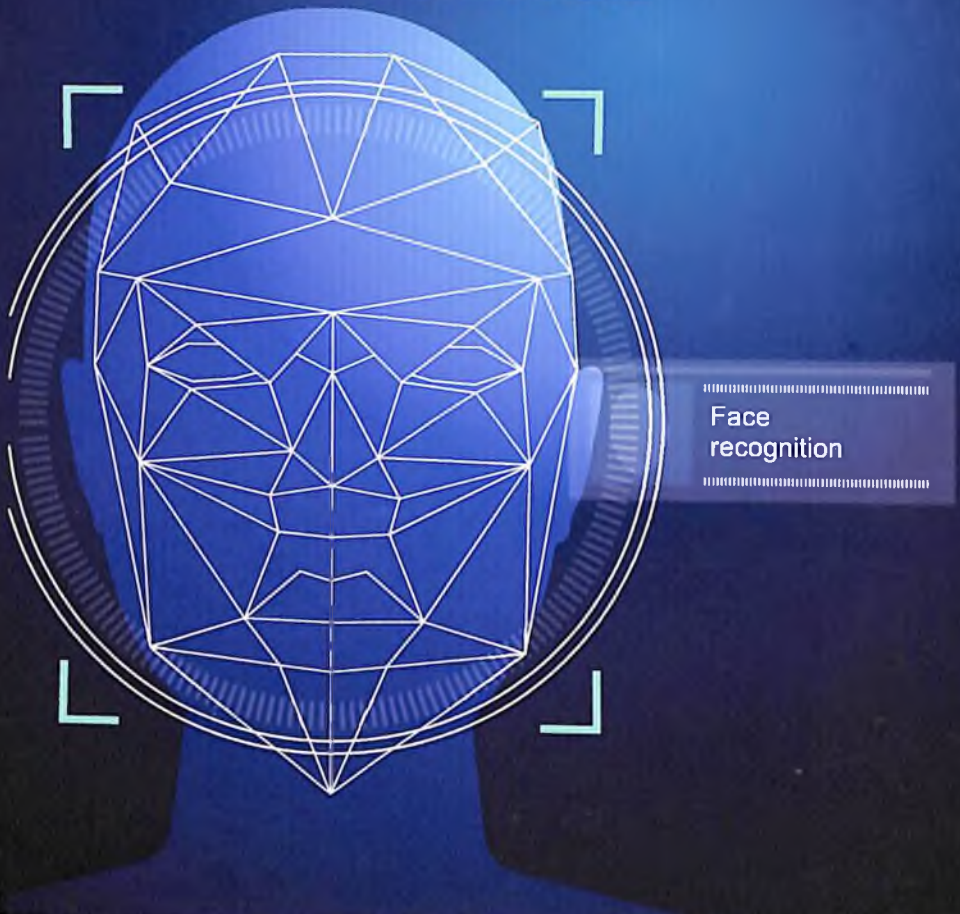
K.A.Tashev,
Z.T.Xudoyqulov, Sh.Z.Islomov

YUZ TASVIRI ASOSIDA SHAXSNI IDENTIFIKATSIYALASH VA AUTENTIFIKATSIYALASH JARAYONINING SAMARADORLIGINI OSHIRISH



O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

K.A.Tashev,
Z.T.Xudoyqulov, Sh.Z.Islomov

YUZ TASVIRI ASOSIDA SHAXSNI IDENTIFIKATSIYALASH VA AUTENTIFIKATSIYALASH JARAYONINING SAMARADORLIGINI OSHIRISH

(MONOGRAFIYA)

TOSHKENT – 2021

UDK. 004.93.612
KBK: 32.973.26
K.A.Tashev, Z.T.Xudoyqulov, Sh.Z.Islomov. Yuz tasviri asosida shaxsni identifikatsiyalash va autentifikatsiyalash jarayonining samaradorligini oshirish: Monografiya. –T.: «Nihol print», 2021 yil, 124 bet.

ISBN 978–9943–7028–2–0

Monografiyada axborot kommunikatsiya tizimlarida axborotni himoyalashdagi muammolar, axborot xavfsizligini ta'minlashda biometrik parametrlarning ahamiyati, biometrik parametrlarga asoslangan autentifikatsiya usullari, yuz tasviriga asoslangan tanib olishning klassik va sun'iy intellektga asoslangan usullari, ulardan amalda foydalanish holati, yuz tasviriga asoslangan tanib olish usullarining asosiy muolajalari hamda yuz tasviri bo'yicha tanib olishning klassik usullarini samaradorligini oshirishning nazariy va amaliy asoslari muhokama qilingan. Bundan tashqari, to'siq mavjud yuz tasvirini normallashtirish usuli, yuz tasvirini tanib olishning modifikatsiyalangan teran o'rganish tarmog'i, teran o'rganishga asoslangan yuz tasviri bo'yicha identifikatsiyalash jarayonining sxemasi va yuz tasviri bo'yicha identifikatsiya jarayonining dasturiy vositasi ishlab chiqilgan hamda turli holatlardagi yuz tasvirlari bazalari yaratilgan.

Ushbu monografiya axborot xavfsizligi va obyektlarni tanib olish, xususan, yuz tasviriga asoslangan identifikatsiya va autentifikatsiyalash sohasida ilmiy izlanish olib borayotgan mutaxassislar uchun tavsiya etiladi hamda mazkur sohada oliy ta'lim muassasalari talabalari va magistrlarining keng doirasi ham foydalanishi mumkin.

UDK. 004.93.612
KBK: 32.973.26

Taqrizchilar:

B.B.Mo'minov – Muhammad al-Xorazmiy nomidagi TATU "Informatika asoslari" kafedrasi mudiri, t.f.d.;

O.P.Axmedova – UNICON.UZ" DUK – Fan-texnika va marketing tadqiqotlari markazi Axborot xavfsizligi va kriptologiya ilmiy tadqiqot bo'limi boshlig'i, t.f.n.

ISBN 978–9943–7028–2–0

KIRISH

Hozirgi kunda hisoblash mashinalari yordamida tasvirlarni tahlil qilish, ularga ishlov berish, biometrik parametr asosida tanib olish, xususan, yuz tasviri bo'yicha identifikatsiya va autentifikatsiya jarayoni aniqligini oshirish va xatoliklarni kamaytirishga qaratilgan ilmiy tadqiqot natijalari amalda keng joriy qilinmoqda. Jumladan, «Defense One kompaniyasi ma'lumotiga ko'ra, 2018 yilda AQShning bojxona va chegara nazoratida yuz tasvirini tanib olish texnologiyasidan 3 oy davomida foydalanish natijasida mamlakatga ruxsatsiz kirishga urinishlarning 26 ta holatda oldi olingan»[1]. Bu esa yuz tasviri yordamida shaxslarni tanib olishning yangi usul va algoritmlarini ishlab chiqish hamda mavjudlarini takomillashtirish muhim ahamiyat kasb etishini ko'rsatmoqda. Ko'pgina xorijiy mamlakatlarda, jumladan, AQSh, Rossiya Federatsiyasi, Yaponiya, Janubiy Koreya, Xitoy va boshqa davlatlarda shaxsni yuz tasviri asosida identifikatsiyalash va autentifikatsiyalash jarayonini avtomatlashtirishga alohida e'tibor berilmoqda.

Shu sababli, shaxslarni avtomatlashtirilgan identifikatsiyalashning model va algoritmlarini takomillashtirishga hamda kompyuterning o'rganishi texnologiyasi asosida yuz tasviri yordamida shaxslarni tanib olishni aniqligini oshirishga qaratilgan izlanishlar olib borilmoqda. Bu borada, yuz tasviriga asoslangan identifikatsiya va autentifikatsiya jarayonlarida mavjud xavfsizlik muammolarini bartaraf etuvchi, yuz tasvirini aniqlash va tanib olish jarayonidagi xatoliklarni kamaytirishga imkon beruvchi, tezkor usul va algoritmlarni ishlab chiqish zarur hisoblanadi.

Respublikamizda jamoat tartibini nazoratlash maqsadida amalga oshirilayotgan «xavfsiz shahar»[2] konsepsiyasi doirasida jamoat joylarida, tashkilotning kirish joylarida yuz tasviri yordamida shaxslarni tanib olish usul va algoritmlarini ishlab chiqish hamda identifikatsiyalashning avtomatlashtirilgan tizimlarini takomillashtirish muhim vazifalardan biri hisoblanadi.

---

[1] https://www.defenseone.com/technology/2018/11/cbps-facial-biometrics-program-has-caught-26-alleged-imposters/152993/

[2] «Xavfsiz shahar» loyihasini amalga oshirish bo'yicha bosqichma-bosqich chora-tadbirlar va yagona texnologik yondashuvni tashkil qilish to'g'risida O'zbekiston Respublikasi vazirlar mahkamasining qarori, 343-son, 2018y. Toshkent sh.

Monografiyaning birinchi bobida axborot kommunikatsiya tizimlarida xavfsizlikni ta'minlashdagi ochiq muammolar va ularni bartaraf etishning turli usullari, xususan, biometrik parametrlarga asoslangan yondashuv hamda autentifikatsiya masalasini yechishda turli biometrik parametrlardan foydalanishning afzalliklari va kamchiliklari ko'rib chiqilgan.

Ikkinchi bob yuz tasviri bo'yicha tanib olishdan amalda foydalanish, yuz tasvirini aniqlash va tanib olishni amalga oshirish muolajalari, ulardagi ochiq muammolar va ularni bartaraf etish masalalariga bag'ishlangan.

Uchinchi bobda yuz tasviri bo'yicha tanib olishning klassik usullari va ularni samaradorligini oshirish usullari, neyron tarmoqqa asoslangan yuz tasvirini tanib olish usullari ko'rib chiqilgan.

Monografiyaning to'rtinchi bobi neyron tarmoqlarga asoslangan yuz tasviri bo'yicha identifikatsiyalash tizimini ishlab chiqishga bag'ishlangan bo'lib, to'siq mavjud bo'lganda yuz tasvirini normallashtirish usuli, yuz tasvirini tanib olishning modifikatsiyalangan teran o'rganish tarmog'i va turli sharoitlardagi yuz tasviri bazalarini shakllantirish tartibi keltirilgan.

I BOB. AXBOROTNI HIMOYALASHDA BIOMETRIK PARAMETRLARDAN FOYDALANISHDAGI MUAMMOLAR

1.1. Axborot kommunikatsiya tizimlarida xavfsizlikni ta'minlashdagi muammolar va yechimlar

Axborot - kommunikatsiya texnologiyalarining rivojlanishi va Internet tarmog'idan foydalanish hajmining ortishi natijasida tashkilotlar turli tahdidlarga uchramoqda. Buning natijasida tashkilot uchun qimmatli bo'lgan axborot o'g'irlanishi va zarar yetishi holatlari kuzatilmoqda. Bu tahdidlar turli manbaalar, masalan, tashkilot hodimi yoki xakerlar tomonidan amalga oshirilmoqda. Hodim tomonidan qoldirilgan kichik bir zaiflik natijasida tashkilotga katta miqdordagi zarar yetkazilishi mumkin. CSI/FBI tomonidan chop etilgan "11th Annual Computer Crime and Security Survey" ma'lumotiga ko'ra 74,3% xavfsizlik yo'qotilishi viruslar, ruxsatsiz foydalanish, laptop yoki mobil qurilmani o'g'irlanishi yoki axborotni o'g'irlanishi natijasida sodir bo'lsa, bu tahdidlarning 70% tashkilot ichidan amalga oshirilar ekan [79].

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa yoki axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug'diruvchi sharoit va omillar majmui hisoblanadi. Mavjud tahdid turlari va ular natijasida amalga oshirilishi mumkin bo'lgan hujumlar 1.1-jadvalda o'z aksini topgan [96].

1.1-jadval

Tahdid turlari va ularning natijasi bo'lishi mumkin bo'lgan hujumlar

Tahdid turlari	Tahdid natijasida bo'lishi mumkin bo'lgan hujumlar
1	2
Ruxsat etilmagan oshkor bo'lish Konfidensiallikka qaratilgan	*Namoyon bo'lish* - ruxsat etilmagan tomonlar uchun maxfiy axborotni oshkor bo'lishi. *Tutib qolish* – foydalanuvchilarga tegishli maxfiy axborotni bevosita ruxsatsiz boshqarilishi. *Ishtirok etish* - ruxsatsiz bilvosita (kommunikatsiya vositalari orqali) maxfiy axborotni boshqarish. *Suqilib kirish* - ruxsatsiz tizimdagi kamchilikdan foydalanib maxfiy axborotni boshqarish.

1	2
Tortib olish Tizim yaxlitligiga qaratilgan	*Noqonuniy o'zlashtirish* - xizmatni o'g'irlanishi (DoS hujumlarini amalga oshirish uchun). *Noqonuniy fodalanish* - hujumchining zararli vositalar yordamida tizimdan foydalanishi.
Firibgarlik Tizim yoki ma'lumot yaxlitligiga qaratilgan	*Niqoblash* - tahdidchi qonuniy foydalanuvchi kabi tizimdan foydalanadi yoki zararli harakatlarni amalga oshiradi. *Qalbakilashtirish* - foydalanuvchi yolg'on ma'lumotga ishontiriladi. *Rad etish* - harakat uchun javobgarlikni yolg'ondan rad etish orqali boshqa tomonni aldash.
Buzish Tizim yaxlitligi yoki foydalanuvchanligiga qaratilgan	*Ishlash qobilyatini yo'qotish* - fizik buzish yoki tizim qurilmasini buzish orqali tizim foydalanuvchanligiga ta'sir etish. *Buzilish* - tizim yaxlitligini buzishga qaratilgan hujumlar. *To'sqinlik* - kommunikatsiya tizimiga aralashish orqali foydalanuvchanlikni yo'qotish.

Tashkilotda qimmatli axborotni (konfidensiallikni, yaxlitlikni va foydalanuvchanlikni) yo'qotilishi quyidagi darajalarda bo'lishi mumkin [1]:

- *Past.* Bunda tashkilotga buzg'unchining cheklangan ta'siri amalga oshiriladi va buning natijasida tashkilot o'zining asosiy vazifasini bajarish qobiliyatida qoladi, moliyaviy zarar miqdori kichik bo'ladi.

- *O'rta.* Bunda tashkilotga jiddiy ta'sirga ega buzg'unchilik harakati amalga oshirilib, tashkilot vazifalarini bajarishda samaradorlik keskin kamayadi, katta hajmdagi moddiy zararga sabab bo'ladi.

- *Yuqori.* Yetkazilgan zarar miqdori eng yuqori bo'lib, buning natijasida tashkilotning asosiy vazifasini bajarishi to'xtaydi va katta hajmdagi moliyaviy yo'qotishga sabab bo'ladi.

Kompyuter tizimlarini turli qurilmalar, dasturiy vositalar, ma'lumotlar va aloqa liniyalari/tarmoqlardan iboratligini hisobga olib, ularga qaratilgan tahdidlarni quyidagicha tasvirlash mumkin (1.2 - jadval). Ushbu tahdidlarga qarshi tashkilotlarda turli darajadagi xavfsizlik choralari ishlab chiqilgan. Quyidagi 1.1 - rasmda 2016 - yilda turli sohalarda xavfsizlikni amalga oshirilganlik darajasi keltirilgan [7].

Tizimdagi zaifliklar va resurslarga qaratilgan tahdidlarni oldini olishda foydalaniluvchi qarshi choralarni tasniflashning turli yo'llari

mavjud. Xususan, FIPS 200 standartida axborot tizimlarida uzatilayotgan, saqlanayotgan va ishlanayotgan axborotning konfidensiyalligini, yaxlitligini va foydalanuvchanligini himoyalashning 17 ta turli talablari keltirilgan [8]:

- *Foydalanishni nazoratlash.* Axborot tizimini boshqarishda autentifikatsiyadan o'tgan foydalanuvchilar uchun cheklangan imkoniyatlarni yaratish.
- *Ogohlik va ta'lim.* Tashkilotning har bir hodimi va foydalanuvchisi o'z harakatlariga aloqador xavfsizlik risklarini, tashkilotda qabul qilingan qonunlarni va siyosatlarni bilishi yoki u bo'yicha o'qitilishi shart.
- *Audit va javobgarlik.* Qonuniy va noqonuniy tarzda axborot tizimida amalga oshirilgan harakatlarni qaydlash, tahlil qilish va monitoringlash uchun auditlash tizimlarini yaratish va himoyalash zarur.
- *Sertifikatsiya, akkreditatsiya va xavfsizlikni baholash.* Tashkilot axborot tizimida xavfsizlik nazoratlarini doimiy ravishda baholab borish.
- *Konfiguratsiyani boshqarish.* Asos sozlanishlarni va xavfsizlik sozlanishlarini o'rnatish va madadlash.
- *Kutilmagan rejalashtirish.* Kutilmaganda bo'lishi mumkin bo'lgan holatlarda zaxira nusxalash rejasini amalga oshirish va madadlash.
- *Identifikatsiya va autentifikatsiya.* Axborot tizimidagi foydalanuvchilarni, jarayonlarni va foydalanuvchi nomidan ish qiluvchi jarayonlarni identifikatsiyalash va foydalanishga ruxsat berishdan oldin ularni autentifikatsiyalash.
- *Insidentga javob.* Tashkilot axborot tizimlari uchun insidentlarni bartaraf etish imkoniyatlarini o'rnatish va amalga oshirish.
- *Madadlash.* Tashkilot axborot tizimini vaqti - vaqti bilan yoki davriy madadlash.
- *Axborotni saqlash vositalarini himoyalash.* Har ikki holdagi, qog'ozdagi va elektron axborotni saqlash vositalarini himoyalash, ulardan foydalanishni cheklash, turli buzilishlardan himoyalash.
- *Fizik va muhitga bog'liq himoya.* Avtorizatsiyalangan foydalanuvchilarga axborot tizim vositalaridan fizik foydalanishni cheklash.
- *Rejalashtirish.* Tashkilot axborot tizimi uchun xavfsizlik rejalarini amalga oshirish, davriy yangilab borish, hujjatlashtirish va shakllantirish.

- *Hodimlar xavfsizligi.* Tashkilot ichida hodimlarni javobgarlik holatiga mos harakatlarni amalga oshirishlarini kafolatlash.

- *Risklarni baholash.* Uzluksiz ravishda tashkilot harakatlariga bo'lgan xavf - xatarlarni baholash.

- *Tizim va xizmatlarga egalik qilish.* Tashkilot axborot tizimini yetarlicha himoyalashda kerakli resurslarni joylashtirish va ular ustidan nazoratni amalga oshirish.

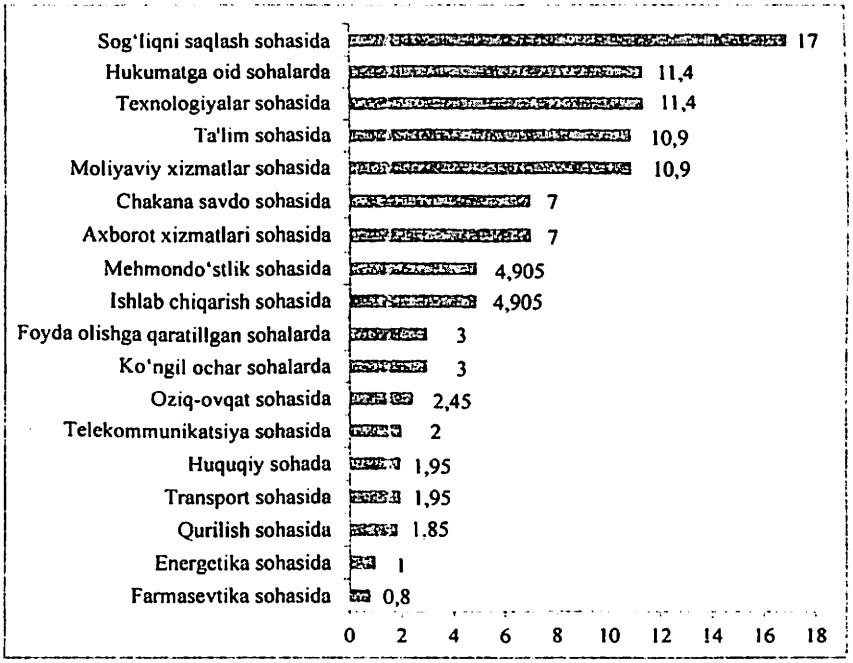
- *Tizim va kommunikatsiyani himoyalash.* Tashkilot tizimining muhim ichki va tashqi chegaralarida kommunikatsiya tizimini himoyalash, monitoringlash va nazoratlash.

- *Tizim va axborot yaxlitligi.* Tizimni va axborotni zararli kodlardan himoyalash, axborotni to'g'riligini ta'minlash.

1.2-jadval

Axborot vositalari va unga qaratilgan tahdidlar

Axborot xususiyati / Vosita	Foydalanuvchanlik	Konfidensiallik	Yaxlitlik
Qurilma	Qurilma yo'qolishi yoki xizmat ko'rsatishdan voz kechish	Shifrlanmagan CD yoki DVD yo'qolishi	-
Dasturiy vosita	Dasturiy vositani o'chirilishi mumkin yoki foydalanuvchiga xizmat ko'rsatishdan voz kechish	Ruxsat etilmagan holda dasturdan nusxa olish	Dasturiy vositani modifikatsiyalash
Ma'lumot	Fayllar o'chirilishi yoki foydalanuvchi uchun yopiq bo'lishi	Ma'lumotni ruxsatsiz o'qish	Fayllarni modifikatsiyalash yoki yangisini yaratish
Aloqa liniyasi/ tarmoq	Xabar o'chirilishi	Xabarni o'qish yoki tarmoq trafigi tinglash	Xabarlarni o'zgartirish, nusxalash yoki yolg'on xabar yaratish

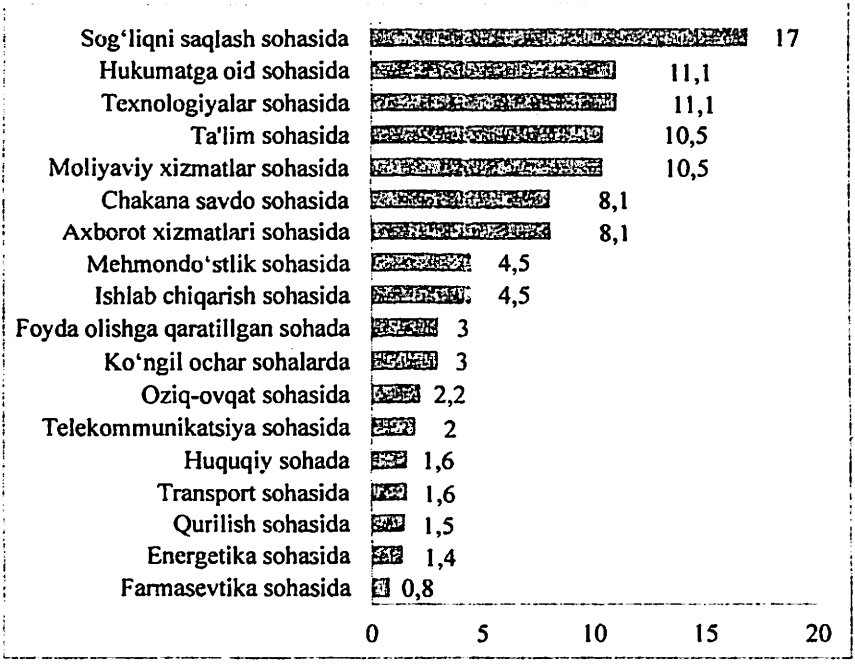


1.1- rasm. Sohalarda xavfsizlikni amalga oshirilganlik darajasi

Yuqoridagi talablar tashkilotni o'z vazifalarini to'liq bajarishida xavfsizlik nuqtai nazaridan amalga oshirilishi kerak bo'lgan me'yorlar bo'lib, bu me'yorlarni bajarishda quyidagi himoya texnologiyalaridan keng foydalaniladi [2]:

- ma'lumotni himoyalash texnologiyalari:
  - axborotning kriptografik himoyalash vositalari;
  - autentifikatsiya texnologiyasi;
- tarmoqlararo axborot almashinuvida axborot xavfsizligini ta'minlash texnologiyalari:
  - tarmoqlararo ekran texnologiyasi;
  - virtual xususiy tarmoq texnologiyasi;
- hujumlarni oldini olish texnologiyalari:
  - hujumlarni aniqlash va ulardan himoyalash texnologiyalari;
  - zararli dasturiy vositalardan himoyalash texnologiyalari.

Bundan tashqari, bu sohalarda 2015 yil aprel va 2016 yil iyun oylari oralig'ida ma'lumotlarni chiqib ketish darajasi ham xavfsizlikni ta'minlanganlik darajasiga va sohaning muhimlik darajasiga bog'liq bo'lgan [7] (1.2 - rasm).



1.2 - rasm. Sohalarda ma'lumotlarni chiqib ketish darajasi

Ma'lumotni yaxlitligini, konfidensialligini va foydalanuvchanligini ta'minlashda kriptografik va ruxsatlarni nazoratlash mexanizmlari muhim ahamiyatga ega. Bu fikrning tasdig'i sifatida barcha tashkilotlarda va ixtiyoriy tizimlarda dastlabki himoya usuli sifatida foydalanilayotgan autentifikatsiya texnologiyasidan yoki turli kriptografik himoya usullaridan foydalanilishini keltirish mumkin.

1.2. Axborot xavfsizligini ta'minlashda biometrik parametrlardan foydalanishning ahamiyati

Hozirda biometrik parametrlardan axborot xavfsizligini ta'minlashda, xususan, autentifikatsiyalashda va kriptografik tizimlarda kalit sifatida keng foydalanilmoqda. Ushbu bo'limda dastlab

autentifikatsiya usullari tahlil qilinib, so'ngra biometrik parametrlardan kalit sifatida foydalanish yondashuviga to'xtalib o'tiladi.

Autentifikatsiya usullarining tahlili. Autentifikatsiya biror kishini yoki biror narsani haqiqatda o'zi ekanligini tekshirish jarayoni bo'lib, odatda ular biror narsani bilishga, biror narsaga egalik qilishga va biror biometrik parametrga asoslangan bo'lishi mumkin [17]. Ba'zi adabiyotlarda autentifikatsiyaning foydalanuvchining joylashgan o'rniga asoslangan usuli ham keltirilgan [9].

Biror narsani bilishga asoslangan autentifikatsiya usuli. Foydalanuvchi bilgan biror narsa asosida autentifikatsiya usuli odatda PIN kod, parol yoki parollar guruhiga aloqador bo'ladi. Parolga asoslangan autentifikatsiya usuli foydalanishga qulay, kompyuter xavfsizligi tizimlarida va mobil qurilmalarida eng keng tarqalgan usul bo'lib, amalga oshirishga qulay, kam xarajatli va oson yangilash imkoniyatiga ega.

Parolga asoslangan autentifikatsiya usuli yuqori himoyani ta'minlamaydi. Bu autentifikatsiya usuli "qo'pol kuch", lug'atga asoslangan, "yelka orqali qarash" va turli parolni o'g'irlash hujumlariga bardoshsiz [8]. Bundan tashqari, parollarga asoslangan autentifikatsiya usulidagi xavfsizlik muammolari inson omiliga bog'liq bo'lib, ular foydalanuvchilarni murakkab parol tanlay olmasliklari yoki uni esdan chiqarishi bilan xarakterlanadi [3]. 1.3 - jadvalda 2016 yilda eng keng tarqalgan parollar va ularni "Randomize" [97] hamda "BetterBuys" [98] vositalari orqali hisoblash vaqtlari keltirilgan [99].

1.3 - jadval

2016 - yildagi eng ommabob parollar va ularni topishda sarflangan vaqt

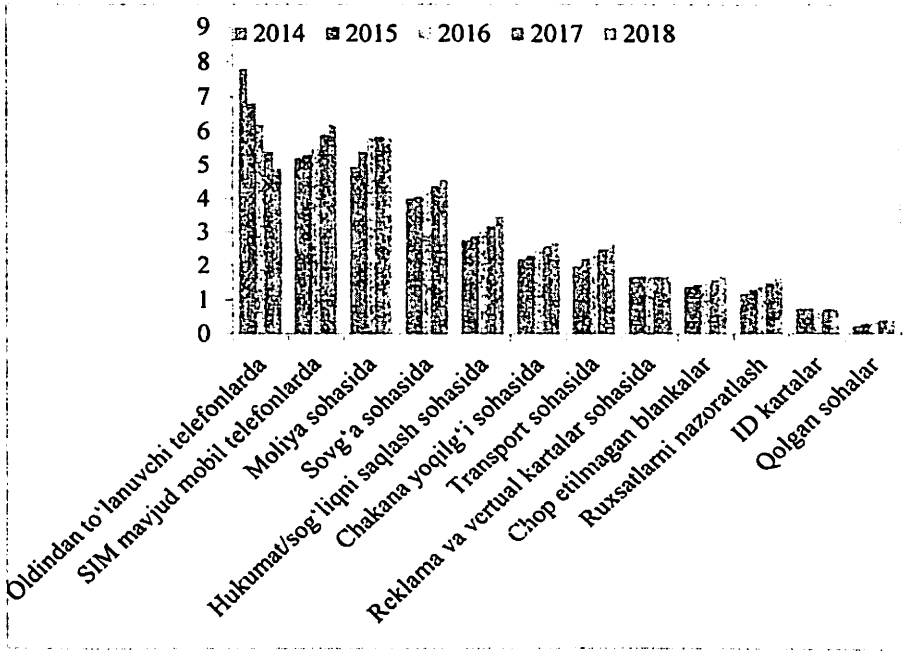
№	2016 yilda eng keng foydalanilgan parollar	"Randomize" vositasidan foydalanib aniqlash vaqti	"BetterBuys" vositasidan foydalanib aniqlash vaqti
1	2	3	4
1.	123456	< 1 sek	0,25 ms
2.	123456789	< 1 sek	0,25 ms
3.	qwerty	< 1 sek	0,25 ms
4.	12345678	< 1 sek	0,25 ms
5.	111111	< 1 sek	0,25 ms
6.	1234567890	3 sek	0,25 ms
7.	1234567	< 1 sek	0,25 ms
8.	Password	1 min. 3 sek	0,25 ms

1	2	3	4
9.	123123	< 1 sek	0,25 ms
10.	987654321	< 1 sek	0,25 ms
11.	qwertyuiop	13 soat 48 min	4 oy 4 kun ...
12.	mynoob	< 1 sek	24 sek
13.	123321	< 1 sek	0,25 ms
14.	666666	< 1 sek	0,25 ms
15.	18atcskd2w	14 kun, 21 soat	8 yil 9 oy ...
16.	7777777	< 1 sek	0,25 ms
17.	1q2w3e4r	16 min 33 sek	0,25 ms
18.	654321	< 1 sek	0,25 ms
19.	555555	< 1 sek	2 min 46 sek
20.	3rjs1la7qe	14 kun 21 soat	8 yil 9 oy ...

Biror narsaga egalik qilishga asoslangan autentifikatsiya usuli. Biror narsaga, masalan, fizik obyektlarga, asoslangan autentifikatsiya usuli foydalanuvchi yonida mavjudlik va unga egalik qilish xususiyatlariga asoslanadi. Bu usulda biror maxfiy axborotni esda saqlash talab etilmaydi (masalan, parollar kabi). Obyekt sifatida mobil qurilmalar yoki tokenlardan foydalanish mumkin. Ushbu autentifikatsiya usuli qurilmaga asoslangani bois, amalga oshirishda va yangilashda yuqori xarajatni talab etadi. Shuning uchun, hozirda obyekt sifatida token qurilmalarining o'rniga mobil telefonlardan foydalanish hajmi ortib bormoqda. Bu mobil qurilmalarning keng tarqalgani va foydalanuvchilarning doimiy "hamrohi" ekanligi bilan xarakterlanadi.

Biror narsaga asoslangan autentifikatsiya usulida tokenni yo'qotib qo'yish xavfi inobatga olinmasa, yuqori darajadagi xavfsizlikni ta'minlaydi. Tokenlar turli hajmda va ko'rinishda bo'lib, olib yurishga qulay. Tokenga qo'yilgan vazifalarga ko'ra ularda turli axborot saqlanadi. Odatda xavfsizlik tokenlari 4 ta turga ajratiladi: statik parol tokenlari, sinxron ishlovchi dinamik parol tokenlari, asinxron ishlovchi parol tokenlari va "savol – javob" tokenlari [100]. Birinchi turdagi tokenlar takrorlash hujumlariga bardoshsiz bo'lib, unda parollar fizik shaklda yashiringan bo'ladi. Ikkinchi turdagi tokenlar vaqtga asoslangani uchun, doim mijoz va server orasida vaqtni sinxronlashni talab etadi. Uchinchi turdagi tokenlarda vaqt parametri mavjud bo'lmaydi va bir martali parol generatorlaridan foydalanilishi mumkin bo'ladi. To'rtinchi turdagi tokenlar turli kriptografik tizimlarga asoslangan bo'lib, biror "savol"ga maxfiy kalit bilan "javob" berishga asoslanadi.

Ushbu autentifikatsiya usulida tokenni yo‘qotish xavfi mavjudligi sababli, unga odatda qo‘shimcha autentifikatsiya faktori qo‘shiladi. Ya’ni, tokenni boshqarish yoki undan foydalanish, masalan, parolga asoslangan autentifikatsiya orqali amalga oshirilishi mumkin.



1.3 - rasm. 2014 - 2018 yillarda global miqiyosida smart kartalarni ishlab chiqarish ko‘rsatkichlari

1.3 - rasmda 2014 - 2018 yillarda global miqiyosida smart kartalar ishlab chiqarishning sohalar bo‘yicha ko‘rsatkichlari keltirilgan bo‘lib, keyingi yillarda foydalanishlarni nazoratlash segmentida smart kartalarni ishlab chiqarish darajasi ortganini ko‘rish mumkin [18].

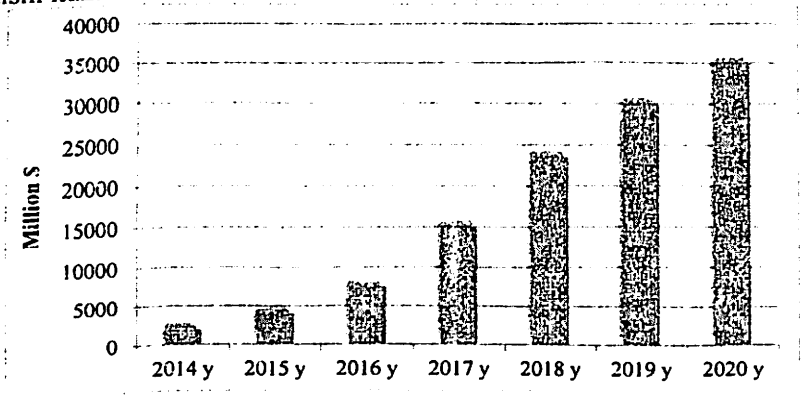
Biror biometrik parametr asosida autentifikatsiya usuli. Uchinchi turdagi autentifikatsiya usuli insonning noyob bo‘lgan biror xususiyati yoki harakatiga asoslanadi. Bu turdagi autentifikatsiya usuli ananaviy autentifikatsiya usullarini aldash mumkin bo‘lgan holda foydalaniladi [9]. Bu usulda xususiyat yoki harakat sifatida:

- barmoq izlarini;
- ko‘z qorachig‘i;
- yuz shakli;

- qo'l shakli;
- ovoz, qo'l yozma shakllari;
- va DNAlarni olish mumkin.

