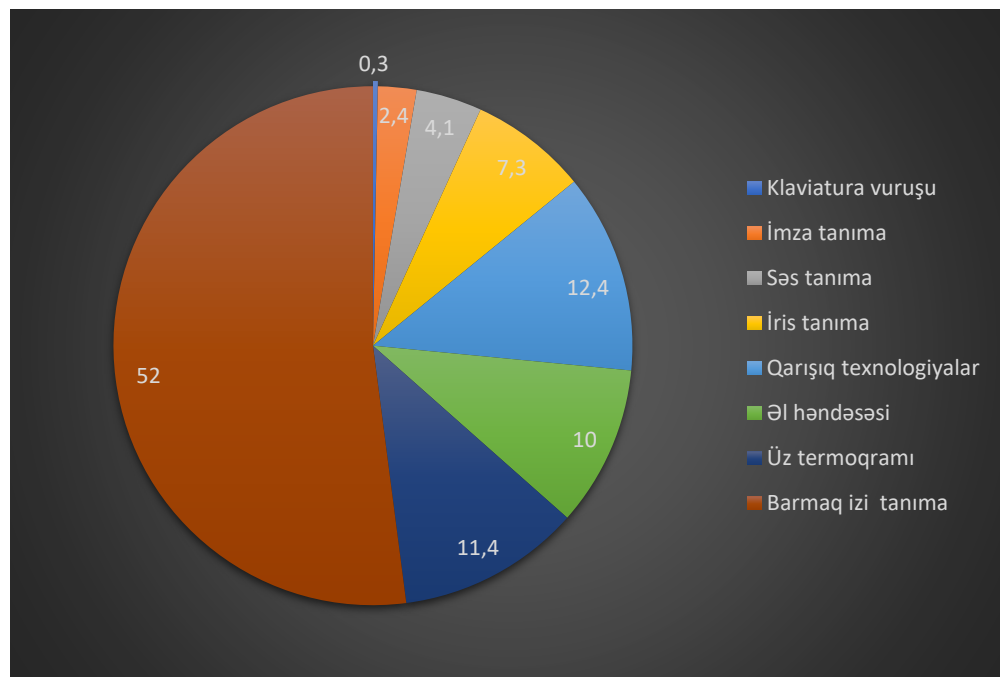
İstifadəçi şəxsiyyətini (biliklərə əsaslanan və ya mənsubiyyətə əsaslanan) və biometrik sistemləri müəyyən edən digər sistemlər oxşar cəhətlərə malikdir, lakin birlərindən fərqləndikləri bir çox məqam var. Biometrik metodlarla müqayisədə biometrik metodlardan başqa metodların ən vacib çatışmazlığı, istifadəçiyə bəzi məlumatları bilmək və yadda saxlamaq və ya daim onunla birlikdə bəzi vasitələr aparmaq, oğurlatmamaq, unutmaq kimi məsuliyyətlər verməsidir. Biometrik sistemlərdə bu belə deyil və şəxsiyyətini yoxlamaq üçün başqa məlumatlara, obyektlərə və s. ehtiyac yoxdur. Biometrik sistemlərin digər sistemlərlə müqayisədə üstünlükləri, dezavantajları, oxşar və fərqli cəhətləri qısaca aşağıdakı kimi ifadə edilir [17].

- Digər identifikasiya metodlarında istifadə olunan məlumatlar hər bir istifadəçi üçün tamamilə fərqli və unikal olsa da, biometrik məlumatlar fərqli ola bilər, lakin oxşarlıqlara malikdir.
- Digər metodlarda istifadə olunan məlumatlar istifadəçi tərəfindən dəyişdirilə bilər (sistem rəhbərinin tələbi ilə, yeniləmə məqsədləri üçün və ya hər hansı digər

səbəbdən). Digər tərəfdən, biometrik məlumatlar, istədiyi zaman dəyişə biləcəyi bir məlumat deyil, qəza, xəstəlik və s. vəziyyətində dəyişir.

- Biometrik sistemlər ümumiyyətlə əlavə aparat və proqram təminatı tələb etsə də, əlavə xərc çəkirlər, digər metodlar ümumiyyətlə mövcud sistemlərə uyğun gəlir.
- Digər metodlar oğurlandıqda və ya oxşar vəziyyətdə olduqda, yenisi ilə əvəz edilə bilər, halbuki biometrik məlumatlar hər hansı bir şəkildə əldə edildikdə bu etibarlı deyildir.
- Biometrik məlumatlar zaman keçdikcə deformasiya ola bilər, lakin digər üsullar üçün bu olmur.

Biometrik sistemlərdən başqa tanıma sistemlərində məlumatları unutmaq, oğurlamaq və itirmək riski çox yüksəkdir. Bununla birlikdə, biometrik sistemlərdə istifadə olunan məlumatlar insanın fiziki və ya davranış xüsusiyyətlərindən olduğuna görə belə bir təhlükə ilə qarşılaşma ehtimalı demək olar ki, yoxdur. Şəkil 2.22-də istifadə olunan biometrik sistemlərin faiz nisbətləri verilmişdir.



Şəkil 2.22. İstifadə edilən texnologiyaya görə bazar faizləri

Digər doğrulama üsulları	Biometrik metodlar
Məlumat itkisi, oğurluq, itirmə təhlükəsi böyükdür	Məlumat itkisi, oğurluq, itmə təhlükəsi demək olar ki, yoxdur
İstifadəçi istədiyi təqdirdə məlumatları asanlıqla dəyişdirə bilər	Biometrik məlumatlar qəza, əzələ itkisi istisna olmaqla dəyişdirilə bilməz.
Hər kəs üçün mövcuddur	Hər hansı bir biometrik tanıma sistemində biometrik xüsusiyyətlərə (barmaq, göz və s.) sahib olmayan insanlar bu sistemə daxil deyildir
Zamanla dəyişməsinə səbəb olacaq bir vəziyyət yoxdur	Biometrik məlumatlar zamanla deformasiya və dəyişdirilə bilər
Ümumiyyətlə mövcud sistemlərə uyğundur	Bu əlavə bir aparat təminatı dəyəri gətirir

Cədvəl 2.3. Biometriyaya əsaslanan metodlarla digər metodların müqayisəsi

Biometrik sistemlərin istifadəsi sahələri

Bu gün biometrik sistemlər aşağıdakı sahələrdə istifadə olunur:

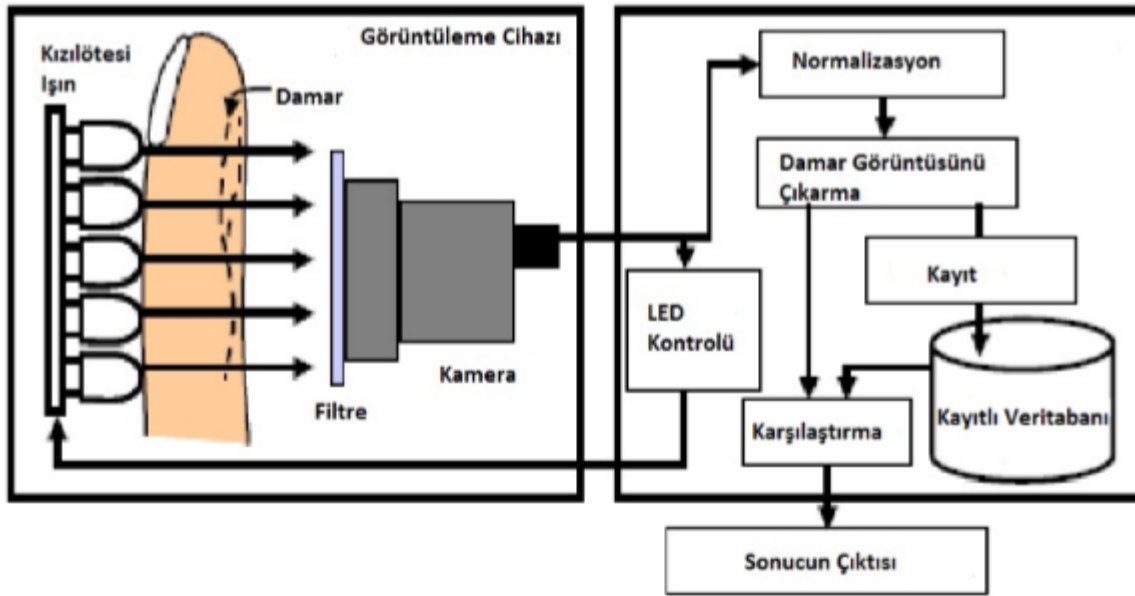
- İşçilərin iştirakı və təqib
- Avtomatik bankomatlarda istifadəçi identifikasiyası
- Çağrı mərkəzlərində identifikasiya
- Hava limanlarında qeydiyyatdan keçmək və yerləşmək işləri
- Onlayn bank istifadəçisinin şəxsiyyəti
- Sərhəd qapıları vasitəsi ilə sərhəd nəzarəti və giriş nəzarət
- Internet bankacılığında kullanıcı tanımlama
- Elektron pul köçürmələrində istifadəçinin identifikasiyası
- Kredit kartı tətbiqetmələri

- Müəssisə şəbəkəsi
- Kompüter təhlükəsizliyi
- Əmanət qutularına giriş təhlükəsizliyi
- Satış terminallarında (POS) istifadəçi identifikasiyası
- Hərbi mənbələrin effektiv izlənməsi
- Çek təsdiqləmə əməliyyatlarında istifadəçinin təhlükəsizliyi
- Xəstəxanalarda və sığorta təşkilatlarında xəstənin izlənməsi və eyniləşdirilməsi
- Dövlət xidmətləri üçün qeydiyyatı izləmə (SSK, vergi, nəqliyyat)
- Hesab açarkən şəxsiyyət
- Bina, obyekt və ofislərə giriş təhlükəsizliyi
- Elektron ticarətdə istifadəçinin identifikasiyası
- Filial bank əməliyyatlarında istifadəçi identifikasiyası

2.5. Barmaq-damar tanıma sistemi

Barmaqdakı damarların paylanma görüntüsü hər bir insan üçün fərqlidir. Barmaq damarlarının tanınması sistemi, bu əsasda hərəkət edən və barmaq damarının görüntüsünü əldə edən və bu görüntünün istifadəsini təsdiqləyən və tanıyan biometrik bir sistemdir. Bu texnologiya barmağın daxili hissəsini göstərdiyindən kir, kiçik kəsiklər, yara və nəmdən təsirlənmir.

Sistemin iş prinsipi. Yan-yana yerləşdirilən bir sıra LED-lərdən yayılan yaxın infraqırmızı radiasiya barmağa keçir və qismən qandakı hemoglobin tərəfindən udulur. Şüaların udulduğu bölgələr (yəni barmağındakı qan damarları) barmağın digər tərəfində yerləşdiyi kamera tərəfindən təsbit edilən görüntüdə qaranlıq bölgələr kimi görünür. Şəkildə emal üsulları tətbiq olunur və barmaq damar motivi çıxarılır. Bu motiv rəqəmsallaşdırılıb və istifadəçinin şəxsiyyəti sistemdə qeyd olunan motiv şablonları ilə müqayisə edilərək təsdiqlənir .



Şəkil 2.23. Barmaq damarlarının tanınması sistemi və işləmə mexanizmi



Şəkil 2.24. Barmaq damar modelinin təsviri

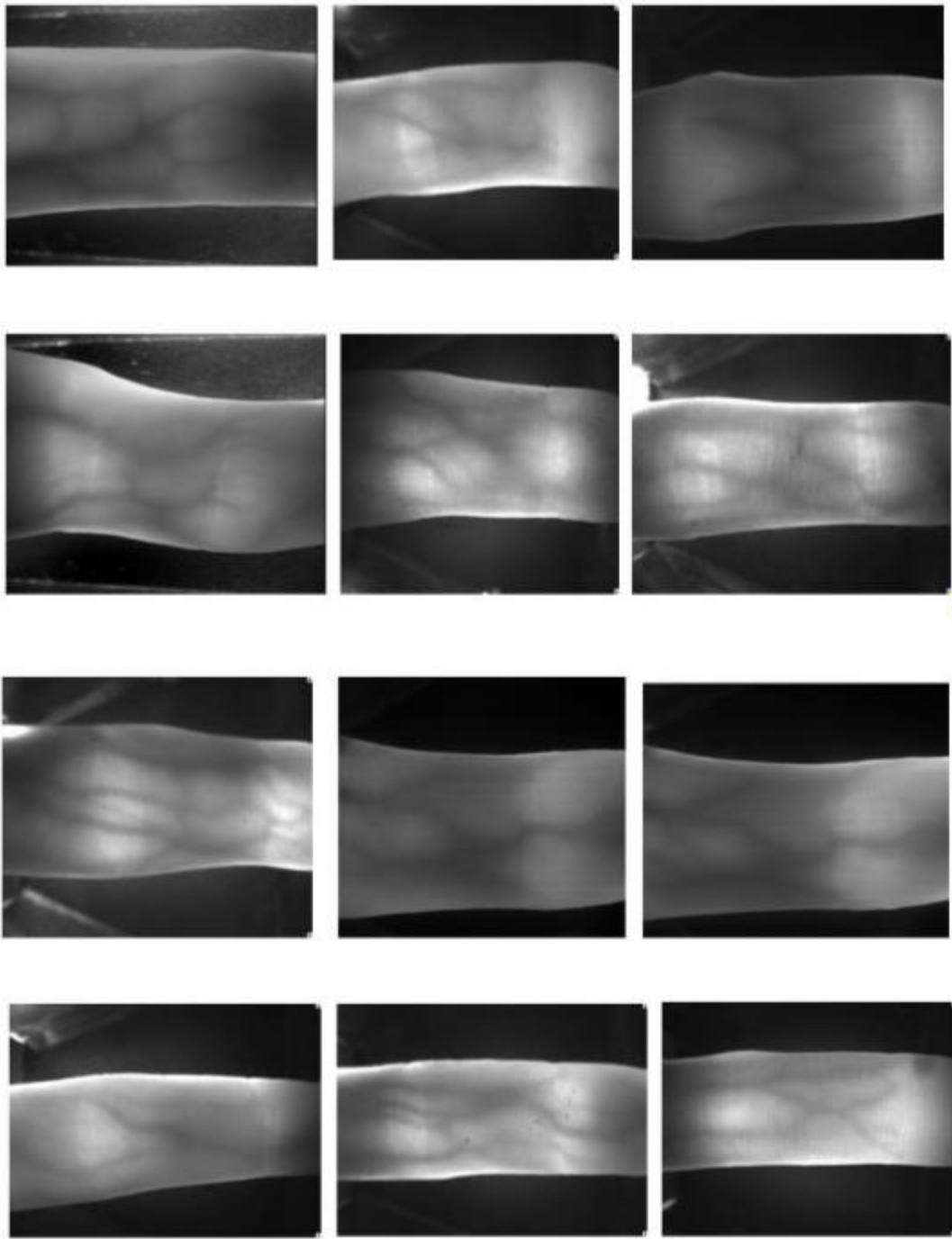
Barmaq damarlarının tanınması texnologiyasını digər biometrik metodlardan fərqləndirən xüsusiyyətlər bunlardır :

- Barmaq damar quruluşu insan həyatı boyu dəyişmir.
- Barmaq damar quruluşları hətta tək əkilərdən də fərqlidir.

- Doğrulama zamanı etibarlı nəticələr verir, çünki hər bir şəxsin barmaq damar quruluşu bənzərsizdir.
- Tezdir, identifikasiya prosesini bir neçə saniyədə tamamlayır.
- Doğrulama üçün bir parol saxlamağa ehtiyac yoxdur.
- Barmaq damar xəritəsini oğurlamaq və kopyalamaq mümkün olmadığı üçün bankomat saxtakarlığı riski minimuma endirilir.
- Barmaq izi ilə fərqlənir. Barmaq izi barmağın xarici səthinin izi olduğu üçün kopyalanmaq asandır. Amma gəmi xəritəsi xarici səthdən təsirlənməyən bir quruluşa malikdir.
- Yalnız canlı barmaqdan istifadə edilə bilər, çünki prosedur zamanı qan axını vacibdir.
- Sistemdən istifadə edərkən barmağın ucu yalnız hizalanma məqsədi ilə oxucuya toxunur. Beləliklə, barmaq izi daha çox gigiyenikdir.
- Oxucunun istifadə etdiyi şüalar insan sağlamlığı üçün zərərli deyil.
- Barmağın dərisindəki kəsiklər, dişlər və s. deformasiyalardan təsirlənmir.
- Müştərilərdən götürülmüş barmaq damar xəritəsi nümunəsindən istehsal olunan məlumatlar şəxsiyyət üçün istifadə edilmir, identifikasiya üçün istifadə olunur. Beləliklə, müştəri cihazı məxfilikdən narahat olmadan istifadə edə bilər.

Barmaq damar şəkillərinin toplanması prosesi

Aşağıdakı şəkildə göstərilən barmaq damar şəkilləri Hong Kong Universitetinin məlumat bazasından internet üzərindən əldə edildi KfV-100 cihazı barmaqların damar tanıma sistemi üçün hazırlanmış cihazların iş məntiqini dərk etmək üçün istifadə edilmişdir.



Şəkil 2.25. Təcrübədə istifadə olunan bəzi barmaq damar şəkilləri

KFV-100 Barmaq damarlarının tanınması cihazı

Bu cihaz Finger Damar Tanıma sistemi üçün hazırlanmışdır. Bazarda bir barmaq damar oxuyucusu olaraq da mövcuddur. Texnologiyanın sürətlə irəliləməsi səbəbindən təhlükəsizlik baxımından yalnız biometrik xüsusiyyətlərin yetərli olmadığı aşkar edildi

və nəticədə istehsal olunan cihazlara və ya şəxsiyyət əsaslı identifikasiya üçün istifadə olunan maqnit kartlarını oxuya biləcək sistemlərə birdən çox biometrik xüsusiyyət tanıya biləcək sistemlər əlavə edildi. Bu məhsul həm barmaq damarlarını tanıyan, həm də istifadəçilər üçün hazırlanan maqnit kartlarını oxuya bilən bir məhsuldur.



Şəkil 2.26. KFV-100 Cihazı

KFV-100 və RFID Modulu (FeliCa və ya MIFARE) xüsusiyyətləri

Aşağıdakı cədvəldə barmaq damarlarını oxuyan cihazın xüsusiyyətləri göstərilir.

CPU	S3C2440 400MHz 32Bit RISC
OS	Linux
FLASH yaddaş	128 MB
RAM	64 MB
LCD	2.8 , TFT Rəngli, Sensor paneli
Görüntü imkanı	320 x 240 (262K Rəng)
İnterfeys	TCP/IP, USB, RS232/422/485, Wiegand 26/34Bit

Relay Input	2 port
Output	2 port
Storage for vein pattern	300,000 Max
Storage for log	1,000,000 Max
RFID(Optional)	13.56MHz, 125MHz, 900MHz
Ölçüsü	92 x 214 x 84(mm)
İşləmə istiliyi	0~40°C
Rütubətlik	20~80%RH
Barmaq damarının ölçüsü	Approx 500 byte
Eyniləşdirmə metodu	1:1 or 1:N (N : up to 1,000)
FRR(False Reject Rate)	0.01% under(JIS based testing)
FAR(False Accept Rate)	0.0001% under(JIS based testing)
FTER(Failure to Enroll Rate)	0.08%(IBG Test 2006)

Cədvəl 2.4. KFV-100 cihazının xüsusiyyətləri

KFV-100 cihazından istifadə etmək üçün əvvəlcə əl barmaqlarından biri aşağıdakı kimi yerləşdirilir (düzgün şəkildə), dırnaq ucu sensorun yerləşdiyi ərazinin ucunda yerləşən yanib-sönən loka toxunaraq. Bu mərhələdə barmağın daxili səthi sensorla üz-üzədir, barmaq sensorun yerləşdiyi hissəyə düzgün yerləşdirilir.



Şəkil 2.27. Barmağın KfV-100 cihazına yerləşdirilməsi

Barmaq düzgün yerləşdirildikdən sonra cihaz aşağıdakı şəkildəki kimi 4 dəfə təkrarlanmalıdır. Barmaq düzgün yerləşdirilibsə, rəhbər yaşıldan mavi rəngə çevriləcəkdir. Bu müddətin sonunda cihazı barmağınıza qoyarkən heç bir səhv olmazsa, cihaz 10 rəqəmli şifrə (2147483645, 2147483641 kimi) yaradacaqdır.



Şəkil 2.28. KfV-100 cihazının barmaq damar xəritəsinə görə parolun yaradılması prosesi

Barmaq izi oxu sistemi- personal izləmə, barmaq izi dəyişdirmə, yemək salonu və üzv izləmə sistemləri bir çox kateqoriyada istifadə olunur və ən çox istifadə sahələri personalın barmaq izi oxu sistemləridir. Bəs, personalların barmaq izi oxu sistemi necə işləyir? Barmaq izi oxu cihazı, personalın girdiyi və çıxdığı bir divar və ya turniket sisteminə quraşdırılmışdır. Personalların barmaq izləri barmaq izi oxuyucusuna təqdim olunur.

İşçilər daha sonra təqdim edilən barmaq izlərini oxuduqda, barmaq izi oxu cihazı oxunan barmaq izlərini yadda saxlayır və istədikləri zaman barmaq izi oxu sistemi proqramına göndərir. Barmaq izi oxuma sistemi proqramında, sistem işçilərə və işçilərə veriləcək maaşları, işçilərin hansı saatda işə gəldiyini, hansı saatda işdən çıxdığı kimi hesabatlarla maaşları hazırlaya bilər.



Şəkil 2.29. Barmaq izi oxuma sistemi

Barmaq izinin istifadəsi sahələri çox genişdir. Müəssisələr barmaq izi istifadəsinin aparıcı sahələridir. Barmaq izləri iş yerlərindən, ictimai qurumlardan və təşkilatlardan başqa hərbi bölgələr, bələdiyyələr, fabriklər, idman salonları, xəstəxanalar, ticarət mərkəzləri, mağazalar və s. yerlərdə də istifadə olunur. Bu cihazlarla, kadr izləmə, yemək salonunu izləmə, üzv izləmə, giriş nəzarət izləmə və tələbə izləmə barmaq izinin istifadəsi sahələrində edilə bilər. Barmaq izi oxu cihazları ilə işçiləri izləmək üçün personal izləmə proqramını bu cihazlarda quraşdırmaq lazımdır. Üzv təqibi üçün üzv təqib proqramı, yemək salonunu izləmək üçün yemək salonu izləmə proqramı, keçid nəzarəti izləmək üçün keçid nəzarət proqramı və tələbəni təqib etmək üçün tələbə təqib proqramı istifadə etmək tələb olunur. Bütün bu izləmə proqramlarının ahəngdar istifadəsi səbəbindən barmaq izinin istifadə sahələri artdı.