Bu turdagi autentifikatsiya usullari asosan obyektlardan foydalanishni nazoratlashda, biometrik pasport tizimlarida, mobil qurilmalardan ruxsatsiz foydalanishni cheklashda va boshqa sohalarda keng qo'llanilmoqda. Biometrik autentifikatsiya usullarida biometrik parametrlarni shikastlash orqali (masalan, barmoqni kesib olish) skanerlarni aldash yoki biometrik parametrlarni qalbakilashtirish orqali xavfsizlik muammolari kelib chiqishi mumkin.

Biometrik parametrlarga asoslangan autentifikatsiya usuli foydalanishga qulay bo'lib, unda esdan chiqarish yoki har doim birga olib yurish kabi muammolar mavjud emasligi sababli, hozirda keng foydalanilmoqda. Xususan, mobil qurilmalarda biometrik xususiyatlardan foydalanish orqali olinadigan daromadning yillar kesimida o'sishi 1.4 - rasmda keltirilgan [10]. Ushbu statistik ma'lumotlarga tayanib biometrik parametrlarga asoslangan autentifikatsiya usullari mavjud vositalar miqdori keyingi yillarda ham ortishi kuzatish mumkin.



1.4 - rasm. Mobil qurilmalarda biometrik texnologiyalardan olinadigan daromadning yillar kesimida o'zgarishi

Autentifkatsiya usullarini taqqoslash omillari. Odatda autentifikatsiya usullarini taqqoslashda ma'lum omillardan foydalaniladi. Ushbu omillar ichida muhimlari quyidagilar [21]:

Kalit sohasi va entropiya. Kalit sohasi autentifikatsiyalashda foydalanilayotgan parametrlarning umumiy miqdorini ifodalaydi

(masalan, agar parol 8 ta belgi uzunligiga teng bo'lsa va unda 256 ta turli belgilardan foydalanilsa, kalit sohasi 256^8 ga teng bo'ladi). Entropiya foydalanilgan autentifikatsiya usulida biometrik parametrning tahdidchiga no'malumlik darajasini ko'rsatadi (masalan, parolning entropiyasi kriptografik kalitnikiga qaraganda ancha past).

- *Host tomonning himoyasi.* Autentifikatsiya usulida foydalanilgan parametrlar hostda qanday shaklda saqlanishi va himoyalanishini aniqlaydi.

- *Qulaylik va narx.* Foydalanilayotgan autentifikatsiya tizimlarini amalga oshirishdagi xarajatlarni va ularni foydalanuvchilar tomonidan qabul qilinish darajasini ifodalaydi.

- *Xavfsizlik muammolari.* Bu xususiyat autentifikatsiya usullarida qanday xavfsizlik muammolari, tahdidlar mavjudligi orqali aniqlanadi. Autentifikatsiya usullariga qaratilgan hujumlarga, kalitlarni to'liq tanlash, parollardan foydalanish, nusxalash, o'g'irlash, takrorlash, zararli dasturlar asosida amalga oshiriladigan, DoS va rad etish hujumlarini misol keltirish mumkin.

Yuqorida tahlil etilgan omillarga asoslangan holda mavjud autentifikatsiya usullarining qiyosiy tahlili 1.4 - jadvalda keltirilgan. Jadvalda keltirilgan natijalardan shuni aytish mumkinki, biometrik parametrlarga asoslangan autentifikatsiya usullari qolgan usullarda mavjud muammolarni o'zida bartaraf etgan. Biroq, biometrik parametrlardan olinadigan axborot noravshan ko'rinishda bo'lishi, xususiyatlarning qalbakilashtirish imkoniyati va tizimni amalga oshirishdagi yuzaga keladigan to'siqlar sababli ba'zi xavfsizlik muammolari vujudga kelishi mumkin. Shunday bo'lsada, hozirda biometrik autentifikatsiya usullari muhim obyektlarni himoyalashda, kompyuter tizimlaridan ruxsat etilmagan foydalanishlarni oldini olishda keng foydalanilmoqda [101].

Biometrik parametrlardan kriptografik kalit sifatida foydalanish. Biometrik parametrlarda esdan chiqarish yoki uni doim birga olib yurish muammolari bo'lmaganligi sababli, biometrik autentifikatsiya usullari keng foydalanilmoqda. Biometrik parametrlarga asoslangan autentifikatsiya usullarida biometrik xususiyatlar ma'lum bir (shablonlar deb ataluvchi) ko'rinishlarga o'tkazilib, so'ngra ma'lumotlar ba'zasida saqlanadi. Biometrik shablonlarni saqlashda quyidagi usullardan keng foydalaniladi [22]: qisqaruvchi biometriklar (cancelable biometrics) va biometrik kriptotizimlar (biometric cryptosystems). Birinchi holda biometrik xususiyatlar biror o'zgartirish orqali boshqa domenga

o'tkaziladi va tekshiriladi. Qisqaruvchi biometriklar bir tomonlamalik va takrorlanmaslik xususiyatlari bilan ajralib turadi. Biometrik kriptotizimlar esa biometrik parametrni biror kriptografik kalit bilan bog'lash yoki biometrik parametrdan kriptografik kalitni hosil qilishga asoslanadi va autentifikatsiyalashda aynan bog'langan kriptografik kalitni yoki qayta generatsiyalangan kalitlarni solishtirish orqali amalga oshiriladi.

1.4 - jadval

Autentifikatsiya usullarining qiyosiy tahlili

Autentifikatsiya usuli / Taqqoslash omili	**Biror narsani bilishga asoslangan**	**Biror narsaga egalik qilishga asoslangan**	**Biometrik xususiyatga asoslangan**
Kalit sohasi va entropiya	Past	Yuqori	Biometrik parametrga bog'liq
Host tomonning himoyasi	Xeshlangan ko'rinishda	Qurilma xotirasida himoyalangan ko'rinishda	Bir tomonlama funksiyalar, biometrik - kriptografik tizimlar
Qulaylik darajasi	Yuqori	O'rta	O'rta
Narx	Past	Yuqori	Yuqori
Xavfsizlik muammolari	Kalitlarni to'liq tanlash, lug'atga asoslangan, elka orqali qarash, keylogger dasturlar, esdan chiqarilishi va h.	Kalitlarni to'liq tanlash, o'g'irlash	Yolg'ondan rad etish xatoligi, yolg'ondan tasdiqlash xatoligi, qalbakilashtirish, nusxalash, tizimni aldash.

Biometrik shablonlarni himoyalashda biometrik kriptotizimlardan foydalanish imkoniyati, biometrik xususiyatlardan kriptografik kalit sifatida foydalanish mumkinligini bildiradi. Biometrik parametrlardan kalit sifatida foydalanish qator imkoniyatlarni yaratadi: kriptografik kalitni esda saqlash yoki biror vosita asosida xavfsiz olib yurishni talab etmaydi, kalitni tahdidchi tomonidan qo'lga kiritish imkoniyati mavjud emas hamda shaxsiy axborotni saqlashga qulay hisoblanadi. Hozirgi

kunda biometrik kriptografik tizimlarga *priv-ID* [102], *Genkey AS* [103], *Precise Biometrics AB* [104] tizimlarini misol tariqasida keltirish mumkin.

1.3. Mavjud biometrik autentifikatsiya usullarining qiyosiy tahlili

Biometrik tizimlardan odatda identifikatsiya va tekshirish (autentifikatsiya) tizimlari ko'rinishida foydalaniladi [80]:

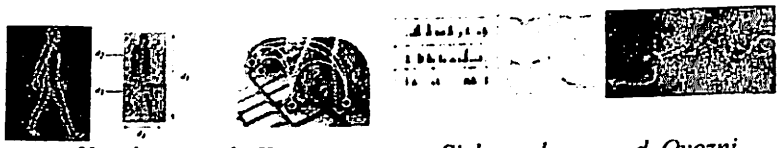
Identifikatsiya tizimlari: birga - ko'p tekshirishni amalga oshirib, biror biometrik parametrni bazadan qidirish va uning shaxsini aniqlash uchun foydalaniladi (masalan, IAFIS FBI [105]).

Tekshirish tizimlari: birga - bir tekshirishni amalga oshirib, ba'zadagi bir parametrni da'vogar parametr bilan solishtiradi va olingan natijaga binoan jarayon muvafaqqiyatli yoki muvafaqqiyatsiz yakunlanishi mumkin.

Biometrik parametrlarga asoslangan autentifikatsiya usulining samaradorligi va xavfsizligi unda foydalanilgan biometrik parametr turiga bog'liq bo'ladi. Shu sababli, tizim talabidan kelib chiqib mos biometrik parametrni tanlash muhim ahamiyat kasb etadi.

Biometrik parametrlar odatda fizik va xulq – atvor xususiyatlariga ajratiladi. Fizik biometrik parametrlar asosan odamning tanasidagi xususiyatlar bo'lsa, xulq-atvor ko'rinishidagilari esa odamning harakatlariga bog'liq bo'ladi. Xulq-atvor biometrik tizimlar asosan foydalanuvchilarning xulqi, harakatlari va kayfiyatining vaqt bo'yicha o'zgarishini identifikatsiyalashga asoslanadi. Ushbu biometrik tizimlar fizik parametrlarga o'xshab foydalanuvchining bevosita hamkorligini ya'ni e'tiborini talab etmaydi hamda shaffof, foydalanuvchiga mos va qulay hisoblanadi. Bu usulning kamchiligi sifatida fizik biometrik tizimlar bilan taqqoslaganda past darajali noyoblik va autentifikatsiya usulining sifatini pastligini keltirish mumkin. Ularga misol qilib, insonning harakati asosida, ovozi asosida, yozish shakli asosida autentifikatsiya tizimlarini olish mumkin (1.5 - rasm).

Ovoz. Mazkur usulda foydalanuvchining ovoziga ko'ra tanib olish amalga oshirilib, hozirda turli tizimlarda keng foydalanilib kelinmoqda (masalan, Applening Siri ilovasi, Google Voice ilovasi, Microsoftning Cortana va h.).



a. Harakatni tanib olish *b. Kompyuter klaviaturasida yozish* *c. Sichqoncha-ning harakati* *d. Ovozni tanib olish*

1.5 - rasm. Xulq-atvor biometrik tizimlari

Ushbu autentifikatsiya usuli katta xarajatni talab etmaydi (faqat mikrafon qurilmasi talab etiladi) va foydalanuvchilar tomonidan yaxshi qabul qilinadi. Ushbu usulning kamchiligi sifatida ovozni yozish qurilmalari orqali yozib olish va qayta eshittirish, ovozni vaqt o'tishi bilan o'zgarishi va inson holatiga bog'liq bo'lishini keltirish mumkin. Ovozga asoslangan autentifikatsiya usullarida olib borilgan natijalar asosan ochiq ma'lumotlar bazasida shakllantiriladi. Ularga quyidagilarni misol keltirish mumkin: Microphone array database [106], Census (AN4) database [107], Let's Go Speech Dialog Data [108] va h.

Harakat. Harakat orqali tanib olish usulida aniqlanuvchi xususiyat sifatida harakatlanish tarzi va oyoqlarni ko'chish holatlari olinadi. Sababi ushbu jarayonda biometrik parametrlar ishtirok etadi va har bir inson o'zining harakatlinish yo'li va usuliga ega. Dastlabki tibbiyot natijalari shuni ko'rsatdiki inson harakatlanishida 24 ta o'zaro farq qiluvchi tashkil etuvchi xususiyat mavjud bo'lib, agar harakatlanish davomida ushbu xususiyatlardan foydalanilsa, harakatlanishni takrorlanmas deb qaralsa bo'ladi. Ushbu usul orqali insonni tanib olish, aniqlash uzoq vaqt talab etadi va ko'plab tekshirishlarni talab etadi [80].

Harakatni tanib olish tizimlari model va qiyofaga asoslangan usullarga bo'linadi [4]. Modelga asoslangan yondashuvlar vaqt bo'yicha nusxalarning o'zgarishi video ma'lumotdan ajratib olinadi va uning parametrlari tahlil qilinadi. Qiyofaga asoslangan yondashuvlar foydalanuvchining harakati va uning shakli (tuzilishi, qiyofasi) tahlil qilinadi. Kamera foydalanuvchining harakat davomidagi o'zgarishlarni kuzatadi va yozib oladi. Ushbu usulning samaradorligi kameraning sifatli suratga olishiga bog'liq hisoblanadi. Yurish yo'nalishining keskin o'zgarishi uning samaradorligini kamaytirishga olib kelishi mumkin. 2D tasvirlardan foydalanilganda geometrik signallarni qo'llash ko'rish nuqtalarini oshirishi mumkin. Bundan tashqari, 3D tasvirlardan foydalanish uning samaradorligini yanada oshiradi.

Harakatga asoslangan autentifikatsiya tizimlari asosan tibbiy diagnostikada va biometrik identifikatsiya tizimlarida keng foydalaniladi [109]. Harakatga asoslangan autentifikatsiya usullarida ko'plab ochiq ma'lumotlar bazasidan keng foydalaniladi: CASIA Gait Database[110], OU-ISIR Gait Database [111], TUM-IITKGP Gait Database [112] va boshqalar.

Kompyuter klaviaturasida yozish ("Husnixat"). Husnixatga asoslangan autentifikatsiya usullari foydalanuvchining klaviatura orqali ma'lumot kiritish xususiyatlariga ko'ra tanib olishni amalga oshiradi. Tekshirish statik (matnga bog'liq) va dinamik (matnga bog'liq bo'lmagan) holatda bo'lishi mumkin. Tekshirishdagi muhim xususiyatlar sifatida quyidagilarni keltirish mumkin: samarali kiritilgan belgilar orasidagi vaqt, klaviaturani bosish vaqti, belgini kiritish tezligi, xatolar ketma-ketligi, raqamlardan foydalanish va h. Ko'p foydalanuvchilarga ega tizimlarda husnixatga asoslangan autentifikatsiya usullaridan foydalanish noyoblik xususiyati yuqori emasligi bois samarasiz hisoblanadi. Bu yondashuv ko'p foydalanuvchili tizimlarda qo'llanilmasada, tekshirish uchun qulay hisoblanadi. Mazkur usulda foydalanuvchi ro'yxatdan o'tish jarayonida login, parol yoki maxsus belgilarni takror kiritishi mumkinligi bois, foydalanuvchilarga ko'p holatlarda noqulaylik tug'diradi. Biroq, husnixatga asoslangan autentifikatsiya usullari odatda boshqa usullar bilan mujassamlashgan holda amalga oshirilishi mumkin [23].

Husnixat xususiyatiga asoslangan autentifikatsiya usullari ko'plab kompyuter tizimlarida keng foydalanilmoqda: Typing DNA, ID Control, BehavioSec [113]. Mazkur sohada keng foydalaniluvchi ochiq bazalarga quyidagilarni misol keltirish mumkin: CMU Keystroke Dynamics – Benchmark Data Set, CMU Free vs. Transcribed Text, Keystroke Dynamics – Android platform, BioChaves Keystroke Databases, Keystroke100 Dataset va h. [114].

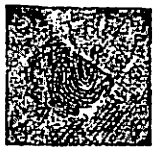
Fizik biometrik parametrlar. Savdo va biznes maqsadida ishlab chiqilgan biometrik tizimlarning katta qismi fizik biometrik parametrlarga asoslangan. Ushbu biometrik parametrlarga quyidagilarni kiritish mumkin (1.6 – rasm):

- yuz tasviri;
- yuz tamografiyasi;
- barmoq izi;
- qo'l geometriyasi;
- quloq geometriyasi;

-ko'z qorachig'i;
-ko'z to'rpardasi.


a. Yuz

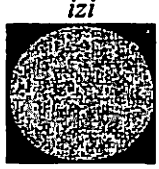

b. Yuz tamografiyasi


c. Barmoq izi


d. Qo'l geometriyasi


e. Quloq geometriyasi


f. Ko'z


g. Ko'z qorachig'i


k. Qon tomirlarining izi

1.6 – rasm. Fizik biometrik parametrlar

Yuz tasviri. Yuz orqali tanib olish keng tarqalgan biometrik autentifikatsiya usullaridan biri hisoblanadi. Ushbu usulda autentifikatsiyalash jarayonida shaxsi aniqlanishi lozim bo'lgan foydalanuvchi hech qanday qurilmaga tegishi talab etilmaydi. Jarayon kam vaqtni olib, asosiy kamchiligi sifatida o'rtacha 10% holatlarda yolg'ondan rad etish xatoligining mavjudligini ko'rsatish mumkin [80].

Ushbu usulda ma'lumotlarni to'plash va ma'lumotlar bazasini hosil qilish boshqa usullarga (DNA ga asoslangan yoki ko'z qorachig'i (Iris recognition) ga asoslangan) qaraganda oson. Bu esa yuz orqali tanib olish usulini keng tarqalishiga asos bo'lib xizmat qilmoqda.

Inson yuzi ko'plab xususiyatlarga ega. Ushbu xususiyatlar miqdori taxminan 80 tani tashkil etib, quyidagilar yuzni tanib olish algoritmlarida muhim parametr sifatida foydalaniladi:

- ko'zlar orasidagi masofa;
- burun (enining) o'lchami;
- ko'z chuqurlarining o'lchami;
- yanoq shakli;
- jag' shakli.

Yuz tasviriga asoslangan autentifikatsiya tizimlarini ishlab chiqarish bo'yicha dunyoning yetakchi tashkilotlari NEC [115], COGNITEC[116], Neurotechnology [117] va h. faoliyat yuritmoqda. Yuz tasviriga asoslangan autentifikatsiya sohasi keng tarqalgan va

rivojlanayotgan soha bo'lganligi bois mazkur sohada ko'plab ochiq kutubxonalar va pullik dasturiy ta'minot vositalardan keng foydalanilmoqda (OpenCV, Face++, FaceMark, FaceRect, Kairos va h.). Tadqiqotchilar tomonidan ilmiy tadqiqotlarda Color FERET Database, SCface - Surveillance Cameras Face Database, Yale Face Database, NLPR Face Database va h. yuz tasvirlari bazalaridan foydalanilmoqda.

Barmoq izi. Barmoq izini tanib olish tizimlari huquq organlari va kompyuter tizimlarida keng va samarali qo'llaniladigan usul hisoblanadi. Ushbu texnologiya laptoplarda, mobil telefonlarda yoki shaxsiy raqamli yordamchilarni o'z ichiga oluvchi turli platformalarda va qurilmalarda qo'llaniladi. An'anaviy barmoq izini tanib olish tizimlari mavjud barmoqni o'quvchi datchiklar yordamida barmoqni tekkizish yoki sirg'anishi asosida o'qib oladi. Uning yagona kamchiligi sifatida barmoq sirtidagi o'zgarishlarni, qoplamalar paydo bo'lishi yoki teri ahvoli (kirligi, terlashi, namligi)ni keltirish mumkin. Teridagi holatlarga qaramasdan tizimni samarali ishlashini ta'minlash maqsadida ulanishsiz (kontaktsiz) barmoq izini o'qib oluvchi datchiklar qo'llanilmoqda. Uning ikki turi mavjud: aks ettiririshga va uzatishga asoslangan. Aks ettiririshga asoslangan barmoq izini ulanishsiz o'qib olish texnologiyalarida barmoqni yorituvchi ikkita manba mavjud bo'lib, yorituvchi tomonidan kelgan nurning bir qismi barmoqni aks ettirishda, qolgan qismi optik tekshiruvchiga yuboriladi. Qurilma barmoq izining sohasiga qarab turli yorug'lik darajasi bilan ta'minlab beradi. Bundan tashqari, boshqa parametrlar: fokusning kengligi, kameraning ko'rish sohasi, yorug'lik manbalarining nurlanishi va chastotasi, shuningdek, teri holatining kir yoki nam holatga o'zgarishi tanib olishga samarali natijaga ta'sir etishi mumkin.

Barmoq iziga asoslangan tanib olish usullari real hayotda keng foydalanilib, ularga biometrik pasport tizimlarini, FBIning IAFIS tizimini, mobil qurilmalarda autentifikatsiyalashda qo'llanilishini misol keltirish mumkin. Barmoq iziga asoslangan autentifikatsiya algoritmlarini testlashda amalda FVC2000, FVC2002, FVC2004 bazalaridan keng foydalaniladi.

Qo'l geometriyasi. Qo'l geometriyasiga asoslangan tizimlar barmoqning va qo'lning uzunligi, eni, qalinligi va sirtining o'lchamlariga ko'ra amalga oshiriladi. Ushbu usul yetarli darajada takrorlanmas xususiyatlarning kamligi sababli past darajadagi xavfsizlikni ta'minlaydi. Shuning uchun, ularni ko'p foydalanuvchili tizimlarda qo'llab bo'lmaydi. Bundan tashqari, qo'lning shaklini suratga

olish qurilmasi qimmat. Qo'l geometriyasiga asoslangan autentifikatsiya usullari hukumat, moliya/bank, imigratsiya/sayohat, obyektlar himoyasida va h. sohalarda keng foydalanilmoqda. Hozirda mazkur sohada 3M Company, Fingerprint Cards AB, Cross Match Technologies Inc., Fulcrum Biometrics LLC., Safran SA, Fujitsu Ltd., RCG Holdings Limited va h. kompaniyalari yetakchilik qilmoqda [118]. Qo'l geometriyasiga asoslangan autentifikatsiyalashda Bosphorus Hand Database [119] bazasidan keng foydalaniladi.

Ko'zning rangdor pardasi (qorachig'i). Ko'zning rangdor pardasi orqali tanib olish biometrik tizimlardan eng ishonchlilaridan biri hisoblanadi. Ushbu usul yuqori noyoblik va barqarorlik (vaqt o'tishi bilan o'zgarmas) xususiyatlariga ega bo'lib, yuqori samaradorlikka ega bo'lgan biometrik faktor hisoblanadi [11]. Mazkur usulda autentifikatsiyalash ko'zning rangdor pardasidagi ranglarning turli tumanligi, notekisligi va qirralarining o'lchamlari asosida amalga oshiriladi. Uning asosiy bosqichlari quyidagilardan iborat:

– ko'z qorachig'ini tasvirga olish;

– xususiyalarni belgilash va segmentlash orqali ko'zning rangdor pardasini aniqlash;

– biometrik shablon yaratish;

– biometrik shablonni mavjudlari bilan taqqoslash.

Bu usulning afzalligi ikkita bir xil ko'z qorachig'ining mavjud bo'lish ehtimolini 10^{70} dan birga tengligi bilan belgilanadi. Biroq, boshqa biometrik parametrlarga nisbatan foydalanuvchidan ko'p diqqat va qimmat qurilmalar talab etiladi. Ko'z qorachig'iga asoslangan autentifikatsiya usullari biometrik pasport tizimlarida (United Arab Emirates IrisGuard's Homeland Security Border Control - BAAda barcha chegaralarda ko'z qorachig'iga asoslangan autentfikasiyadan foydalaniladi), ko'plab banklarda (masalan, IrisGuard), Hindistondagi Aadhaar tizimiga va h. sohalarda keng qo'llanilib kelinmoqda. CASIA-IrisV3, IIT Delhi Iris Database va UBIRIS bazalari mazkur sohada tadqiqotlar olib borishda keng foydalanilmoqda.

Biometrik parametrlarning tahlili. Odatda biometrik autentifikatsiya tizimlarida biometrik parametrlar quyidagi omillar orqali taqqoslanadi [80]:

– *universallik (universality)* - har bir insonda biometrik parametrning mavjud bo'lishi;

– *takrorlanmaslik (distinctiveness)* – biometrik parametrning

ikkita inson uchun bir xil bo'lmasligi;

– *o'zgarmaslik (permanence)* - biometrik parametrni vaqt o'tishi bilan o'zgarmasligi;

– *to'planuvchanlik (collectability)* – biometrik parametrdan kerakli axborotni to'planuvchanlik darajasini ko'rsatadi;

– *amalga oshirish (performance)* – biometrik parametrga asoslangan autentifikatsiya usulini amalga qo'llash darajasini ko'rsatadi;

– *muvofiqlik (acceptability)* - biometrik autentifikatsiya usulini insonlar tomonidan qabul qilinish darajasini ko'rsatadi;

– *aldanuvchanlik (circumvention)* – mazkur omil autentifikatsiya tizimini qalbaki texnologiyalar yordamida aldanish darajasini belgilaydi.

Mavjud biometrik parametrga asoslangan autentifikatsiya usullarining yuqoridagi xususiyatlar bo'yicha tahlili 1.5 –jadvalda aks ettirilgan.

1.5 – jadval

Biometrik autentifikatsiyalash usullarining qiyosiy tahlili (Y – yuqori, O' – o'rta, P - past)

Biometrik xususiyat	Universallik	Takrorlanmaslik	O'zgarmaslik	To'planuvchanlik	Amalga oshirish	Muvofiqlik	Aldanuvchanlik
DNA	Y	Y	Y	P	Y	P	P
Quloq	Y	O'	Y	O'	O'	Y	O'
Yuz	Y	P	O'	Y	P	Y	Y
Yuz termogrammasi	Y	Y	P	Y	O'	Y	P
Barmoq izi	O'	Y	Y	O'	Y	O'	O'
Harakat	O'	P	P	Y	P	Y	O'
Qo'l geometriyasi	O'	O'	O'	Y	O'	O'	O'
Qo'l tomiri holati	O'	O'	O'	O'	O'	O'	P
Ko'z qorachig'i	Y	Y	Y	O'	Y	P	P
Ko'z to'r pardasi	Y	Y	O'	P	Y	P	P
Imzo	P	P	P	Y	P	Y	Y
Ovoz	O'	P	P	O'	P	Y	Y

Biometrik tizimlarda xalaqitlar natijasida ko'p muammolar yuzaga kelishi mumkin. Bu xalaqitlarga ro'yxatga olish va tanib olish jarayonlari orasidagi farqni misol keltirish mumkin. Biometrik autentifikatsiya tizimlarida foydalanuvchini tanib olish darajasi ma'lum chegara qiymat asosida aniqlanadi. Bu chegara qiymat foydalanuvchilarni ikkita: haqiqiy va haqiqiy bo'lmagan foydalanuvchilar guruhiga ajratadi. Biroq, biometrik tizimlarda chegara qiymatini tanlashda yo'l qo'yilgan xatolik va biometrik xatoliklar natijasida ko'p holatlarda mazkur cheraga yaqinida avariyaga uchraydi. Biometrik tizimlarda ko'plab xatolik turlari mavjud bo'lib, ularning ichidan yolg'ondan tasdiqlash, yolg'ondan rad etish va teng xatolik darajasi xatoliklari muhim hisoblanadi [80].

Yolg'ondan tasdiqlash darajasi (False acceptance rate, FAR). Bu xatolik tizimga kiritilgan biometrik shablonni bazadagi muqobili bilan taqqoslashdagi yolg'ondan muvaffaqqiyatli deb topish darajasini belgilaydi. Biometrik kriptotizimlarning yolg'ondan tasdiqlash darajasi tizim tomonidan noto'g'ri generatsiya qilingan to'g'ri kalitlar darajasini aniqlaydi, ya'ni, qonuniy bo'lmagan foydalanuvchidan generatsiya qilingan to'g'ri kalitlar miqdorini aniqlaydi.

Yolg'ondan rad etish darajasi (False rejection rate, FRR). Bu xatolik tizimga kiritilgan shablonni bazadagi muqobili bilan taqqoslashdagi yolg'ondan muvafaqiyatsiz deb topish darajasini belgilaydi. Biometrik kriptotizimlarning yolg'ondan rad etish darajasi tizim tomonidan noto'g'ri generatsiya qilingan noto'g'ri kalitlar darajasi bilan aniqlanadi, ya'ni, haqiqiy foydalanuvchi uchun generatsiya qilingan noto'g'ri kalitlar darajasini aniqlaydi.

Teng xatolik darajasi. Bu xatolik darajasi har ikkala tasdiqlash va rad etish xatoliklarining teng bo'lgan miqdori bilan aniqlanadi. Tezkor tasdiqlash talab etilganda aksariyat holatlarda ushbu xatolikdan foydalaniladi.

Biometrik autentifikatsiya tizimlarini ochiq bazalar asosida tahlili. Biometrik xatoliklarni hisoblash odatda quyidagi ochiq bazalar doirasida amalga oshiriladi:

– NIST Speaker 99: mazkur baza ovozga asoslangan autentifikatsiyalash usulini tekshirish uchun NIST tomonidan yaratilgan;

– FRVT 2000 (Facial Recognition Vendor Test): mazkur baza yuz tasviriga asoslangan autentifikatsiya usullarini tahlillashga asoslangan bo'lib, DARMA tomonidan ishlab chiqilgan;

– FVC 2000 (Fingerprint Verification Competition): mazkur baza Boloniya universiteti tomonidan barmoq iziga asoslangan autentifikatsiya usullarini tahlillash maqsadida ishlab chiqilgan;

– CESG Biometric Testing Report: mazkur biometrik bazalar to'plami yuz tasviri, barmoq izi, qo'l shakli, ko'z qorachig'i, qon tomir va ovozga asoslangan autentifikatsiya usullarini testlashga mo'ljallangan bo'lib, CESG tomonidan yaratilgan.

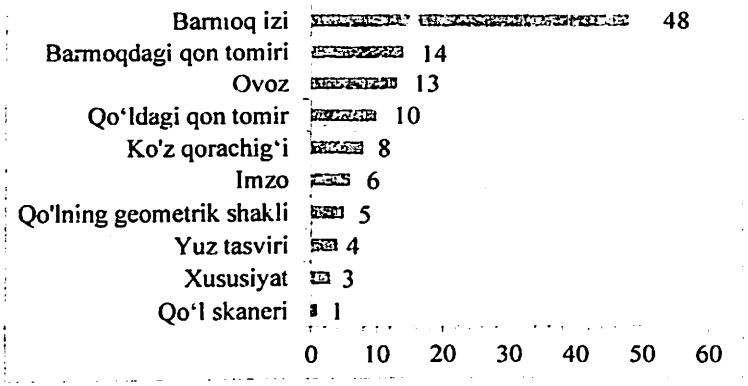
1.6 – jadvalda ba'zi biometrik autentifikatsiya usullarini yuqoridagi bazalarda olingan xatoliklar natijasi keltirilgan.

1.6 - jadval

Biometrik autentifikatsiya usullarini turli bazalardagi xatoliklar ko'rsatkichi

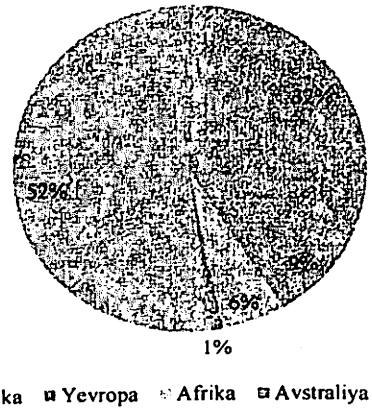
Biometrik xususiyatlar	Qurilma va foydalanuvchi orasi	Jarayon tezligi	Baza nomi	Urinishlar	Rad etish xatoligi	Tasdiqlash xatoligi
Yuz tasviri	~20 m	O'rtacha	FRVT	1	16 %	16 %
			CESG	3	6 %	6 %
Barmoq izi	30 sm	Yuqori	FVC	1	2 %	0,02 %
			CESG	3	2 %	0,01 %
Qo'l shakli	10 sm	Yuqori	CESG	1	3 %	0,3 %
			CESG	3	1 %	0,15 %
Ko'z qorachig'i	30 sm	O'rtacha	CESG	1	2 %	0,0001 %
			CESG	3	0,25 %	0,0001 %
Ovoz	20 sm	Yuqori	NIST	1	7 %	7 %
			CESG	3	2 %	0,03 %

Biometrik parametrlar ko'plab sohalarda xavfsizlikni ta'minlashda keng foydalanilmoqda. Mobil qurilmalarda biometrik parametrlarga asoslangan autentifikatsiya usulini mavjudligi, mobil bankingdagi autentifikatsiya muammolarini yechishda qo'llanilmoqda. 1.7 – rasmda bank sohasida turli biometrik autentifikatsiya usullaridan foydalanishning ulushi keltirilgan bo'lib, barmoq iziga asoslangan vositalar qolganlariga nisbatan keng tarqalgan [10].



1.7 – rasm. 2016 – yilda bank sektorlarida biometrik autentifikatsiya usullaridan foydalanish ko'rsatkichi (% larda)

Biometrik autentifikatsiya usullaridan bank sohasida foydalanish bo'yicha Osiyo va Amerika qit'asida joylashgan davlatlar yetakchilik qilib, ularning umumiy ko'rsatkichlari 1.8 – rasmda keltirilgan.



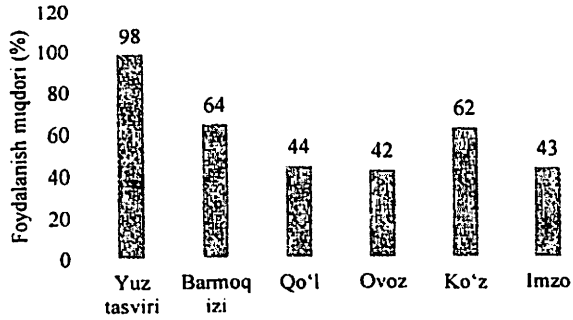
1.8 – rasm. Turli mintaqalarda bank sohasida biometrik autentifikatsiya usullaridan foydalanish ko'rsatkichlari

Mos biometrik autentifikatsiya usulini tanlashda turli holatlarni, sharoitlarni va tizimga qo'yilgan talabni inobatga olish zarur bo'ladi. Olib borilgan tahlil natijalariga ko'ra ishonchlik, foydalanishdagi qulaylik, xavfsizlik darajasi va narx omillari bo'yicha barmoq iziga

asoslangan autentifikatsiya usulini eng mos deb tanlash mumkin. Ko'z qorachig'i va ko'z to'r pardasiga asoslangan autentifikatsiya usulining xavfsizlik darajasi o'ta yuqori bo'lib, qimmat qurilmalarni va foydalanuvchidan diqqatni talab etadi. Bundan tashqari, foydalanuvchiga qulay bo'lgan, kam xarajatli va amalga oshirish imkoniyati yuqori bo'lgan (nisbatan xavfsizlik darajasi past) usul sifatida yuz tasviriga asoslangan autentifikatsiya usulini keltirish mumkin.

So'ngi yillarda biometrik parametrlarga asoslangan autentifikatsiya usullari jadallik bilan rivojlanib bormoqda. Yuqorida biometrik autentifikatsiya usullarida tanlangan biometrik xususiyatlarning tahlili amalga oshirilib, unda kam xarajat talab etadigan, foydalanuvchilar tomonidan yaxshi qabul qilinadigan va xavfsiz deb yuz tasviri olindi.

Yuz tasviriga asoslangan autentifikatsiya usuli boshqa biometrik parametrlar (qo'l, ko'z, ovoz, imzo, barmoq) orasida MRTD (Machine-Readable Travel Documents) tizimida eng ko'p foydalanilishi bilan ajralib turadi (1.9 - rasm).



1.9 – rasm. MRTD tizimlarida biometrik parametrlardan foydalanish darajasi

Bundan tashqari, yuz tasviriga asoslangan autentifikatsiya usullari quyidagi afzalliklarga ega:

– *Qisqa vaqt:* biometrik parametrlar ichida yuz tasviri eng qisqa vaqt talab qiladigan autentifikatsiya usullaridan biri hisoblanadi. Shuning uchun, mazkur autentifikatsiya usuli real – vaqt tizimlarida keng foydalaniladi.

– *Yuqori xavfsizlik:* yuz tasviriga asoslangan autentifikatsiya usuli (xususan, uch o'lchamli yuz tasviriga asoslangan) amalga oshirilish darajasiga ko'ra yuqori xavfsizlikni ta'minlaydi.