Kart girişı idarəetmə sistemləri personalın izlənməsi üçün ən çox istifadə olunan sistemlərdir. Bu sistemlər işçilərin girəcəyi və çıxacağı yerlərdə yerləşir. Ayrıca kart girişı idarəetmə sistemləri ilə turniket, qapı və maneə tetikleyicisini də verə bilərsiniz. Bu sistemlərdə istifadə edilən kartlar yaxınlıq və ya mifarey xüsusiyyətləri olan kartlardır. Bu kartlarda istədiyinizi çap edə bilərsiniz. Necə? Kart çap printeri ilə. Kart çap printerləri, personalın izlənməsi üçün istifadə ediləcək kartlarda çap üçün xüsusi üstünlük verilir. Kartlara iki tərəfli kağız yazdırmaqla işçilərinizin kartlarını yalnız giriş və çıxışda deyil, həm də müştərilərinizlə görüşlər zamanı təqdimat kartı kimi bir kart asma ilə keçirməsini təmin edə bilərsiniz .



Şəkil 2.30. Kart girişı idarəetmə sistemləri

FƏSİL III. BIOMETRİK TEXNOLOGİYALARIN İSTİFADƏ MEXANİZMİ

3.1. Milli biometrik eyniləşdirmə sistemlərinin tədqiqi

Milli biometrik identifikasiya sisteminin memarlığı dövlət proqramında mahiyyət etibarilə irəli sürülür. Əvvəla, milli biometrik identifikasiya sisteminin memarlığına aydınlıq gətirilməli, mürəkkəb sistem kimi onun riyazi modeli yaradılmalıdır və fərqli parametrlərin model üzərində təcrübələri aparılmalıdır. Biometrik eyniləşdirmə sistemləri hələ ölkəmizdə istehsal olunmadığı məlumdur. Hazırkı dövrdə bu texnologiyanın iqtisadi bazarda rolu olduqca sürətlə dəyişir. Beynəlxalq Biometrics Qrupunun bir araşdırmasına görə, 2006-cı ildə biometrik cihazların global dövriyyəsi 1,8 milyard dollara çatdı. Təhlilçilərə görə, 2010-cu ildə bu rəqəm 30% artaraq 4,9 milyarda çatacaq. Biometrik fərdiləşdirmə mərkəzləri milli biometrik eyniləşdirmə sisteminin strukturunda və inkişafında mühüm rol oynayır. Texniki cəhətdən, biometrik fərdiləşdirmə mərkəzləri nəhəng bir verilənlər bazasında real vaxt eyniləşdirmə tələbi axınlarını emal edə bilən proqram təminatı ilə birlikdə qapalı şəbəkələr və telekommunikasiya cihazlarıdır. Belə mərkəzlərə AFIS (Avtomatik Barmaq İzlərinin İdarəetmə Sistemi) deyilir.

3.1.1. Avtomatik barmaq izi tanıma sistemi- AFİS

Avtomatik barmaq izi identifikasiyası , bilinən və bilinməyən izlərin verilənlər bazasına qarşı barmaq izlərini uyğunlaşdırmaq üçün kompüterdən istifadə prosesidir . Avtomatik barmaq izi tanıma sistemləri (AFIS) ilk növbədə hüquq-mühafizə orqanları tərəfindən cinayət identifikasiyası məqsədi ilə istifadə olunur, bunlardan ən başlıcası, cinayət törətməkdə şübhəli bilinən və ya şübhəli şəxsin digər açılmamış cinayətlərlə əlaqələndirilməsində istifadə olunur.

Avtomatik barmaq izi yoxlanışı, iştirak və giriş nəzarəti sistemləri kimi tətbiqlərdə istifadə olunan yaxından əlaqəli bir texnikadır. Texniki səviyyədə, yoxlama sistemləri iddia edilən şəxsiyyəti (istifadəçi PIN və ya şəxsiyyət vəsiqəsini təqdim etməklə başqa biri olduğunu iddia edə bilər və barmaq izindən istifadə edərək

şəxsiyyətini təsdiqləyə bilər), eyniləşdirmə sistemləri şəxsiyyəti yalnız barmaq izlərinə əsaslanaraq təyin edir.

AFIS-lər geniş seçki, şəxsiyyət vəsiqəsi, sürücü lisenziyası və ya bənzər bir sistemə daxil olmasının qarşısını almaq üçün geniş miqyaslı mülki şəxsiyyətlərdə istifadə edilmişdir. Mülki AFIS-in digər bir faydası, həssas vəzifələrə və uşaqlarla yaxın təmasda olan təhsil işçilərinə müraciət edənlərin vəziyyətini yoxlamaqdır.

Barmaq izinə uyğun alqoritmlər I tip (yalnız müsbət) və II tip (yanlış mənfəi) səhv nisbətləri baxımından çox dəyişir. Ayrıca, görüntü nöqtəsindən görünən dönmə dəyişməzliyi və müstəqillik kimi xüsusiyyətlər baxımından fərqlənir. Alqoritmın dəqiqliyi, çap uyğunluğu sürəti, zəif görüntü keyfiyyətinə dayanıqlıq və yuxarıda qeyd olunan xüsusiyyətlər sistemin fəaliyyətinin vacib elementləridir.

Barmaq izi uyğunluğu böyük hesablama yükünə malikdir. Bəzi daha böyük AFIS satıcıları xüsusi hardware yerləşdirirlər, digərləri uyğun sürət və ötürmə qabiliyyətinə sahib olmaq üçün proqram təminatından istifadə edirlər. Ümumiyyətlə, ən azı iki mərhələli bir axtarışın olması arzu olunur. Birinci mərhələ ümumilikdə global barmaq izi xüsusiyyətlərindən istifadə, ikinci mərhələ isə minutia matçdır.

AFIS-in işləmə mexanizmi necə baş verir?

Yüksək inkişaf etmiş alqoritmlərdən səmərəli istifadə prosesin vacib elementidir. İllər ərzində bu cür alqoritmlər davamlı olaraq real dünya təcrübəsinə əsaslanaraq hazırlanmışdır.

Ümumi nümunələrə aşağıdakılar daxildir .

- Şəkil genişləndirilməsi

Adından göründüyü kimi, görüntünün artırılması alqoritmləri gizli və ya əvvəlcədən yazılmış şəkillərin əsas keyfiyyətinə təsir edə biləcək sayısız-hesabsız problemləri həll edir.

- Çıxarış xüsusiyyətləri

Bədi çıxarış alqoritmləri bir çapı digərindən fərqləndirən minutiae nöqtələrini (adətən arxa ucları) müəyyən etmək üçün hazırlanmışdır.

Bunlar məsamələr və ya toxumalar kimi dəqiq olmayan nöqtələri tapan alqoritmlər tərəfindən də dəstəklənə bilər. Həqiqətən, həm minutiae, həm də minutiae olmayan alqoritmlərin birləşməsi bir uyğunlaşma axtarışında xüsusilə güclü ola bilər.

- **İndeksləşdirilmə**

Barmaq izlərinin avtomatik indeksləşdirilməsi, bir AFIS-in uyğunlaşmalar axtararkən emal etməli olduğu çoxlu sayda məlumatları məhdudlaşdıraraq tapşırığı yerinə yetirmək üçün tələb olunan vaxtı əhəmiyyətli dərəcədə azaldır.

- **Uyğunlaşdırma**

AFIS və onun operatorları tərəfindən istifadə olunan uyğun alqoritmlərin dizaynı və seçimi, potensial oyunların, saxta pozitivlərin və saxta neqativlərin sayına əhəmiyyətli dərəcədə təsir göstərir. Alqoritmlər bir uyğun hesab təmin etmək üçün bir AFIS tərəfindən də istifadə olunur. Bu, bir sıra nəşrlərin verilənlər bazasında tapılan başqa bir nəşr ilə uyğunlaşacağına inamı əks etdirir.

AFIS asayiş keşikçilərinə necə kömək edir?

Kompüterlərin meydana gəlməsi inkişaf etmiş dünyada cinayətlərin artması ilə əlaqədar geniş yayılmış narahatlıqla üst-üstə düşdü.

ABŞ-da RAND Corporation tərəfindən hazırlanan bir hesabat xüsusilə təsirli idi.

Əhəmiyyətli olan o, cinayət məsuliyyətini daha təsirli şəkildə yaxşılaşdırmaq üçün fiziki sübutlardan, xüsusən də barmaq izlərindən istifadə etmək imkanlarını vurğuladı.

Bu məqsədə çatmaq üçün texnologiyanın inkişaf etdirilməsinin potensialını bilən FTB, İngiltərə Daxili İşlər Nazirliyi və Yaponiya və Fransadakı polis məmurları da araşdırma təşəbbüsləri etdilər. Birlikdə bu iş AFIS-in inkişafına başlamağa kömək etdi.

Avtomatik barmaq izi uyğunluğu

Müasir AFIS-in təkamülü bir neçə texnoloji uğur tələb edirdi və bu çətinliklərin miqyasını nəzərə almamaq lazımdır. Bacarıqlı və təcrübəli işçilərin işini səmərəli şəkildə artırmaq üçün bir neçə vacib vəzifəni tez, etibarlı və dəqiq şəkildə yerinə yetirmək lazım idi.

Xüsusilə bunlar daxildir .

- mürəkkəb barmaq izi şəklini şərti kartda oxumaq və çəkmək;
- çəkilən görüntüdə 'minutiae' (fərqli xüsusiyyətlər) aşkar edilməsi;
- indeksləşdirmə qeydləri;
- məlumat bazasını (məsələn, şübhəli və ya hadisə yerindən) oxşar qeydlərin böyük bir verilənlər bazası ilə müqayisə etmək.

Əsas texniki məsələlər həll edildikdən sonra AFIS öz dəyərini real dünyada sübut etməli idi. Bu baxımdan, 1984-cü ildə San Fransisko rəsmilərinə verilən bir sistem xüsusilə vacib olduğunu sübut etdi. Xüsusilə, şəhərin yeni AFIS-i tamamilə yeni bir 'cinayət səhnəsi' fəlsəfəsinin bir hissəsi idi.

Bu hərəkət xüsusi hazırlanmış laboratoriyaları və alətləri ilə təchiz olunmuş xüsusi hadisə yerində araşdırma qrupunun yaradılmasını özündə cəmləşdirdi. Təsir kəskin və geniş şəkildə elan edildi və gizli təzyiqlərin müəyyənləşdirilməsində on qat artım və oğurluq nisbətlərinin qəfil azalması daxil edildi. Bir AFIS-in istifadəsi - və fiziki sübutların toplanması və təhlilinə daha diqqətli bir yanaşmaya əsaslandırıldı. ABŞ-ın əsas yurisdiksiyalarında əvəzsiz bir vasitəyə çevrildi. Məhkəmə analitikləri və qazandıqları iş haqqında daha çox məlumat əldə etmək üçün bu gün bir videoya qısa bir giriş necə təqdim etmək üçün, SFPD'nin Auto Biometrik Eyniləşdirmə Sistemi Kaliforniya icmasında ictimai təhlükəsizliyin artırılmasına kömək edir.

AFIS-in bazar payı

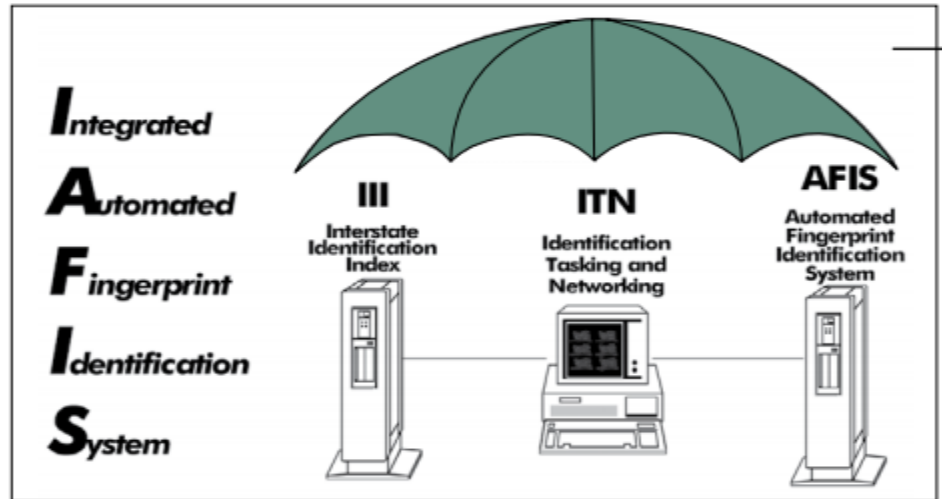
1999-cu ilə qədər dünyada 500 AFIS quraşdırılmışdır. Bu gün Market Research Future-nin 2020-ci ilin Yanvar ayında keçirdiyi bir araşdırmaya görə, avtomatik barmaq izi tanıma sisteminin bazar ölçüsünün (aparət və proqram təminatı) 2022-ci ilə

qədər 2017-ci ildən 2022-ci ilə qədər CAGR-in 22.0% olduğu ilə 13 milyard dollara çatacağı təxmin edilir. Şimali Amerika ən böyük bazar payıdır və bu dövrdə inkişaf etməsi gözlənilir. Asiya-Sakit okean ikinci ən böyük bölgədir .

3.1.2. IAFIS, IDENT(HART) və EURODAC

1980-ci illərdən bəri AFIS tətbiqlərinin sayı artdıqca, integrasiya və əməkdaşlığa ehtiyac da artdı.

IAFIS- AFIS ilə IAFIS arasındakı fərq nədir? AFIS, IAFIS-in FBI AFIS adını verdiyi ümumi bir termindir. IAFIS İntegrasiya edilmiş Avtomatik Barmaq İzləri Tanıma Sisteminin qısaltmasıdır. 1999-cu ildə yaradılan IAFIS, sonrakı nəsillərin identifikasiyası (NGI) səviyyəsinə yüksəldildi və dünyanın ən tarixi cinayət məcmuəsi oldu .



Şəkil 3.1. IAFIS İntegrasiya edilmiş Avtomatik Barmaq İzləri Tanıma Sistemi

FBI Cinayət Ədaləti Məlumat Xidməti tərəfindən saxlanılan aylıq məlumat formasına görə, 2019-cu ilin noyabr ayının sonunda 149 milyondan çox cinayətkar və mülki şəxsin barmaq izlərini saxlayır. Xüsusilə, sistem arxitekturası, yerli, əyalət, federal və beynəlxalq hüquq-mühafizə icmalarına, vətəndaş təşkilatlara, il ərzində 365 gün ərzində 24 saat ərzində kritik məlumatlara səmərəli daxil olmaq və ya dəyişdirmək üçün imkan yaradır.

IDENT(HART)- ABŞ-da biometriya, ölkəyə qanunsuz girmə hallarının aşkarlanması və qarşısını almaq, uyğun miqrasiya güzəştlərini təmin etmək və idarə etmək, qanuni səyahət və ticarəti asanlaşdırmaq üçün də istifadə olunur. Daxili Təhlükəsizlik Nazirliyi biometrik məlumatların xəritələşdirilməsi, saxlanması və bölüşdürülməsi texnologiyasını təqdim edən Biometrik Şəxsiyyət İdarəetmə İdarəsi (OBIM) vasitəsilə biometrik identifikasiya xidmətləri göstərir.

Avtomatik Biometrik Eyniləşdirmə Sistemi və ya *IDENT* adlanan sistem 200 milyondan çox unikal şəxsiyyəti özündə saxlayır və gündə 300.000-dən çox biometrik prosesi həyata keçirir. *IDENT* ABŞ hökumətinin ən böyük biometrik mağazasıdır və milli təhlükəsizlik, müdafiə və ədalət vəzifələrini dəstəkləmək üçün Müdafiə Nazirliyi və Ədalət Nazirliyi ilə kritik biometrik məlumatları bölüşür [24].

HART (Vətən inkişaf etmiş tanıma texnologiyası), gələcək illərdə mövcud *IDENT*-i əvəz edəcək yeni nəsil sistemdir. Daha yüksək tutum, artan emal sürəti, təkmilləşdirilmiş funksionallıq və daha çox istifadəçinin səmərəliliyi artacaq. *HART*, həmçinin 500 milyon insan üçün biometrikliyi əhatə edir.

EURODAC və Avropa giriş-çıxış sistemi- Eynilə, Eurodac biometrik sistemi (Euro pean Dac tiloscopy System) Avropanın 32 ölkəsinə xidmət edən ən böyük çoxsaylı yurisdiksiyadır. Eurodac Avropa Birliyinin sığınacaq barmaq izi məlumat bazasıdır və hər bir üzv dövlətdən gələn sığınma barmaq izlərini və nizamsız sərhəd keçid məntəqələrində tutulan insanların barmaq izi məlumatlarını özündə ehtiva edir.

3.2. Biometrik texnologiyanın test edilməsi

Biometrik cihazların, sistemlərin, alqoritmlərin sınaqlarının təşkili milli biometrik identifikasiya sisteminin yaradılması cəhətindən vacibdir. Biometrik sistemə sürətlə artan tələbə baxmayaraq, əsas suala obyektiv və əqlabatan bir cavab tapmaq lazımdır - bu gənc texnologiyalar çətinliklərin öhdəsindən gələ bilməyə nə dərəcədə hazırdır və ya hazırlıq müddətinin nə qədər olması lazımdır ? Biometrik sistemin keyfiyyət meyarlarını, qiymətləndirmə metodlarını inkişaf etdirmək, bu və ya başqa bir tətbiq sahəsinə olan tələbləri müəyyən etmək vacibdir. Biometrik sistemin vacib

xüsusiyyətlərindən biri onun dəqiqliyidir, yəni sistemin fərqli insanların biometrik xüsusiyyətlərini düzgün ayırd etmə qabiliyyətinin olmasıdır. Biometrik sistemlərdə bunlar, sistemin özünü tanımadığı zaman səhvin birinci növü adlanır (False Reject Rate-Yanlış Rədd etmə Nisbəti FRR), sistem digərini buraxan zaman, yəni başqanı özü kimi qəbul edən zaman səhvin ikinci növü adlanır (False Accept Rate-Yanlış Qəbul etmə Nisbəti FAR). FRR və FAR alqoritmlərin hamısında bir-biri ilə əlaqədə olurlar.

Biometrik tanıma sistemi iki fərqli rejimdə işləyə bilər: eyniləşdirmə və ya yoxlama. Eyniləşdirmə şəxsiyyətin biometrik xüsusiyyətlərindən hesablanmış biometrik nümunəni araşdıraraq şəxsiyyətini tapmağa çalışmaqdır.

Eyniləşdirmə vəziyyətində sistem bir neçə insanın nümunələri ilə öyrədilir. Hər bir insan üçün bu təlim mərhələsində bir biometrik şablon hesablanır. Müəyyən ediləcək bir nümunə, hər məlum nümunəyə uyğun gəlir və nəxişlə şablon arasındakı bənzərliyi müəyyən edən bir xal və ya məsafə verir. Sistem, nümunəni ən çox oxşar biometrik nümunə olan şəxsə təyin edir. Saxta nümunələrin (bu vəziyyətdə sistemə bilinməyən insanların bütün nümunələri) düzgün müəyyən edilməməsi üçün oxşarlıq müəyyən səviyyəni keçməlidir. Bu səviyyəyə çatmazsa, nümunə rədd edilir.

Yoxlama halında, bir şəxsin şəxsiyyətinin priori olduğu iddia edilir. Yalnız təsdiq edilmiş nümunə şəxsin fərdi şablonu ilə müqayisə olunur. Təsvirə bənzər, nəxiş və şablon arasındakı oxşarlığın etibarlı sistemə və ya əraziyə girişi təmin etmək üçün kifayət olub olmadığı yoxlanılır.

Bir nəxiş və biometrik şablon arasındakı bənzərliyi ifadə etmək üçün nöqtələrdən istifadə edirik (çəkilər də deyilir). Hesab nə qədər yüksəkdirsə, aralarındakı oxşarlıq da bir o qədər yüksəkdir. Əvvəlki hissədə izah edildiyi kimi, sistemə giriş yalnız təlim keçmiş şəxs (şəxsiyyət) və ya nümunə təsdiqlənmiş şəxs (şəxsiyyət) müəyyən bir hədddən yüksək olduqda verilir.

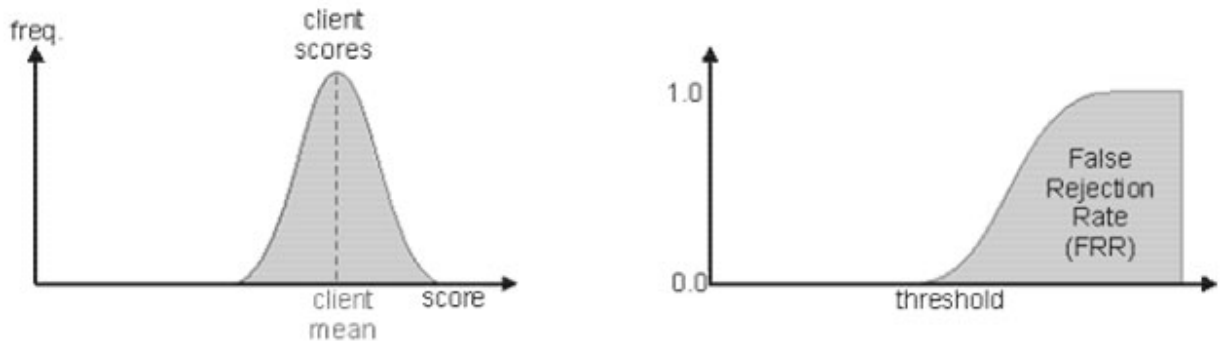
Nəzəriyyə olaraq, müştəri reytingləri (sistem tərəfindən bilinən insanların nümunə balları) həmişə fırıldaqçılardan daha yüksək olmalıdır. Bu doğrudursa, iki

hesab qrupunu bir-birindən ayıran bir eşik, müştəriləri və təqlidçiləri ayırd etmək üçün istifadə edilə bilər.

Bir neçə səbəbə görə bu fərziyyə real dünya biometrik sistemlərinə aid deyil. Bəzi hallarda, emulator nümunələri bəzi müştəri nümunələrinə nisbətən daha yüksək ballar yaradır. Buna görə təsnifat həddi seçilsə belə, bəzi təsnifat səhvlərinin baş verməsi bir həqiqətdir.