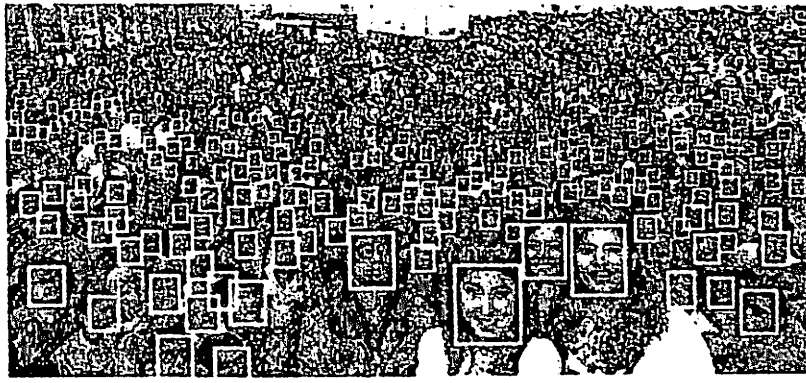
– *Avtomatlashtirilgan tizim*: inson ishtirokisiz autentifikatsiya tizimini amalga oshirish mumkin.

– *Ommaviy joylarda foydalanish:* yuz tasviriga asoslangan autentifikatsiya foydalanuvchilar uchun qulay bo'lib, bir vaqtning o'zida bir nechta foydalanuvchilarni autentifikatsiyalash imkoniyatini yaratadi. Buning uchun foydalanuvchilardan yuqori e'tibor talab etilmaydi.

II BOB. YUZ TASVIRI BO'YICHA TANIB OLISH USULI VA UNING AMALIY AHAMIYATI

2.1. Yuz tasviri bo'yicha tanib olishdan amalda foydalanish

Yuz tasviri asosida identifikatsiya va autentifikatsiya tizimlarining xatolik darajasi yuqori va tezligi pastligiga qaramasdan, ular talabgordan alohida e'tibor talab qilmasligi, masofadan va omma ichidan uni tanib olish imkoniyati bilan ajralib turadi (2.1-rasm). Xususan, qidiruvdagi shaxslarni topishda amalda keng qo'llaniladi. Shuning uchun ham yuzni tanib olish usullari ustida ko'plab tadqiqotlar olib borilmoqda va ularning asosiy maqsadi mavjud xatoliklarni minimallashtirishdan iborat.



2.1-rasm. Omma ichidan shaxslarni yuz tasviri asosida tanib olish

Foydalanishni nazoratlash. Yuz tasiviri bo'yicha tanib olishning keng tarqalgan yo'nalishlaridan biri foydalanishni nazoratlashdir. Birinchi navbatda, xodimdan hech qanday qo'shimcha harakatlarni talab etmasdan tizimdan foydalanishga ruxsat beradi. Ikkinchidan, tanib olish jarayoniga xalaqit beruvchi barcha faktorlarning: yorug'lik, orqa fondagi tasvirni boshqarish imkoniyati mavjud. Yuz tasviri bo'yicha tanib olish foydalanishlarni nazoratlashda ikki holatda qo'llanilishi mumkin:

1. Identifikatsiya holati. Ruxsat faqatgina yuz tasvirini tanib olish tizimi tomonidan olingan ma'lumotlar asosida beriladi. Masalan, bazada 100 ta xodim mavjud va bitta xodim tizimga kirishga uringanida tizimda birga yuz (1:100) tekshiruvi amalga oshiriladi. Agar uning ma'lumotlari yuzta odamdan biriga teng ekanligi aniqlansa, unda xodim sifatida ruxsat taqdim etilishi mumkin. Bularga, HikVision tomonidan taqdim

etilgan qurilmalarni misol keltirish mumkin. Shuningdek, identifikatsiyalash orqali tashqaridan kirib keladigan begona odamlarni aniqlash mumkin. Kirish qat'iyan man etilgan va faqat sanoqli odamlarning kirishiga ruxsat etilgan tizimlarda begona odamlarning ruxsatsiz kirishining oldi olinadi.

2. Autentifikatsiya holati. Ushbu holatda identifikatsiyalash RFID, smart karta, barmoq izi va boshqa shu kabi vositalar orqali aniqlanadi. Ushbu foydalanuvchining shaxsiga aniqlik kiritilgandan so'ng, uning haqiqatdan o'zi ekanligi tekshiriladi. Identifikatsiya holatidan farqli ravishda birga bir (1:1) tekshiruvi amalga oshiriladi. Autentifikatsiya holatida o'rta sifatli yuz tasvirini tanib olish tizimlarini qo'llash ham yetarli. U ko'pgina: biznes markaz, o'quv binolari, ishlab chiqarish va boshqa shu kabi hududlarga kirishda qo'llaniladi.

Transport. Transportda yuz tasvirini tanib olish quyidagi maqsadlarda qo'llanilishi mumkin.

– yo'qolgan odamlarni aniqlashda;

– qidiruvdagi jinoyatchilarni topishda;

– odamlarning qaysi hududga tegishli ekanligini aniqlashda;

– xizmat ko'rsatish sohalarida uning yuz ko'rinishidan qoniqishni aniqlash;

– umumiy foydalanish transportlarida yo'lovchilar sonini aniqlashda;

– to'lovlarni yuz tasviri asosida tasdiqlashda.

Transportda yo'lovchilar sonini online aniqlash yo'lovchi tashish tizimini samarali boshqarishga imkoniyat yaratadi. Bundan tashqari, yo'l haqi kirimini hisoblash va to'lovlar bilan bog'liq qoidabuzarliklarni aniqlashga ko'mak beradi.

Ish vaqtini hisoblash. Xodimlar ishga kelgan va ketgan vaqtini qayd jurnaliga yozish orqali ish vaqti hisoblangan bo'lsa, hozirgi axborot texnologiyalari rivojlangan bir davrda, yuz tasviri asosida uning bino hududida bo'lgan vaqti avtomatik hisoblanadi. Xodimning ish vaqtini hisoblash foydalanishni nazoratlashning bir qismi sifatida foydalanilishi mumkin. Uning quyidagi afzalliklari mavjud:

– qo'shimcha qurilma va alohida e'tiborsiz ish vaqtini hisoblash xodimlarga qulayiik yaratadi;

– boshqa xodimlarga xabar bermagan holda ularning ish vaqtlarini hisoblaydi.

Ish vaqtini hisoblashda yuz tasviri bo'yicha tanib olish ikki turdagi holatda qo'llash mumkin:

– *Server + dasturiy mahsulot + IP kamera.* Bu juda qimmat hisoblansada, hodimlarga sezdirmasdan va ularga axborot bermasdan ish vaqtini hisoblashga erishish mumkin.

– *Maxsus terminallar.* Barcha tashkilot xodimlar yuz tasviri bo'yicha identifikatsiya qurilmalaridan o'tishi lozim. Ushbu qurilmadan o'tmagan xodim uchun maosh hisoblanmaydi. Bu kabi qurilmalar faqat yuz tasviri bo'yicha tanib olishga yo'naltirilganligi bois, undagi FAR va FRR xatoliklari nolgacha kamaytirilgan.

Jamoat joylarida tanib olish. Jamoat joylarida va ko'chalarda, ya'ni odamlar ko'p joyda jinoyatchilarni aniqlashda qo'llaniladi. Bu jarayon o'ta murakkab hisoblansada, huquqni muhofaza qiluvchi organlar uchun muhim. Unda quyidagi murakkab holatlar mavjud:

– yorug'likning teng bo'lmagan taqsimlanishi: kunduzi, kechqurun, quyoshning turli tomondan tushishi yuz tasviri bo'yicha tanib olish sifatiga salbiy ta'sir qiladi;

– bitta kadrda ko'p sonli odamlar bo'lishi.

Yoshni aniqlash. Yuz tasviri bo'yicha tanib olish dastlab xavfsizlik masalalarida qo'llanilgan bo'lsa, hozirgi kunda tijorat maqsadida turli interaktiv yo'nalishlarda ham qo'llanilib kelinmoqda. Ixtiyoriy savdo yoki marketing tashkilotlari uchun tashrif buyuruvchilarning yoshi haqidagi ma'lumot zarur axborot hisoblanadi. Yoshni aniqlash tizimlari va dasturlariga talab butun dunyoda oshmoqda. Skybiometry va Vocord kabi online xizmatlar asosida yoshni aniqlashni imkoniyatlari mavjud (2.2-rasm).

2.2-rasm. Jinsni aniqlash (F – ayol, M – erkak)

Jinsni aniqlash. Ko'pchilik tijorat tashkilotlari mijozlari bilan ishlashda jinsini aniqlash dasturlaridan keng foydalanadilar. Yevropa davlatlari fuqarolarining tashqi ko'rinishi va kiyinishidan uning jinsini

aniqlash murakkab hisoblansada, zamonaviy axborot texnologiyalari bilan bunga yechim topish mumkin (2.2-rasm). Bundan tashqari, kino va konsertlarga tashrif buyuruvchilar va muxlislar orasidan qaysi jins a'zolarining soni ko'pligini aniqlash maqsadlarida ham qo'llanishi mumkin. Jinsni aniqlash funksiyasi ko'pgina yuz tasviri bo'yicha tanib olish dasturlarida mavjud.

Alohida tashrif buyuruvchilarni aniqlash. Tashrif buyuruvchilar sonini aniqlashda infraqizil yoki lazer nurlaridan foydalanilgan. Ular shaxsga aniqlik kiritmasada odamlarning umumiy sonini ko'rsatib beradi. Ammo, shunday holatlar mavjudki, tashriflar sonini oshirish yoki boshqa maqsadlarda qayta-qayta kirish amalga oshirilishi mumkin. Bundan tashqari, mashhur shaxslarning tashriflarini alohida qayd etish uning tashrif buyuruvchilari sonining ortishiga olib kelishi mumkin.

Avtorizatsiya. Yandeks taksi tizimlarida haydovchilarni avtorizatsiyadan o'tkazish uchun tanib olish xizmatlaridan foydalanilmoqda. Bundan tashqari, boshqa turdagi xizmat va qurilmalardan foydalanish uchun ham yuz tasviri bo'yicha tanib olish imkoniyatlaridan foydalanish mumkin.

To'lov tizimlari. Elektron to'lov tizimlarida karta egasi o'zining haqiqiyligini isbotlashda yuz tasviri bo'yicha tanib olishdan foydalanishadi. 2017 yilda Xitoyda "To'lov uchun tabassum" [41] xizmati orqali haridorga chegirma berish yo'lga qo'yilgan. To'lov tizimlarida qo'shimcha vositalarsiz, yuz tasviri yordamida to'lovni ishonchli amalga oshirish imkoniyati yuzaga keladi.

Tashkilotlarni boshqarish tizimlarida. Yuz tasviri bo'yicha tanib olish quyidagi imkoniyatlarni taqdim etadi:

– tashrif buyuruvchilar statistikasini aniqlash;

– yuz tasviridan chegirmalarni tasdiqlashda foydalanish;

– xodimlarning ish vaqtini hisoblash;

– mijozning profili ijtimoiy tarmoqlarda mavjudligini aniqlash (Vkontake).

Yuqoridagilardan tashqari, yuz tasviri bo'yicha tanib olish quyidagi maqsadlarda foydalanilgan (2.3-rasm):

– Xitoyda hojatxonalarda bitta odam bir marta belgilangan qog'ozni olishi uchun yuz tasviri bo'yicha tanib olish qo'llaniladi;

– maktablarda faqatgina ularning tashrifini emas, o'quvchilarning, darsga munosabati: o'qishi, tinglashi, yozishi va savol berishlarini qayd etish maqsadida ham qo'llash mumkin;

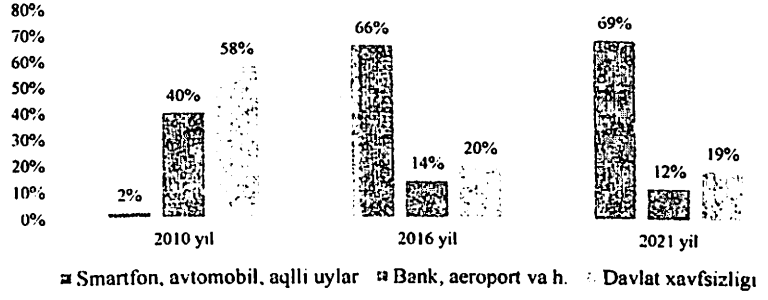
– mobil tashkilotlarda SIM-kartalarni sotish va uning egasini tekshirish;

– bank tizimlarida;

– huquqni muhofaza qilish sohasida;

– aeroportlarda;

– kinoteatrlarda tomoshabinlarning yoshi va jinsini aniqlash maqsadlarida qo'llash mumkin.



2.3-rasm. Yuz tasviri bo'yicha tanib olishning sohalarda qo'llanilish dinamikasi

Yuqoridagilardan kelib chiqib, yuz tasvirini tanib olish usullarini qo'llanilish sohalarini to'rtta katta guruhga ajratish mumkin.

1. *Turli holatdagi yuz tasvirlarini tanib olish* (2.4-rasm). Bitta holatdagi yuz tasviri mavjud va u orqali qolgan holatlarini bashorat qilish lozim [42]. Uning quyidagi ko'rinishlari mavjud:

– turli holatdagi yuz tasvirlarini tanib olish;

– yosh o'zgarishi asosida tanib olish;

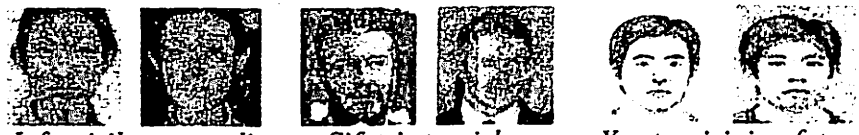
– yuz tasvirini o'zgartirish.

Turli holatdagi yuz tasvirlarini tanib olish | *Yosh o'zgarishi asosida tanib olish* | *Yuz tasvirini o'zgartirish*

2.4-rasm. Turli holatdagi yuz tasvirlarini tanib olish

2. *Geterogen yuz tasvirini tanib olish.* Ko'rinishi murakkab yoki yuz tasviri xususiyatlarini aniqlash qiyin sharoitlarda qo'llaniladi [43]. Uning quyidagi ko'rinishlari mavjud (2.5-rasm).

– infraqizil nur orqali;
– sifatsiz tasvirlar;
– yuz tasvirining foto-roboti.

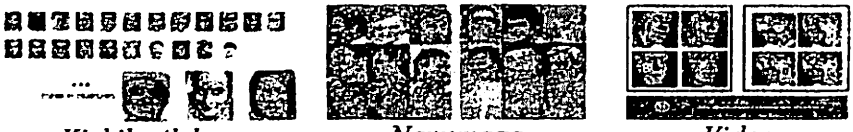


Infraqizil nur orqali *Sifatsiz tasvirlar* *Yuz tasvirining foto-roboti*

2.5-rasm. Geterogen yuz tasvirini tanib olish

3. *Ko'p sonli yoki yagona yuz tasviri namunasi orqali tanib olish.* Yuz tasvirining turli ko'rinishdagi namunalari kichik o'lchamlarda keltiriladi va u asosida xususiyatlar ajratilib, tanib olishga jo'natiladi [26]. Uning quyidagi turlari mavjud (2.6-rasm):

– kichik o'lcham;
– namunaga asoslangan;
– video.



Kichik o'lcham *Namunaga asoslangan* *Video*

2.6-rasm. Ko'p sonli yoki yagona yuz tasviri namunasi orqali tanib olish

4. *Yuz tasvirini tanib olish mahsulotlarini sanoatda qo'llash.* Foyda olish maqsadida turli yo'nalishlarda ishlab chiqilgan yuz tasvirini tanib olish usul va vositalarini keltirish mumkin [27]. Kriminal sohada yuz tasvirining kichik bo'lagi mavjud, u orqali shaxsni aniqlash hamda ikki o'lchamli yuz tasviridan uning uch o'lchamli namunasini shakllantirish va mobil qurilma, shaxsiy kompyuterlarda yuz tasvirini tanib olishni qo'llanilishi shular jumlasidandir. Uning quyidagi turlari mavjud (2.7-rasm):

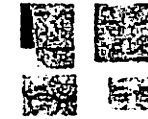
– uch o'lchamli (3D);
– qalbakilashtirishga qarshi;
– mobil qurilma va shaxsiy kompyuterlar;
– qismlarga asoslangan.

Uch o'lchamli

Haqiqiy Qalbakilashtirishga qarshi

Qalbaki

Mobil qurilma



Qismlarga asoslangan

2.7-rasm. Yuz tasvirini tanib olish mahsulotlarini sanoatda qo'llash namunalari

2.1-jadvalda yuz tasviri bo'yicha tanib olish usullarining sohalar bo'yicha qo'llanilish tavsifi keltirilgan.

2.1-jadval

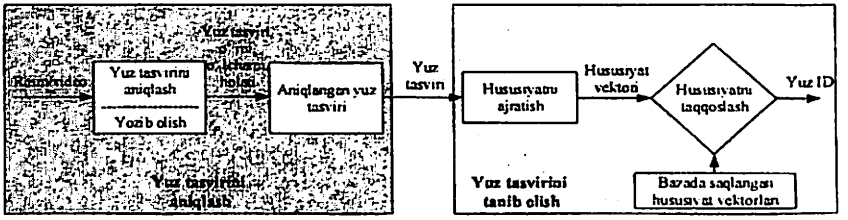
Yuz tasviri bo'yicha tanib olish usullarining sohalar bo'yicha qo'llanilish tavsifi

Soha	Ilovalar
Axborot xavfsizligi	–Ruxsatlarni nazoratlash (operatsion tizim, ma'lumotlar bazasi). –Ma'lumotlar xavfsizligi (tibbiyot ma'lumotlari). –Foydalanuvchilarni autentifikatsiyalash (savdo, bank xizmati).
Ruxsatlarni boshqarish	–Xavfsiz autentifikatsiya (alohida sohalar uchun). –Ruxsatga asoslangan tizimlar. –Log fayllar yoki audit uchun ruxsat.
Biometrik	–Shaxsni identifikatsiyasi (ID, passport, saylovchilarni ro'yxatga olish, haydovchilar lisenziyasini tekshirish). –Identifikatorni avtomatik tasdiqlash (chegarada)
Huquqni himoya qilish tashkilotlari	–Video kuzatuv. –Jinoyatchini tanib olish. –Jinoyatchini kuzatish. –Yuz tasviridan kriminalistikada foydalanish.
Shaxsiy xavfsizlik	–Uydagi video kuzatuv. –Haydovchini kuzatish tizimi.
Hordiq chiqarish tizimlari	–Uydagi o'yin tizimlari. –Foto-kamera ilovalari.

2.2. Yuz tasvirini aniqlash va tanib olish muolajalari

Yuz tasviriga asoslangan biometrik identifikatsiya va autentifikatsiya tizimlarida asosiy vazifa rasmning yuz tasviri joylashgan qismini aniqlash va shaxsning shablonga moslik darajasini yoki aniqlangan yuzni kimga tegishligini tekshirishdan iborat.

Yuz tasvirining identifikatsiyalash jarayoni ikki bosqichdan iborat bo'lib, birinchi bosqichda rasm yoki video oqimidan yuz tasvirini topish amalga oshiriladi. Ikkinchi bosqichda esa, yuz tasviri tanib olish amalga oshiriladi [28] (2.8-rasm).



2.8-rasm. Yuz tasvirining identifikatsiyalash jarayoni

Umumiy holda yuz tasvirini bazada mavjud tasvirlar bilan taqqoslash jarayoni quyidagi bosqichlarda amalga oshiriladi:

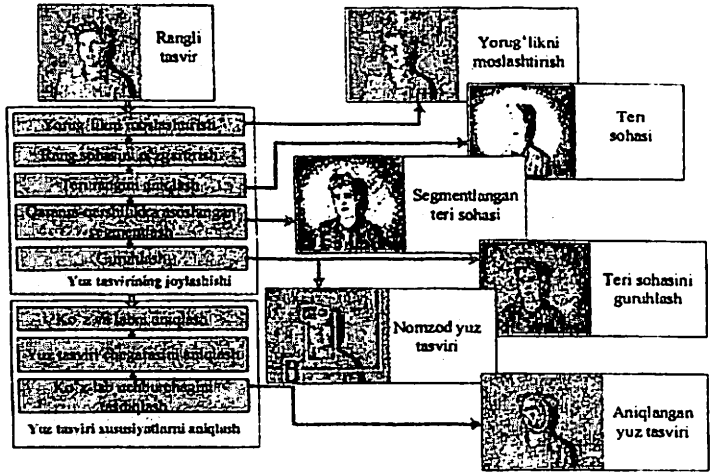
– *birinchi bosqich:* umumiy tasvirdan yuz tasviri va uni joylashgan o'rni aniqlanadi hamda yuz tasviri o'lchami va holatiga aniqlik kiritiladi. Yuz tasvirini aniqlashda uning qismlari navbatma-navbat aniqlanadi va ularni birlashtirib umumlashgan tasvir hosil qilinadi. Umumlashgan tasvir bazada saqlangan shablonlarga mos bo'lgan taqdirda, yuz tasviri aniqlangan hisoblanadi. Yuz tasvirini aniqlash jarayoni sifatining yuqoriligi yuz tasvirini tanib olish samaradorligini oshirishga xizmat qiladi [29];

– *ikkinchi bosqich:* yuz tasviridan geometrik kattaliklar, asosiy parametrlar, belgilar va yoritilganlik xususiyatlari ajratib olinadi. Aniqlangan yuz tasviridan bevosita tanib olish tizimlarida foydalanish qator kamchiliklarga ega. Xususan, aniqlangan yuz tasviri turli o'lchamlarda va turli rang modellarida bo'ladi. Mazkur kamchiliklarni bartaraf etish uchun xususiyatlarni ajratib olish jarayoni amalga oshiriladi va unda yagona o'lchamga keltirish, informativ xususiyatlarni aniqlash, turli to'siqlar hamda xalallarni olib tashlash amalga oshiriladi [81]. Ushbu bosqichdan so'ng yuz tasviri qismlarini aniq o'lchamga ega vektorlar ko'rinishida yoki aniq joylashgan nuqtalar to'plami sifatida ifodalash imkoni yaratiladi;

– *uchinchi bosqich:* yuz tasvirini aniqlash va ulardan informativ xususiyatlarni ajratib olish jarayonlaridan so'ng, ularni bazadagi mavjudlari bilan taqqoslash – *yuz tasvirini tanib olish* jarayoni amalga oshiriladi [82]. Yuz tasvirini avtomatik tanib olishni ta'minlashda dastlab yuz tasviri bazasini shakllantirish talab etiladi. Bir shaxsga tegishli bir nechta yuz tasvirlaridan olingan informativ xususiyatlar vektori yoki tasvirning o'zi bazada foydalanuvchining identifikatori bilan qayd etiladi. Yuz tasvirini tanib olish tizimlarida kiruvchi tasvir asosida yuz tasviri aniqlanib, informativ xususiyatlar ajratiladi va bazadagilari bilan taqqoslanadi.

Yuz tasvirini aniqlash masalasini yechish tasvirlarni segmentlash, zarur sohani aniqlash, taqqoslash, shuningdek, orqa fondagi yuz tasviri xususiyatlarini qayta ishlash orqali amalga oshiriladi. Hozirda ko'plab sohalarda tasvirlarni qayta ishlash mavjud: videoni kodlash, kontentga asoslangan tasvirni ajratib olish, video konferensiya, shaxslarni kuzatish, obyektlarni aniqlash va h. Yuz tasviri videodagi boshqa tasvirlar kabi o'zgaruvchan va u vaqt o'tishi bilan o'z pikselini biridan boshqasiga o'zgartiradi. Shuning uchun video tasvir va kuzatuv kameralari yordamida onlayn yuz tasvirini aniqlash ko'p vaqt hamda murakkab hisoblashlarni talab etadi. Videoning bir sekundi kamida 24 ta freym (tasvir)dan tashkil topgan bo'lsada, yuz tasvirini aniqlashda uning barchasini o'rganish talab etilmaydi.

Teri rangiga asoslangan yuz tasvirini aniqlash jarayonining asosiy bosqichlari 2.9-rasmda keltirilgan [30]. Ranga asoslangan yuz tasvirini aniqlash usullari yuz terisining rangi asosida kalit nuqtalarni ajratib olishga qaratilgan. Tasvirga berilgan yorug'lik turli-tuman bo'lganligi uchun undagi ranglar ham turli ko'rinishda akslanadi. Yuz xususiyatlari yoritilganlik darajasi past nuqtadan yoritilganlik darajasi yuqori bo'lgan nuqtaga qarab aniqlanadi. Ko'z va og'iz oson hamda ishonchli nuqtalar asosida aniqlanganligi bois, birinchi navbatda ushbu nuqtalar aniqlanadi va ular "ko'z xaritasi" va "og'iz xaritasi" deb nomlanadi. Natijada ikkita ko'z va og'iz orqali o'tuvchi uchburchak hosil bo'ladi. Ko'z va og'iz asosida yuz chegarasi belgilanadi yoki hosil bo'lgan uchburchak atrofida taxminiy chegara hosil qilinadi. Ushbu chegara to'rtburchak yoki aylana ko'rinishga ega bo'lib, rasmdagi yuz tasvirlarini ajratib turadi.



2.9-rasm. Teri rangiga asoslangan yuz tasvirini aniqlash jarayoni bosqichlari

Yuz tasvirini aniqlashdagi ushbu ikki vazifani bajarish natijasida yangi kiruvchi tasvirdan ajratib olingan yuz tasviri paydo bo'ladi. Yuz tasvirini aniqlashning mavjud sinflari, usullari, algoritmlari va ularning tavsifi 2.2-jadvalda keltirilgan [31].

2.2-jadval

Yuz tasvirini aniqlashning mavjud sinflari, usullari, algoritmlari va ularning tavsifi

Usullar va algoritmlar / Sinflar	Usullar	Tegishli algoritmlar	Tavsifi
1	2	3	4
Bilimga asoslangan	Iyerarxik bilimlarga asoslangan gorizontal va vertikal proyeksiyalash	Mozaik yuz tasvirlari algoritmi, yoritilgan sharoitlar algoritmi	Ishlash mumkin bo'lmagan xususiyatlar uchun qo'llaniladi
Xususiyatga asoslangan	Tasodifiy graflarni taqqoslash	Graf modeli algoritmi	Bilimlar natijasidagi oddiy xususiyatlar birlashtiriladi

1	2	3	4
	Vektorlarni qo'llash	Vektorlarni qo'llash algoritmi	Yuz tasvirini aniqlashda lokal va global vektorlardan foydalanish
Namunalarni taqqoslashga asoslangan	Faol tashqi ko'rinishga asoslangan	Asosiy komponent algoritmi, faol tashqi ko'rinish algoritmi	Yuz tasviri va uning tashqi ko'rinishi asosida o'rganiladi
Teri rangiga asoslangan	Misollarga asoslangan o'rganish	Yo'naltirilgan gradiyentlar gistogrammasi algoritmi, Gaus aralashmasi algoritmi	Gaus aralashmasi yordamida yuz va yuz bo'lmagan xususiyatlar aralash holda o'rganiladi
	Moslashuvchan o'sish asosidagi Viola - Djones xususiyatlari	Moslashuvchan o'sish algoritmi, Viola-Djones algoritmi	Viola - Djones xususiyatlarini aniqlash va uning tezligini oshirishda moslashuvchan o'sishni qo'llash

Yuqorida keltirilgan sinflarga mansub algoritmlar asosida yuz tasvirini aniqlash darajasi va o'rtacha vaqti bo'yicha testlash amalga oshirildi (2.3-jadval). Testlash natijasiga ko'ra vektorlarni qo'llash algoritmida aniqlash darajasi yuqori bo'lsada, ko'p vaqt sarflanishi ko'rsatgan.

2.3-jadval

Yuz tasvirini aniqlash darajasi va o'rtacha vaqti

Aniqlash ko'rsatkichlari / Aniqlash algoritmlari	**Aniqlash darajasi (%)**	**Aniqlashning o'rtacha vaqti (s)**
Gaus aralashmasi algoritmi	66	0,41
Viola-Djones algoritmi	87	0,443
Vektorlarni qo'llash algoritmi	93	1,669

Demak, yuz tasvirini aniqlashda mavjud muammolarni bartaraf etishda modellarga (yuz tasviri ko'rinishidagi) yoki tashqi ko'rinishga (yuz tasviriga xos xususiyatlarga) asoslangan usullardan foydalanish yuqori samara beradi. Bundan tashqari, neyron tarmoqlar, piksel xususiyatlari, sinflarga ajratish va shu kabi usullarni qo'llash orqali ham aniqlash samaradorligini oshirish mumkin [32].

Yuqoridagi usullarning turli, ko'p insonlar bo'lgan rasm, tasvir to'liq inson yuziga o'xshash rangda bo'lganda, yon tomondan turgan hol va h. holatlarda yuzlarni aniqlash ko'rsatkichlari 2.4 – jadvalda keltirilgan. Bunda ☺ - yuqori aniqlikda yuzni aniqlash, © - gohida yuz bo'lmagan sohani ham yuz deb topish va ® - yuzni umuman aniqlay olmaslik [19].

2.4 – jadval

Turli holatlarda yuzlarni aniqlash usullarining tahlili

Usullar / Xususiyatlar	Teri rangidan foydalanib	Haar xususiyat klassifikatorlaridan	Yuz xususiyatlaridan
Ko'p odamlar mavjud tasvir	®	©	☺
Tasvirning barcha qismi yuz terisi rangi kabi	®	®	☺
Yon tomonlama yuz tasviri	©	©	☺
Yengsiz ko'ylak holatda	©	©	☺
Yuz to'silgan holat	©	☺	©
Aks qaytaruvchi ko'z oynak	®	☺	®
Noaniq tasvir	☺	©	☺
Bir xil rang	©	☺	☺

Aniqlangan yuz tasviridan xususiyatlarni ajratish yuz tasvirini tanib olishdagi asosiy qadamlardan biri. Bunda ajratilgan xususiyatlar saralanadi va shaxsni identifikatsiyalash uchun bazada saqlanadi. 2.5-jadvalda yuz tasvirini tanib olishning klassik usullarida qo'llaniladigan xususiyatlarni ajratish algoritmlari keltirilgan.

2.5-jadval

Xususiyatlarni ajratish algoritmlari

Algoritm	Tavsifi
Bosh komponentlar tahlili (PCA)	Bosh vektor va chiziqli xaritaga asoslangan.
Kernel PCA	Bosh vektor, chiziqli xarita va kernel sathiga asoslangan.
Chiziqli diskriminant tahlil (LDA)	Bosh vektor va takomillashgan chiziqli xaritaga asoslangan.
Mustaqil komponentlar tahlili (ICA)	Chiziqli xaritaga va Gaussian filtrga asoslangan.
Neyron tarmoq	PCA asosidagi neyron tarmoq.
Faol tashqi ko'rinish modeli (ASM, AAM)	Statik usul va chegaralarni qidirishga asoslangan.
Gabor to'lqinlari	Biologik xususiyatlar va chiziqli filtrlarga asoslangan.
Diskret kosinus akslantirish (DCT)	Chiziqli funksiya va Fure akslantirishga asoslangan.

Yuz tasviri asosida tanib olish jarayoning aniqligi xususiyatlarni ajratib olishning samaradorligi bilan qiyoslanadi.

Ushbu usullar asosida turli algoritmlar ochiq kodli va tijoriy shaklda ishlab chiqarilgan bo'lib, ular hozirda amaliyotda yuzlarni tanib olish tizimlaridan keng foydalanilmoqda. Quyida ular ichida keng tarqalgan: Intel OpenCV (OCV), Luxand FaceSDK (FSDK), Face Detection Library (FDLib), SIFinder (SIF), University of Surrey (UniS), FaceOnIt (FoI) va Neurotechnology VeriLook (VL) algoritmlarining tahlili keltirilgan (2.6 - jadval). Algoritmlarning samaradorligini yaxshilash uchun ular quyidagicha sozlandi:

- OCVda – *min_neighbors* parametri (sohada yuz borligini aniqlash uchun minimal urinishlar soni);
- SIFda – yuz bo'lgan va yuz bo'lmagan klasslarni ajratuvchi gipertekislikni siljitish parametri;
- FDLibda – yuzni aniqlashning "qat'iyligini" nazoratlash parametri;
- UniSda – yuz bo'lishining ishonchlilik chegarasini ko'rsatuvchi parametr;
- FoIda - yuz bo'lishining ishonchlilik chegarasini ko'rsatuvchi parametr;
- FSDKda - *FSDK SetFaceDetectionThreshold*ning qiymati;

- VLda - yuz bo'lishining ishonchlilik chegarasini ko'rsatuvchi parametr.

2.6–jadval

Muayyan parametrlarga asosan yuzni aniqlash algoritmlarining qiyosiy tahlili

Algoritmlar	FRR	FAR	O'rtacha vaqt, ms	Aniqlash usuli
OCV (2)	0.0628	0.0423	90	Haar klassifikator
SIF (-3)	0.2362	0.0454	260	SVM klassifikator
FDLib (1)	0.4565	0.1868	64	SVM klassifikator
UniS (20)	0.1444	0.0426	176	Kombinatsion
FoI (5)	0.2222	0.0044	84	Haar klassifikator
FSDK (5)	0.0805	0.0294	1305	Yuz xususiyatlari
VL (2)	0.0523	0.0062	47	Yuz xususiyatlari

Yuqoridagi tahlil natijalaridan kelib chiqib shuni aytish mumkinki, VL yuzni aniqlash algoritmi qolgan algoritmlar ichida eng samarali va tezkor bo'lib, tijorat maqsadida foydalaniladi. Undan so'ng esa ochiq kodli sanalgan OCV algoritmi samarali va FDLibga qaraganda nisbatan ko'proq vaqt talab etadi.

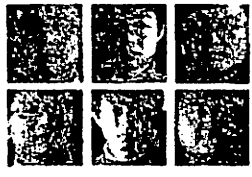
2.3. Mavjud muammolar va ularni bartaraf etish bo'yicha tavsiyalar

Yuz tasviri bo'yicha identifikatsiya tizimlarida yuz tasvirining sifati uning aniqligini belgilaydi. Quyida yuz tasviri bo'yicha identifikatsiya tizimlarida yuz tasviri bilan bog'liq muammolar keltirilgan:

Yuz tasvirlarining tartibsiz joylashuvi. Yuz tasvirini tanib olishda video yoki rasmdan yuz tasvirini aniqlash dastlabki jarayon hisoblanadi. Video oqimi holatida har doim ham yuz tasviri ketma-ketligi vujudga kelmaydi. Boshqacha aytganda, shaxsning harakatda bo'lishi natijasida yuz tasvirining doimiy paydo bo'lishi holati kuzatilmaydi. Rasm orqa fonining ham turli holatda bo'lishi bu muammoni yanada murakkablashtiradi (2.10-rasm).

2.10-rasm. Yuz tasvirlarining tartibsiz joylashuvi

Yoritilganlik. Foydalanuvchi yuz tasvirini olish jarayonida muhitning yoritilganlik darajasining turliligi tanib olish jarayoniga ham jiddiy ta'sir qiladi [33]. Xususan, ikki o'lchamli yuz tasvirlariga asoslangan tanib olish tizimlarida yoritilganlikning ta'siri sezilarli darajada bo'ladi (2.11-rasm).



2.11-rasm. Turli yorug'lik darajasida olingan yuz tasvirlari

Yosh ta'siri. Shaxs yuz tasvirining ko'rinishi vaqt o'tishi bilan o'zgarib boradi. Ya'ni, shaxs qarishi bilan uning yuz suyaklari o'z hajmini va holatini o'zgartirgani bois, yuz tasviri xususiyatlari: ko'zning joylashuvi, burun va jag'ning o'zgarishi kuzatiladi [34] (2.12-rasm). Buning natijasida yuz tasviridagi muhim nuqtalarning o'rni o'zgaradi va u aniqlash jarayoniga ta'sir etadi. Xususan, 20-40, 41-65 va 65-undan yuqori yoshdagi shaxslarning uch o'lchamli yuz tasvirlari o'rtasida juda katta farq bo'lishi aniqlangan [35].

2.12-rasm. Shaxs qarishi natijasida yuz tasvirining o'zgarishi (chap tomonda 35 yoshli, o'ng tomonda 65 yoshli shaxs yuz tasviri)

Masofaning o'zgarishi. Kamera va shaxs orasidagi masofaning ortishi yuz tasviri sifatining o'zgarishiga olib keladi va buning natijasida

yuz tasviridagi muhim nuqtalarni aniqlash imkonining pasayishi va FAR/FRR xatoliklarining ortishi kuzatiladi. Natijada "sifatsiz" deb ataluvchi muammo hosil bo'ladi [83]. Ushbu muammo olingan yuz tasvirining o'lchami 16×16 dan kichik bo'lganligida yuzaga keladi [36].

Yuz tasvirini qalbakilashtirish hujumi. Ikki o'lchamli (2D) yuz tasviriga asoslangan tanib olish usullarini yuz tasviri bo'lgan sifatli rasm bilan aldash imkoniyati mavjud [37] (2.13-rasm). Ushbu muammo hattoki uch o'lchamli (3D) yuz tasvirlariga asoslangan tanib olish tizimlarida ham uchraydi (3D Mask Attack Database hujumi).

Haqiqiy yuz tasviri *Rasm asosida* *Video asosida* *3D niqob asosida*

2.14-rasm. Yuz tasvirini qalbakilashtirish

O'xshash yuz tasvirlari. Turli shaxslar orasida yuz tuzilishi bir – biriga o'xshash bo'lganlari ham topiladi [38]. Bu esa yuz tasviriga asoslangan tanib olish tizimlariga murakkablik tug'diradi (2.14-rasm).

2.14-rasm. O'xshash yuz tasvirlari

Yuz tasviridagi to'siqlar. Yuz tasvirining ayrim qismlarida to'siqlar paydo bo'lishi, uni aniqlash jarayonini susaytiradi. To'siq sifatida ko'zoynak, yorug'lik, soqol, mo'ylov, soch, telefonda so'zlashuv, bosh kiyim va boshqalarni keltirish mumkin (2.15-rasm). Tanib olish jarayonida yuz tasvirining to'liq bo'lmasligi esa, xatolik darajasining ortishiga va natijada samaradorlikning pasayishiga sabab bo'ladi [39].

2.15-rasm. Yuz tasviridagi to'siqlar

Yuz tasvirining holati. Tanib olish tizimlarida yuz tasviri holatining "to'g'ri-old" ko'rinishida bo'lmasligi yuz tasvirini to'liq ifodalash imkonini bermaydi [40]. Yuz tasviri holatining ma'lum burchakga og'ishi yoki yuqorida/pastda bo'lishi natijasida yuz tasvirini tanib olish va hatto yuz tasvirini aniqlash imkoniyati ham pasayishi mumkin (2.16-rasm).

2.16-rasm. Turli burchak va holatlardan olingan yuz tasvirlari

Turli ko'rinishdagi yuz tasvirlari. Shaxs yuz tasvirining turli holatlarda bo'lishi (kulishi, yig'lashi, ajablanishi va h.) natijasida tanib olish jarayonining sifati pasayishi mumkin (2.17-rasm). Masofadan tanib olish tizimlarida foydalanuvchilar harakatini boshqarishning imkoniyati yo'qligi sababli, ushbu holat ko'p uchraydi va jiddiy muammolardan biri sanaladi.

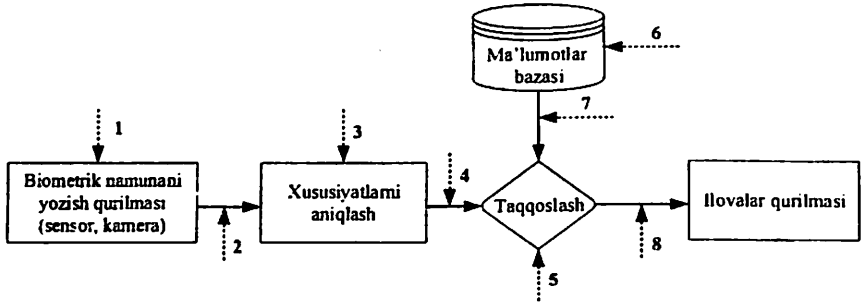
2.17-rasm. Turli ko'rinishli yuz tasvirlari

Biometrik identifikatsiya va autentifikatsiya tizimlariga qaratilgan hujumlar. Yuz tasviri bo'yicha identifikatsiya tizimlarida yuz tasviri bilan bog'liq muammolardan tashqari, tashqi muhitdan bo'ladigan tahdid va hujumlar borki, tizimning to'g'ri ishlashiga halaqit beradi. Natijada, yuz tasviri bo'yicha identifikatsiya tizimlari yuz tasvirini aniqlash va tanib olish darajasini oshirishning samaralari algoritmlariga qo'shimcha axborot xavfsizligi muammolarini ham qamrab olishi lozim. Biometrik parametr skaner tomonidan o'qib olinishidan bazada mavjud xususiyatlar bilan taqqoslanishiga qadar bo'lgan oraliqdagi hujumlar 2.18-rasmda aks ettirilgan [41].

Biometrik tizimlarda bo'lishi mumkin bo'lgan hujumlarni to'g'ridan-to'g'ri va bilvosita turlariga ajratish mumkin [84].

To'g'ridan-to'g'ri hujumlar. Ushbu hujumlar biometrik tizimda qo'llaniladigan usul, algoritm va parametr formati haqidagi aniq

bilimlarga asoslanmaydi. U faqat 1-tur, sensorga qaratilgan hujumlarni o'z ichiga oladi.



2.18-rasm. Biometrik tizimdagi hujum nuqtalari

1-tur hujum. Biometrik parametrlarni o'qib oluvchi skanerga yuz tasvirini yoki barmoq izi nusxasini taqdim etish orqali ushbu hujum amalga oshiriladi. Biometrik parametrning nusxasi o'ziga mos holda har xil formatda bo'lishi mumkin. Masalan, yuz tasviri bo'yicha tanib olish tizimida buzg'unchi mavjud foydalanuvchining rasmi, videosi, uch o'lchamli (3D) nusxasi yoki rezina niqobidan foydalanishi mumkin. Hozirgi kunda Lenova, Toshiba yoki Asus kabi kompaniyalar tomonidan ishlab chiqilgan, kompyuterlarda o'rnatilgan yuz tasvirini tanib oluvchi biometrik tizimni qalbakilashtirish hujumi bilan oson aldash mumkin. Chunki, ulardagi yuz tasvirini tanib olish tizimlarida qalbaki va haqiqiy yuz tasvirini farqlash imkoniyati mavjud emas.

Bilvosita hujumlar. To'g'ridan-to'g'ri hujumlardan farqli ravishda tanib olish tizimining strukturalari, funksiyalari va algoritmlari haqidagi bilimlarni talab etadi. Bu turdagi hujumlar 2, 3, 4, 5, 6, 7 va 8-turlarni o'z ichiga oladi.

2-tur hujum. Biometrik namuna skaner tomonidan o'qib olinganidan so'ng kommunikatsiya kanali orqali xususiyatlarni ajratish bosqichiga uzatiladi. Xususiyatlarni ajratish bosqichi va skaner o'rtasida kanal mavjud bo'lib, u orqali biometrik parametr o'g'irlanishi mumkin. Oldin saqlangan biometrik parametr, sensorni chetlab o'tishi uchun, xususiyatlarni ajratish bosqichiga qayta yuklanadi. Bu "qayta yuklash hujumi" deb nomlanadi.

3-tur hujum. Bu nuqtada amalga oshirilgan hujum "xususiyatlarni ajratish qismidagi hujum" deb nomlanadi. Bunda hujumchi tomonidan

kiritilgan va sensor tomonidan olingan haqiqiy namunalarning aralashgan holda hosil qilingan xususiyat qiymatlari olinadi.

4-tur hujum. 2-tur xujumga o'xshash, ammo, xususiyatlarni ajratish va taqqoslash qismlari o'rtasidagi kommunikatsiya kanalidan haqiqiy foydalanuvchining xususiyatlarini ushlab qolish va o'g'irlashga qaratilgan. Ushbu qiymatlar keyinchalik taqqoslash bosqichida foydalanilishi mumkin. Ular "xususiyatlarni ajratish va taqqoslash qismlari o'rtasidagi hujum" deb nomlanadi.

5-tur hujum. Kiruvchi xususiyatlarning qiymatlariga bog'liq bo'lmagan holda, autentifikatsiyadagi taqqoslash qismini katta ehtimollik bilan chetlab o'tish imkoniyati tug'iladi. Shuning uchun ham, ushbu hujum "taqqoslash bosqichidagi hujum" deb nomlanadi.

6-tur hujum. Hujumchi tomonidan biometrik namunalar joylashgan bazaga yangi namuna kiritilsa, mavjud namunalar o'zgartirilsa yoki mavjud namunalar o'chirilsa ushbu turdagi hujum yuzaga kelishi mumkin. Ushbu hujum turini amalga oshirish murakkab jarayon hisoblanib, ma'lumotlar bazasi xavfsizligi vositalari yordamida himoyalanganligi bilan xarakterlanadi. Samarali hujumni amalga oshirish uchun tizim funksiyalarini yaxshi o'zlashtirish lozim bo'ladi.

7-tur hujum. Biometrik namunalar, taqqoslash uchun bazadan kommunikatsiya tarmog'i orqali uzatilganida, bu turdagi hujumlarni amalga oshirish imkoniyati tug'iladi. Hujumchi biometrik namunaga o'zgartirish kiritadi. Mazkur hujum "taqqoslash va ma'lumotlar bazasi o'rtasidagi kommunikatsiya tarmog'idagi hujum" deb nomlanadi.

8-tur hujum. Ushbu hujumda taqqoslash natijasi qayta yoziladi. Buzg'unchi taqqoslash natijasini taqqoslash moduli va ilova qurilmasi orasidagi kanal orqali uzatilganida taqqoslash darajasini o'zgartirishga urinib ko'radi.

Ushbu 8 turdagi hujumlarni ko'rib chiqish natijasida, biometrik autentifikatsiya tizimining qaysi nuqtasida himoyani kuchaytirish kerakligi aniqlanadi.

Biometrik identifikatsiya va autentifikatsiya tizimlarida hujumlar bo'lishiga qaramasdan ushbu parametrlarga asoslangan foydalanishni nazoratlash tizimlari, amalda turli maqsadlarda va turli darajalarda foydalanilmoqda.

Standartlarga moslik. Biometrik parametrlarga asoslangan vositalarni keng miqyosda ishlab chiqish va ularning mosligini ta'minlash ma'lum xalqaro standartlarga asoslanadi. Ularga ISO (*International Organization for Standardization*) – xalqaro standartlar

tashkiloti va IEC (*International Electrotechnical Commission*) – xalqaro elektro-texnik komissiyalari tomonidan ishlab chiqilgan standartlarni misol keltirish mumkin.

Biometrik parametrlar asosida ishlab chiqilayotgan autentifikatsiya vositalarini ishlashda umumiylikni ta'minlash uchun olingan tasvirlarni saqlash, zichlash va ularning o'lchami quyidagi standartlarga asoslanishi mumkin [85]:

- yuz tasviri uchun - ISO/IEC 19794-5;
- barmoq izi tasviri uchun - ISO/IEC 19794-4;
- ko'z qorachig'i tasviri uchun - ISO/IEC 19794-6.

Xususan, ISO/IEC 19794-5 standarti bo'yicha yuz tasviriga quyidagi talablar qo'yiladi:

- raqamli rasm attributlariga qo'yilgan talablar (rasm o'lchami, rasm sifati);
- rasmga tushish senariylariga qo'yilgan talablar (yoritilganlik, yuz tasviri holati va ko'rinishi);
- fotografik xususiyatlar (kamera fokusi va uning holati). Bunda, olingan yuz tasvirining sifati 300 dpi da va ko'zlar orasidagi masofa taqriban 90 piksel bo'lishi, har bir pikselda 24 bit bo'lganida tasvirning o'lchami 640 Kb bo'lishi hamda ular JPEG va JPEG2000 formatda bo'lishi talab etiladi. Ushbu holda olingan tasvirning o'lchami kamida 12Kbni tashkil etadi.

Yuqorida keltirilgan muammolar yuzni tanib olishning barcha tizimlarida mavjud bo'lib, ularni minimallashtirish uchun xususiy talablarga, foydalanuvchi va ishlab chiqaruvchilar tavsiyalariga rioya qilish zarur. 2.7-jadvalda mavjud muammolarni bartaraf etish uchun tavsiyalar keltirilgan.

2.7-jadval

Yuz tasvirini aniqlash, tanib olish jarayonidagi muammolar va ularni bartaraf etish bo'yicha tavsiyalar

Muammoning nomlanishi	**Bartaraf etish yo'llari**
1	**2**
Yuz tasvirlarining tartibsiz joylashuvi	Yuz tasvirini aniqlash kameralari va bir sekundagi o'rganiladigan freymlar sonini oshirish.
Yoritilganlik	Yuz tasviri bazalarini shakllantirishda yoritilganlikni e'tiborga olish va uch o'lchamli yuz tasvirlaridan foydalanish.

1	2
Yosh ta'siri	Yuz tasviri bazalarini tez-tez yangilab turish.
Masofaning o'zgarishi	Yuqori sifatli kameralardan va bir xil o'lchamli rasmlardan foydalanish.
Yuz tasvirini qalbakilashtirish hujumi	Harakatni aniqlash, haqiqiylikka tekshirish, qo'shimcha faktorlarni qo'llash.
O'xshash yuz tasvirlari	Boshqa biometrik xususiyatlar va ikkinchi faktorlardan foydalanish.
Yuz tasviridagi to'siqlar	Uch o'lchamli namuna va boshqa biometrik xususiyatlardan foydalanish.
Yuz tasvirining holati	O'rganish uchun turli ko'rinishdagi tasvirlardan foydalanish.
Turli ko'rinishdagi yuz tasvirlari	Uch o'lchamli namuna va o'rganish uchun turli ko'rinishdagi yuz tasvirlaridan foydalanish.

Yuz tasvirini aniqlash va tanib olish jarayonidagi muammolar va ularni bartaraf etish uchun keltirilgan tavsiyalar tanib olish samaradorligini oshirishga xizmat qiladi.

2.4. Yuz tasviri bo'yicha tanib olish usullarini taqqoslash omillari

Biometrik tizimlarda halaqitlar natijasidagi katta muammolar vujudga keladi. Halaqitlar ro'yxatga olish va tanib olish jarayonlari orasidagi farqlarni ifodalaydi. Biometrik autentifikatsiya tizimlarida foydalanuvchini tanib olish darajasi ma'lum chegara orqali aniqlanadi. Bu chegara foydalanuvchilarni ikkita guruhga, haqiqiy va haqiqiy bo'lmaganlariga ajratadi. Biroq, biometrik tizimlar chegarani tanlashda, xatolik natijasida shu chegara yaqinida noxush holatga uchraydi.

Quyida biometrik tizimlardagi mavjud xatoliklar tavsiflangan. Xatoliklar darajasini hisoblashda quyidagi kattaliklardan foydalaniladi[42]:

- TP – haqiqatdan mavjud (True Positive);
- TN – haqiqatdan mavjud emas (True Negative);
- FN – yolg'ondan mavjud emas (False Negative);
- FP – yolg'ondan mavjud (False Positive).

Yolg'ondan tasdiqlash darajasi *(Falce acceptance rate, FAR).* Bu ehtimollik tizimning yangi kiritilgan parametr va shablon orasidagi taqqoslanishning yolg'ondan muvafaqqiyatli deb topishi darajasini belgilaydi. U noto'g'ri taqqoslanishlar foizini ko'rsatadi va quyidagicha hisoblanadi:

$$FAR = \frac{FN}{TP+FN}.$$

Yolg'ondan rad etish darajasi *(Falce rejection rate, FRR)*. Bu ehtimollik tizimning yangi kiritilgan parametr va shablon orasidagi taqqoslashning yolg'ondan muvafaqqiyatsiz deb topish darajasini belgilaydi. U joiz kirishlarni rad etish darajasini ko'rsatadi va quyidagicha hisoblanadi:

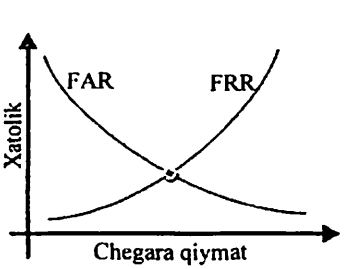
$$FRR = \frac{FP}{TN+FP}.$$

Teng xatolik darajasi *(Equal error rate, EER)*. Bu xatolik darajasi tasdiqlash va rad etish xatoliklarining teng bo'lgan miqdori bilan aniqlanadi. Tezkor tasdiqlash talab etilgan vaqtda bu xatolikdan ko'p hollarda foydalaniladi. Amalda olib borilayotgan ilmiy izlanishlar FAR va FRR xatoliklarini nolga tenglashtirishga qaratilgan bo'lib, ushbu holat autentifikatsiya jarayonini ideal darajasini belgilaydi. Uning qiymati ROC (*Receiver Operating Characteristic*) grafigi asosida FAR va FRR egri chiziqlarning teng qiymatni qabul qilishlari asosida hisoblanadi (2.19-rasm).

O'rganish jarayonidagi xatolik *(Failure to Enroll Rate, FER)*. O'rganish jarayonida namunani hosil qilishdagi muvaffaqiyatsiz urinishlarning darajasini belgilaydi. Bunda foydalanuvchi o'zining ma'lumotlarini tizimga o'rgatish uchun kiritishga harakat qiladi. Sifatsiz biometrik parametr kiritilganida tizim rad javobini beradi va u quyidagicha hisoblanadi:

$$FER = \frac{FE}{E},$$

bu yerda, FE - o'rganish jarayonida muvaffaqiyatsiz namunalar soni, E –kiritilgan namunalar soni.



2.19-rasm. ROC egri chizig'i

Tutib olishdagi xatolik darajasi *(Failure to Capture rate, FCR).* Avtomatlashtirilgan tizimlarda to'g'ri taqdim etilgan biometrik parametrni aniqlashda tizim tomonidan yo'l qo'yiladigan xatolik darajasi:

$$FCR = \frac{FC}{N},$$

bu yerda, FC – tutib olish jarayonida muvaffaqiyatsiz namunalar soni, N – tutib olish jarayoniga kiritilgan namunalar soni.

O'rtacha xatoliklar. Biometrik tizimlarning samaradorligini baholashda algebraik va geometrik o'rtacha xatoliklardan foydalaniladi.

O'rtacha algebraik xatolik (*Half Total Error Rate, HTER*) quyidagicha hisoblanadi:

$$HTER = \frac{FAR+FRR}{2}.$$

O'rtacha geometrik xatolik (*Geometric Mean, GM*) esa, quyidagi formula orqali hisoblanadi:

$$GM = \sqrt{\frac{TP}{TP+FN} \cdot \frac{TN}{TN+FP}}.$$

Qurilma va subyekt orasidagi masofa (Sensor Subject Distance, SSD). Turli biometrik parametrlar uchun shaxs va biometrik parametrni o'quvchi qurilma orasidagi masofa turlicha bo'lishi mumkin.

Quyida yuqorida keltirilgan xatoliklar asosida yuz tasviriga asoslangan tanib olishning qiyosiy tahlili keltirilgan (2.8-jadval). Ushbu xatoliklarning qiymatlari tadqiqotlar asosida olingan natijalarga tayangan holda, o'rtacha qiymatda hisoblangan.

2.8-jadval

Yuz tasviriga asoslangan tanib olishning qiyosiy tahlili

Xatoliklar (%)	FAR	FRR	EER	FER	FCR	HTER	GM	SSD
Yuz tasviri	1.1	2	-	2.7	5	2.85	3	~20 m

Yuz tasvirini sinflarga ajratishda uchta jarayondan foydalaniladi:

O'xshashlik. Namunaning sinflardan biriga tegishli ekanligi va uning o'xshashlik darajasini anglatadi. Masalan, Evklid masofasi asosida aniqlanishi mumkin. U namunadagi qiymatlarning o'rtacha vektori asosida aniqlanadi [43]. Kernel sathiga asoslangan algoritmlarni ham ushbu yondashuvga kiritish mumkin.

Ehtimolligi. Ehtimollikni aniqlashda Bayes qarorlar qoidasi qo'llaniladi. Bayes qoidalari xususiyatlarni baholashda samarali yo'l hisoblanadi [86]. Bayes qarorlar qoidasini hisoblashning bir nechta yondoshuvlari mavjud. Uni quyidagicha ifodalash mumkin:

$$p(Z|w_i)P(w_i) = \max\{p(Z|w_i)P(w_i)\},\ Z \in w_i.$$

Bu yerda, w_i – yuz sinfi, Z – PCA algoritmi asosida o'lchami kichiklashtirilgan yuz tasviri. Uni quyidagicha kengaytirilgan holda ifodalash mumkin:

$$p(Z|w_i) = \frac{1}{(2\pi)^{\frac{m}{2}}|\sum i|^{\frac{1}{2}}} \exp\left\{-\frac{1}{2}(Z - M_i)^t \sum_i^{-1}(Z - M_i)\right\}.$$

Bu yerda, $\sum i$ – kovariatsion (covariance) o'lcham, M_i - w_i sinfidagi o'rtacha matrisa.

Chegaraviy qaror. Bayes sinfiga mos holda yaratilgan va tanlangan o'lchamlarga bog'liq. U test va nomzod namunalar o'rtasidagi xatolik mezonini kamaytirishga qaratilgan. Unga misol sifatida chiziqli diskriminant tahlil (LDA) algoritmini keltirish mumkin. U ham PCA algoritmiga asoslanadi. Ushbu algoritm o'rtacha kvadratik xatoni kamaytirishga xizmat qiladi. Shuningdek, neyron tarmoqlar yordamida chiziqsiz chegaraviy qarorlar yuzaga keladi va sinflashtirish konfidensialligini ta'minlaydi.

Qaror daraxti sinflashtirishning asosiy turi hisoblanadi. Xususiyatlarni ketma-ket tanlovini yuzaga keltiradi va daraxtning har bir

ildizi muhim sanaladi. O'rganish mobaynida ildizga ega xususiyatlar yanada rivojlantiriladi [44].

Vektorlarni qo'llab-quvvatlash usuli ham sinflashtirishda keng qo'llaniladi. Unga yaqqol misol sifatida vektor mashinalarini qo'llab-quvvatlash (SVM) algoritmini keltirish mumkin. SVM algoritmi sinflashtirish bilan bog'liq bir nechta muammolarni yechishga qaratilgan bo'lib, uning ikkita uslubi mavjud [87]:

Bittasi barchasiga qarshi uslubi. SVM bitta sinfda o'rganiladi va boshqalari aynan ushbu sinfdan andoza oladi.

Qismlarga asoslangan uslub. Daraxtning barcha ildizlari ikki sinfga tayanadi. Eng yuqorida joylashgan ildiz oxirgi qarorni ko'rsatadi.

III BOB. YUZ TASVIRI BO'YICHA TANIB OLISHNING KLASSIK VA SUN'IY INTELLEKTGA ASOSLANGAN USULLARI

3.1. Yuz tasvirini tanib olishning klassik usullari

Namunalarni tanib olish usullari to'rt guruhga bo'linadi [45]:

- nusxalarni taqqoslash;
- statik yondashuv;
- sintaktik yondashuv;
- neyron tarmoqlar.

Namunalarni taqqoslash usulida har bir kiruvchi namuna bazadagi bir nechta namuna bilan taqqoslanadi va unga mosi tanlanadi.

Statik yondoshuvda o'rganish uchun olingan namunadan kerakli qiymatlar ajratiladi, tanib olishda esa turli kompyuter bilimlariga tayaniladi.

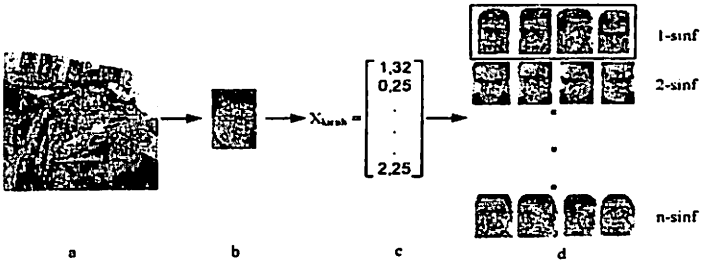
Sintaktik yondashuv inson bilimlariga yoki fizik qonun-qoidalarga asoslangan tanib olish usuli deb ham nomlanadi. Masalan so'zlarni sinflash yoki to'g'rilash gramatikaning yordamiga tayanadi. Kompyuter bilimlarini qurishda bir nechta qonun-qoidalar kiritiladi va ushbu qonun-qoidalar asosida qarorlar qabul qilinadi.

Neyron tarmoqlar freymlarga asoslangan holda amalga oshiriladi. Unda bir nechta bilimlar, darajalar, takomillashtirish mezonlari va o'zgarishlar mavjud bo'lib, tanib olish tizimlarida juda keng qo'llaniladi.

Yuz tasviri bo'yicha identifikatsiyada tanib olish jarayoni muhim hisoblanib, kiritilgan tasvir xususiyatlari bazadagilari bilan solishtiriladi va qaysi subyektga tegishli ekanligi aniqlanadi [46]. Ushbu jarayon tasvirdan yuz tasvirini aniqlash, yuz tasviri bo'lgan qismni ajratib olish, xususiyat vektorini shakllantirish va taqqoslash bosqichlaridan iborat (3.1-rasm).

Yuz tasvirini tanib olishda yuz tasvirining tashkil etuvchi qismlarining mavjudligini tekshirish alohida ahamiyatga ega. Yuzlarni tanib olish va xususiyatlarni ajratish to'rtta usul yordamida amalga oshiriladi:

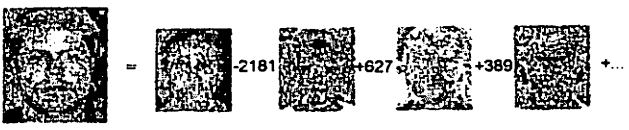
Tashqi ko'rinishga asoslangan usullar. Yuzning ayrim qismlaridan axborot yig'ish, ularni qayta ishlash va shu asosida yuzni tanib olish amalga oshiriladi. Boshqa usullardan farqli ravishda yuzni to'liqligicha o'rganadi. Ushbu usul asosida yuzlarni tanib olishning PCA, LDA, ICA va bazaga asoslangan algoritmlarini keltirish mumkin.



3.1-rasm. Yuz tasviri bo'yicha identifikatsiya jarayonlari. (a) yuz tasvirini aniqlash, (b) yuz tasviri qismini ajratish, (c) xususiyatlar vektorini shakllantirish, (d) kiruvchi vektor bilan bazada saqlangan vektorlarni taqqoslash

Asosiy komponentlarga asoslangan (PCA – Principial component analyzing) algoritmlar. Bir nechta yuzlarning tasviri yig'iladi (turli ko'rinishdagi yuz tasvirlarining soni ko'p bo'lishi tanib olish sifatini oshirishga asos bo'ladi) va n×n o'lchamga keltiriladi. Dastlab n×n matritsa va keyin $n^2 \times 1$ vektor ko'rinishiga o'tkaziladi [13]. Barcha yuz tasvirlarda kuchli va kuchsiz xususiyatlar bo'lib, PCA kuchli komponentlarni ajratib oladi, kuchsizlarini tashlab ketadi va natijada tasvir o'lchami kamayadi.

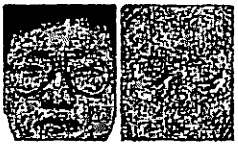
Yuz bazalarida mavjud yuzlarning proyeksiyalarini qo'llagan holda xususiy vektorlar tashkil etiladi va ular asosida haqiqiy yuz keltirib chiqariladi (3.2-rasm). Proyeksiyalashdan keyin olingan o'zgarishlar haqiqiy yuzni keltirib chiqarishda yuqori natija ko'rsatadi, ammo, yuzni tanib olishda bu proyeksiyalashning ahamiyati yo'q [47].



3.2-rasm. Xususiy yuz asosida haqiqiy yuzni qurish

Chiziqli diskriminativ tahlil (LDA – Liner discriminant analyzing) algoritmi [48]. LDA ham PCA ga o'xshash yuz tasviri o'lchamini kamaytiradi va qisqartirish mobaynida asosiy o'zgarishlarni yozib boradi. Bundan tashqari, LDA orqali yorug'lik o'zgargan hollarda ham, PCA ga nisbatan yuqori natija ko'rsatadi. LDA uchun bazani tashkil

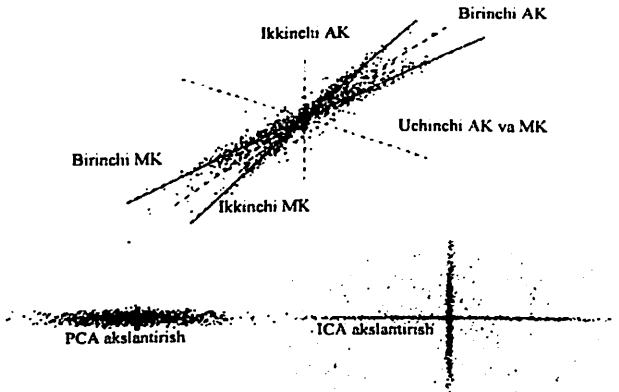
etishda ko'zoynak va ko'zoynaksiz, soqol va soqolsiz va boshqa shu kabi holatlarni e'tiborga olish lozim (3.3-rasm).



3.3-rasm. Ko'zoynakli odamning LDA algoritmida proyeksiyasi

LDA algoritmi raqamlashtirishda eng samarali proyeksiyalashni ta'minlab beradi va PCAga o'xshab ko'p energiya sarflamaydi. Hisoblash uchun yuklanish juda kam bo'ladi.

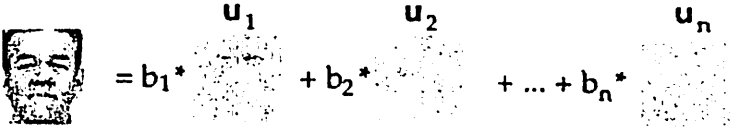
Mustaqil komponentlarni tahlillash (ICA – independent component analyzing) [5]. PCA algoritmiga nisbatan piksellar o'rtasida aloqalar ko'p va uning davomchisi hisoblanadi. 3.4-rasmda PCA va ICA algoritmlarining yuqori darajali o'zgarmas kattaliklar uchun proyeksiyalar keltirilgan. Pastdagi tasvirdan ko'rish mumkinki, PCA da ICA ga nisbatan o'zaro bog'liq piksellar o'rtasidagi farq juda katta.



3.4-rasm. Birinchi, ikkinchi va uchinchi darajali statik ma'lumotlarni yaratish va uni proyeksiyalashda qo'llash (AK – asosiy komponent, MK – mustaqil komponent)

ICA yuz tasvirlarida 3.5-rasmda ko'rsatilgandek, ko'z, qosh, burun va og'iz kabi mustaqil komponentalarni ajratib chiqadi. Har bir mustaqil komponentning og'irligi (tashqi ko'rinishi) asosida tasvir tanib olinadi. Bu yerda, u – asosiy komponentalarning matrisasi, b – ICAning

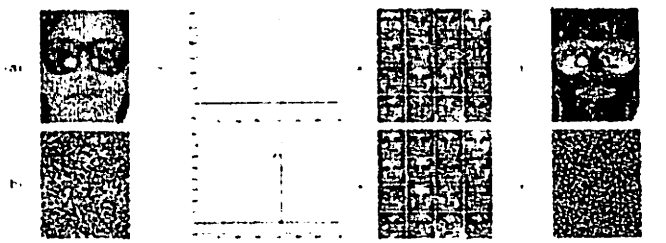
tasvirlanish vektori. Ushbu vektor ICA uchun to'plangan yuz bazalarining o'xshash bitlari orasidagi farq asosida hisoblanadi.



3.5-rasm. Yuz tasvirini u va b orqali hisoblash

Laplas yuzlar va chiziqsiz o'lchamni kamaytirish. Yuzlarni tanib olish uchun tasvirlarni qisqartirishda chiziqli akslantirishlardan foydalanishga nisbatan chiziqsiz akslantirishlardan foydalanish sifatli tasvirlarni qayd etadi. Bunda akslantirishlar lokal saqlash (LPP - locality preserving projections) algoritmi asosida amalga oshiriladi [49].

Siyrak tasvirlash asosida bardoshli yuzni tanib olish. PCA, LDA va shu kabi algoritmlarda yuzning barcha xususiyatlari e'tiborga olinadi, shuning uchun ham hisoblash tezligi yetarli darajada past bo'ladi. Vrixt [50] tomonidan taklif etilgan yuzlarni tanib olishda qo'llaniladigan siyrak kodlar algoritmi yuzning aynan kalit qismlarini yozib oladi va u orqali tanib olishni amalga oshiradi. Yuzda qo'shimcha to'siqlar paydo bo'lganda siyrak kodlash asosida amalga oshirilgan tanib olish tizimi samaradorligi kamayadi (3.6-rasm). Kirishdagi rasmga mos bazadan yuzni topadi va unga mos xususiyatlarni taqqoslaydi.



3.6-rasm. Siyrak kodlash asosida to'siq mavjud yuzni tanib olish

3.1-jadvalda PCA, ICA va LDA algoritmlarining tanib olish aniqligi keltirilgan [51]. Undan ko'rish mumkinki eng yaxshi ko'rsatkich PCA algoritmiga tegishli.

Xususiyatlarga asoslangan usullar. Ushbu usullar, tashqi ko'rinishga asoslangan usullardan farqli ravishda, tasvirlarni qayta ishlash, kompyuterning ko'rish qobiliyati va odam qiyofasiga xos bilimlar to'plamidan foydalanib amalga oshiriladi. Ushbu usullarga

Gabor to'lqin xususiyatlari va Lokal ikkilik namuna (LBP)ni keltirish mumkin.

3.1-jadval

Tashqi ko'rinishga asoslangan usullarga tegishli algoritmlarning tahlili

Algoritm nomi	Tanib olish aniqligi (%)
PCA	82,26
ICA	81,00%
LDA	78,08

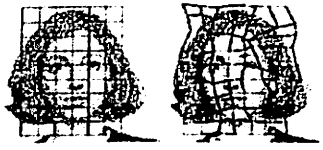
Elastik graflarni taqqoslash bilan Gabor to'lqin xususiyatlariga asoslangan algoritmlar. Lades [52] o'zining yuzni tanib olish ilovasida elastik graflardan xususiyatlarni topish, yuz modelini qurish va o'lchovlar orasidagi masofalarni hisoblashdan foydalangan. Ushbu holatda xususiyat mavjud nuqtadan lokal xususiyatlarni ajratib olish vazifasini Gabor to'lqinlari orqali amalga oshirilgan. Har bir nuqtadagi Gabor to'lqinlarining koeffitsentlar to'plami yuzni tanib olishda muhim rol o'ynaydi.

Graflarga asoslangan usullar ikki bosqichda amalga oshiriladi:

– I yuz tasviri uchun olingan tasvir graf g^I;

– ushbu yuz uchun tanlab olingan model graf g^M.