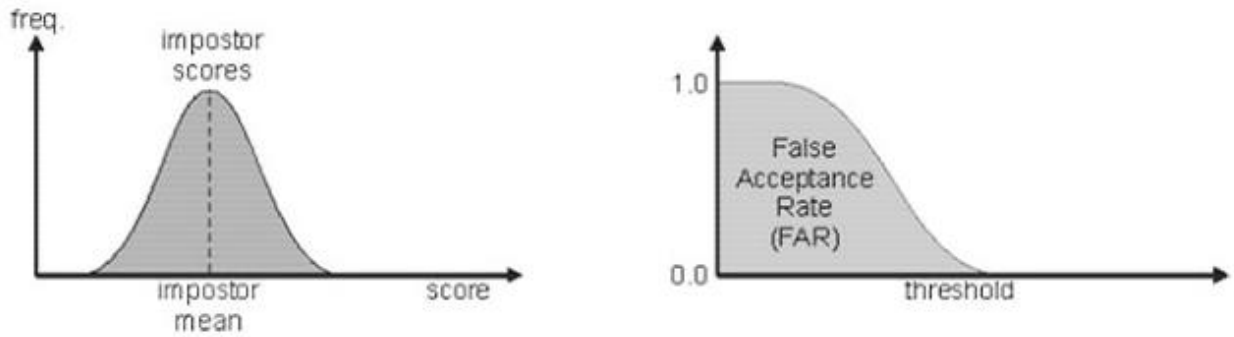
Məsələn, belə bir yüksək həddi seçə bilərsiniz, həqiqətən heç bir yaramaz nöqtə bu həddi keçməyəcəkdir. Nəticədə heç bir nümunə sistem tərəfindən səhv hesab edilmir. Digər tərəfdən, ən yüksək fırıldaqçılıqdan daha aşağı bal alan müştəri nümunələri səhv qəbul edilir. Bunun əksinə olaraq, hər hansı bir müştəri modelinin səhv qəbul edilməməsi üçün çox aşağı olan həddi seçə bilərsiniz. Digər tərəfdən, digər saxtakar nümunələr yalnız sayılır. Bu iki nöqtə arasındakı kəsişmə yerini seçsəniz, həm tanınmazlıqlar, həm də yanlış fərziyyələr meydana çıxır.

Aşağıdakı şəkillər bu məsələni daha yaxşı başa düşməyə kömək edəcəkdir. Böyük bir miqdarda test məlumatları ilə sınaqdan keçirilən biometrik bir yoxlama sistemini nəzərdən keçirək. Test məlumatları həm saxtakar, həm də müştəri nümunələrindən ibarətdir. Əvvəlcə saxtakar nümunələrə nəzər salaq. Müvafiq nöqtələr müəyyən bir orta bal ətrafında birtəhər paylanacaq. Bu, soldakı ilk şəkildə göstərilir. Bu nümunədə, Gauss'ın normal paylanması seçilmişdir.



Şəkil 3.2. False Rejection Rate(Yalnış rəddetmə nisbəti)

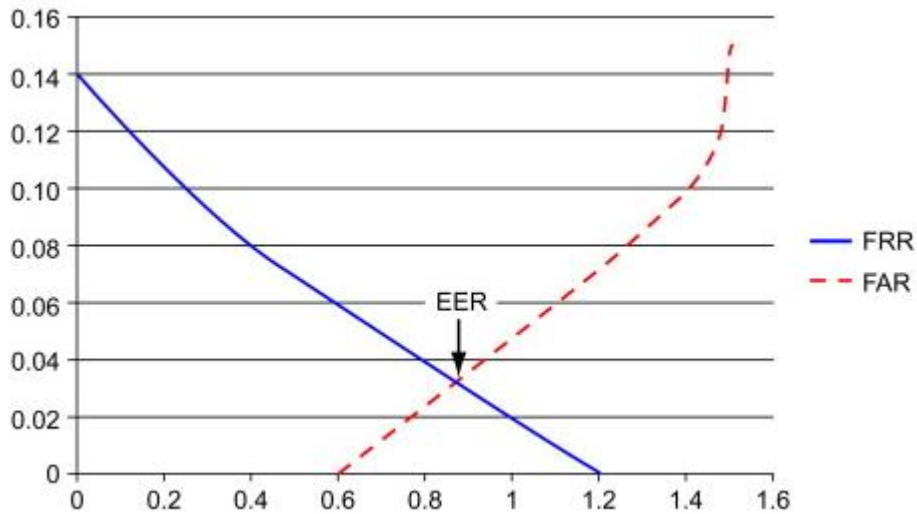
Müştəri modellərinə keçək. Təqlidçi ballara bənzər, müştəri modelinin balları müəyyən bir orta dəyər ətrafında dəyişir. Aşağıdakı iki görüntünün solunda göstərildiyi kimi, müştəri modellərinin orta balı saxta naxışların orta dəyərindən yüksəkdir. Təsnifat ballarına çox yüksək təsnifat həddi tətbiq olunarsa, bəzi müştəri nümunələri səhv qəbul edilmişdir. Hədəfin dəyərindən asılı olaraq, heç biri və bütün müştəri modelləri arasında səhv rədd ediləcəkdir. Rədd edilmiş müştəri nümunələrinin sayını müştəri nümunələrinin ümumi sayına bölmək yanlış rəddetmə dərəcəsi (FRR) adlanır. FAR-a görə, onun dəyəri sıfırla bir arasında dəyişir. Sağdakı şəkil, sol tərəfdəki şəkildə göstərilən hesab paylaması üçün FAR-ı dəyişir.



Şəkil 3.3. False Acceptance Rate(Yanlış qəbuletmə nisbəti)

Bir biometrik sistemin işini ölçərkən bir çox amillərə baxa bilərik, lakin sistemin necə işlədiyini ölçmək üçün bir neçə ilkin ölçmə xüsusilə vacibdir. Yanlış qəbuletmə dərəcəsi (FAR) və yalan rədd etmə dərəcəsi (FRR) bunlardan ikisidir. FAR, həqiqətən imtina etməyimiz lazım olan bir istifadəçini qəbul etdiyimiz zaman meydana gəlir. Bu cür problemlərə yanlış pozitiv də deyilir. FRR qanuni bir istifadəçini qəbul etməyimiz lazım olduqda rədd etmək problemidir. Bu tip problem biometriya dünyasından kənarda saxta mənfi hallar kimi tanınır.

Bu vəziyyətlərin hər ikisi son dərəcə arzuolunmazdır. Bu cür sistemlərlə əldə etməyə çalışdığımız şey, səhv səhv nisbətləri (EER) adlanan iki növ səhv arasındakı tarazlıqdır. Şəkil 3.2-də göstərdiyimiz kimi həm FAR, həm də FRR-ni bir qrafikdə çəksək, EER iki xətlərin kəsişdiyi nöqtədir. EER bəzən biometrik sistemlərin dəqiqliyini ölçmək üçün istifadə olunur.



Şəkil 3.2. FAR və FRR əyriələrinin kəsişmə nöqtəsi

False Accept Rate- FAR

Yanlış qəbul icazəsiz bir sənədin etibarlı hesab edildiyi zaman baş verir. Bir təşkilatın biometrik nəzarəti çoxsaylı yalan rəddlər verərsə, ümumi audit, subyektlərin şəxsiyyətini təsdiq edərkən topladığı məlumatların miqdarını azaltmaqla sistemin düzgünlüyünü azaltmaq məcburiyyətində ola bilər. Məlumat nöqtələri endirildikdə, təşkilat yanlış qəbul etmə riski ilə üzləşir. Təşkilat, icazəsiz istifadəçi əldə etmək riski altındadır. Bu tip səhvlərə II növ səhv də deyilir.

40-dan çox məlumat nöqtəsi adətən barmaq izi skanı ilə toplanır və müqayisə edilir. Sistemin dəqiqliyi daha az minutia (on və ya daha çox) əlavə etməklə azaldıla bilər. Bu FRR-ni aşağı salır, lakin FAR-ı qaldırır. Ayrıca bir istifadəçinin barmaq izlərini təqlid etmək daha asan olma ehtimalını artırır.

False Reject Rate- FRR

Yalan imtina nisbəti doğrulama tapşırığı üzərində işləyərkən biometrik göstəriciləri ölçmək üçün istifadə olunan bir statistikdir və ümumiyyətlə sistemin yalan rədd edilməsinin bir faizi olaraq hesablanır. Fərdi bir şəxsin mövcud biometrik şablonuna uyğun gəlmədiyi zaman yalan rədd edilir. Məsələn: John John olduğunu iddia edir, lakin sistem təsdiqləməyi səhv şəkildə rədd edir. Sistemdə qeydiyyat

alındıqlarını və onların tanınması və təsdiqlənməsinin lazım olduğunu bilən son istifadəçi üçün xüsusilə əsəbi ola bilər, amma nədənsə sistem taramasını səhv rədd edir. Bu, lazımsız qeydlərə səbəb ola bilər, xidmətə təsir göstərə bilər, işçiləri qıcıqlandırır və məhsuldarlığa mənfi təsir göstərir [25].

3.3. Biometrik eyniləşdirmə sistemlərinin təhlükəsizliyinin qiymətləndirilməsi

Biometrik sistem informasiya təhlükəsizliyinin sisteminin ən vacib elementidir. Buna görə də yüksək təhlükəsizliyin tələbinə cavab verməlidirlər. Təəssüflər olsun ki, biometrik sistem istehsalçılarının təhlükəsizliyin tələblərini çox vaxt nəzərə almadıqları məlumdur. Bunun ən yaxşı nümunəsi bir neçə ölkələrdə biometrik pasportların təhlükəsizliyinin pozulması əlamətləridir. Bu sahə üzrə tədqiqat bir sıra formada – biometrik identifikasiya təhlükəsizliyini tam təmin etmək üçün aparıla bilər: sensor və cihazlar, network, saxlanma və proqram təminatları və s. Bundan əlavə, həyatı boyu biometrik pasportların iş proseslərini nəzərə alan bir təhlükəsizlik modelinin hazırlanmasına, mikroçipdə saxlanılan məlumatların qorunması üçün texnologiyaların öyrənilməsinə üstünlük verilməlidir. Biometrik texnologiyanın qiymətləndirilməsi ilə yanaşı fərdi biometrik texnologiyanın zəifliyinin ətraflı dəyərləndirilməsi də aktual bir məsələdir. Əlavə olaraq Elektron imza texnologiyasının tətbiqi, korporativ sistemlərin açıq açar infrastrukturunu və sertifikatlaşdırma mərkəzinin yaradılması üçün ideyaların ərsəyə gətirilməsi və başqa şeylər nəzərdə tutulur.

3.4. Biometrik eyniləşdirmə texnologiyalarının standartlaşdırılması üsulları

NIST(National Institute of Standards and Technology - Milli Standartlar və Texnologiya İnstitutu), şəxsiyyət sistemlərini inkişaf etdirmək üçün təxminən beş illik təcrübəyə malikdir. NIST, digər federal qurumlar, akademiyalar və sənaye tərəfdaşları ilə əməkdaşlıq edərək biometrik standartlara dair hökumət və bazar tələblərinə cavab verir.

- Biometrik standartların vaxtında inkişafına dəstək olmaq;

- Seçilən biometrik standartların tətbiqini sınaqdan keçirmək üçün uyğunluq test arxitekturası və test alətlərini inkişaf etdirmək;
- Barmaq izi, üz, iris, səs, multimodal texnika və ortaya çıxan identifikasiya texnologiyaları da daxil olmaqla biometrik texnologiyaların istifadəsini yaxşılaşdırmaq və inkişaf etdirmək üçün ölçmə, qiymətləndirmə və standartları araşdırmaq;
- Şəxsiyyət idarəetmə, kritik standartlar və elektron şəxsiyyətlərin qarşılıqlı əlaqəsi üçün ümumi modellər və ölçüləri inkişaf etdirmək.