Ushbu ikki bosqich amalga oshirilishi uchun yuqori darajali o'lchovni anglatuvchi funksiya - $S(g^M, g^I)$ minimum qiymat qabul qilganda ham muhim ahamiyatga ega bo'ladi (3.7-rasm).

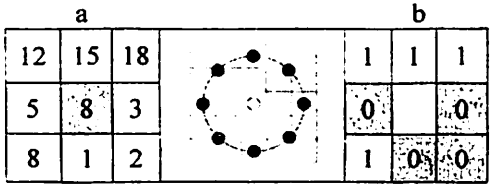


3.7-rasm. Yuzning graf modeli

Lokal ikkilik xususiyatlar (LBP) algoritmi. Gabor to'lqin xususiyatlarini qo'llagan holda yuz tasviridan lokal ikkilik namuna gistogramlarini ajratib olish va ular asosida muhim axborotga ega bo'lish taklif etilgan [53]. LBP algoritmi tasvirni 3×3 o'lchamda kesib oladi, matritsaning markazini belgilab, u asosida atrofidagi piksellarning qiymatlaridan yangi ikkilik xususiyatni shakllantiradi (3.8-rasm).

Yuzlarni tanib olishda LBPning 8×1 usulidan foydalanilganda 90%, 16×2 usulida esa, 70% natija qayd etiladi. Shuning uchun, yuqori

hisoblash imkoniyatiga ega kompyuterlardan foydalanilsa aniqlik va tezlik oshadi.



3.8-rasm. LBP nuqtalarini hisoblash

3.3-jadvalda Gabor to'lqin xususiyatlariga asoslangan va LBP algoritmining o'zgartirilgan algoritmlarining yuzlarni tanib olish aniqliklari keltirilgan [54]. Ushbu testlash ORL yuz bazalarida olib borilgan bo'lib, natijalar aynan ushbu yuz bazasining xususiyatlariga asoslangan. Bu yerda, GSF (Gabor Surface Feature) – gabor yuzasidagi xususiyatlar.

3.3-jadval

Xususiyatlarga asoslangan usullarning tahlili

Algoritm nomi	Tanib olish aniqligi (%)	
	Maxsus sharoitda	Real holatda
LBP	97	64
GSF	99,3	71,4

Namunalarga asoslangan usullar. Yuqorida keltirilgan ikki usul bazada saqlangan namunalar asosida xususiyatlar hosil qilinadi va tanib olish amalga oshiriladi. Yuzlar o'zgarishi bilan ularning yangisi bazada saqlanadi, bu esa, bazaning ortishiga olib keladi. Ular masofalarga va o'lchamlarga ko'p bog'liq emas, namunalarga asoslangan usullar esa, masofalarga bog'liq hisoblanadi. Namunalardagi o'xshash o'lchovlar yozib olinadi, o'rganiladi va keyinchalik taqqoslash uchun bazada yozib qo'yiladi. Bir nechta namunalardan foydalanishdan maqsad, ikki holatdagi yuzning o'xshash o'lchovlari yuzni tanib olishda qo'llaniladi. Aktiv namuna (AAM- Active Appearance Model) va Aktiv tashqi ko'rinish (ASM - Active Shape Model) [57] algoritmlari mazkur usul asosida amalga oshiriladi. Ushbu algoritmlar ishning yuzni aniqlash usullari qismida yoritilgan bo'lib, yuzning tashqi ko'rinishini ifodalashda qo'llaniladigan c parametr vektor tanib olishda asos bo'lib xizmat qiladi. Agar bazada mazkur odamning turli yoritilgan va

ko'rinishdagi holatlari mavjud bo'lsa, AAM uchun samarali vektorga erishishish mumkin.

Yuzning holatiga bog'liq holda sinflar tashkil etiladi va har bir sinf uchun o'lchov yaratiladi, hosil bo'lgan qiymatlar yuzni tanib olishda qo'llaniladi. Sinflar o'rtasidagi o'zgarishlarni aniqlash va tasvir o'lchamini kamaytirishda LDA algoritmidan foydalanish tanib olish samaradorligini oshirishi mumkin.

3.4-jadvalda AAM va ASM algoritmlarining 68 ta nuqta asosida tanib olish darajalari keltirilgan [56]. Ushbu algoritmlarning samaradorligini oshirish uchun yuz bazalaridagi yuzlarning turli ko'rinishdagi tasvirlarini ko'paytirish lozim.

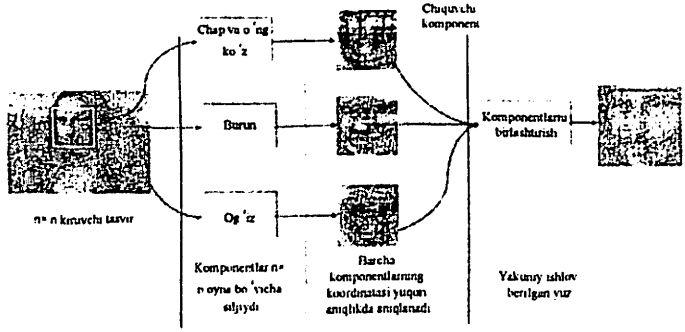
3.4-jadval

AAM va ASM algoritmlarining tahlili

Algoritm nomi	Tanib olish aniqligi (%)
AAM	69,8
ASM	74,5%

Qismlarga asoslangan usullar. Boshqa usullardan farqli ravishda yuzning yoki yuzdagi yorug'lik va holat o'zgargan qismlarining xususiyatlari asosida tanib olish amalga oshiriladi. Xususiyatlarga asoslangan usullardan farqi, yuzning faqat muhim qismlarini yozib oladi va mashina o'rganishi usullaridan foydalangan holda barcha qismlar birlashtiriladi.

Vektorlarni qo'llash (SVM- Support vector machine) asosida yuzni tanib olish algoritmi. Uch xil ko'rinishdagi yuz asosida ularning tuzilishi aniqlanadi va SVM (keyingi qismda ko'riladi) asosida tanib olish amalga oshiriladi.



3.9-rasm. Komponentlar yordamida yuzni tanib olish

Odatiy holatda yuz aniqlanganda tizimda bitta yuz qabul qilinadi, ammo, SVM orqali tahlil qilishda uchta yuz talab etiladi (3.9-rasm). Shuning uchun aniqlash jarayonida imkon qadar uchta va undan ko'p yuzni aniqlab bazaga yozib qo'yish talab etiladi. Chunki, bitta yuz orqali piksellardagi o'zgarishlarni aniqlash imkoni mavjud emas.

O'lchamga bog'liq bo'lmagan xususiyatlarni transformatsiyalash (SIFT- Scale-invariant feature transform) algoritmi obektlarni aniqlashda va tanib olishda juda samarali hisoblanadi [57]. Bunda odamlarni tanib olish kalit nuqtalarni sinflarga ajratish va o'zgarmas xususiyatlarni taqqoslash orqali amalga oshiriladi.

3.5-jadvalda SVM va SIFT algoritmlarining FERET yuz bazasida aniqlash darajalarining tahlili keltirilgan [58]. Ushbu algoritmlarning samaradorligini oshirish uchun samarali yuz bazalaridan foydalanish tavsiya etiladi.

3.5-jadval

SVM va SIFT algoritmlarining tahlili

Algoritm nomi	Tanib olish aniqligi (%)
SVM	77,5
SIFT	83,9%

Yuz xususiyatlarini ajratish va uni bazadagi qiymatlar bilan taqqoslash yuzni tanib olish jarayonining asosini tashkil etadi. Ko'pchilik hollardan yuz xususiyatlarini ajratish va tanib olish bosqichlari bitta qism sifatida o'rganiladi. 3.6-jadvalda yuzni tanib olishning mavjud usullari va ularning tavsifi keltirilgan [59].

3.6-jadval

Yuzni tanib olishning mavjud usullari va ularning tavsifi

Usullar	Tegishli algoritm	Tavsifi
1	**2**	**3**
Tashqi ko'rinishga asoslangan	Asosiy komponentalarni tahlillash	Xususiy yuzlar hosil qilinadi va ular tanib olishda qo'llaniladi.
	Chiziqli diskriminant tahlil	Fisher yuzni tanib olishda qo'llaniladi.
	Mustaqil komponentlarni tahlillash	Mustaqil komponentlarni ajratib oladi va ular asosida tanib olish amalga oshiriladi.

1	2	3
Tashqi ko'rinishga asoslangan	Laplas yuzlar	Aniqlangan qismlarning o'lchamini chiziqsiz kamaytirish.
	Siyrak kodlash	Siyrak tasvirlash uchun L1 minimallashtirish va mujassamlashtirilgan kodlar lug'atidan foydalaniladi.
Xususiyat-larga asoslangan	Gabor to'lqinlari va dinamik ulanish	Gabor xususiyatlari yuz joylashgan qismdan yuz xususiyatlarini birga-bir taqqoslash orqali ajratib olinadi.
	Gabor to'lqinlari va elastik graflarni taqqoslash	Gabor xususiyatlari yuz xususiyatlari joylashgan qismdan ajratib olinadi va bardoshli akslantirishlar birlashtiriladi.
	Lokal ikkilik xususiyatlar	Piksellarga mos holda o'lchami kichiklashtiriladi, yuz aniqlanadi va tanib olinadi.
Namuna-larga asoslangan	Aktiv namuna va aktiv tashqi ko'rinish	O'rganiluvchi xususiyatlarni sinflashtirish uchun aktiv namuna va tashqi ko'rinish parametrlari qo'llaniladi.
Qismlarga asoslangan	Vektorlarni qo'llash	Amaliyotda vektorlarni qo'llash har bir odam uchun samarali bo'lmasligi mumkin, shuning uchun global komponentlarni akslantirishdan foydalaniladi.
	Xususiyatlarni transformatsiyalash	Yuzlarni taqqoslashda o'lchamga bog'liq bo'lmagan xususiyatlarni transformatsiyalashning maxsus xususiyatlarini qo'llaydi.

3.7-jadvalda algoritmlarning tanib olish aniqligi va tanib olishning o'rtacha vaqtlari keltirilgan [60]. Ushbu jadval 3.6-jadval asosida shakllantirilgan va unda tegishli usullarga mansub sara algoritmlarning ko'rsatkichlari keltirilgan. Tahlil qo'llanilish sohasi va maqsadiga bog'liq holda mos algoritmni tanlash imkonini beradi.

3.7-jadval

Algoritmlarning tanib olish aniqligi va tanib olishning o'rtacha vaqti

Usul	Algoritm	Tanib olish aniqligi (%)	Tanib olishning o'rtacha vaqti (s)
1	2	3	4
Tashqi ko'rinishga asoslangan	Asosiy komponentalarni tahlillash	82,26	1,7

1	2	3	4
	Chiziqli diskriminant tahlil	81	
Tashqi ko'rinishga asoslangan	Mustaqil komponentlarni tahlillash	78,08	1,7
Xususiyatlarga asoslangan	Lokal ikkilik xususiyatlar	64	0,5
	Gabor to'lqinlari	71,4	
Namunalarga asoslangan	Aktiv namuna	69,8	1,3
	Aktiv tashqi ko'rinish	74,5%	
Qismlarga asoslangan	Vektorlarni qo'llash	77,5	0,4
	O'lchamga bog'liq bo'lmagan xususiyatlarni transformatsiyalash	83,9%	

Tashqi ko'rinishga asoslangan usullarga tegishli algoritmlarning ko'rsatkichi yuqori bo'lsada, tanib olish uchun ko'p vaqt sarflanadi. Shuning uchun, o'lchamga bog'liq bo'lmagan xususiyatlarni transformatsiyalash algoritmidan foydalanish maqsadga muvofiq.

Yuzni tanib olshi usullarining turli murakkab sharoitlardagi ko'rsatkichlari 3.8-jadvalda keltirilgan. Bunda 2 - yuqori aniqlikda yuzni tanib olish, 1 - gohida yuz bo'lmagan sohani ham yuz deb tanib olish va 0 - yuzni umuman taniy olmaslik [60].

3.8-jadval

Turli murakkab sharoitlarda yuzni tanib olish usullarining ko'rsatkichlari

Usullar / Xususiyatlar	Tashqi ko'rinishga asoslangan	Xususiyatlarga asoslangan	Namunalarga asoslangan	Qismlarga asoslangan
1	2	3	4	5
Ko'p odamlar mavjud tasvir	2	1	0	0
Tasvirning barcha qismi yuz terisi rangi bilan bir xil	0	0	1	0
Yuz tasvirining yon tomondan	1	1	0	1

1	2	3	4	5
ko'rinishi				
Yengsiz ko'ylak holatda	1	1	1	1
Yuzda to'siq mavjud	1	0	0	1
Aks qaytaruvchi ko'z oynak bilan	0	0	0	0
Noaniq tasvir	0	1	0	0
Bir xil rang	0	0	0	1

Jadvaldan ko'rinib turiptiki, tashqi ko'rinishga asoslangan yuzni tanib olish usuli turli hollarda ham yaxshi ko'rsatkichlarni taqdim etadi. Ammo, vaziyatga bog'liq holda har bir usulning afzalligi va kamchiligi mavjud bo'lib, ular 3.9-jadvalda keltirilgan [60].

3.9-jadval

Yuzni tanib olish usullarining vaziyatga bog'liq holda afzalligi va kamchiligi

Yuzni tanib olish usullari	Afzalligi	Kamchiligi
1	2	3
Tashqi ko'rinishga asoslangan	Yuzning ayrim qismlaridan axborot yig'ish, ularni qayta ishlash va shu asosida yuzni tanib olish amalga oshiriladi. Yuz to'liq ko'ringan holatda uning barcha qismini o'rganadi. Yorug'lik o'zgarishiga bardoshli.	Yuzning turli holatdagi tasvirlarini talab etadi. Xususiyatlarni ajratishda kuchsizlarini e'tiborga olmaydi. Ko'p vaqt va rusurs talab etadi.
Xususiyat-larga asoslangan	Ixtiyoriy holatdagi yuzdan Gabor to'lqinlari asosida kalit nuqtalar orasidagi masofalarni o'lchash imkoniyati mavjud. Yuzning old ko'rinishdan tanib olishda yuqori samara beradi.	Yuzning holati o'zgarishi tanib olish darajasini kamaytiradi. Bazada barcha ko'rinishdagi yuz tasvirlari bo'lishini talab etadi va bu baza hajmining ortishiga olib keladi.
Namunalarga asoslangan	Yuzdagi kalit nuqtalar va ular orasidagi masofalarga tayanadi. Ro'yxatga olish davomida yuz tasvirlarining ko'pligi yuqori darajali tanib olishni ta'minlaydi.	Yoritilganlikka ta'sirchan. Tanib olishdan oldin yuzning sinfi aniqlanadi, bu esa tanib olish vaqtining ortishiga olib keladi.

1	2	3
Qismlarga asoslangan	Yuz va orqa fon bir xil rang holatida bo'lganda ham tanib olishni amalga oshirish imkoniyati mavjud.	Yuzning to'rli yorug'lik, holat va ko'rinishdagi tasvirlari talab etiladi.

Bazadagi subyektlarga tegishli yuz tasvirlari sonining ko'pligi yuqori aniqlikni ta'minlasada, tanib olish vaqti yuqori. Aksariyat hollarda yuz tasviri xususiyatlarini ajratish va tanib olish jarayonlariga bitta bosqich sifatida qaraladi. Yuz tasvirini tanib olishning tashqi ko'rinishga, xususiyatga, namunaga va qismga asoslangan usullari mavjud. PCA algoritmi asosida yuz tasvirini tanib olishga ko'p vaqt sarflansada, tanib olish aniqligi yuqori (3.10-jadval).

3.10–jadval

Turli yuzlarni tanib olish algoritmlarining mavjud yuz tasviri bazalaridan olingan natijalari [60]

Yuz bazasi	**Yuzni tanib olish algoritmi**	**Tanib olish ko'rsatkichi (%)**
AR	PCA	55,4
	SVM + PCA	92,67
	SVM + ICA	94
	2D-PCA	96,1
ORL	PCA	90
	2D-PCA	96
	Takomillashgan 2D-PCA	98,33
	SVM + PCA	97
	Gabor + ICA	100
	PCA	80,5
	Fisherfaces + LBP	99,87
YALE	SVM + PCA	99,39
	PCA	88,1
	SVM + ICA	99,39
	2D-PCA	84,24
	PCA va 2D-PCA	92,3

Jadvalda keltirilgan natijalar maxsus sharoitlarda olingan tadqiqotlar asosida keltirilgan bo'lib, real holatga tatbiq etilsa, tanib olish aniqligi kamayadi. Shuningdek, yuz tasvirini tanib olishda quyidagi muammolar mavjudki, ularni bartaraf etish dolzarb hisoblanadi:

– tanib olish sifatini oshirish uchun turli holatdagi yuz tasvirlari talab etiladi;

– yuz tasviri bazalarining ko'payishi o'rganish va tanib olish vaqtini ortishiga olib keladi;

– yuz tasviri holatining o'zgarishi va undagi to'siqlar tanib olish natijasiga salbiy ta'sir etadi;

– yoritilganlikni o'zgarishi tanib olish aniqligini kamaytiradi;

– FAR va FRR xatoliklari yuqori, ya'ni o'rtacha xatolik darajasi 3,7% dan katta.

Shuning uchun tanib olish aniqligini oshirishda mashina o'rganishi usullaridan foydalanish o'rinli hisoblanadi.

Hozirda an'anaviy ko'rinishdagi yuz tasvirini tanib olish usullaridagi mavjud muammolarni bartaraf etishda sun'iy intellekt usullaridan keng foydalanilmoqda [88]. 3.11-jadvalda klassik va sun'iy intellekt usullarining aniqlik darajalari keltirilgan.

3.11-jadval

Klassik va sun'iy intellekt usullarining aniqlik darajalari

Usullar	**Aniqligi (%)**
Klassik	
Asosiy komponentlarni tahlillash	85,7
Sun'iy intellekt	
Neyron tarmoq	98,2
Svyortkali neyron tarmoq	99
Teran o'rganish	99,45

3.2. Yuz tasviri bo'yicha tanib olishning klassik usullari samaradorligini oshirish

Yuz tasvirini tanib olishning klassik algoritmlarining kamchiligi mavjud va ularni bartaraf etishda tadqiqotchilar tomonidan mavjud algoritmlarni mujassamlashgan holda qo'llash, ularning samaradorligini oshirish usullari va algoritmlari taklif etilgan. Mashinalarning hisoblash imkoniyati oshgani sari uning imkoniyatlaridan foydalanib, amallarni bajarish ommalashib bormoqda. Bu esa, sun'iy intellektual tizimlarining yuzaga kelishiga olib keldi.

Yuzlarni aniqlash va tanib olish samaradorligini oshirishda SVM, PCA, AdaBoost, mashina o'rganishi va neyron tarmoqlardan keng qo'llanilib kelinmoqda.

SVM (Support Vector Machines). Yuzni tanib olish tizimlari bazasida minglab odamlarning turli ko'rinishdagi tasvirlari saqlanadi. Kamera tomonidan tasvirga olingan rasmdan odamni tanib olish uchun, ushbu odamga tegishli ma'lumotlar barcha bazadagi yuz tasvirlariga taqqoslab chiqiladi. Ushbu holatda bazadagi yuz tasvirlarini saralash muammosi yuzaga keladi. SVM ushbu yuz tasvirlarini ro'yxatga olish mobaynida saralaydi va tanib olishda faqatgina o'ziga tegishli yuz sinfiga murojaat etadi. SVMning ikkinchi jihati, faqatgina o'ziga tegishli yuz tasvirini ikkilik ko'rinishga o'tkazadi va boshqa ko'rinishlarini shu orqali hisoblab chiqaradi. Ko'pchilik yuzni tanib olish algoritmlari tashqi ko'rinish yoki yuz sohasiga asoslanadi. SVM esa, ayni bir odamning ikkita yuzini taqqoslab, muhim qiymatlarini ajratib olish asosida amalga oshiriladi [20].

Shuning uchun SVM algoritmi uchun qiymatlar aynan mana shu ikki sinf orasidan tanlab olinadi va $\{x_i, y_i\}$ qiymatlar to'plamini qabul qiladi. Bu yerda, x_i – yuz ma'lumoti, y_i esa, -1 yoki 1 qiymat qabul qilib, ma'lumotning xususiyatini anglatadi. SVMning chiqishi N_s madadlash vektorlaridan iborat qiymat ko'rinishida aks etadi. Har bir qiymat o'z xususiyati, og'irligi va o'zgarmas kattaliklariga ega (3.10-rasm).

a. FERET ma'lumotlar bazasidagi yuz tasviri

b. SVM qayta ishlanishidan keyingi yuz tasviri

3.10-rasm. SVM uchun tanlab olingan yuz tasviri

PCA (Principal Components Analysis). Yuzlarni tanib olish usullari va algoritmlari bilan tanishish qismida PCA algoritmi haqida batafsil ma'lumot keltirilgan. Mazkur algoritmning asosiy vazifasi xususiy vektor va uning qiymati asosida yuzni tanib olish samaradorligini oshirishdan iborat. U namunalarni tanib olishning sun'iy intellekt algoritmlari turiga tegishli. Uning afzalliklaridan biri ma'lumotlar ichidan zarur namunani barcha namunalarning o'lchamlarini kamaytirish orqali topish. Unda grafik ma'lumotlarni qayta ishlash majburiyati mavjud emas. Namunalarni raqamli

ko'rinishda qayta ishlovchi va ma'lumotlarni tahlillovchi eng yaxshi vosita.

Adabust. Yuzni tanib olishning dastlabki bosqichi yuzni aniqlash samaradorligini oshirishda qo'llaniladi. Viola Jones kabi yuzni aniqlash algoritmlaridagi kuchsiz parametrlarga qo'shimcha qiymatlar kiritadi va uning imkoniyatlarini oshiradi [14]. Yuzni aniqlash uchun to'plangan barcha tasvir uchun og'irlik belgilanadi va shu asosida aniqlash samaradorligi ortadi. Ammo, kuchsiz parametrlarni ham saqlab qo'yish zarur, chunki kuchsiz va kuchli qiymatlar asosida olingan natijalar birlashtiriladi. Bu aniqlash ishonchliligini oshiradi.

Parallel hisoblash. Yuz qismlarini alohida hisoblash maxsus protsessorlardan foydalangan holda amalga oshiriladi. M×N o'lchamli yuzni o'rganishda tasvir 24×24 o'lchamli oynalarga ajratiladi. Shundan so'ng, CPU va GPUning imkoniyatidan kelib chiqqan holda, bir nechta qismlarga bo'lib, parallel hisoblash bajariladi. Mazkur usul tanib olish aniqligini oshirmasada, jarayon uchun sarflanadigan vaqtni kamaytiradi [61].

Mashina o'rganishi. O'rganish tasvirlar soni ko'pligi yuzni tanib olish va aniqlash jarayoni yuqori aniqlikda bajarilishini ta'minlab beradi. Shuning uchun bir yuzning turli ko'rinishdagi tasvirlari (8-20 ta) o'rganiladi. Ushbu tasvirlarni saralash va o'rganish mashina va insonning faol ishtirokini talab etadi. Shu kabi muammolarni hal etish va inson ishtirokini kamaytirish maqsadida mashina o'rganishi algoritmlari va texnologiyalari ishlab chiqilgan [62]. Mashina o'rganishi algoritmlari ayni yuzning turli ko'rinishdagi tasvirlarini qayta ishlash asosida uning muhim parametrlarini ajratib oladi va keyingi jarayon uchun bazada saqlab qo'yadi.

Mashina o'rganishi inson ishtiroki asosida statik va inson ishtirokisiz dinamik bo'lishi mumkin [63]. Statik ko'rinishda yuzning qismlarini belgilashda yoki yuz mavjud tasvirlarni saralashda inson ishtirokini talab etishi mumkin. Bu ko'p vaqt sarfini talab etsada, yolg'ondan qabul qilish va rad etish xatolik darajalari juda kichik bo'ladi. Dinamik ko'rinish tezligi ancha yuqori, inson ishtirokini talab etmaydi va yolg'ondan qabul qilish va rad etish darajalari katta bo'lishi mumkin. Ikki usul ham bir maqsadda yuz tasviridan xususiyatlarini ajratib olish va ulardan yuzni tanib olishda qo'llaniladi.

Mashina o'rganishining matematik asoslashda X qiymat va uning sinfi C parametrlaridan foydalaniladi. Bunda $P(C,X)$ nuqtaning yuzga tegishlilik ehtimolligini anglatadi. Nuqtaning asosiy xususiyatini

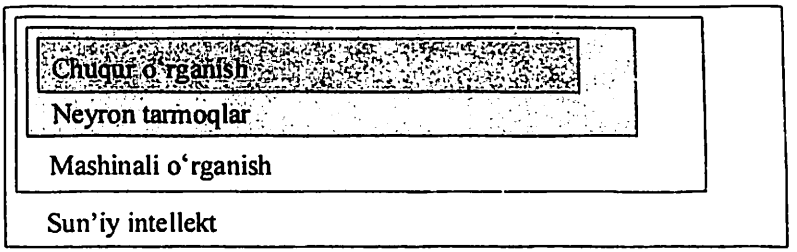
aniqlashda C ning ahamiyati yuqori. Shuning uchun nuqtaning ehtimolligini aniqlashda parametr algebrasidan foydalanish samaradorlikni oshiradi. Bunda, $P(C,X|\theta)$ parametr model mos keladi. Olingan ehtimolliklar $P(C,X)$ va $P(C,X|\theta)$ ko'rsatilgan shartni qanoatlantirgan holda bitta guruhga tegishli bo'lsa, unda mos keladi, aks holda mos kelmaydi. Umuman olganda quyidagi tenglik bajarilishi lozim:

$$P(C,X) = P(C,X|\theta).$$

Bu yerda, θ – nutaga qo'shilgan shovqin.

Ma'lumotlar belgili va belgisiz bo'ladi. Belgisiz ma'lumotlar bilan ishlashdan oldin uni saralash amalga oshirilishi lozim. Ma'lumotlarni saralashda turli sinflashtirish algoritmlaridan foydalaniladi. Bunda, yuzni tanish algoritmi orqali saralashni amalga oshirish tanib olish samaradorligini oshiradi. Chunki, maxsus saralash algoritmlari tanib olish jarayoni uchun muhim bo'lgan ma'lumotlarni qoldirib ketishi mumkin.

Sun'iy intellekt usullarining shajaraviy ketma-ketligi 3.11-rasmda tasvirlangan.



3.11-rasm. Sun'iy intellekt usullari

Mashina o'rganishi usullar yuzlarning turli holatdagi (asosan barcha holatdagi yuzlar) tasvirlariga asoslangan va ularning ichida chuqur o'rganish (deep learning) ga asoslangan usullar eng yuqori natijani qayd etadi. Ammo, ularda quyidagi muammolar mavjudki, ularni bartaraf etish muhim vaziflardan hisoblanadi:

– yuzning barcha holatlari asosida yuz bazasini shaklantirish;

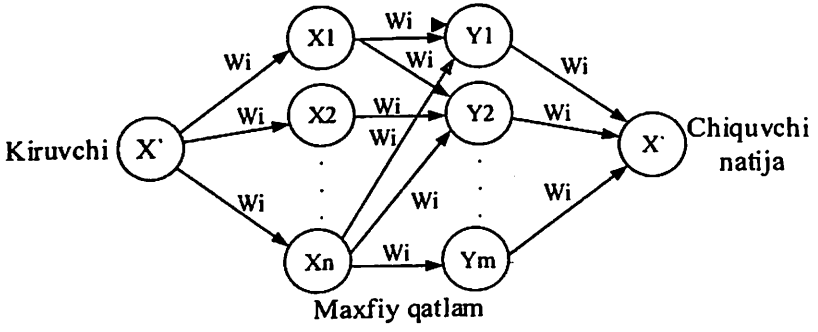
– yuzda to'siqlar hosil bo'lishi;

– chuqur o'rganishga asoslangan tarmoqlarda qo'llaniladigan filtrlar hisoblash mashinalariga yuklanishni yuzaga keltiradi va ko'p vaqt sarflanadi;

– yangi yuzni o'rganish uchun ko'p vaqt talab etiladi.

3.3. Yuz tasvirini tanib olishning neyron tarmoqlarga asoslangan usuli

Neyron tarmoqlar mashina o'rganishining asosiy usullaridan biri hisoblanadi [6]. U aniq va noaniq, hamda, chiziqli va chiziqsiz ma'lumotlar oqimini sinflashda eng samarali usullardan hisoblanadi. Neyron tarmoqlar nafaqat yuzlarni tanib olish tizimlarida, balki ovoz, barmoq izlari, ko'z va boshqa shu kabi tanib olish tizimlarida ham qo'llaniladi. 3.12-rasmda neyron va uning og'irligi aks ettirilgan.



3.12-rasm. Neyronlar va ularning og'irligi

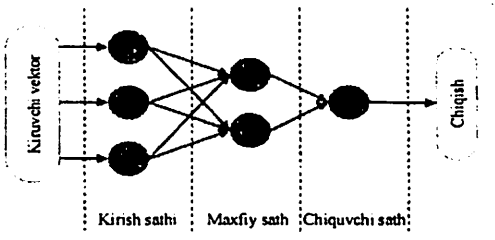
Ikkinchi qatlamdagi neyronning qiymati birinchi qatlamdan kelayotgan neyronlar, ularga mos og'irliklarini yig'indisi orqali aniqlanadi.

$$Y_2 = X_1 * W_i + X_2 * W_i + X_n * W_i$$

Bu yerda, X_1, X_2 va X_n – neyronga kiruvchi qiymatlar, W_i – neyron og'irligi.

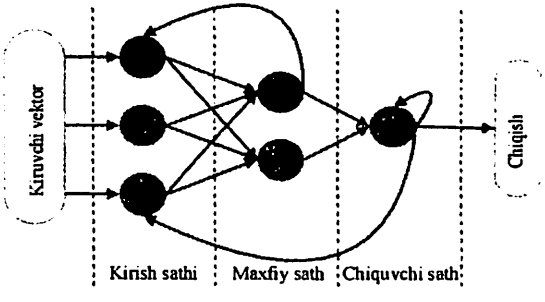
Neyron tarmoqlar oldinga harakatlanuvchi va takrorlanuvchi katta guruhlarga bo'linadi:

Oldinga harakatlanuvchi neyron tarmoqlar kirish, chiqish va maxfiy qatlam elementlaridan tashkil topgan (3.13-rasm). Hisoblashlar bitta yo'nalish bo'ylab amalga oshiriladi. Har bir kiruvchi qiymat neyron og'irligi asosida hisoblanadi va keyingi qatlamga o'tkaziladi. Keyingi qatlamda esa, dastlabki kabi hisoblashlar amalga oshiriladi va yakuniy natija chiqquncha davom etadi. Ushbu tur neyron tarmoqlar: chiziqli, chiziqli bo'lmagan va radial asos funksiyali turlarga bo'linadi [64].



3.13-rasm. Oldinga harakatlanuvchi neyron tarmoqlar

Takrorlanuvchi neyron tarmoqlarda neyronlarning harakati bir xilda emas, o'zgaruvchan yo'nalishda harakatlanadi (3.14-rasm). Ya'ni, neyronlardan biri orqaga siljiydi va hisoblashda takror qo'llaniladi. Shuning uchun ushbu guruh neyron tarmoqlar uchun ichki soha yaratiladi va u yerda bir nechta dinamik hisoblashlar amalga oshiriladi. Qaytgan neyronlar asos yo'nalish orqali uning barcha qadamlarida bir xilda davom etadi.



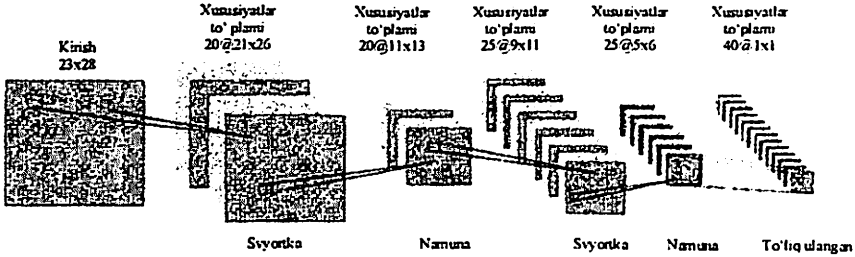
3.14-rasm. Takrorlanuvchi neyron tarmoqlar

Bundan tashqari, bir qatlamli va ko'p qatlamli neyron tarmoqlar mavjud. Bir qatlamli neyron tarmoq maxfiy qatlamida bir marta hisoblash amalga oshiriladi. Ko'p qatlamli neyron tarmoqda esa, maxfiy qatlamda bir nechta qadamlar asosida hisoblashlar amalga oshiriladi.

*Svyortkali neyron tarmoq (*SNT*)* – neyron tarmoqlarning takomillashgan ko'rinishi hisoblanib, uning neyron tarmoqlardan farqi, unda mantiqiy maxfiy qatlamlarda filtrlarni qo'llash imkoniyatining mavjudligi hisoblanadi. Svyortkali neyron tarmoq ichida bir nechta, o'zaro bog'langan, ikki o'lchamli massivlar hosil qilinadi va ularning umumiy og'irligi o'rganiladi. O'rganish iyerarxik ko'rinishda amalga oshiriladi. 3.15–rasmda keltirilgan 23×28 tasvir bir nechta (21×26, 11×13 va boshqa) filtrlar orqali tekislanadi va natijada 40 ta bir

o'lchamli massiv hosil qilinadi. Mazkur massiv keyinchalik yuzni tanib olishda qo'llaniladi.

Svyortkali neyron tarmoq: svyortka, padding, to'liq ulangan va normallashtirish bosqichlaridan tashkil topgan. $W \times H \times N$ o'lchamli qatlam uchun: W – tasvir eni, H – balandligi, N – filtrlar sonini anglatadi.



3.15-rasm. Svyortkali neyron tarmoq

Chuqur o'rganish svyortka, puling, qo'shish yoki ayirish (padding) va to'liq ulangan qatlamlardan tashkil topgan. Svyortka qatlami SNT va chuqur o'rganishga asoslangan SNT uchun asosiy bosqich bo'lib, u filtrlar asosida barcha sohalardan xususiyatlarni ajratib olishga qaratilgan. Har bir filtr bo'yi va enidan kelib chiqib, kichik qiymatlarga ega i-xususiyatlar to'plamini tasvirlash uchun $x_i^{(l)}$ dan foydalaniladi.

$$x_j^{(l+1)} = s(\sum_i F_{ij}^{(l)} * x_i^{(l)} + b_j^{(l)})$$

Bu yerda, $x_j^{(l+1)}$ – chiquvchi qiymat, $F_{ij}^{(l)}$ - $x_i^{(l)}$ ga bog'langan filtr, l – sath, $b_j^{(l)}$ - j-chiquvchi xususiyatlar to'plami uchun og'ish vektori (bias), $s()$ – 2D raqamli svyortkani ifodalovchi chiziqsiz funksiya [65]. DL asosida yaratilgan yuzni aniqlash tizimi 140×140 o'lchamli tasvirlardan 97,45% aniqlikda yuzlarni aniqlay oladi. COCO funksiyasidan foydalanib yaratilgan, DL yuzni aniqlash usuli 99,86% aniqlikni ta'minlaydi [66]. 3.12-jadvalda klassik va sun'iy intellektual usullarining aniqlik darajalari keltirilgan.