Bu səylər şəxsiyyət idarəetmə sistemlərinin keyfiyyətini, istifadəsini, qarşılıqlı əlaqəsini və ardıcılığını artırır, məxfiliyi qorumaq və ABŞ maraqlarının beynəlxalq səviyyədə təmsil olunmasını təmin edir. Əslində, NIST araşdırması, biometrik tanınmadan asılı olan ABŞ sənayesi və ABŞ hökuməti üçün ən yeni texnoloji meyarları və rəhbərliyi təqdim etmişdir.

Bu təsiri əldə etmək üçün, NIST Milli Elm və Texnologiya Şurasında (NSTC) Biometriya və Şəxsiyyət İdarəetmə Alt Komitəsi və Standartlar və Uyğunluq Qiymətləndirmə və Tədqiqat, İnkişaf, Test və Qiymətləndirmə İşçi Qruplarında fəal iştirak edir və eyni zamanda bir neçə USG integrasiya biometrik iş qruplarında yer alır.

2002-ci ildə JTC 1/SC 37-nin fəaliyyətə başlamasından bəri NIST, NIST mütəxəssislərinə bu SDO-da beynəlxalq biometrik standartların hazırlanmasını təmin etdi. JTC 1/SC 37 tərəfindən hazırlanmış standartlar beynəlxalq və milli bazarlarda geniş qəbul edilmişdir. Maşın oxunan səyahət sənədləri üçün Beynəlxalq Mülki Aviasiya Təşkilatı (DƏM) və dənizçilərin yoxlanılması və identifikasiyası üçün Birləşmiş Millətlər Təşkilatının Beynəlxalq Əmək Ofisi (BƏT) kimi bəzi beynəlxalq təşkilatlar bəzi tələblərini öz tələblərində müəyyənləşdirirlər.

ICAO dünya pasportlarını səyahət sənədlərinin təhlükəsizliyini, məlumatların bütövlüyünü və şəxsiyyət idarəetmə səviyyəsini yeni səviyyəyə qaldırdı. Qlobal qarşılıqlı məqsəd uyğunluğu asanlaşdırmaq üçün, ICAO, MRTD üçün maşın köməyi ilə təsdiqlənmə üçün qlobal bir araya bilən biometrik (məcburi siyahıda) olaraq tanıma

seçmişdir. Bundan əlavə, ICAO, bir seçim olaraq, barmaq və iris spesifikasiyalarını daxil etmək qabiliyyətini seçdi. 2012-ci ilin dekabr ayına olan məlumata görə, ICAO-nun qiymətləndirməsi JTC 1/SC 37 standartlarından istifadə edərək bu tətbiq üçün 430 milyon ePasport nəşr olunduğunu bildirdi. Bu proqram, ISO/IEC JTC 1 alt komitələri və ICAO vasitəsi ilə dünya hökumətləri vasitəsi ilə sektor arasında səmərəli əməkdaşlıq və əməkdaşlıq üçün bir model olaraq xidmət edir. BƏT-in tələbləri JTC 1/SC 37 tərəfindən hazırlanan barmaq minutiae və barmaq görüntüsü məlumat mübadiləsi formatlarının ilk nəşridir.

Biometrik beynəlxalq standartlara istinad edən müxtəlif ölkələrdə tətbiq olunan nümunələrinə İspaniya (elektron şəxsiyyət vəsiqələri və İspan elektron pasportları üçün) və Hindistan (standartlara əsaslanan biometriya əsasında dünyanın ən böyük şəxsiyyət təminatı sistemlərindən birini istifadə edən Hindistan) daxildir.

Biometrik tətbiqlərin proqram interfeysləri

ISO / IEC 19784-1: 2006 (BioAPI spesifikasiya)

ISO/IEC 19784-1: 2006, bir proqram tətbiqinin bir və ya bir neçə biometrik texnologiya ilə əlaqə qurmasına (xidmətlərindən yararlanmasına) imkan verən müəyyən bir interfeys təqdim edir. Buraya geniş biometrik tətbiqetmələr və biometrik texnologiyanın əksər formaları üçün uyğun olan yüksək səviyyəli ümumi biometrik identifikasiya modeli daxildir. Bir biometrik sistemin tərkib hissələrini müxtəlif satıcılar tərəfindən təmin etməyə və tam müəyyən edilmiş Proqram Tətbiq İnterfeysləri (API), müvafiq Xidmət Təminatçısı İnterfeysi (SPI) və əlaqəli məlumat strukturları ilə birlikdə işləməyə imkan verən bir memarlıq modeli müəyyən edilmişdir. ISO / IEC 19784-1: 2006, qeydiyyat, yoxlama və identifikasiyanın əsas biometrik funksiyalarını əhatə edir və bir tətbiqin biometrik qeydlərin saxlanması idarə etməyə imkan verən verilənlər bazası interfeysini özündə cəmləşdirir. ISO/IEC 19784-1: 2006, ISO/IEC 19785 və 19794-ə uyğun bir biometrik məlumat quruluşunu göstərir [27].

İSO / İEC 19784-2: 2007 (Biometrik Arxivləmə Fəaliyyətləri Təminatçısı İnterfeysi)

İSO/İEC 19784-2: 2007 biometrik xidmət təminatçısı (BSP) və BioAPI üçün biometrik arxiv funksiyası təminatçısı (BAFP) arasındakı interfeysi müəyyənləşdirir. BAFP, fiziki saxlama mühitinin növündən asılı olmayaraq biometrik arayış məlumatlarının saxlanması, axtarışı və idarə olunması üçün bütün funksiyaları əhatə edir. Bir BAFP istifadə edərək, bir BSP verilənlər bazası serverləri, smart kartlar, verilənlər bazası veb xidmətləri və s. Ehtiyac kimi müxtəlif saxlama vasitələrinə xüsusi müraciət edilməməlidir. Mediya nə olursa olsun, BSP həmişə bir BAFP üçün eyni interfeysdən istifadə edir [28].

İnterfeys təsviri, müxtəlif BAFP-ların birləşdirilməsi və sökülməsi, biometrik məlumat qeydlərinin sorğusu və biometrik məlumatların qeydlərinin saxlanması üçün idarəetmə funksiyalarını əhatə edir.

Biometrik mübadilə formatlarının vahid quruluşları

İSO / İEC 19785-1: 2006 (Məlumat elementlərinin dəqiqləşdirilməsi)

İSO/İEC 19785-1: 2006 Ümumi Biometrik Dəyişiklik Formaları Çərçivəsində (CBEFF) standart biometrik məlumat qeydləri (BIR) üçün əsas quruluşu müəyyənləşdirir. Bu quruluş üç hissədən ibarətdir: standart biometrik başlıq (SBH), biometrik məlumat bloku (BDB) və təhlükəsizlik bloku (SB). CBEFF eyni zamanda SBH və SB-lərdə istifadə edilə bilən bir neçə məlumat maddəsini və onların standartlaşdırılmış mücərrəd dəyərlərini (CBEFF BDB-ni qeyri-şəffaf məlumatlar kimi qəbul edir) müəyyənləşdirir. CBEFF, CBEFF tərəfindən 'patron' adlandırılan təşkilatların 'boss formatları' adlandırdığı A format spesifikasiyalarını təyin və yayımlaya biləcəyi mexanizmləri də müəyyənləşdirir. CBEFF istifadəçilərə tam standartlaşdırılmış və işlənə bilən, lakin xüsusi bir tətbiq mühitinin ehtiyaclarına uyğunlaşdırılan spesifikasiyalar hazırlamağa imkan verir [29].

CBEFF yalnız bir BDB (sadə A) olan və ən azı bir BDB (kompleks A) olan A-lar üçün qaydaları müəyyənləşdirir. CBEFF, bir BDB formatını və təhlükəsizlik

xüsusiyyətlərini (şifrələmə və bütövlüyü) müəyyən edən məcburi məlumat maddələrini təyin edir. CBEFF tərəfindən təyin olunan bütün digər məlumat elementləri və yumşaq dəyərlər istəyə bağlıdır. CBEFF istifadəçilərə tətbiq mühitinin tələb etdiyi əlavə məlumatlar və yumşaq dəyərləri təyin etməyə imkan verir.

İSO / İEC 19785-2: 2006 (Biometrik Qeydiyyat Təşkilatlarının əməliyyatları üçün nəzərdə tutulan prosedurlar)

İSO/IEC 19785-2: 2006, Biometrik Qeydiyyatın Ümumi Biometrik Dəyişiklik Formaları Çərçivəsində (CBEFF) fəaliyyət göstərməsini tələblərini göstərir. Qeyd Təşkilatı, biometrik məlumat blokları, biometrik məlumatların daxil edilməsi təhlükəsizlik blokları və / və ya CBEFF istifadəçi formatları üçün standart və ya mülkiyyət format spesifikasiyalarına cavabdeh olan təşkilatlara veb sayt vasitəsilə bənzərsiz biometrik təşkilatı identifikator dəyərlərinin təyin edilməsi və yayılması üçün cavabdehdir. məhsullarına biometrik məhsulun təsviri dəyərlərini təyin etmək istəyən təşkilatlar [30].

Biometrik məlumatları mübadiləsi formatı

İSO / İEC 19794-1: 2006 (Vahid quruluş)

Biometrik məlumat mübadiləsi standartları biometrik komponentlərin qarşılıqlı əlaqəsi üçün çox vacibdir. İSO/IEC 19794-1: 2006 biometrik məlumat mübadiləsi formatlarının ümumi aspektlərini və müəyyən formatları standartlaşdırarkən nəzərə alınacaq şərtləri göstərir. Biometrik məlumatları əməliyyat səviyyələrinə görə təsnif edir və bu, əsasən biometrik məlumat mübadiləsi formatları üçün adlandırma anlayışını yaradır [31].

İSO / İEC 19794-2: 2005 (Barmaq izlərinə nəzarət nöqtəsi)

İSO/IEC 19794-2: 2005, minutiyanın əsas konsepsiyasından istifadə edərək barmaq izlərinin nümayişi üçün bir konsepsiya və məlumat formatlarını göstərir. Avtomatik barmaq izi tanınması da daxil olmaqla geniş tətbiqlərdə tətbiq oluna və istifadə edilə biləcəyi üçün ümumi bir haldır. İSO/IEC 19794-2: 2005 əlaqəli terminlərin təriflərini, minutiyanı necə müəyyənləşdirəcəyini izah edir, həm ümumi

istifadə üçün, həm də kartlarla istifadə üçün məlumatları daxil edən məlumat formatları və uyğunluq məlumatlarını ehtiva edir. Uyğunlaşma və qərar parametrləri üçün təlimatlar və dəyərlər məlumatlı əlavədə verilmişdir [32].

ISO/IEC 19794-2: 2005 özündə bunları ehtiva edir.

- barmaq izinin minutiae əsaslı nümayəndəliyi üçün istifadə olunan əsas məlumatlar;
- bu məlumatların mübadiləsi və saxlanması üçün üç məlumat formatı: rekord əsaslı bir format və bir kartda uyğun oyun tətbiqində bir smart kartda istifadə üçün normal və yığcam formatlar;
- İstisnalı genişləndirilmiş məlumat formatları, məsələn, silsilələrin sayı və əsas və delta yeri kimi əlavə məlumatları daxil etmək.

ISO/IEC 19794-2: 2005 aşkarlama, saxlama və uyğun sistemlər arasında barmaq minutiae məlumatlarının mübadiləsini təmin edir.

ISO / IEC 19794-3: 2006 (Barmaq təsvirinin spektral məlumatları)

Barmaq izi spektral məlumat mübadiləsi formatı ISO/IEC 19794-3: 2006, barmaq izi görüntüsündən alınan yerli və ya qlobal spektral məlumatların göstərilməsi üçün tələbləri müəyyənləşdirir. Format spektral göstəricilərin seçilməsində rahatlıq təmin etmək üçün hazırlanmışdır; çünki spektral komponentlər miqdarlı kosinusoidal üçlü, Diskret Furyer Dəyişikliyi və ya Gabor filtrlərinə əsaslanı bilər. Format, bütün məlumat barmaqlarının saxlanmasıdan daha yığcam şəkildə məlumatların təqdimatını təmin edən dəyişkən sayda spektral komponentlərin qorunmasına imkan verir [33].

ISO / IEC 19794-4: 2005 (Barmaq izi məlumatları)

ISO/IEC 19794-4: 2005, bir ISO/IEC 19785-1 CBEFF məlumat quruluşu daxilində bir və ya daha çox barmaq və ya ovuc görüntüsü sahələrindən məlumatların saxlanması, qeyd edilməsi və ötürülməsi üçün məlumat qeydləri mübadiləsi formatını müəyyənləşdirir. Bu, barmaq təsviri məlumatlarını mübadilə və müqayisə etmək üçün istifadə edilə bilər. Bir mövzunu təsdiqləmək və ya müəyyənləşdirmək üçün istifadə edilə bilən barmaq görüntüsü məlumatlarının mübadiləsi üçün məzmunu, formatı və

ölçü vahidlərini müəyyənləşdirir. Məlumat müxtəlif məcburi və seçim maddələrindən, o cümlədən tarama parametrləri, sıxılmış və ya sıxılmamış şəkillər və satıcıya məxsus məlumatlardan ibarətdir. Bu məlumat, barmaq görüntüsü sahələrindən alınan məlumatlara əsaslanaraq avtomatik cihazlara və identifikasiya və ya identifikasiya sistemlərinə etibar edən təşkilatlar arasındakı mübadilə üçündür [34].

İSO / İEC 19794-5: 2005 (Üz təsviri məlumatları)

İSO/IEC 19794-5: 2005, insanın yoxlanılması və kompüterin avtomatik tanınması kontekstində istifadə ediləcək görünüşlərin görünüşü üçün səhnə, foto, rəqəmsallaşdırma və format tələblərini göstərir. Bu formatda səhnə və fotoqrafiya tələblərini müəyyənləşdirməyə yanaşma, fotosəkilin necə çəkilməsini dikte etməkdənsə, fotosəklin necə görünməsinin məhdudiyyətlərini diqqətlə müəyyənləşdirməkdir. Bir forma, cinsiyyət, poza və göz rəngi kimi bir üz müşahidəçisi tərəfindən görünə bilən görünən məlumatların göstərilməsinə imkan yaratmaq üçün hazırlanmışdır. Rəqəmsal görüntü formatı İSO standartı JPEG və ya JPEG2000 ola bilər. Nəhayət, ən yaxşı təcrübə əlavələri, səyahət sənədləri və rəqəmsal sıxılma əleyhinə üz tanıma performansını üçün şəkil çəkməyə dair təlimat verir [35].

İSO / İEC 19794-6: 2005 (İris görüntü məlumatları)

İSO/IEC 19794-6: 2005, iris tanıma istifadə edərək biometrik identifikasiya sistemləri üçün iki alternativ şəkil mübadiləsi formatını göstərir.

Birincisi, xam, sıxılmamış bir sıra sıxlığı və ya İSO/IEC 15444 ilə müəyyənləşdirilmiş bir sıxılmış format ola bilən xətti görüntü saxlama formatına əsaslanır.

İkinci format, müəyyən bir əvvəlcədən hazırlanma və görüntü seqmentləşdirmə mərhələlərini tələb edən, ancaq iris məlumatlarını ehtiva edən daha yığcam məlumat quruluşu istehsal edən bir qütb görüntü spesifikasiyasına əsaslanır.

İSO/IEC 19794-6: 2005-də göstərilən iris görüntü formatlarından birinə uyğun gələn məlumatların CBEFF Biometrik Məlumat Blokuna (BDB) ISO/IEC 19785-1-də göstərildiyi kimi CBEFF uyğun quruluşa daxil edilməsi nəzərdə tutulur [36].

İSO / İEC 19794-9: 2007 (Damar təsviri məlumatları)

İSO/İEC 19794-9: 2007, insanın damar biometrik görüntü məlumatlarının mübadiləsini təyin edir. Xüsusiyyətlərin müəyyən bir tərifini, damar biometrik şəkillərinin və spesifik xüsusiyyətlərin saxlanması və ötürülməsi üçün məlumatların qeyd formatını, nümunə qeydini və uyğunluq meyarlarını müəyyənləşdirir.

İSO/İEC 19794-9: 2007 xam və ya emal edilmiş damar biometrik şəkillərinin dəyişdirilməsini tələb edən tətbiqlər üçün hazırlanmışdır. Tələb olunan saxlama yerinin miqdarı ilə məhdudlaşmayan tətbiqlər üçün hazırlanmışdır. Məlumatların saxlanması və ya ötürülməsi üçün tələb olunan mənbələr və məlumatların keyfiyyətini dəqiqliyinin yaxşılaşdırılması potensialı arasında güzəşt və ya güzəstdir. Əsasən, digər görüntü mənbələrindən köçürülmüş damar biometrik görüntü məlumatlarını müəyyənləşdirmək və ya yoxlamaq üçün müxtəlif alqoritmlər təqdim etməkdir. Bu gün görüntü dəyişdirmək üçün İSO/İEC 19794-9: 2007-dən istifadə edə bilən damar biometrik texnologiyalar, əlin, ovucun və barmağın arxasından istifadə edən texnologiyalardır [37].

Biometrik məhsuldarlıq testi və hesabat

İSO / İEC 19795-1: 2006 (Prinsip və quruluş)

İSO/İEC 19795-1: 2006, biometrik sistemlərin səhv dərəcələri və istehsal nisbətləri baxımından qiymətləndirilməsi ilə məşğul olur. Biometrik qeydiyyat, yoxlama və identifikasiyada müxtəlif səhv nisbətləri ilə əlaqəli ölçülər dəqiq göstərilmişdir. Qiymətləndirmənin planlaşdırılması mərhələləri ilə performans qiymətləndirmələrinin aparılması üçün təkliflər və şərtlər verilir, qeydiyyat, yoxlama və ya şəxsiyyət əməliyyatı məlumatlarının toplanması, səhv nisbətlərinin təhlili, hesabat vermək və nəticələrin təqdimatı. Təqdim olunan prinsiplər biometrik metodlar, tətbiqlər və test məqsədləri ilə həm oflayn, həm də onlayn test metodologiyaları üçün ümumi olur. Bu prinsiplər məlumatların düzgün toplanmaması və ya analitik prosedurlar səbəbindən qərəzlərin qarşısını almağa kömək edir; sərf olunan səy üçün

sahə performansını daha yaxşı qiymətləndirmək və test nəticələrinin tətbiq olunma hədlərini dəqiqləşdirmək [38].

İSO / İEC 19795-2: 2007 (Texnologiya və ssenari qiymətləndirilməsi üçün test etmə metodologiyası)

İSO/IEC 19795-2: 2007 iki xüsusi biometrik performans test metodologiyasına müraciət edir: texnologiya və ssenari qiymətləndirilməsi. Biometrik testlərin böyük əksəriyyəti bu iki ümumi qiymətləndirmədən biridir. Texnologiya qiymətləndirmələri əvvəllər toplanmış korpuslar vasitəsilə qeyd və müqayisə alqoritmlərini qiymətləndirsə də, ssenari qiymətləndirmə sensorlar və alqoritmlər real vaxt rejimində Test mövzularından toplanmış nümunələri qiymətləndirir. Birincisi, bir alqoritmın əsas fərqləndirici gücünü göstərən böyük həcmli müqayisə balları və namizəd siyahıları yaratmaq üçün hazırlanmışdır. İkincisi, Test mövzusu sisteminin qarşılıqlı əlaqələri də daxil olmaqla, modelləşdirilmiş mühitlərdə fəaliyyətin ölçülməsi üçün nəzərdə tutulmuşdur [39].

İSO/IEC 19795-2: 2007 məlumatların toplanması, təhlili və hesabatın iki əsas növünə xas olan tələblər və tövsiyələr təqdim edir: texnologiya qiymətləndirilməsi və ssenari qiymətləndirilməsi.

Aşağıdakı sahələrdə tələbləri müəyyənləşdirir:

- texnologiyaların və ssenarilərin qiymətləndirmək üçün nəzərdə tutulan protokolların hazırlanması və tam açıqlanması;
- biometrik qiymətləndirmə növləri ilə əlaqəli parametrləri əks etdirən biometrik qiymətləndirmələrin aparılması və hesabatlandırılması.

İSO / İEC 24709-1: 2007 (prosedur və metod)

İSO/IEC 24709-1: 2007 BioAPI (İSO/IEC 19784-1) ilə uyğun olduğunu iddia edən biometrik məhsulların uyğunluğunu yoxlamaq üçün anlayışlar, çərçivə, test üsulları və meyarları göstərir. BioAPI uyğunluq test paketlərini müəyyənləşdirmək, test ifadələrini yazmaq və fitness testi zamanı aparılacaq prosedurları müəyyən etmək üçün təlimatlar verilir. Uyğunluq test üsulu BioAPI-yə uyğun olduğunu iddia edən biometrik

məhsulların uyğunluq testi ilə əlaqədardır. Doğrulama dilinin sxemlərinin tərifləri normativ əlavələrdə verilmişdir [40].

**İSO / İEC 24709-2: 2007 (Biometrik xidmət təminatçıları üçün test
təsdiqləmələri)**

İSO/IEC 24709-2: 2007, İSO/IEC 24709-1-də göstərilən doğrulama dilində yazılmış bir sıra test iddialarını müəyyənləşdirir. Bu iddialar İSO /IEC 24709-2: 2007 (bir testlər laboratoriyası kimi) istifadəçisinə İSO/ İEC 19784-1 uyğun olduğunu iddia edən hər hansı bir biometrik xidmət təminatçısının (BSP) istənilən istifadəçisinin uyğunluğunu yoxlamağa imkan verir. İSO/IEC 24709-2: 2007-də göstərilən hər bir sınaq iddiası sınılanmış bir tətbiqin bir və ya daha çox xüsusiyyətindən istifadə edir. Təsdiqləmə, təsdiqləmə dilinin tələb etdiyi kimi paketlərə yerləşdirilir (paket başına bir və ya daha çox təsdiq). Bu iddialar BSP-lərin bütün uyğun alt siniflərin uyğunluğunu yoxlamağa imkan verir və uyğun əlavələr və əlavə xüsusiyyətlərə uyğun olaraq təşkil edilir [41].