3.12-jadval

Klassik va sun'iy intellektual usullarining tahlillash

Usul	Aniqligi (%)
Asosiy komponentlarni tahlillash	85,7
Neyron tarmoq	90,2
Svyortkali neyron tarmoq	96%
Chuqur o'rganish	97,45

Chuqur o'rganish usullari yuqori aniqlikka ega, ammo namunalarni o'rganish va tanib olish uchun ko'p vaqt sarflanadi. Uni kamaytirish uchun parallel hisoblash imkoniyatlari va grafik protsessordan foydalanish lozim.

3.13-jadval

Turli o'lchamdagi tasvirlardan yuzni aniqlash va tanib olishning grafik va markaziy protsessorlarda sarflangan vaqti

		Tasvir o'lchami					
		480*360		650*400		700*580	
		GPU	CPU	GPU	CPU	GPU	CPU
Yuzni aniqlash	**Sarflangan vaqt (ms)**	102	780	160	900	350	1406
Yuzni tanib olish		90	207	127	279	312	300

Testlash va tanib olish jarayonlarida ikki namuna o'rtasidagi farq asosida yuz kimga tegishli ekanligini aniqlash mumkin. Ushbu namunadagi bir xil nuqtalar orasidagi masofalar bazada saqlab qo'yiladi va test yuz tasviri bilan taqqoslanadi [89]. Masofalarni o'lchash yuzni tanib olishdagi eng oxirgi jarayon hisoblanadi. U asosida o'rganish va testlashdagi yuz tasvirlari orasidagi farqni aniqlash mumkin. Test tasviri qaysi namuna bilan eng kichik masofaga erishgani, uning shu namuna bilan bir odamga tegishligini anglatadi. Boshqa tomondan o'rganish, hamda test yuzlar asosida namunalar hosil qilinadi va ushbu namunalar orasidagi farq o'lchanadi. Yuzlar orasidagi farqlarni hisoblashda quyidagi usullardan foydalaniladi [67]:

Evklid masofa. Ikki nuqta orasidagi masofani o'lchashga qaratilgan usuldir. U Pifagor teoremasi asosida amalga oshiriladi. Bazadagi namuna va test yuz orasidagi masofalar taqqoslanadi, masofaga mos holatda sinflashtiriladi va qaysi tasvirlar orasidagi farq eng kichik bo'lsa, demak, yuzlar bir xildir. Evklid masofa quyidagi formular orqali aniqlanadi:

$$d_2(x,y) = \sqrt{\sum_{i=1}^{l} |x_i - y_i|^2}$$

Bu yerda, x_i – test tasviridagi nuqta, y_i - o'rganish tasviridagi nuqta, l – xususiyatlar soni.

Kvadratik Evklid masofasi. Ushbu masofa Yevklid masofasiga o'xshash, farqi, kvadrat hisoblanadi, ammo ildiz hisobga olinmaydi.

$$d_2(x,y) = \sum_{i=1}^{l} |x_i - y_i|^2$$

Manhetten masofasi. Shahar bloki, L1 masofa, L1 normasi nomlari bilan keng tarqalgan usullardan biri bo'lib, shaharning ma'lum yo'llari chegarasida yotuvchi nuqtalar orasidagi masofalarni o'lchashga qaratilgan. Ikki obyekt koordinatalari orasidagi farqni aniqlashga mo'ljallangan.

$$d_1(x,y) = \sum_{i=1}^{l} |x_i - y_i|$$

Chebishev masofasi. Ikki nuqta orasidagi eng katta masofani aniqlashga qaratilgan usul. U $L\infty$ ko'rinishida ham keng tarqalgan.

$$lim_{l\to\infty}(\sum_{i=1}^{l} |x_i - y_i|^l)^{1/l}$$

Yuqorida keltirilgan barcha yuz xususiyatlari farqini aniqlash usullari PCA algoritmi yordamida aniqlangan nuqtalar orasidagi masofalarni o'lchashda va ularni darajasi bo'yicha taqqoslashda qo'llaniladi. Olingan masofalarning kichikligi o'rganish va testlash yuzining bir odamga tegishli ekanligini isbotlaydi.

Yuz asosida autentifikatsiyalash tizimlarida yuzning faqatgina old ko'rinishdagi namunasi qo'llaniladi va yuzning yuzlab xususiyatlari orasidagi farqni aniqlashga ehtiyoj tug'ilmaydi. Shuning uchun Geodezik masofa kabi osonroq hisoblanadigan usullardan foydalanish

mumkin. Buning uchun yuzning kalit nuqtalari: burun, og'iz, ko'zlarni aniqlash va ular orasidagi masofani o'lchash yetarli hisoblanadi.

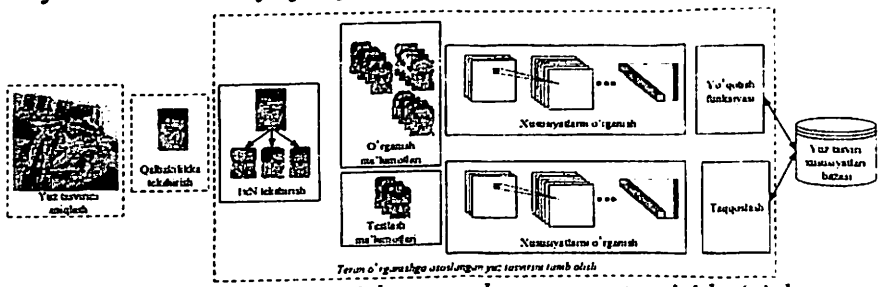
Yuqorida keltirilgan yuz xususiyatlari orasidagi farqlarni hisoblash usullari ichida Evklid va kvadratik Evklid eng samarali usullar hisoblanadi. Shuningdek, ular adabiyotlarda birinchi va ikkinchi normalar nomi ostida ham qo'llaniladi. Manhetten masofasi ikki nuqta o'rtasidagi farqlarni hisoblab, oddiy yig'indi asosida jamlanadi. Chebishev masofasi esa, olingan natijani xususiyat soniga qarab, tekislashga qaratilgan [90].

IV BOB. NEYRON TARMOQLARGA ASOSLANGAN YUZ TASVIRI BO'YICHA IDENTIFIKATSIYALASH TIZIMI

4.1. Teran o'rganishga asoslangan yuz tasviri bo'yicha identifikatsiyalash jarayonining sxemasi

Teran o'rganish usullari yuqori aniqlikka ega, ammo namunalarni o'rganish va tanib olish uchun ko'p vaqt sarflanadi, shuningdek, FAR va FRR xatoliklari yuqori [68]. Ularni kamaytirish uchun parallel hisoblash usullari [91] va grafik proesessordan foydalanish yuqori samara beradi. Sh.X.Fozilov va T.S.Jumayevlarning A5 deb nomlangan algoritmi asosida yuz tasviri bo'yicha tanib olishda 83% aniqlikni ko'rsatgan. Shuningdek, 24 ta xos sonlar va Gabor filtrlaridan foydalanilganda 92% aniqlikka erishilgan, ammo hisoblash parametrlari soni ortishi evaziga tezlik pasayadi [15].

4.1-rasmda taklif etilgan teran o'rganishga asoslangan yuz tasviri bo'yicha identifikatsiya jarayoni sxemasi keltirilgan.



4.1-rasm. Teran o'rganishga asoslangan yuz tasviri bo'yicha identifikatsiya jarayoni sxemasi

Teran o'rganishga asoslangan yuz tasviri bo'yicha identifikatsiya jarayoni sxemasi quyidagi bosqichlardan tashkil topgan:

Yuz tasvirini aniqlash: yuz tasvirini aniqlash uchburchak usuli asosida amalga oshiriladi.

Qalbakilikka tekshirish: rasm asosida qalbakilashtirilgan yuz tasviri piksel usuli asosida aniqlanadi.

Teran o'rganishga asoslangan yuz tasvirini tanib olish: unda $1 \times N$ tekshirishdan foydalaniladi. O'rganish ma'lumotlari asosida yangi foydalanuvchi qo'shiladi va testlash ma'lumotlaridan tanib olishda foydalaniladi. Xususiyatlarni o'rganish teran o'rganish tarmoqlari asosida amalga oshiriladi. Yo'qotish funksiyasi muhim xususiyatlarni ajratishda qo'llaniladi va ular keyinchalik taqqoslash uchun

foydalaniladi. Barcha xususiyatlar yuz tasviri xususiyatlari bazasida saqlanadi.

Teran o'rganish svyortka, puling (pooling), qo'shish yoki ayirish (padding) va to'liq ulangan qatlamlardan tashkil topgan. Svyortka qatlami SNT va teran o'rganishga asoslangan SNT uchun asosiy bosqich bo'lib, u filtrlar asosida barcha yuz tasviri sohalaridan xususiyatlarni ajratib olishga xizmat qiladi [69].

Teran o'rganishga asoslangan yuz tasvirini tanib olishda *Aleks. vizual geometriya guruhi, Google, rezident va zichlash-faollashtirish* tarmoqlari asosiy o'rin tutadi [70].

Teran o'rganish tarmoqlari yuz tasvirining turli holatdagi (asosan barcha holatdagi yuz) tasvirlariga asoslangan. Mazkur sohada quyidagi muammolar mavjud:

– yuz tasvirining barcha holatlari asosida yuz tasviri bazasini shaklantirishning murakkabligi;

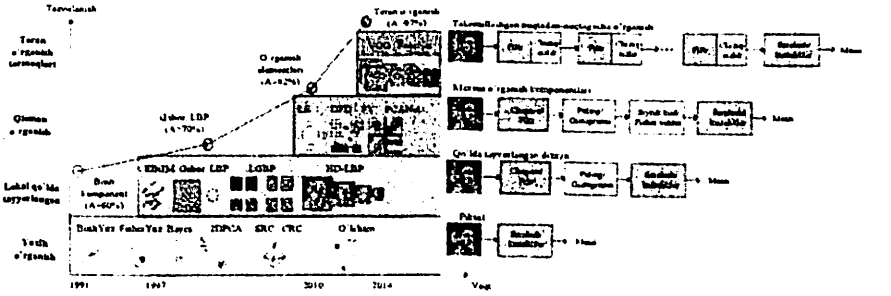
– yuz tasvirida to'siqlar paydo bo'lishi;

– teran o'rganishga asoslangan tarmoqlarda qo'llaniladigan filtrlar hisoblash mashinalariga yuqori yuklanishni yuzaga keltirishi;

– yangi yuz tasvirini o'rganish uchun ko'p vaqt talab etilishi.

Ushbu muammolarni bartaraf etish yuz tasvirini tanib olish samaradorligini oshirish bilan bog'liq.

Teran o'rganish tarmoqlari yuz tasvirini tanib olish sohasida ixtiyoriy sharoitda yuqori natijalarga erishish mumkinligi ko'rsatib berdi. 4.2-rasmda yuz tasvirini tanib olish usullari va algoritmlarining rivojlanish dinamikasi keltirilgan bo'lib, unda klassik usullar, xususiyatlarni o'rganishga ilk qadam va teran o'rganish usullarigacha aniqlik darajasi (A) bo'yicha tasvirlangan.



4.2-rasm. Yuz tasvirini tanib olish usullari va algoritmlarining rivojlanish dinamikasi

2014 yildan boshlab teran o'rganish tarmoqlari yaratila boshlangan. O'rganish xususiyatlari filtrlar yordamida chiziqsiz ko'rinishga keltiriladi. Ushbu jarayon bir necha marta takrorlanganligi bois, ko'p sonli kuchli xususiyatlarni ajratishga erishiladi. Natijada tanib olish aniqligi ortadi. Oxirgi paytlardagi ilmiy ishlar natijalari tanib olish aniqligining 99% dan ortganini ko'rsatmoqda [70] (4.1-jadval).

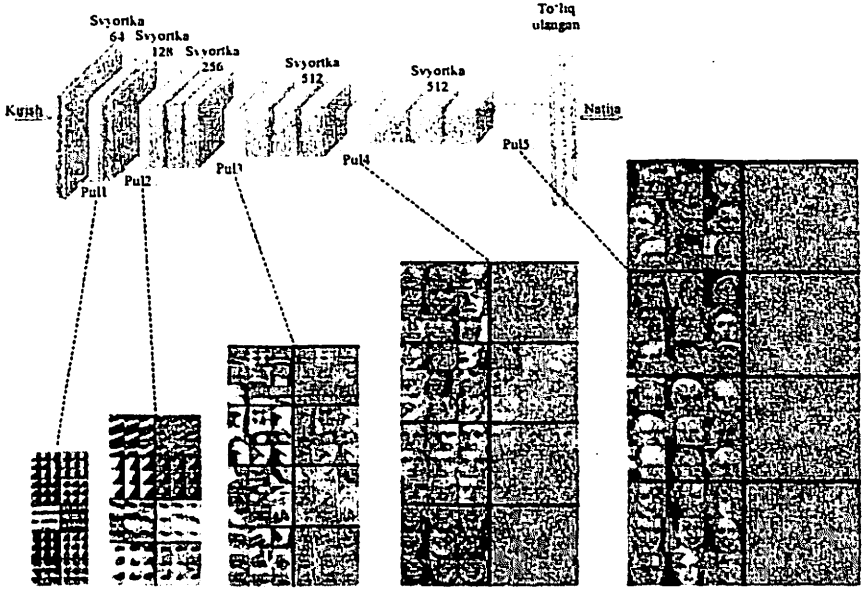
4.1-jadval

Teran o'rganishga asoslangan yuz tasvirini tanib olish aniqligi va uning xususiyatlari

Usul	E'lon qilingan vaqti	Yo'qotish funksiyasi	Arxitektura	Tarmoqlar soni	Ma'lumotlar bazasi	Aniqligi (%)
1	2	3	4	5	6	7
Light SNN	2015	Softmax	Light SNN	1	MS-Celeb-1M	98,8
Center loss	2016	Center loss	Lenet+-7	1	CASIA-WebFace, CACD2000, Celebrity+	99,28
L-softmax	2016	L-softmax	VGGNet-18	1	CASIA-WebFace	98,71
Range loss	2016	range loss	VGGNet-16	1	MS-Celeb-1M, CASIA-WebFace	99,52
L2-softmax	2017	L2-softmax	ResNet-101	1	MS-Celeb-1M	99,78
Normface	2017	contrastive loss	ResNet-28	1	CASIA-WebFace	99,19
vMF loss	2017	vMF loss	ResNet-27	1	MS-Celeb-1M	99,58
Marginal Loss	2017	Marginal Loss	ResNet-27	1	MS-Celeb-1M	9,48
SphereFace	2017	A-softmax	ResNet-64	1	CASIA-WebFace	99,42
CCL	2018	center invariant loss	ResNet-27	1	CASIA-WebFace	99,12
AMS loss	2018	AMS loss	ResNet-20	1	CASIA-WebFace	99,12

1	2	3	4	5	6	7
Cosface	2018	Cosface	ResNet-64	1	CASIA-WebFace	99,33
Arcface	2018	Arcface	ResNet-100	1	MS-Celeb-1M	99,83
Ring loss	2018	Ring loss	ResNet-64	1	MS-Celeb-1M	99,5

Teran o'rganish tarmoqlarida filtrlar yordamida ishlov berilgan har bir qadam svyortkalash deb nomlanib, filtrlar soni uning nechtaligini aniqlaydi. Masalan, 24×24×64 o'lcham keltirilgan. Bitta tasvir o'lchami 24×24 va 64 ta filtrdan tashkil topgan. Puling (pul) jarayoni orqali uning o'lchami kamaytiriladi. 4.3-rasmda bir nechta qadamdan iborat teran o'rganish tarmog'i tasvirlangan. Har bir qadamda puling va svyortkadan keyin hosil bo'lgan tasvirlarning ko'rinishini tasavvur etish mumkin. Oxirgi qadamlarda kuchli xususiyatlar soni ortadi va kuchsizlari tashlab ketiladi. To'liq ulangan tarmoq kuchli xususiyatlarni yanada saralaydi va u bitta yoki bir nechta bo'lishi bo'ladi.



4.3-rasm. Teran o'rganish tarmog'ining iyerarxik arxitekturasi

Yuz tasvirini o'rganish tarmoqlari yuz tasvirining turli holatda va ko'rinishda bo'lishini talab etadi. Yuz tasvirining bo'lishi mumkin bo'lgan barcha holatlarining qamrab olinganligi tanib olish aniqligining oshishiga olib keladi. Turli ko'rinishdagi yuz tasvirlari birga-ko'p va ko'pga-bir usulda shakllantiriladi.

Birga-ko'p. Yuz tasvirining bir nechta ko'rinishlari mavjud va ular asosida bitta shaxsning yuz tasviriga tegishli xususiyatlar hosil qilinadi.

Ko'pga-bir: Shaxsning old holatdagi yuz tasviri mavjud va u asosida boshqa ko'rinishdagi yuz tasvirlari shakllantiriladi.

Hosil qilingan yuz tasviri o'rganish uchun tarmoqqa kiritiladi. Tarmoqlar ikki turdagi arxitekturaga ega:

– Asos tarmoq: AlexNet, VGGNet, GoogleNet, ResNet, SENet, mahsus va mujassamlashgan arxitekturali.

– Bir nechta tarmoq: ko'p ko'rinishli, ko'p qismli va ko'p vazifali.

4.2-jadvalda yuz tasvirini qayta ishlash yondashuvlari va algoritmlari keltirilgan.

4.2-jadval

Yuz tasvirini qayta ishlash yondashuvlari va algoritmlari

Yuz tasvirini qayta ishlash	**Algoritmlar**	**Tavsifi**
Birga-ko'p	SAE, CNN, GAN	Turli ko'rinishdagi yuz tasvirlaridan asos yuz tasviri shakllantiriladi.
Ko'pga-bir	3D model, 2D teran model, tasvirlarni ko'paytirish	Bitta yuz tasviridan turli ko'rinishdagi yuz tasvirlarini shakllantiriladi.

Tarmoqdan chiqqan xususiyatlar saralash uchun yo'qotish funksiyasiga yuboriladi. Olingan kuchli xususiyatlar yo'qotish funksiyasi yordamida saralanadi va natijalar bazada saqlanadi. Quyidagi turdagi yo'qotish funksiyalari mavjud [70]:

– Evklid masofasiga asoslangan yo'qotish funksiyasi;

– Burchak kosinusiga asoslangan yo'qotish funksiyasi;

– Softmax yo'qotish funksiyasi va uning ko'rinishlari.

4.2. To‘siq mavjud yuz tasvirini normallashtirish usuli

Uchburchak usuli asosida aniqlangan yuz tasviri tanib olish bosqichiga o‘tkaziladi. Tanib olishda qo‘llaniladigan, yuqori aniqlik darajasiga ega teran o‘rganish usullari ma’lum yuz tasviri bazalari asosida o‘rganiladi. Yuz tasvirini tanib olish algoritmlarining ishlash samaradorligini testlashda qo‘llaniladigan ko‘pchilik bazalarda yuz tasvirida mavjud to‘siqlar e’tiborga olingan. Lekin, yuz tasvirini tanib olishda tasodifiy paydo bo‘ladigan to‘siqlar ham mavjudki (4.4-rasm), ularning barchasini yuz tasviri bazalariga kiritish imkoniyati yo‘q.

Shuning uchun aniqlangan yuz tasvirini tanib olish bosqichiga o‘tkazishdan avval uni ishlash talab etiladi. To‘siq mavjudligi aniqlangan yuz tasvirini tanib olishda lokal xususiyatlarga, siyrak kodlashga va ajratilgan to‘siqlarni tahlillashga asoslangan usullardan foydalaniladi [16].

4.4-rasm. Tasodifiy to‘siqlar

To‘siq mavjud yuz tasvirini tanib olish algoritmlarining qiyosiy tahlili 4.3-jadvalda keltirilgan.

4.3-jadval

To‘siq mavjud yuz tasvirini tanib olish algoritmlarining qiyosiy tahlili

Xatoliklar (%) / Algoritmlar	FAR	FRR
Chegaralarni tekshirish algoritmi	16,67	0
Gabor to‘lqini va geometrik tahlillash algoritmi	8,33	25
Teri rangi darajasi algoritmi	29,17	8,33
Vektorlarni qo‘llash orqali to‘siqlarni aniqlash algoritmi	72,22	16,67

Demak, to‘siq mavjud yuz tasvirini tanib olish algoritmlarida xatolik darajasi yuqori va ularni minimallashtirish uchun avval to‘siq mavjud yuz tasvirini normallashtirish lozim.

Quyida to'siq mavjud yuz tasvirini PCA algoritmi [71] asosida *normallashtirish* usuli ishlab chiqildi. Ushbu usul uchta bosqichdan iborat:

– yuz tasviri sinfini aniqlash;
– normal yuz tasvirlarini hosil qilish;
– kiruvchi yuz tasvirini normallashtirish.

Yuz tasviri sinfini aniqlash quyidagi qadamlardan iborat:

1. Aniqlangan yuz tasvirini 4.5-rasm asosida tegishli sinfi (old, o'ng va chap tomon) aniqlanadi. Buning uchun aniqlangan yuz tasviridan ko'zlarning o'lchamlari quyidagi formula orqali hisoblanadi:

$$a = \sqrt{(X_A - X_B)^2 + (Y_A - Y_B)^2};$$
$$b = \sqrt{(X_{A_1} - X_{B_1})^2 + (Y_{A_1} - Y_{B_1})^2},$$

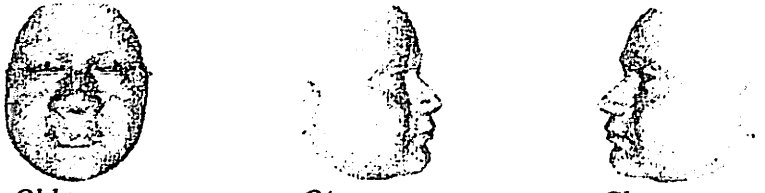
bu yerda, X_A, X_B, Y_A, Y_B – chap ko'zning chetki nuqtasi koordinatlari, X_{A_1}, X_{B_1}, Y_{A_1}, Y_{B_1} – o'ng ko'zning chetki nuqtasi koordinatlari.

2. a va b parametrlarning natijalariga tayangan holda, quyidagi shartlar tekshiriladi.

Agar, $\frac{a}{b} = [0{,}8 - 1{,}2]$ bo'lsa, birinchi sinf qaraladi.

Agar, $\frac{a}{b} > 1{,}2$ bo'lsa, ikkinchi sinf qaraladi.

Agar, $\frac{a}{b} < 0{,}8$ bo'lsa, uchinchi sinf qaraladi.



Old tomon *O'ng tomon* *Chap tomon*

4.5-rasm. Yuz tasviri holatiga bog'liq holda sinflashtirish

Bu yerda, a - chap ko'zning o'lchami, b - esa o'ng ko'zning o'lchami hisoblanadi.

Normal yuz tasvirlarini generatsiyalash quyidagi qadamlardan iborat:

1. 100 ta shaxsning har bir sinfga tegishli 300 ta yuz tasviri olinadi va yagona yuz tasviri hosil qilinadi. Uning ketma-ketligi quyidagicha:

a) $M \times N$ o'lchamdagi $Z_i \{z_1, z_2, \dots, z_{100}\}$ tasvirlar to'plami olinadi. Testlash uchun 256×256 o'lchamdagi tasvir olinadi va 65536 o'lchamdagi vektor hosil qilinadi. Hosil bo'lgan $\bar{Z}$ tasvirlarning o'rtachasi quyidagi formula asosida aniqlanadi:

$$\overline{Z_m} = \frac{1}{N}\sum_{i=1}^{N} z_{i_m},$$

bu yerda, N=100, m=65536. $\overline{Z_{m_r}}$, $\overline{Z_{m_g}}$ va $\overline{Z_{m_b}}$ - lar mos qizil, yashil va ko'k ranglar uchun o'rtacha qiymatlar yuqoridagi formula asosida hisoblanadi.

b) vektor qiymatlarini tarqalish darajasini aniqlash uchun o'rtacha qiymatlarga mos holda kovaratsion matritsa hisoblanadi:

$$C_m = \frac{1}{N}\sum_{i=1}^{N}(z_i - \overline{Z_m})(z_i - \overline{Z_m})^T,$$

bu yerda, T – transponerlangan matritsani anglatadi. Agar RGB rang modelidagi tasvir olingan bo'lsa, kovaratsion matritsa quyidagicha hisoblanadi:

$$C_{m_r} = \frac{1}{N}\sum_{i=1}^{N}(z_{i_r} - \overline{Z_{m_r}})(z_{i_r} - \overline{Z_{m_r}})^T;$$

$$C_{m_g} = \frac{1}{N}\sum_{i=1}^{N}(z_{i_g} - \overline{Z_{m_g}})\left(z_{i_g} - \overline{Z_{m_g}}\right)^T;$$

$$C_{m_b} = \frac{1}{N}\sum_{i=1}^{N}(z_{i_b} - \overline{Z_{m_b}})(z_{i_b} - \overline{Z_{m_b}})^T.$$

bu yerda, z_{i_r}, z_{i_g} va z_{i_b} mos holda qizil (red), yashil (green) va ko'k (blue) ranglarning qiymatlari bo'lib, $r, g, b = 0 - 255$.

s) Matritsaning xos vektorlari (eigenvectors) va unga mos xos qiymatlar (eigenvalues) quyidagi formula asosida aniqlanadi.

$$C_m V = V\lambda.$$

bu yerda, V - xos vektorlar to'plami va λ - xos qiymatlar. Xos qiymatlar determinantni kengaytirish usuli yordamida hisoblab topiladi va olingan qiymatlar asosida matrisalarni ko'paytirish yordamida xos vektorlar hisoblanadi [92].

Xos qiymatlarni hisoblash quyidagicha amalga oshiriladi. Bu yerda, I – birlik vektor.

$$C_m V = VI\lambda;$$
$$V(C_m - I\lambda) = 0;$$
$$det(C_m - I\lambda) = 0;$$
$$\begin{vmatrix} C_{1,1} - \lambda & C_{1,2} & \cdots & C_{1,m} \\ C_{2,1} & C_{2,2} - \lambda & \cdots & C_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ C_{m,1} & C_{m,2} & \cdots & C_{m,m} - \lambda \end{vmatrix} = 0.$$

Ushbu tenglikdan m ta λ xos qiymatlar hisoblanadi va quyidagi tenglik asosida xos vektorlar aniqlanadi:

$$\begin{pmatrix} C_{1,1} - \lambda & C_{1,2} & \cdots & C_{1,m} \\ C_{2,1} & C_{2,2} - \lambda & \cdots & C_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ C_{m,1} & C_{m,2} & \cdots & C_{m,m} - \lambda \end{pmatrix} \cdot \begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Mazkur tenglik asosida m ta V xos vektorlar hosil bo'ladi. Qizil (red), yashil (green) va ko'k (blue) ranglarlarning xos qiymatlari va xos vektorlari mos holda yuqoridagi tenglik asosida hisoblanadi.

d) Xos vektorlar unga mos xos qiymatlar bilan yuqoridan pastga qarab saralanadi (katta qiymat yuqorida, kichik qiymat pastda).

e) Har bir o'rtacha markazlashtirilgan tasvirlar xususiy sohalardan foydalangan holda proyeksiyalanadi va quyidagi formula yordamida hisoblanadi.

$$W_{i_r} = V_{i_r}^T (z_{i_r} - \overline{Z_{m_r}});$$
$$W_{i_g} = V_{i_g}^T (z_{i_g} - \overline{Z_{m_g}});$$
$$W_{i_b} = V_{i_b}^T (z_{i_b} - \overline{Z_{m_b}}).$$

Ushbu amallar o‘ng va chap tomondagi tasvirlar uchun ham bajariladi.

2. Har bir sinf uchun alohida yuz tasvirlari hosil qilinadi. Bunda 3 ta normal yuz tasviri hosil bo‘ladi. Normal tasvirlar bazada saqlanadi va aniqlangan yuz tasvirida to‘siq borligi aniqlansa, kiruvchi tasvirni normallashtirish bosqichi asosida to‘siq olib tashlanadi hamda tanib olish jarayoniga yuboriladi. Aks holda, to‘g‘ridan-to‘g‘ri tanib olish jarayoniga o‘tkaziladi.

Kiruvchi yuz tasvirini normallashtirishda sinfga mos normal tasvir va uning o‘lchamiga tenglashtirilgan kiruvchi tasvirlar piksellarining o‘rtacha qiymatlari hisoblanadi.

$$NT_i = \frac{(W_i + Z_i)}{2}.$$

Yuqoridagi hisoblash barcha piksellar uchun amalga oshiriladi va natijada bir xil o‘lchamdagi normallashgan tasvir hosil bo‘ladi. Bu yerda, NT_i – normallashtirilgan tasvir, W_i – normal tasvir, Z_i – kiruvchi tasvir, i=3.

Normal yuz tasvirlarini hosil qilish algoritmi quyidagi qadamlardan iborat:

1-qadam: aniqlangan yuz tasviridan a va b ko‘z o‘lchamlari hisoblanadi.

2-qadam: yuz tasvirining sinfi aniqlanadi.

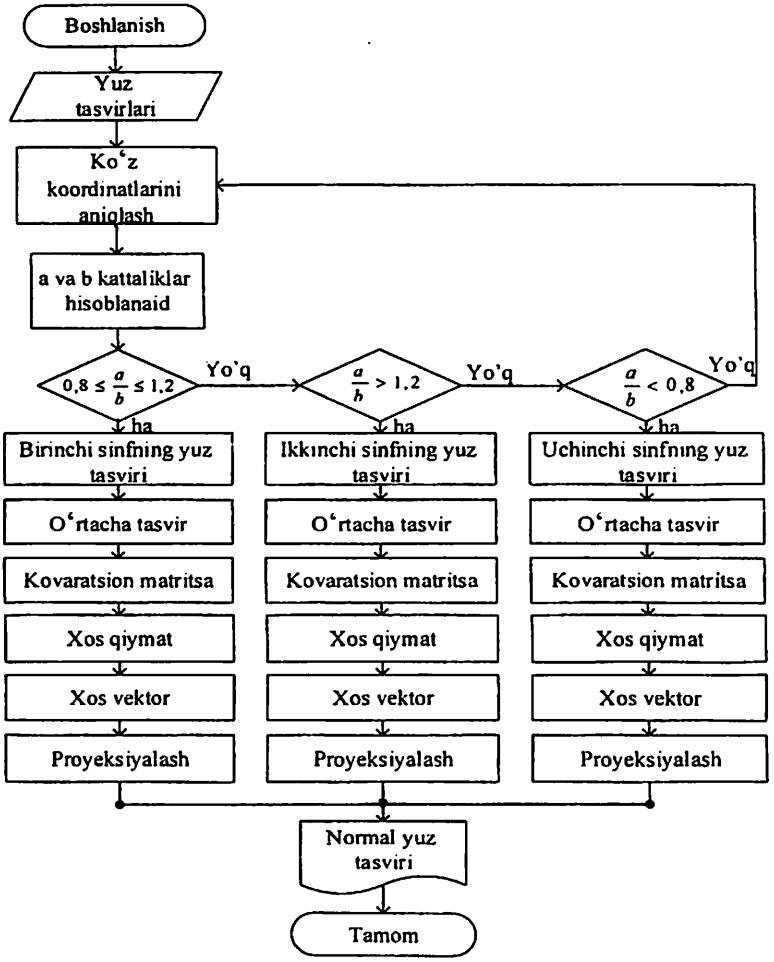
3-qadam: 100 ta shaxsning 3 tadan jami 300 ta yuz tasviri olinadi va yuz tasvirini normallashtirish usuli asosida (a-e qadamlar) proyeksiyalar hisoblanadi va normal tasvir olinadi.

Keyingi holatlar uchun ham yuqoridagi qadamlar takrorlanadi. Normal yuz tasvirlarini hosil qilish algoritmining blok sxemasi 4.6-rasmda keltirilgan.

Yuz tasvirini normallashtirishning mazkur usuli aniqlangan yuz tasvirida to‘siq mavjud holatlarda qo‘llaniladi. Yuz tasvirida tasodifiy yuzaga kelgan to‘siqlar yuz tasvirining uchta: old, chap va o‘ng tomondan ko‘rinishlari asosida aniqlanadi. Agar to‘siq mavjud bo‘lmasa, normallashtirish usulidan foydalanilmaydi.

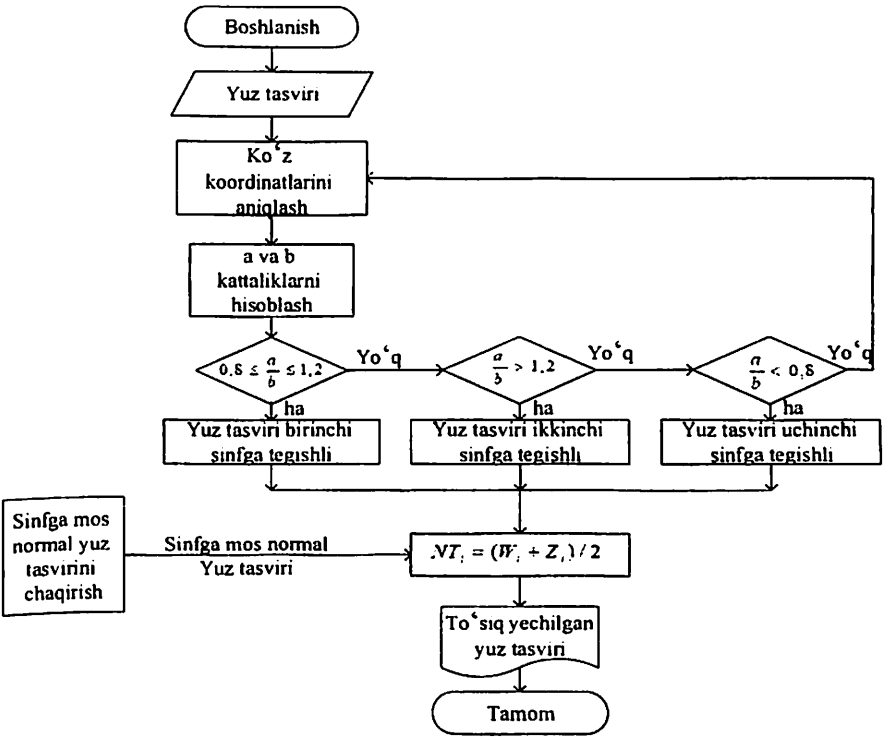
Taklif etilgan yuz tasvirini normallashtirish usuli aniqlangan yuz tasvirini tanib olishda yuqori samara beradi. Yuz tasvirini normallashtirish yuz tasvirida to‘siqlar mavjud bo‘lganda qo‘llanilib,

tasodifiy to‘siqlar Viola Jones xususiyatlari asosida yuz tasviri qismlarini aniqlashga mo‘ljallangan.



4.6-rasm. Normal yuz tasvirlarini hosil qilish algoritmining blok sxemasi

To‘siq mavjud yuz tasvirini normallashtirish algoritmining blok sxemasi 4.7-rasmda keltirilgan.



4.7-rasm. To'siq mavjud yuz tasvirini normallashtirish algoritmining blok sxemasi

Ushbu holda yuz tasvirining ehtimolli uchta sinfiga alohida e'tibor qaratish lozim. Normallashtirish bosqichidan o'tgan yuz tasviri tanib olish bosqichiga yuboriladi. Yuz tasvirini tanib olish xatoligini kamaytirish uchun ishlab chiqilgan yuz tasvirini normallashtirish usulini qo'llash sharti quyidagicha:

Aniqlangan yuz tasvirida:
Normallashtirish qo'llaniladi:
chap ko'z, o'ng ko'z mavjud va burun, og'iz mavjud emas;
Normallashtirish qo'llanilmaydi:
chap ko'z, o'ng ko'z, burun mavjud;
chap ko'z, o'ng ko'z, burun, og'iz mavjud;

Shartdan ko'rinib turibdiki, yuz tasvirini normallashtirish jarayoni har doim ham talab etilmaydi.

4.3. Yuz tasvirini tanib olishning modifikatsiyalangan teran o'rganish tarmog'i

Yuz tasvirini tanib olish aniqligini oshirishda teran o'rganish usullaridan foydalanish yuqori samara beradi. Biroq, ularda ham ayrim kamchiliklar mavjud bo'lib, 4.4-jadvalda tanib olish tarmoqlaridagi muammolar va ularni bartaraf etish bo'yicha takliflar keltirilgan.

4.4-jadval

Tanib olish tarmoqlaridagi muammolar va ularni bartaraf etish bo'yicha takliflar

Muammolar	Takliflar
Xatoliklarni minimallashtirish	Samarali teran o'rganish tarmog'idan foydalanish.
Namunalarni o'rganish va testlash uchun vaqt sarfini kamaytirish	Samarali filtr o'lchamlaridan foydalanish.
Chiziqli filtrlar	Tasodifiy filtrlardan foydalanish va ularni chiziqsiz ko'rinishga o'tkazish.
Muhim xususiyatlarni ajratish	Samarali yo'qotish funksiyasidan foydalanish.

Yuz tasviridan xususiyatlarni ajratib olish ILSVRC-2017 tanlovida g'olib bo'lgan va xatolik darajasi o'rtacha hisobda 2,27% ga teng SEnet - zichlash-faollashtirish (SEnet - Squeeze-and-Excitation Networks) tarmog'idan foydalanish maqsadga muvofiq hisoblanadi (4.5-jadval)[93].

4.5-jadval

Tanib olish tarmog'i va xatolik darajasi

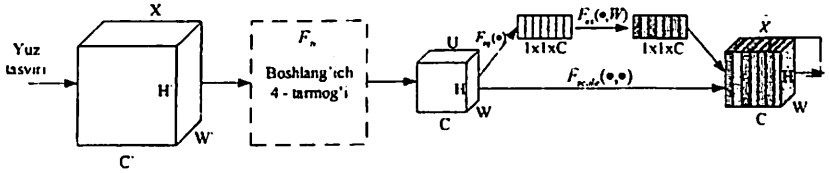
Xatolik darajasi / Tarmoqlar	Xatolik darajasi
Zichlash-faollashtirish tarmog'i	0,0227
Ikki yo'lli tarmoq	0,027
Qoldiq tarmoq	0,032
Piramida tarmoq	0,033

Zichlash-faollashtirish tarmog'i asosida yuz tasvirini tanib olish. U ikki bosqichdan tashkil topgan:

1. *S (Squeeze)* – zichlash bosqichi.
2. *E (Excitation)* – faollashtirish bosqichi.

Zichlash bosqichidan chiqqan matritsa faollashtirish bosqichi yordamida odingi holatiga qaytariladi va xususiyatlarning eng kuchlilari saralab olinadi.

4.8-rasmda yuz tasvirini tanib olish samaradorligini oshirishning modifikatsiyalangan zichlash-faollashtirish tarmog'i keltirilgan [72].



4.8-rasm. Yuz tasvirini tanib olishning modifikatsiyalangan zichlash-faollashtirish tarmog'i

Birinchi navbatda F_{tr} funksiyasi yordamida $H' \times W' \times C'$ o'lchamdagi tasvir $H \times W \times C$ o'lchamidagi tasvirga quyidagi formula asosida keltiriladi:

$$u_c = v_c \cdot X = \sum_{s=1}^{C'} v_c^s \cdot x^s,$$

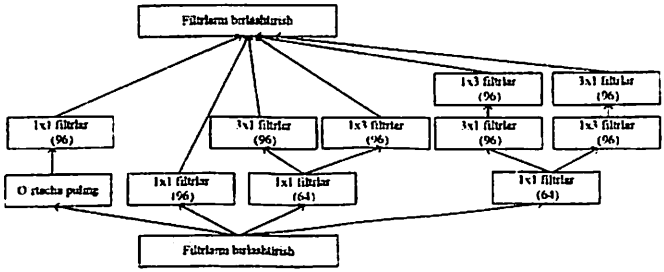
bu yerda, $v_c = [v_c^1, v_c^2, \dots v_c^{C'}]$ – kernel filtrlari, X= $[x^1, x^2, \dots x^{C'}]$ – yuz tasvirlari, s – bitta sathdagi kernel filtri tartib raqami. F_{tr} funksiyasi o'rnida boshlang'ich 4 - tarmog'ini qo'llash tanib olish samaradorligini oshirish, hisoblash qurilmalariga yuklanishni kamaytirish va chiziqsiz funksiyalardan foydalanish imkoniyatlarini taqdim etadi (4.6-jadval).

4.6-jadval

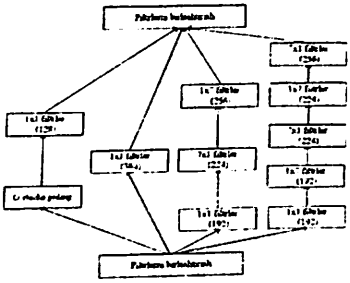
ILSVRC 2012 tarmog'idan olingan 50 000 ta tasvirning xatolik natijalari

Xatolik / Tarmoq	Top-1 xatolik (%)	Top-5 xatolik (%)
Boshlang'ich 3-tarmoq	18,9	4,3
Boshlang'ich-qoldiq tarmoq	18,8	4.3
Boshlang'ich 4-tarmoq	17,7	3,8

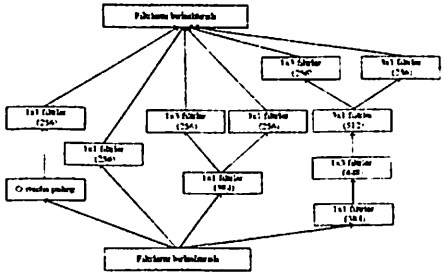
Boshlang'ich 4-tarmoq. Ushbu tarmoq uchta boshlang'ich qismtarmoqdan tashkil topgan bo'lib, uning holatlari 4.9-rasmda va umumiy sxemasi 4.10-rasmda tasvirlangan.



Boshlang'ich-A. 35×35 *holat bilan*



Boshlang'ich-B 17×17 *holat bilan*



Boshlang'ich-C 8×8 *holat bilan*

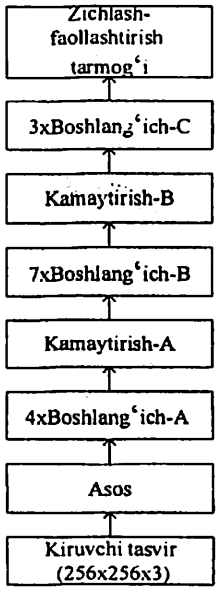
4.9-rasm. Boshlang'ich 4-tarmoqning A, B, C turlari va mos o'lcham holatlari

Ushbu tarmoqda hisoblash tezligini oshirish uchun 1×1 filtrlaridan foydalanilgan. Bundan tashqari, hisoblash uchun sarflanadigan vaqt va hisoblashlar sonini kamaytirish maqsadida, $n \times n$ filtr o'rniga $1 \times n$ va $n \times 1$ filtrlarni ketma-ket qo'llash maqsadga muvofiq. Natijada, hisoblash parametrlari soni $n^2 - 2n$ ga kamayadi.

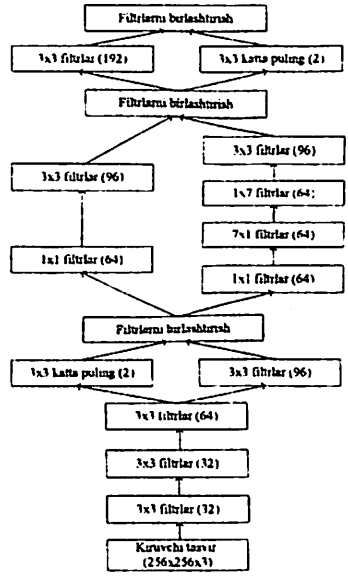
Bu yerda, $n \times n$ filtr o'lchami bo'lib, svyortka qadamidan keyin T – tasvir o'lchami quyidagi formula orqali hisoblanadi:

$$T = \left(\frac{n_x+2p-f}{s} + 1\right) \cdot \left(\frac{n_y+2p-f}{s} + 1\right),$$

bu yerda, n_x ва n_y kiruvchi tasvir o'lchami, p – padding (mazkur holda qo'llanilmagan), f – filtr o'lchami, s – qadam.



Boshlang'ich 4-tarmoqning sxemasi



Asos

4.10-rasm. Boshlang'ich 4-tarmoqning umumiy sxemasi

Boshlang'ich 4-tarmoq va uning boshlang'ich A, B va C tarmoqlarida chiziqsiz xususiyatlarga erishish maqsadida parallel hisoblash usullari qo'llanilgan. Parallel svyortkalar filtrlarni birlashtirish funksiyasi yordamida birlashtiriladi va chiziqsiz qiymatlarni hosil qilish uchun yana parallel hisoblashga o'tiladi.

Tarmoqda katta puling qo'llanilgan bo'lib, belgilangan sohadagi katta qiymatlarni olishni anglatadi. Boshlang'ich 4-tarmog'idan chiqqan natija zichlash-faollashtirish tarmog'ining zichlash bosqichiga jo'natiladi.

Zichlash bosqichida $H \times W \times C$ o'lchamidagi tasvir F_{sq} funksiyasi yordamida $1 \times 1 \times C$ o'lchamga keltiriladi va u quyidagi formula asosida hisoblanadi:

$$z_c = F_{sq}(u_c) = \frac{1}{H \cdot W} \sum_{i=1}^{H} \sum_{j=1}^{W} u_c(i,j).$$

Keyingi bosqichda faollashtirish funksiyasi hisoblanadi. Vektorning o'lchamini kamaytirish, so'ngra oshirish orqali chiziqsizligi ta'minlanadi. U quyidagi formula asosida hisoblanadi:

$$s_c = F_{ex}(z_c, W) = \sigma\big(g(z_c, W)\big) = \sigma(W_2\delta(W_1 z_c)),$$

bu yerda, δ – ReLu [94] funksiyasi hisoblanib, uning qiymati (0:1) oraliqda bo'ladi. ReLu funksiyasi quyidagicha hisoblanadi:

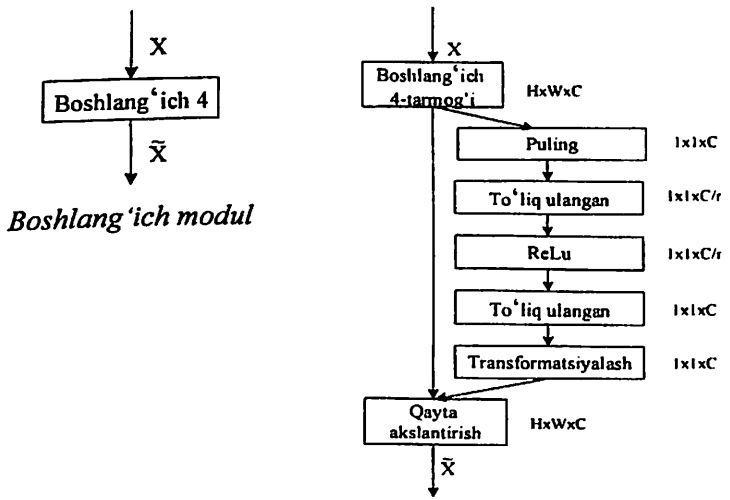
$$ReLu = W \cdot x,$$

bu yerda, W - neyron salmog'i, x – esa, neyron qiymati.

σ – Sigmoid [73] funksiyasi hisoblanib, u quyidagicha hisoblanadi:

$$\sigma(x) = \frac{1}{1+e^{x}}.$$

Zichlash-faollashtirish tarmog'ini Boshlang'ich 4-tarmog'ida qo'llash 4.11-rasmda keltirilgan.



4.11-rasm. Zichlash-faollashtirish tarmog'ini boshlang'ich 4-tarmog'ida qo'llash

$W_1 \in \mathbb{R}^{\frac{C}{r}xC}$ – C va r parametrlari yodamida vektor o'lchamini kichiklashtirish. r – kamaytirish ko'rsatkichi (ishda r parametr uchun samarali qiymat sifatida 16 tanlangan).

$W_2 \in \mathbb{R}^{C \times \frac{C}{r}}$ – C va r parametrlari yordamida vektor o'lchamini kattalashtirish.

Keyingi bosqichda chiquvchi qiymat U faollashtirish funksiyasi yordamida qayta transformatsiyalanadi.

$$\widetilde{x_c} = F_{scale}(u_c, s_c) = s_c \cdot u_c,$$

bu yerda, $u_c \in \mathbb{R}^{HxW}$.

Yuz tasviri xususiyatlari orasidagi farqlarni hisoblash va bir xil xususiyatlarni kamaytirish uchun yo'qotish funksiyalaridan (loss function) foydalanildi va ular yordamida to'liq ulangan tarmoq qatlamidan chiqqan o'xshash natijalarni saralash amalga oshirildi.

4.7-jadvalda yo'qotish funksiyalarining aniqligi keltirilgan bo'lib, L2-softmax yo'qotish funksiyasining aniqlik darajasi qolganlariga nisbatan yuqori [73]. Shuning uchun to'liq ulangan tarmoq qatlamidan chiqqan xususiyatlarni saralash uchun L2-softmax funksiyasi tanlandi.

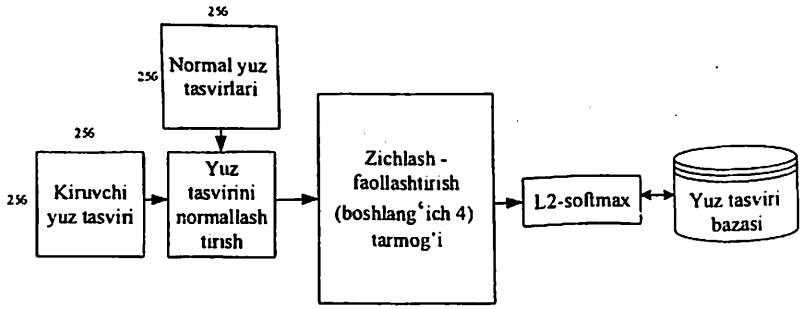
4.7-jadval

Yo'qotish funksiyalarining aniqligi

Yo'qotish funksiyasi	Aniqligi (%)
softmax	87,35
L-softmax	88,71
A-softmax	89,42
Uch marta yo'qotish	89,63
L2-softmax	89,78

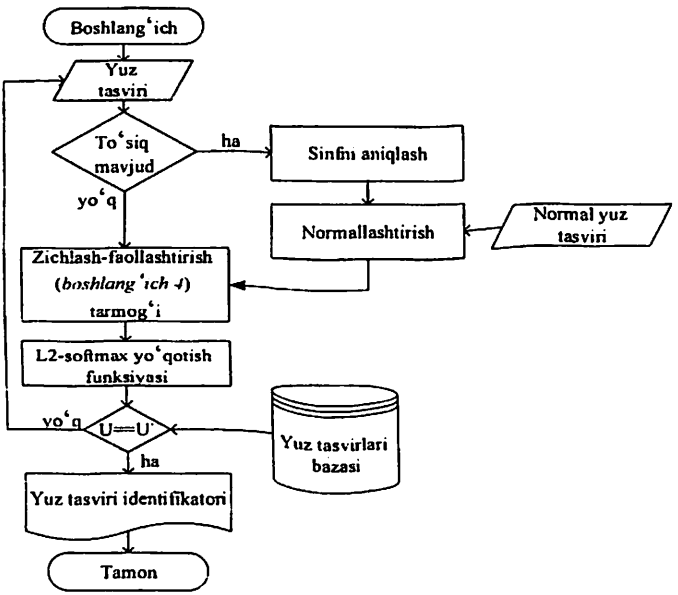
L2-softmax yo'qotish funksiyasi. Ushbu funksiya boshqa yo'qotish funksiyalariga nisbatan xususiyatlar orasidagi farqni aniq ko'rsatish va hisoblash imkoniyatini beradi.

L2-softmax [73; 4-5-b] yo'qotish funksiyasiga asoslangan yuz tasviri bo'yicha identifikatsiyaning umumiy sxemasi 4.12-rasmda keltirilgan.



4.12-rasm. Yuz tasviri bo'yicha identifikatsiyalashning umumiy sxemasi

Tasvirda to'siq mavjudligi aniqlanmasa, aniqlangan yuz tasviri to'g'ridan-to'g'ri tarmoqqa kiritiladi. Chunki, yuz tasvirida to'siq mavjud bo'lmagan holda normallashtirishni qo'llash xatoliklarni oshiradi. 4.13-rasmda yuz tasvirini tanib olish algoritmining blok sxemasi keltirilgan.



4.13-rasm. Yuz tasvirini tanib olish algoritmining blok sxemasi

Zichlash-faollashtirish tarmog'ida qo'llanilgan parametrlarning qiymatlari 4.8-jadvalda keltirilgan.

4.8-jadval

Zichlash-faollashtirish tarmog'ida qo'llanilgan parametrlarning qiymatlari

Qiymati va vazifasi / Belgilanishi	Qiymati	Vazifasi
f – filtr	$3 \times 3, 1 \times 1$ $7 \times 7 = 1 \times 7 + 7 \times 1$ $3 \times 3 = 1 \times 3 + 3 \times 1$	Kiruvchi tasvirni tasodifiy qiymatlar yordamida ishlash.
s – qadam	2	Filtr va puling uchun qadam uzunligi.
r – kamayish ko'rsatkichi	16	Faollashtirish funksiyasini hisoblashda vektorni kattalashtirish va kichiklashtirish.

Tanib olish tezligini oshirish va hisoblash parametrlari sonini kamaytirish uchun samarali filtr o'lchamlaridan foydalanish maqsadga muvofiq.

Bu yerda, 7×7 filtrlar o'rnida 1×7 va 7×1 filtrlarni qo'llash maqsadga muvofiq. Chunki, $7 \cdot 7 = 49$ ta parametr $1 \cdot 7 + 7 \cdot 1 = 14$ ta parametr. Umumiy hisobda ushbu filtr o'lchamlarini tarmoqda qo'llash asosida hisoblash elementlari soni 1,95 marta kamayadi. Shuningdek, olingan natija saqlanadi.

4.9-jadvalda tarmoqlarda va taklif etilgan usulda qo'llanilgan filtrlar va parametrlar sonining farqi keltirilgan.

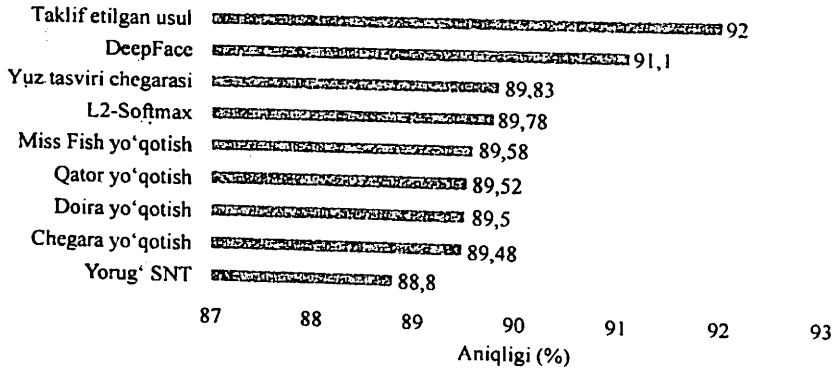
4.9-jadval

Filtrlarning samarali qiymatlari

Ko'rsatkichlar / Tarmoq nomi	Filtr o'lchamlari	Parametrlar soni	Yolg'ondan rad etish xatoligi
Boshlang'ich 4-tarmoq	$3 \times 3, 1 \times 1, 1 \times 7, 7 \times 1$	4,7 Mb	8,5 %
Zichlash - faollashtirish	$7 \times 7, 3 \times 3, 1 \times 1$	28,1 Mb	8,1 %
Taklif etilgan tarmoq	$3 \times 3, 1 \times 1, 7 \times 1, 1 \times 7, 3 \times 1, 1 \times 3$	14,4 Mb	8 %

Zichlash – faollashtirish tarmog'ini qo'llash orqali yolg'ondan rad etish xatoligi 8,1 % ga kamaytirishga erishilgan, ammo unda hisoblash parametrlar soni ko'p, ya'ni shaxsni tanib olish uchun, taklif etilgan tarmoqqa nisbatan, ikki barobar ko'p vaqt sarflanadi. Shuningdek, zichlash – faollashtirish tarmog'iga nisbatan yolg'ondan rad etish xatoligi 0,1% ga kamaygan.

Taklif etilgan usulni mavjudlari bilan LWF yuz tasviri bazasidan olinganlari bilan taqqoslash natijalari 4.14-rasmda keltirilgan.



4.14-rasm. Taklif etilgan usulni mavjudlari bilan LWF bazasida olingan tahlil natijalari

4.10-jadvalda to'siq mavjud yuz tasvirini tanib olishda normallashtirish qo'llanilgan va qo'llanilmagan hollari uchun xatolik va parametrlar soni keltirilgan.

Jadvaldagi ma'lumotlar to'siq mavjud yuz tasvirlari asosida keltirilgan, shuning uchun xatolik darajasi yuqori. Normallashtirish usuli qo'llanilgan holda Gflops deyarli ortmaydi, ya'ni 0,01 Mbga farq qiladi.

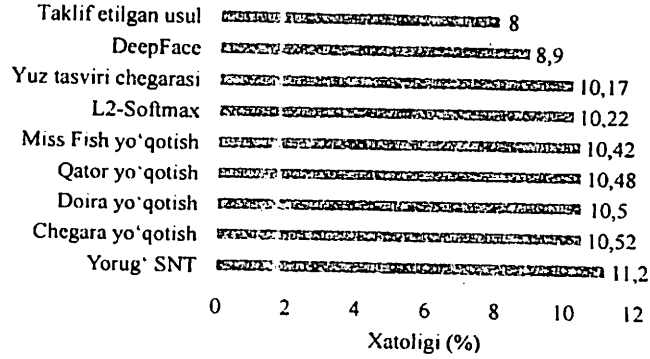
4.10-jadval

Normallashtirish qo'llanilgan va qo'llanilmagan hollar uchun xatolik darajasi va parametrlar soni

Ko'rsatkichlar / Usul	Yolg'ondan rad etish xatoligi (%)	Parametrlar soni
Normallashtirish qo'llanilmagan	35	14,4 Mb
Normallashtirish qo'llanilgan	14	14,41 Mb

To‘siq mavjud yuz tasviri normallashtirish usuli orqali to‘siqdan ozod etiladi va tanib olish tarmog‘iga uzatiladi.

Taklif etilgan usulning LWF yuz tasviri bazasida olingan test natijalari 4.15-rasmda keltirilgan.



4.15-rasm. Taklif etilgan usulning LWF yuz tasviri bazasida olingan test natijalari

Yuz tasvirini tanib olishning modifikatsiyalangan tarmog‘ini qo‘llash asosida tanib olish aniqligi LFW yuz tasviri bazasida olingan tahlil natijalariga ko‘ra, 92 % gacha oshirgan va yolg‘ondan rad etish xatoligi esa 8 % gacha kamaygan.

4.4. Yuz tasviri bazasini shakllantirish tartibi

Yuz tasviri bo‘yicha identifikatsiya samaradorligini oshirishda yuz tasviri bazalarini to‘g‘ri shakllantirish va ulardan foydalanish katta ahamiyatga ega. Teran o‘rganish usullari orqali to‘planadigan yuz tasviri xususiyatlarining soni, bazadagi har bir shaxsga tegishli tasvirlar soniga bog‘liq. Agar bazadagi tasvirlar soni ortsa, yuz tasviri xususiyatlari ham ortadi, bu esa tanib olish aniqligini ortishiga va xatoliklarni pasayishiga olib keladi [74].

Yuz tasviri bazalarini shakllantirishga bir nechta talablar mavjud. Ularga orqa fonning shaffof bo‘lishi, shaxsning tana qismi ishtirok etmasligi, tasvir sifatining yetarli darajada ekanligi, to‘siqsiz va bitta tasvirda bitta yuz tasviri bo‘lishi va boshqa shu kabi talablar mavjud.

Quyida yuz tasvirini tanib olishda qo‘llaniladigan keng tarqalgan yuz tasviri bazalari keltirilgan.

LFW (*Labeled Faces in the Wild* – yorliqli yuz tasvirlari) yuz tasviri bazasi Internet tarmog'idan to'plangan 13 mingta yorliqli yuz tasvirlaridan iborat. Bazada 1680 ta shaxsning ikki va undan ortiq turli ko'rinishdagi yuz tasvirlari to'plangan.

Web yuz tasvirlari. Teran o'rganish tarmoqlari uchun yaratilgan, birinchi ochiq yuz tasviri bazalari to'plami hisoblanadi [75]. U 1940-2014 yillar oralig'ida Internet tarmog'ida joylashtirilgan bayram va bazmlarning video va rasm ma'lumotlaridan kesib olingan yuz tasvirlaridan tashkil topgan. Bazani shakllantirishda rasm va videodagi yuz tasvirlari kesib olingan va bir xil yuz tasvirlari saralangan. Shuningdek, tasvirlar ularni kengaytirish usullari yordamida ko'paytiriladi. Ushbu yuz tasviri baza 10575 ta shaxsning 494414 ta turli ko'rinishdagi tasvirlaridan iborat. Web yuz tasvirlari bazasidan namunalar 4.16-rasmda keltirilgan.

Oq bilan belgilangan yuz tasvirlari aniqlanmagan

Sariq bilan belgilangan yuz tasviri egasi bazada mavjud emas

4.16-rasm. Web yuz tasvirlari bazasidan namuna

Tadbir-1M. Bir millionta (M) turli tadbirlardan olingan yuz tasvirlaridan iborat ochiq baza hisoblanadi [76]. Unda 100 000 ta shaxsning 100 tadan jami 10 million yuz tasviri to'plangan. Bundan tashqari, 2000 dan ortiq kasb va 200 dan ortiq millatlarga mansub shaxslarning yuz tasvirlari o'z aksini topgan. Unda kam ko'ringan, ko'rinmagan va to'siq mavjud yuz tasvirlari mavjud emas. Ya'ni, u aynan yuz tasviri mavjud rasmlardan tashkil topgan. U ikki ko'rinishdagi bazaga ajratiladi:

a) tasodifiy yuklangan tadbirlardan yuz tasvirlarini ajratib olish asosida;

b) tanlangan va mashhur shaxslar ishtirok etgan tadbirlardan yuz tasvirlarini ajratib olish asosida.

Tadbir-1M bazasidagi Chak Palxnikka tegishli yuz tasvirlari 4.17-rasmda keltirilgan.

4.17-rasm. Tadbir-1M bazasidagi Chak Palxnikka tegishli yuz tasvirlari

Ushbu rasmda qizil rang bilan belgilangan tasvir ushbu tadbirga aloqasi yo'q va to'q kulrang esa, yuz tasviri mavjud emasligini anglatadi.

Teran o'rganish tarmoqlarida qo'llaniladigan yuz tasviri bazalari xususidagi ma'lumotlar 4.11-jadvalda keltirilgan.

4.11-jadval

Teran o'rganish tarmoqlarida qo'llaniladigan yuz tasviri bazalari

Ma'lumotlar / Yuz tasviri bazasi	Nashr etilgan vaqt	Tasvirlar soni	Shaxslar soni	Bitta shaxsning yuz tasvirlari	Resurslar
LFW yuz tasviri bazasi	2012	13 000	1 680	2/50	Internet tarmog'i
Tadbir-1M (birinchi nashr)	2016	10 M	100 000	100	Ijtimoiy tarmoq va tadbirlar
Tadbir-1M (ikkinchi nashr)	2016	1,5 M	20 000	1/-/100	Ijtimoiy tarmoq va tadbirlar
Tadbir-1M (uchinchi nashr)	2018	4M 2,8 M (Osiyo)	80 000 100 000 (Osiyo)	-	Ijtimoiy tarmoq va tadbirlar
Web yuz tasvirlari	2014	494414	10575	2/46 va 8/804	Mashhur shaxslar
Tadbir-Yuzlar+	2014	202599	10177	19.9	Maxfiy
Google	2015	>500 M	>10M	50	Maxfiy
Facebook	2014	4,4 M	4 000	800/1100/ 1200	Maxfiy

Keltirilgan yuz tasviri bazalaridan Tadbir-1M bazasi ko'p sonli shaxslarning tasvirlarini o'zida jamlagan va ochiq holda Internetda mavjud. Shuning uchun ham ushbu baza asosida tadqiqotlar olib borish maqsadga muvofiq hisoblanadi.

Universitet_MB. Ushbu yuz tasviri bazasi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari Universitetining talabalari ishtirokida tayyorlangan [77]. Unda jami 209 ta talabaning o'ng, chap, tepa, past va old – jami 11 holatdagi tasvirlari to'plangan. Har bir tasvir 256 × 256 o'lchamda kesib olingan. Universitet_MB yuz tasviri bazasidan namuna 4.18-rasmda keltirilgan.

4.18-rasm. Universitet_MB yuz tasviri bazasidan namuna

Ushbu yuz tasviri bazasini shakllantirishda tasvirlarni ko'paytirish usullari [78] yordamida har bir yuz tasviri holatining 12 ta turli ko'rinishdagi (yuz tasvirining ayrim qismlarini kesib olish, yuz tasvirini ma'lum burchakka burish, yon tomondagi tasvirni aksini yaratish va boshqa holatlar) tasvirlari hosil qilinadi. Buning natijasida 11 ta ko'rinishda suratga olingan shaxsning tasviri 132 ta bo'ladi. Quyida tasvirlarni ko'paytirish xususiyatlari keltirilgan:

rotation_range=30: tasvirni 30 gradusga burishni anglatadi;

width_shift_range=0.1: 0,1 kattalikka eni bo'yicha zichlash;

height_shift_range=0.1: 0,1 kattalikka bo'yi bo'yicha zichlash;

shear_range=0.2: 0,2 kattalikka qisqartirish yoki kattalashtirish;

zoom_range=0.2: tasvirning umumiy o'lchamini 0,2 kattalikka qisqartirish;

horizontal_flip=True: gorizantal burish.

Keltirilgan xususiyatlarning barchasida kamida 2 tadan holat hisobga olinganida, bitta tasvir 12 taga ko'payadi. Tasvirlarni ko'paytirish orqali hosil qilingan tasvirlarni testlash uchun qo'llash mumkin emas, ular xususiyatlarni hosil qilishda qo'llaniladi.

Yuz tasviri bazasini shakllantirishda unga bo'lishi mumkin qalbakilashtirish hujumini oldini olish choralarini ishlab chiqish mumkin. Buning uchun, uch o'lchamli yuz tasvirlaridan iborat yuz tasviri bazasini shakllantirish talab etiladi [95].

Uzb_MB. Ushbu yuz tasviri bazasi mashhur o'zbek san'atkorlarining Internet tarmog'ida joylashgan yuz tasvirlari asosida

to‘plangan. Unda tadbir, konsert, kino va reklamalardan ajratib olingan 133 ta san’atkorning 50 tadan jami 6650 ta yuz tasviri shakllantirilgan. Shaxslarning turli ko‘rinishdagi va qiyofadagi tasvirlari o‘z aksini topgan. Uzb_MB yuz tasviri bazasidan namuna 4.19-rasmda keltirilgan.

4.19-rasm. Uzb_MB yuz tasviri bazasidan namuna

Ushbu bazada mavjud shaxsga tegishli tasvirlar keltirilgan bo‘lib, bitta tasvirda ikkita yuz bo‘lishi mumkin emas. Ammo, yuz tasvirida o‘zgarishlar yuz berishi (soqol, ko‘zoynak, bosh kiyim va boshqa holatlar) mumkin. Ushbu holatlarni o‘zida aks ettirgan namunalar 4.20-rasmda keltirilgan.

4.20-rasm. Yuz tasvirida o‘zgarishlar mavjud holatlar

Universitet_MB va Uzb_MB yuz tasviri bazalari xususidagi ma’lumotlar 4.12-jadvalda keltirilgan.

4.12-jadval

Yuz tasviri bazalarining parametrlari

Ma’lumotlar / Yuz tasviri bazasi	Nashr etilgan vaqt	Tasvirlar soni	Shaxslar soni	Bitta shaxsning yuz tasvirlari	Resurslar
Universitet_MB	2016 y.	27 588	209	132	TATU talabalari
Uzb_MB	2019 y.	6 650	133	50	Internet resurslari va ijtimoiy tarmoqlar

Uzb_MB yuz tasviri bazasi doirasida olingan muvaffaqiyatli namunalar va yuz tasvirini aniqlashda yuzaga keladigan xotoliklarga namunalar, mos ravishda 4.21 va 4.22 - rasmlarda keltirilgan.

4.21-rasm. Yuz tasvirini aniqlash namunalari

a b c d e

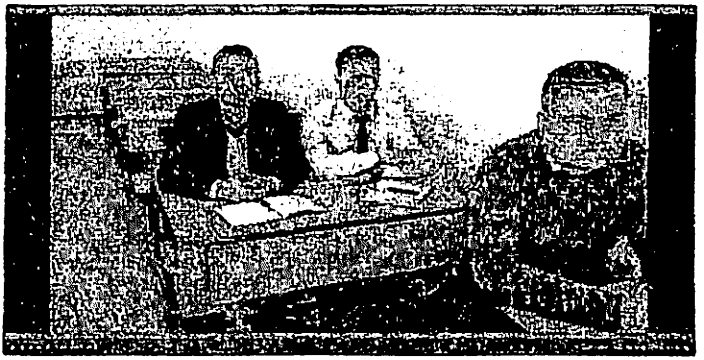
4.22-rasm. Rasmdan yuz tasvirini aniqlashda xatolik yuz bergan holatlar

Uzb_MB yuz tasviri bazasidan olingan tanib olish namunalari 4.23-rasmda keltirilgan.

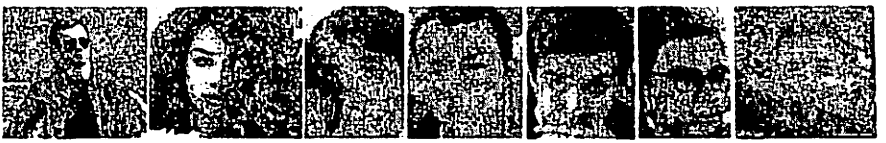
4.23-rasm. Rasm asosida yuzni tanib olish

Video fayldan shaxslarni tanib olish samaradorligini baholashda har bir shaxsni tanib olish ko'rsatkichi to'g'ri yoki noto'g'ri ekanligi ma'mur tomonidan tahlil qilinishi lozim (4.24-rasm).

Yuz tasvirini normallashtirish jarayoni qo'llanilganda tanib olish samaradorligini baholash maqsadida 100 ta shaxsning har birining 4 tadan turli ko'rinishidagi to'siqlar mavjud yuz tasviri bazasi shakllantirildi. Ulardan namunalar 4.25-rasmda keltirilgan.



4.24-rasm. Video asosida yuz tasvirini tanib olish



4.25-rasm. To'siqlar mavjud yuz tasviri bazasidan namunalar

4.26-rasmda kichik to'siq mavjud yuz tasvirlarni tanib olishdagi xatolikdan misollar keltirilgan.