NƏTİCƏ VƏ TƏKLİFLƏR

İnformasiya texnologiyalarının sürətli inkişafı nəticəsində bir çox yeni vasitə və qurğular həyatımızın bir hissəsinə çevrildi. Cihazların rahatlığına alışmış insanlar tez bir zamanda avtomatlaşdırma sistemlərindən asılı olurlar. Məsələn, bəzi iş yerlərində girişlərdə avtomatik açılan və bağlanan qapılar rahat bir vasitə hesab edilə bilər. Xüsusilə ölkə sərhədlərini keçəndə təhlükəsizlik elementlərinin xeyli artdığı görülür. Barmaq izlərini götürmək, barmaq izlərini sonrakı girişlərlə müqayisə edərək ölkəyə girməyi asanlaşdırır. Təhlükəsizlik təcrübələri ilə yanaşı, saxta məhsullar da gündəmdədir və bir çox sistem ciddi hücumlara məruz qalır. Bu çərçivədə ağla gələn ilk şey təhlükəsizlik, kart, açar və s. Bu, oğurluq və icazəsiz şifrə mübadiləsi kimi bir çox problemi aradan qaldıran biometrik metodların inkişafına səbəb oldu.

Etibarlı identifikasiya bu gün çox vacibdir. Üç identifikasiya üsulu arasında ,yəni bilik bazası identifikasiyası, mənşəli əsaslı autentifikasiya və biometrik əsaslı identifikasiya arasında biometrik eyniləşdirmə ən etibarlı metod kimi tanınır. Tədqiqatçılar yüksək dəqiqliyi təmin etmək üçün tədqiqatlarını yeni biometrik sistemlər üzərində cəmləşdirirlər. Ancaq bu texnologiyanın geniş yayılması üçün xərcləri daha əlverişli etmək lazımdır. Biometrik sistemlərin əhəmiyyəti fərdi xüsusiyyətlərin inkişaf etdirilməsidir. Xüsusi xüsusiyyətlər, köçürmələrin mümkün olmadığı təqdirdə yüksək təhlükəsizliyi təmin edir. Buna görə, bu xüsusiyyətlərlə biometrik sistemlər pasport nəzarətindən bank əməliyyatlarına qədər geniş tətbiq tapır və vacib bir tədqiqat mövzusu olaraq ortaya çıxır.

Biometrik sistemin əsas üstünlüyü insanların heç yerdə unutmağı və itirməməsini təmin edən bir əza ilə tanıya bilməsidir. Buna görə gələcək üçün planlaşdırılan təhlükəsizlik sistemlərinin əsas məqsədi insanların heç bir kart və ya açar daşımadan və ya şifrələri yadda saxlamadan asanlıqla tanınmasıdır. Barmaq damar tanıma cihazları mövcuddur və onların istifadəsi son illərdə artmışdır. Məsələn, xəstəxanalarda personalın davamiyyəti barmaq damarlarını oxuyanların sayəsində avtomatik olaraq müəyyən edilə bilər. Gizli qapılar, sistemlər və ya barmaq damar oxuyucularından asılı

olaraq açılan bir avtomatlaşdırma sisteminə giriş artıq James Bond filmlərində tapılır və istifadəsi gündən-günə artır.

Bu işdə, biometrik parametrlərlə informasiya təhlükəsizliyi və onlardan hazırda ən çox istifadə olunan barmaq damarları vasitəsi ilə avtomatlaşdırma sistemlərinin istifadəsi və necə tətbiq olunduğu araşdırılır.

Barmaq damarlarının biometrik sistemlərdə tətbiqi ilə təhlükəsizlik məqsədi ilə hazırlanan və ya inkişaf etdirilən avtomatlaşdırma sistemlərinin bəzən qeyri-kafi olacağı qənaətinə gəlinmişdir, buna görə birləşdirilmiş biometrik sistemlərin istifadəsi bir həll olacaqdır. Barmaq damar oxuyucusu və barmaq izi oxuyucusunu eyni cihazda birləşdirərək, eyni vaxtda ikiqat nəzarət edilə bilsə, təhlükəsizlik daha da artırılacaqdır.

Bu dissertasiya işinin nəticəsi olaraq biometrik təhlükəsizlik sistemləri üçün ikiqat nəzarəti həyata keçirəcək birləşmiş sistem araşdırması tövsiyə olunur. Bu kombinə edilmiş sistemin həm barmaq damarlarını, həm də barmaq izlərini eyni anda tanıyan bir modul bir xüsusiyyətə sahib olduğu təqdirdə sistemin təhlükəsizliyinin böyük dərəcədə artacağı qənaətidədir.

ƏDƏBİYYAT

1. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi məsələləri // İnformasiya cəmiyyəti problemləri, №1(7), 2013, s. 3-13
2. https://az.wikipedia.org/wiki/İnformasiya_təhlükəsizliyi#cite_note-1
3. <https://www.toppr.com/guides/accountancy/application-of-computers-in-accounting/meaning-and-elements-of-computer-system/>
4. <http://www.turkeyforum.com/satforum/archive/index.php/t-202.html> (21.05.2011)
5. <https://www.biometricupdate.com/201802/history-of-biometrics-2>
6. http://www.slidefinder.net/b/biyometri_bektas/13993600 (21.05.2011)
7. <http://alper-ozen.blogcu.com/bilgisayar-destekli-kimlik-tespit-sistemlerindebiyometrik-yonte/9553687> (14.05.2011)
8. <http://www.pitsteknoloji.com/biyometrik-sistemler.php> (21.05.2011)
9. <http://www.iscturkey.org/2010/2008/2006/pdf/poster/78.pdf> (25.05.2011)
10. www.iscturkey.org/2010/2008/2006/pdf/poster/78.pdf (21.05.2011)
11. Yıldız, F. ve Baykan, N. A., 2011. Çapraz İlişki Metoduyla İris Tanıma, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi, 10, 19-37.
12. http://k.domaindlx.com/kirbas/e_is/Veri_ve_Ag_Guvenligi.pdf (22.05.2011)
13. <http://www.epasaport.gov.tr/hakkinda/biyometrikfoto.aspx> (27.01.2013)
14. Dede, G. ve Sazlı, M. H., 2009. Biyometrik Sistemlerin Örüntü Tanıma Perspektifinden İncelenmesi ve Ses Tanıma Modülü Simülasyonu, EEIBM Ulusal Kongresi (Elektrik – Elektronik-Bilgisayar ve Biyomedikal Mühendisliği 13. Ulusal Kongresi ve Fuarı), ‘Teknolojide Buluşuyoruz’, ODTÜ, Ankara, 23-26 Aralık.

- 15.<http://www.ergosis.com.tr/avucici-damar-tanima-teknolojisi.html>
(20.10.2012)
- 16.<http://www.nanobiz.com.tr/images/products/mobiyosys%20broşuru.pdf>
(22.05.2011)
- 17.<http://www.appliedbiometrics.com/technology/finger-vein-recognition>
(18.05.2011)
- 18.www.internethaberoku.com/Biyokimlik-biyometrik-tanima-sistemi-wordh3251.html (22.05.2011)
- 19.<http://www4.comp.polyu.edu.hk/~csajaykr/fvdatabase.htm> (18.10.2011)
- 20.<https://www.perkotec.com/ciaat-ctc-940-cift-tarafli-plastik-kart-yazici-printer>
21. Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı.
22. J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer Verlag, 2005, 370 p.
23. Дж.Кирк, RFID-паспорт взломан, Computerworld Россия, 2007, № 9.
- 24.<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history>
- 25.<https://www.m2sys.com/blog/important-biometric-terms-to-know/false-rejection-rate-what-does-it-mean-and-why-should-i-care/>
- 26.<https://www.nist.gov/speech-testimony/standards-biometric-technologies#:~:text=The%20recommended%20standards%20include%20ANSI,and%20JTC%201%20SC%2037>
- 27.<https://www.iso.org/standard/33922.html>
- 28.<https://www.iso.org/standard/43303.html>
- 29.<https://www.iso.org/standard/41047.html>
- 30.<https://www.iso.org/standard/41048.html>

- 31.<https://www.iso.org/standard/38745.html>
- 32.<https://www.iso.org/standard/38746.html>
- 33.<https://www.iso.org/standard/38747.html>
- 34.<https://www.iso.org/standard/38748.html>
- 35.<https://www.iso.org/standard/38749.html>
- 36.<https://www.iso.org/standard/38750.html>
- 37.<https://www.iso.org/standard/43637.html>
- 38.<https://www.iso.org/standard/41447.html>
- 39.<https://www.iso.org/standard/41448.html>
- 40.<https://www.iso.org/standard/38819.html>
- 41.<https://www.iso.org/standard/43352.html>

SUMMARY

This dissertation consists of table of contents, an introduction, three chapters and proposal and reserch results. The content of the presentation from 80 pages, presented from 34 drawings and 4 tables.

The first chapter of the dissertation provides an overview of information security. The first paragraph describes the threats to information security and ways to combat them, the types of threats and ways to prevent them. The second paragraph deals with current issues of information security. These are legal and economic problems.

The second chapter of the dissertation consists of 5 paragraphs. these paragraphs are further subdivided into certain sub-paragraphs. The second chapter covers sections such as biometrics, biometric parameters, processing locations. In the first paragraph, what biometric systems are and what they do is inviolable as the history of biometric systems. The second paragraph is the value of biometrics and the superiority and health of biometric systems. The third paragraph deals with the types of biometric systems. These include fingerprint recognition, iris, retina recognition, DNA, voice recognition, facial thermogram, hand geometry and others. The fourth paragraph discusses the mechanism of operation of biometric devices and the areas in which they are used. The fifth paragraph deals with finger vein recognition technology, the most popular biometric tool.

The third chapter consists of 4 paragraphs. The first paragraph discusses the study of the national biometric identification system and the automatic fingerprint recognition system(AFIS). The automatic fingerprint recognition system in turn includes subsystems such as the integrated automatic fingerprint recognition system, IDENT and EURODAC. The second paragraph discusses the process of testing biometric technologies. They are divided into 2 parts, FAR and FRR. The third paragraph deals with the assessment of the security of biometric systems. The fourth paragraph deals with the standardization of biometric technologies.

РЕЗЮМЕ

Эта диссертация состоит из оглавления, введения, трех глав и предложений и результатов исследования. Содержание презентации из 80 страниц, представлено из 34 рисунков и 4 таблиц.

Первая глава диссертации дает обзор информационной безопасности. Первый абзац описывает угрозы информационной безопасности и способы борьбы с ними, типы угроз и способы их предотвращения. Второй абзац посвящен актуальным вопросам информационной безопасности. Это юридические и экономические проблемы.

Вторая глава диссертации состоит из 5 абзацев. эти пункты далее подразделяются на определенные подпункты. Вторая глава охватывает такие разделы, как биометрия, биометрические параметры, места обработки. В первом абзаце, что такое биометрические системы и что они делают, нерушимо как история биометрических систем. Второй параграф - ценность биометрии и превосходство и здоровье биометрических систем. Третий параграф касается типов биометрических систем. К ним относятся распознавание отпечатков пальцев, радужная оболочка глаза, распознавание сетчатки, ДНК, распознавание голоса, термограмма лица, геометрия кисти и другие. В четвертом абзаце обсуждается механизм работы биометрических устройств и области, в которых они используются. Пятый абзац посвящен технологии распознавания вен пальцев, наиболее популярному биометрическому инструменту.

Третья глава состоит из 4 абзацев. В первом абзаце обсуждается исследование национальной системы биометрической идентификации и системы автоматического распознавания отпечатков пальцев (AFIS). В свою очередь, система автоматического распознавания отпечатков пальцев включает подсистемы, такие как интегрированная система автоматического распознавания отпечатков пальцев, IDENT и EURODAC. Во втором абзаце обсуждается процесс тестирования биометрических технологий. Они разделены на 2 части, FAR и FRR. Третий параграф посвящен оценке безопасности биометрических систем. Четвертый абзац посвящен стандартизации биометрических технологий.