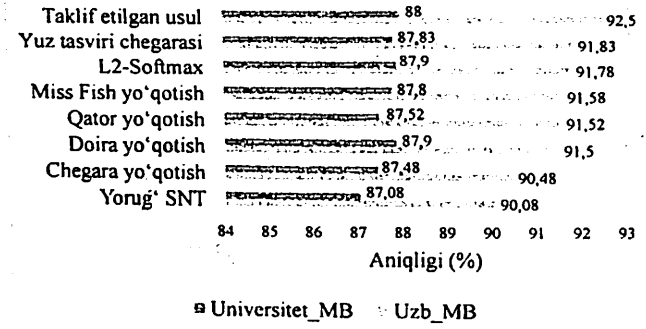
a)

b)

4.26-rasm. Kichik to'siq mavjud yuz tasvirlarini tanib olishdagi xatolikka misollar

Yuz tasvirini tanib olishning teran o'rganishga asoslangan usullarining Universitet_MB va Uzb_MB yuz tasviri bazalarida testlash aniqligi 4.27-rasmda keltirilgan.

Rasmda keltirilgan ma'lumotlarga ko'ra, Universitet_MB va Uzb_MB yuz tasviri bazalarida yuz tasvirini tanib olish usullari 88 % va 92,5 % aniqlikni ko'rsatdi. Tanib olish samaradorligini oshirish uchun yuz tasviri bo'yicha identifikatsiya dasturida foydalanuvchining yangi yuz tasvirlarini qo'shish imkoniyati mavjud bo'lishi lozim.



4.27-rasm. Yuz tasvirini tanib olishning teran o'rganishga asoslangan usullarining Universitet_MB va Uzb_MB yuz tasviri bazalarida tanib olish aniqligi

Tavsiyalar. Yuz tasviri bo'yicha tanib olishni amalga oshirish uchun ma'lum talablar va tavsiyalar mavjud. Umumiy holda yuz tasviri orqali tanib olish tizimini ishlab chiqishda quyidagi holatlarning talab darajasida ekanligiga alohida e'tibor qaratish lozim:

- kameraning sifati;
- mavjud yuz tasviri rasmining sifati;
- yoritilganlik;
- yuz tasvirining holati;
- yuz tasvirining belgilari;
- yuz tasvirini aniqlash vaqti;
- ko'zoynak, kosmetika.

Yuz tasviri bazalarini shakllantirishda va testlashda yuz tasvirining quyidagi holatlariga e'tibor qaratish lozim:

- yuz tasviridagi to'siqlar;
- og'izni keng ochib kulishi;
- qoshning o'sishi;
- ko'zning yumilishi;
- ko'zning kameradan boshqa tomonga qarashi;
- qovog'ini solishi.

Demak, tanib olishdagi muammolarni bartaraf etish uchun yuqorida keltirilgan talab va tavsiyalarga asoslangan yuz tasviri bazasi va tanib olishning samarali usulini ishlab chiqish lozim.

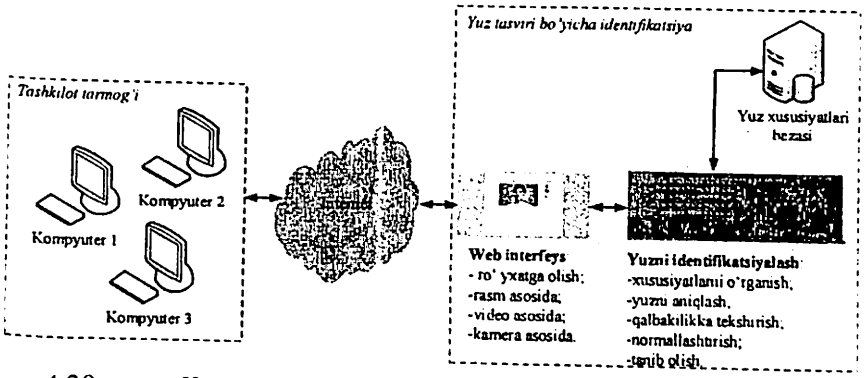
Yuz tasviri bazasini talab bo'yicha tashkil etish uning aniqligini oshirishga xizmat qiladi [15].

4.5. Yuz tasviri bo'yicha identifikatsiya jarayonining dasturiy vositasi

Yuz tasviri bo'yicha identifikatsiya jarayoni dasturiy vositasining ishlash sxemasi 4.28-rasmda keltirilgan bo'lib, u ikki qismdan iborat:

foydalanuvchi qismi – foydalanuvchi uchun qulay web-interfeys yaratilgan, u orqali foydalanuvchi ro'yxatdan o'tish jarayonida zarur bo'lgan yuz tasviri bazasi shakllantiriladi hamda rasm, video va kamera orqali keluvchi oqim asosida identifikatsiya jarayoni amalga oshiriladi;

server qismi – foydalanuvchi qismida o'rnatilgan web-interfeys va uning bazasi web-serverga o'rnatilgan. Undagi yuz tasvirini ro'yxatga olish, xususiyatlarini ajratish, shuningdek, yuz tasviri bo'yicha identifikatsiya jarayonining barcha bosqichlari mazkur qismda amalga oshiriladi.



4.28-rasm. Yuz tasviri bo'yicha identifikatsiya jarayoni dasturiy vositasining ishlash sxemasi

Yuz tasviri bo'yicha identifikatsiya jarayoni dasturiy vositasida quyidagi funksiyalar mavjud:

ro'yxatga olish – bitta shaxsga tegishli bir nechta (20 tadan ko'p tavsiya etiladi) turli holat (o'ng, chap, old, tepa va past) va ko'rinishidagi (kulgan, yig'lagan, xafa bo'lgan) yuz tasvirlaridan iborat baza shakllantiriladi. Hosil bo'lgan baza teran o'rganish tarmog'iga yuz tasviri xususiyatlarini ajratish uchun yuklanadi va natijada har bir foydalanuvchiga tegishli tasvirning muhim xususiyatlaridan iborat bo'lgan *.pickle* kengaytmali baza shakllantiriladi.

Bitta shaxsga tegishli bir nechta yuz tasvirini to'plashda suratga tushirish imkoniyatiga ega bo'lgan barcha qurilmalardan foydalanish mumkin.

Ro'yxatga olishda tasvir xususiyatlari bitta massivga biriktirilishi va uning o'lchami uchun talab qo'yilganligi bois, katta hajmli tasvirlar maxsus *imresize(i)* funksiyasi asosida kichik o'lchamga keltiriladi. Bu esa, o'rganish jarayonining tez amalga oshirilishiga yordam beradi.

Bitta foydalanuvchiga tegishli barcha yuz tasvirlari nomlangan katalogda saqlanganligi sababli, ushbu nom identifikatsiya jarayonida foydalanuvchi yorlig'i sifatida xizmat qiladi. Tanib olishda xususiyatlar mos kelganida ushbu yorliq taqdim etiladi.

yuz tasvirini aniqlash – ishlab chiqilgan uchburchak usuli asosida *.dlib* (*detection library* – aniqlash kutubxonasi) kutubxonasi yaratilgan va yuz tasvirini aniqlash jarayoni amalga oshiriladi. Tanib olish ko'rsatkichining samaradorligi yuz tasvirini aniqlash natijasiga bog'liq;

qalbakilikka tekshirish – haqiqiy bo'lmagan yuz tasviri piksellarga asoslangan usul yordamida aniqlanadi. Ushbu jarayon tanib olish jarayonida yolg'ondan rad qilish xatoligini ortishiga olib kelishi sababli, talab etilmaydigan joylarda ushbu funksiyani o'chirib, to'g'ridan-to'g'ri tanib olish jarayoniga o'tish mumkin. Ushbu funksiya kamera orqali identifikatsiyani amalga oshirishda qo'llaniladi;

normallashtirish – aniqlangan yuz tasviridan to'siqlarni olib tashlashda asosiy komponentlar orqali ishlab chiqilgan yuz tasvirini normallashtirish usulidan foydalaniladi. Yolg'ondan tasvirida to'siq mavjud bo'lgan holda, tanib olish xatoligi katta bo'lishi mumkin. Shu sababli, ushbu funksiyani shaxs ishtirok etadigan identifikatsiya tizimlarida qo'llash lozim;

tanib olish – ro'yxatga olishda hosil qilingan *.pickle* kengaytmali baza asosida tanib olish amalga oshiriladi. Tanib olish uch xil ma'lumot turi asosida amalga oshiriladi:

Rasm asosida. Tanlangan yuz tasviri kimga tegishli ekanligini aniqlashda qo'llaniladi. Buning uchun yuz tasviri tanlanadi va qidirish qismiga o'tiladi. Natijada, sahifada yashil rangli to'rtburchak bilan belgilangan yuz tasviri va uning egasining nomi yozilgan rasm namoyon bo'ladi.

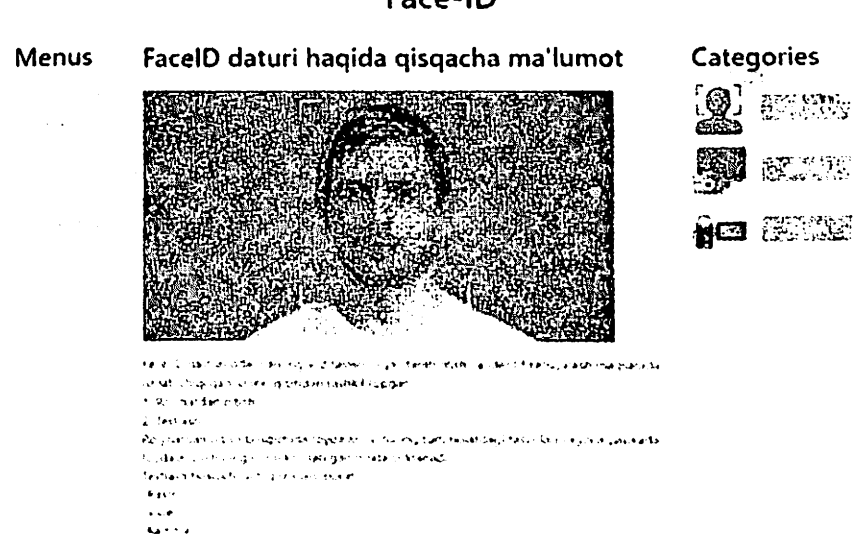
Video asosida. Video faylda yozib olingan shaxslarning yuz tasvirlari bazada ro'yxatdan o'tgan bo'lsa, yashil rangli to'rtburchak bilan belgilangan yuz tasviri va uning egasining nomi yozilgan yangi video fayl hosil bo'ladi. Qidirilayotgan shaxsning harakatlari uning nomi orqali qayd etiladi.

Kamera asosida. Odatda yuz tasviri bo'yicha identifikatsiya vositalari kameralar yordamida tashkilotning kirish qismida o'rnatiladi.

Bazada mavjud shaxslar harakati vaqt asosida qayd etib boriladi. Bu orqali xodimlarning ishga kelgan va ishdan ketgan vaqtlarini qayd etish mumkin. Kamerani kuzatish huquqiga ega hodimda kamera tomonidan yozib olinayotgan video fayl va onlayn ko'rish jarayonida xodimlar identifikatorini ko'rish imkoniyati mavjud bo'ladi.

Teran o'rganish tarmoqlari yuqori hisoblash imkoniyatlariga ega mashinalarni talab etadi. Grafik protsessorlardan foydalanish o'rganish va tanib olish uchun sarflanadigan vaqtni bir necha martaga kamaytirishga imkon beradi.

4.29-rasmda Face-ID dasturining asosiy oynasi keltirilgan bo'lib, menyu, o'rta oyna va kategoriyalardan tashkil topgan. Tanlangan menyu o'rta oynada namoyon bo'ladi.



4.29-rasm. Face-ID dasturining asosiy oynasi

4.13-jadvalda oddiy, yuqori imkoniyatli protsessor va grafik protsessorga ega kompyuterlarda o'tkazilgan testlash vaqtlari keltirilgan. Qayd etilganidek, yuz tasviri bo'yicha identifikatsiya tizimlari uchun sarflanadigan vaqtni kamaytirishga yuqori imkoniyatli protsessor va grafik protsessorga ega hisoblash mashinalaridan foydalanish orqali erishish mumkin.

4.13-jadval

Oddiy, yuqori imkoniyatli protsessor va grafik protsessorga ega kompyuterlarda o'tkazilgan testlash vaqtlari

Kompyuter turi / Vaqt	Intel core i3 3.3GHz, 4Gb tezkor xotira	Core i7 7700K, 16Gb tezkor xotira	Core i7 7700K, 16Gb tezkor xotira, GTX 1080 TI grafik protsessor
O'rganish vaqti (bitta yuz tasviri uchun)	0,5 s	30 ms	10 ms
Testlash vaqti (bitta yuz tasviri uchun)	2 s	0,7 s	0,5 s

Teran o'rganish tarmoqlarida tadqiqotlar olib borish va amaliyotga tatbiq qilish uchun *Nvidia Titan RTX* yoki arzonroq *Nvidia GeForce RTX 2080Ti* grafik protsessorlaridan foydalanish yuqori samara beradi.

Yuz tasviri bo'yicha identifikatsiya jarayoni dasturiy vositasi Python dasturlash tilida yozilgan bo'lib, natijalarni taqdim etish va foydalanuvchi interfeysi qismlari web dasturlash tillarida yaratilgan.

XULOSA

Ushbu monografiya yuz tasviri bo'yicha identifikatsiya va autentifikatsiya jarayoni samaradorligini oshirish masalalariga qaratilgan quyidagi natijalarga erishildi:

Axborot xavfsizligini ta'minlash darajasini oshirishda biometrik parametrlardan foydalanish samaralari va ularning qiyosiy tahlili keltirilgan. Unga ko'ra, yuz tasviri asosida masofadan odamlarni identifikatsiyalash va tashkilot hududidagi shaxslarning harakatini kuzatish imkoniyati yuzaga keladi.

Yuz tasvirini aniqlash samaradorligini oshirish uchun uchburchak usuli ishlab chiqilgan bo'lib, natijada murakkab sharoitlarda ham yuz tasvirini aniqlash hamda yuz tasvirini aniqlash darajasini 99,7% gacha oshirish va yolg'ondan rad qilish darajasini esa, 0,3 % gacha pasaytirish imkonini berdi. Yuz tasviri bo'yicha identifikatsiya tizimlarida mavjud tahdidlar alohida nuqtalar asosida keltirilgan.

Yuz tasviri bo'yicha identifikatsiyada yuz tasvirini aniqlashda an'anaviy usullardan va tanib olishda teran o'rganish usullaridan foydalanishning umumlashgan sxemasi ishlab chiqildi va har bir bosqichida qo'llaniladigan jarayonlar ketma-ketligi keltirildi. Mazkur sxema yuz tasviri bo'yicha identifikatsiya jarayoni samaradorligini oshirishga xizmat qiladi.

Yuz tasviri bo'yicha identifikatsiya va autentifikatsiya jarayonida yuz tasvirida to'siq mavjud holatlar aniqlanganda normallashtirish usuli asosida to'siqni olib tashlash va tanib olish aniqligini oshirish usuli va algoritmi ishlab chiqildi, to'siq mavjud yuz tasvirlari ishtirokida amalga oshirilgan tahlil natijasida yolg'ondan rad etish xatoligini 14 % gacha kamaytirishga imkon berdi. Bundan tashqari, yuz tasvirini tanib olish samaradorligini oshirishning takomillashgan zichlash-faollashtirish tarmog'i taklif etildi, yuz tasvirini tanib olish aniqligi 0,9 % ga ortishiga va yolg'ondan rad etish xatoligini esa 8% gacha pasaytirishga erishildi. Tarmoqdagi filtrni samarali o'lchamga keltirish natijasida, hisoblash parametrlari sonining ikki martagacha kamayishiga, ya'ni hisoblash tezligi ortishiga imkon berdi.

Yuz tasvirini tanib olishning teran o'rganish tarmoqlarida qo'llaniladigan yuz tasviri bazalari talablariga mos Universitet_MB va Uzb_MB yuz tasviri bazalari shakllantirildi. Ochiq yuz tasviri bazalari va yuz tasvirini tanib olish usullari asosida tahlil etilganida, ularning tanib olish ko'rsatkichlari yuqori, ya'ni tanib olishning taklif etilgan

usulida 92,5 % aniqlikni ko'rsatdi. Tanib olish aniqligini yanada oshirish uchun yuz tasviri bazalarini shakllantirishga tavsiyalar ishlab chiqildi va ular yuz tasviri bo'yicha identifikatsiya jarayoni samaradorligini oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Computer SeCurity, PrinciPles and Practice. William Stallings, Lawrie Brown. Copyright © 2015 by Pearson Education, Inc.

2. Информационная безопасность компьютерных систем и сетей. В. Ф. Шаньгин. Москва, ИД «ФОРУМ» - ИНФРА-М, 2011.

3. Information security, Principles and Practice. Mark Stamp. John Wiley & Sons, Inc, 2011.

4. R.D.Seely , M.Goffredo, J. N.Carter, M.S.Nixon (2009), View Invariant Gait Recognition, Handbook of Remote Biometrics for Surveillance and Security.

5. S.Theodoridis and K.Koutroumbas, Pattern recognition, 4th ed., Academic Press, 2009.

6. Рутковская, М.Пилиньский, Л.Рутковский. Нейронные сети, генетические алгоритмы и нечеткие системы // Пер. с польского М.: Горячая линия-Телеком, 2004 – 452 с.

7. 2016 Financial Industry Cybersecurity Report. Security Scorecard R&D Department. August 2016.

8. FIPS PUB 200. Minimum Security Requirements for Federal Information and Information Systems. NIST – 2006.

9. Authentication methods. INF5261. Final report. University of Oslo, Department of Informatics. H.Joachim, J.Mirkovich, I.Milanovich, O.Bakkeli. 2010.

10. Biometrics: the Future of Mobile Payments. U.S. Economic Watch. Nathaniel Karp. 20 July 2015.

11. J. Daugman, Biometric personal identification system based on Iris Recognition, U.S. (1994). Patent 5,291,560.

12. Wang, Yue. "Ant Financial Said To Close $150B Funding Round". Forbes. Retrieved 2018-06-18.

13. R.O.Duda, P.E.Hart, D. G. Stoke, Pattern classification, 2nd ed., John Wiley & Sons, 2001.

14. Linda Shapiro. Recognition, Part II: Face Detection via AdaBoost. CSE 4551 course materials. 2015.

15. Jumayev T.S. Biometrik tizimlarda tasvirlarga dastlabki ishlov berish algoritmlari. 05.01.03 – Informatikaning nazariy asoslari. Texnika fanlari bo'yicha falsafa doktori (Phd) dissertasiyasi avtoreferati. Toshkent - 2018 y. B. 47.

16. Rui Min. Face recognition robust to occlusions. PhD thesis. 2013. Paris. P.183.

17. Council, F.F.I.E., Authentication in an electronic banking enviroment. 2005.

18. 2014 -2018 Global Card Market. Trends & Forecasts. The Next 5 Years? 2015 ICMA EXPO – 25th Anniversary. Phoenix, AZ – March 30, 2015.

19. De Carrera P.F., Marques I. Face recognition algorithms //Master's thesis in Computer Science, Universidad Euskal Herriko. – 2010. – T. 1.

20. C.J.C.Burges. A tuturial on support vector machines for pattern recognition. Data mining and knowledge discovery, (submitted), 1998.

21. Lawrence O'Gorman. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003.

22. A survey on biometric cryptosystems and cancelable biometrics. Christian Rathgeb, Andreas Uhl. EURASIP Journal on Information Security 2011, 2011:3.

23. R. Giot, M. El-Abed, C. Rosenberger, Keystroke dynamics authentication for collaborative systems, Intl. Symposium on Collaborative Technologies and Systems, (2009). Pp.172-179.

24. S. Sengupta, J.-C. Chen, C. Castillo, V. M. Patel, R. Chellappa, and D.W.Jacobs. Frontal to profile face verification in the wild. In WACV, pages 1–9. IEEE, 2016.

25. S.Saxena and J.Verbeek. Heterogeneous face recognition with cnns. In ECCV, pages 483–491. Springer, 2016.

26. S.Hong, W.Im, J.Ryu, and H.S.Yang. Sspp-dan: Deep domain adaptation network for face recognition with single sample per person. arXiv preprint arXiv:1702.04069, 2017.

27. D. Kim, M. Hernandez, J. Choi, and G. Medioni. Deep 3d face identification. arXiv preprint arXiv:1703.10714, 2017.

28. Jain A., Bolle R., and Pankanti S. Introduction to Biometrics: Personal Identification in Networked Society. KluwerAcademic, Boston, 1999, pp. 46-49.

29. Fazilov S.K., Mirzaev N.M., Mirzaeva G.R. Modified Recognition Algorithms Based on the Construction of Models of Elementary Transformations //Procedia Computer Science. – 2019. – T. 150. – pp. 671-678.

30. R.L.Hsu, M.Abdel-Mottaleb, and A.K.Jain, "Face detection in color images" IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 5, 2002. pp. 696–706.

31. Yang M.H., Kriegman D.J., and Ahuja N. "Detecting face in images: a survey," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, pp. 34–58, 2002.

32. Valenti R. et al. Machine learning techniques for face analysis //Machine Learning Techniques for Multimedia. – Springer, Berlin, Heidelberg, 2008. – гг. 159-187.

33. Adini Y. Face recognition: the problem of compensating for changes in illumination direction. IEEE Transactions on Pattern Analysis and Machine Intelligence. Volume: 19, Issue: 7, Jul 1997, pp. 721-732.

34. Live Science Staff. Our Face Bones Change Shape as We Age. January 5, 2011. Live science, pp. 437-447.

35. Sveikata K. et al. Factors influencing face aging. Literature review //Stomatologija. – 2011. – Т. 13. – №. 4. – гг. 113-116.

36. Noyes E., Jenkins R. Camera-to-subject distance affects face configuration and perceived identity //Cognition. – 2017. – Т. 165. – pp. 97-104.

37. Wang C.M. et al. Distinguishing falsification of human faces from true faces based on optical flow information //2009 IEEE International Symposium on Circuits and Systems. – IEEE, 2009. – pp. 2609-2612.

38. Huang G.B. et al. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. – 2008, pp. 1-11.

39. Wenchao Zhang, Shiguang Shan, Xilin Chen and Wen Gao, "Local Gabor Binary Patterns Based on Kullback- Leibler Divergence for Partially Occluded Face Recognition," IEEE signal processing letters, vol. 14, no. 11, november 2007, pp. 875-878.

40. Sonia Ohlyan, Sunita Sangwan. A Survey On Various Problems & Challenges In Face Recognition. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 www.ijert.org Vol. 2 Issue 6, June - 2013, pp. 2533-2538.

41. Rubal Jain, Chander Kant. Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research 2015; 1(07). pp. 283-288. 10.7439/ijasr.

42. Rajana R., Sunnyb A. Detecting Face Spoof Using IDA Features and Colour Texture Analysis. International Journal of Control Theory and Applications. Volume 10 • Number 30 • 2017, pp. 309-316.

43. R. Brunelli and T. Poggio. Face recognition: Features versus templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(10):1042–1052, October 1993

44. A.Jain, R.Duin, and J.Mao. Statistical pattern recognition: A review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1):4–37, January 2000.

45. A.K.Jain, R.P.W. Duin, and J.C.Mao, "Statistical pattern recognition: a review," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 4–37, 2000.

46. M.M.Ghazi and H.K.Ekenel. A comprehensive analysis of deep learning based representation for face recognition. In CVPR Workshops, volume 26, pr. 34–41, 2011.

47. Мищенкова Е.С. Сравнительный анализ алгоритмов распознавания лиц //Вестник Волгоградского государственного университета. Серия 9: Исследования молодых ученых. – 2013. – №. 11.

48. P.N.Belhumeur, J.P.Hespanha, and D.J.Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 711–720, 1997.

49. X.He, S.Yan, Y.Hu, P.Niyogi, and H.Zhang, "Face recognition using Laplacianfaces," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27, no. 3, pp. 328-340, 2005.

50. J.Wright, A.Y.Yang, A.Ganesh, S.S.Sastry, and Y.Ma, "Robust face recognition via sparse representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 31, no. 2, 210-227, 2009.

51. Delac K., Grgic M., Grgic S. Independent comparative study of PCA, ICA, and LDA on the FERET data set //International Journal of Imaging Systems and Technology. – 2005. – T. 15. – №. 5. – S. 252-260. 5-6-betlar

52. M.Lades, J.C.Vorbriiggen, J.Buhmann, J.Lange, C. von der Malsburg, R.P.Wiirtz, and W.Konen, "Distortion invariant object recognition in the dynamic link architecture," IEEE Trans. on Computers, vol. 42, no. 3, pp. 300-311, 1993.

53. T.Ahonen, A.Hadid, and M.Pietik¨ainen, "Face recognition with local binary patterns," Proc. Eighth European Conf. Computer Vision, pp. 469-481, 2004.

54. Yan K., Chen Y., Zhang D. Gabor surface feature for face recognition //The First Asian Conference on Pattern Recognition. – IEEE, 2011. – S. 288-292. 4-5-betlar

55. Исаев А.Л., Газаров Д.А., Евсеев С.Д. Распознавание лиц по изображениям // Символ науки. – 2017. – Т. 2. – №. 4. – S. 70-76.

56. Iqtait M., Mohamad F.S., Mamat M. Feature extraction for face recognition via Active Shape Model (ASM) and Active Appearance Model (AAM) //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2018. – Т. 332. – №. 1. – S. 012032. 6-9-betlar

57. D.G.Lowe, "Distinctive image features from scale-invariant keypoints," Int'l Journal of Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.

58. Patel R., Rathod N., Shah A. Comparative analysis of face recognition approaches: a survey //International Journal of Computer Applications. – 2012. – Т. 57. – №. 17. 7-8-betlar

59. Chao W.L. Face recognition //GICE, National Taiwan University. – 2007. 31-54-betlar

60. Tashev K.A., Xudoykulov Z.T., Islomov Sh.Z. "Yuzlarni tanib olish algoritmlarini tahlillash". «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. 1(45)/2018, 32-41. Toshkent 2018.

61. Bhutekar S.J., Manjaramkar A.K. Parallel face Detection and Recognition on GPU //International Journal of Computer Science and Information Technologies. – 2014. – Т. 5. – №. 2. – S. 5-6-betlar.

62. Valenti R. et al. Machine learning techniques for face analysis //Machine Learning Techniques for Multimedia. – Springer, Berlin, Heidelberg, 2008. – S. 159-187.

63. I.Cohen, N., A.Garg, L.Chen, and T.S.Huang. Facial expression recognition from video sequences: Temporal and static modelling. Computer Vision and Image Understanding, 91(1-2):160–187, 2003.

64. Kasar M.M., Bhattacharyya D., Kim T.H. Face recognition using neural network: a review //International Journal of Security and Its Applications. – 2016. – Т. 10. – №. 3. – S. 81-100.

65. Lu Z., Jiang X., Kot A. Enhance deep learning performance in face recognition //Image, Vision and Computing (ICIVC), 2017 2nd nternational Conference on. – IEEE, 2017. – S. 1-2-betlar.

66. Liu Y., Li H., Wang X. Rethinking feature discrimination and polymerization for large-scale recognition //arXiv preprint arXiv:1710.00870. – 2017. 7-bet.

67. Gawande M.P., Agrawal D.G. Face recognition using PCA and different distance classifiers //IOSR Journal of Electronics and Communication Engineering. – 2014. – T. 9. – №. 1. – pp. 1-5.

68. Hu J., Shen L., Sun G. Squeeze-and-excitation networks //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2018.pp. 7132-7141.

69. Tashev K.A., Khudoykulov Z.T., Islomov Sh.Z. Normalization of Facial Occlusion in Face Recognition. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: Volume-8 Issue-11, September 2019. rr. 2278-3075.

70. Wang M., Deng W. Deep face recognition: A survey //arXiv preprint arXiv:1804.06655. – 2018, rr. 1-24.

71. Li B., Zhang D., Wang K. Online signature verification based on null component analysis and principal component analysis //Pattern analysis and applications. – 2006. – T. 8. – №. 4. – r. 345.

72. Karimov M.M, Islomov Sh.Z, Bekmirzayev O.N, Zokirov O.Yo. Yuzlarni tanib olish samaradorligini oshirish usullari. Muhammad al-Xorazmiy avlodlari ilmiy-amaliy va axborot-tahliliy jurnal. 1(7)2019. ISSN-2181-9211. B. 12-18.

73. Mei Wang, Weihong Deng. Deep Face Recognition: A Survey. arXiv:1804.06655v7. 28 September, 2018, rr. 1-24.

74. Kamilov M., Hudayberdiev M., Khamroev A. Algorithm for the Development of a Training Set that Best Describes the Objects of Recognition //Procedia Computer Science. – 2019. – T. 150. – pp. 116-122.

75. Yi D., Lei Z., Liao S., and Li S. Learning face representation from scratch. arXiv preprint arXiv:1411.7923, 2014, pp. 1-9.

76. Guo Y., Zhang L., Hu Y., He X., and Gao J. Ms-celeb-1m: A dataset and benchmark for large-scale face recognition. In ECCV, pp. 87– 102. Springer, 2016.

77. Karimov M.M. Islomov Sh.Z. "Optimising And Recommendations For Collecting Face Databases" //International Journal of Research in Engineering and Science (IJRES) ISSN (Online). – pp. 2320-2324.

78. Karimov M.M., Tashev K.A., Islomov Sh.Z., Xudoykulov Z.T., Xujayarov I.Sh. Increasing accuracy and reducing time of face

recognition with Euclid norm. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 4, Issue: 4, pp.536 – 540.

79. Classification of security threats in information systems. Mouna Jouini,Latifa Ben Arfa Rabai,Anis Ben Aissa. 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014).

80. Biometric Authentication System: Tools and Techniques. Ishpreet Singh Virk, Raman Maini. International journal of computer application. Issue2, Volume 2 (April 2012).

81. Islomov Sh.Z., Zulfiqorov Z.Z. Yuzlarni tanib olishning asosiy bosqichlari. Elektron xukumat tizimida axborot xavfsizligi muammolari va ularning yechimlari" mavzusi buyicha Respublika seminari, Toshkent, 27 oktyabr, 2017 y, B. 57-60.

82. Tashev.K.A., Nasrullayev N.B., Islomov Sh.Z. Information security monitoring in face recognition system. "Axborot texnologiyalarini rivojlantirish istiqbollari ITPA - 2015" Xalqaro anjumani, 2015 yil, 4-5 noyabr. B. 113-117.

83. Islomov Sh.Z. Using method denoising low frequency noise on low-light image for face recognition. «Axborot va telekommunikatsiya texnologiyalari muammolari» Ilmiy-texnik konferensiyasining ma'ruzalar to'plami, 1-qism, 12-13 mart 2015 y., B. 389-391.

84. Islomov Sh.Z. Biometrik autentifikatsiya tizimlarining bosqichlaridagi xujumlar, "Iqtisodiyotning tarmoqlarini innovasion rivojlanishida axborot-kommunikatsiya texnologiyalarining ahamiyati" mavzusidagi Respublika ilmiy-texnika anjuma. Toshkent, 2019, B. 192-194.

85. Gao X. et al. Standardization of face image sample quality //International Conference on Biometrics. – Springer, Berlin, Heidelberg, 2007. pp. 242-251.

86. C.Liu and H.Wechsler. A unified bayesian framework for face recognition. In roc. of the 1998 IEEE International Conference on Image Processing, ICIP'98, pages 151–155, Chicago, USA, October 1998.

87. G.Guo, S.Li, and K.Chan. Face recognition by support vector machines. In Proc. of the IEEE International Conference on Automatic Face and Gesture Recognition, pages 196–201, Grenoble, France, March 2000.

88. Islomov Sh.Z., Davronova L.U., Ergashev M.M. Yuzlarni tanib olishning samaradorligini oshirish usullari. «Axborot texnologiyalari va

kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari» Respublika miqyosidagi ilmiy-texnik konferensiya, 22-23 noyabr, 2018 yil, Toshkent. B.132-135.

89. Islomov Sh.Z., Mavlonov O.N., Ergashev M.M., Yuz xususiyatlari orasidagi farqni hisoblash usullari. «Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi va kiberxavfsizlik muammolari» Respublika miqyosidagi ilmiy-texnik konferensiya, 22-23 noyabr, 2018 yil, Toshkent. (165-167-betlar).

90. Islomov Sh.Z., Mavlonov O.N., Ergashev M.M. Yuz xususiyatlari orasidagi farqni hisoblash usullari. «Axborot texnologiyalari va kommunikatsiyalari soxasida axborot xavfsizligi va kiberxavfsizlik muammolari» Respublika miqyosidagi ilmiy-texnik konferensiya, 22-23 noyabr, 2018 yil, Toshkent. (pp.165-167)

91. Islomov Sh.Z., Yusupov B.K. Using parallel computing on face recognition systems. "Axborot texnologiyalarini rivojlantirish istiqbollari ITPA - 2015" Xalqaro anjumani, 2015 yil 4-5 noyabr. B. 93-96.

92. Malikovich, K.M., Axmatovich, T.K., Zokirugli, I.S., & Zarif, K. (2014, January). Minimizing in Face Recognition Errors and Preprocessing Time. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE). International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE), pp. 212-217.

93. Hu J., Shen L., Sun G. Squeeze-and-excitation networks //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2018.pp. 7132-7141.

94. Dalal N., Triggs B. Histograms of oriented gradients for human detection //Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on. – IEEE, 2005. – T. 1. – rr. 886-893.

95. Khudoykulov Z.T., Islomov Sh.Z.,. Davronova L.U, Mardiev U.R. New robust face anti-spoofing technique. Кодирование и цифровая обработка сигналов в инфокоммуникациях. материалы международной научно-практической конференции. Минск, 4 апреля 2019 г, pp. 57-61.

96. Tahdid turlari: RFC 4949 (sayt). URL: https://tools.ietf.org/html/rfc4949. (Murojaat vaqti: 30.11.2020)

97. "Randomize" vositasi yordamida parollarni hisoblash vati (sayt). URL: http://random-ize.com/how-long-to-hack-pass/. (Murojaat vaqti: 30.11.2020).

98. "BetterBuys" vositasi yordamida parollarni hisoblash vati (sayt). URL: https://www.betterbuys.com/estimating-password-cracking-times/. (Murojaat vaqti: 30.11.2020).

99. Parollarni aniqlash vati (sayt). URL: http://www.networkworld.com/article/3158213/security/25-most-common-passwords-in-2016-and-how-quickly-they-can-be-cracked.html. (Murojaat vaqti: 30.11.2020).

100. Xavfsiz token (sayt). URL: https://en.wikipedia.org/wiki/Security_token. (Murojaat vaqti: 30.11.2020).

101. Mobil biometric tashkilotlar (sayt). URL: https://www.technavio.com/blog/top-10-mobile-biometrics-companies. (Murojaat vaqti: 30.11.2020).

102. priv-ID biometrik kriptografik tizim (sayt). URL: http://www.priv-id.com/. (Murojaat vaqti: 30.11.2020).

103. Genkey AS (sayt). URL: http://genkeycorp.com/. (Murojaat vaqti: 30.11.2020).

104. Precise Biometrics AB (sayt). URL: http://www.precisebiometrics.com/. (Murojaat vaqti: 30.11.2020).

105. IAFIS FBI identifikatsiya tizimi (sayt). URL: https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis. (Murojaat vaqti: 30.11.2020).

106. Microphone array ovoz ma'lumotlar bazasi (sayt). URL: http://www.speech.cs.cmu.edu/databases/micarray/. (Murojaat vaqti: 30.11.2020).

107. Census (AN4) ovoz ma'lumotlar bazasi (sayt). URL: http://www.speech.cs.cmu.edu/databases/an4/. (Murojaat vaqti: 30.11.2020).

108. Let's Go Speech Dialog Data ovoz ma'lumotlar bazasi (sayt). URL: http://www.speech.cs.cmu.edu/letsgo/letsgodata.html. (Murojaat vaqti: 30.11.2020).

109. Harakatga asoslangan autentifikatsiya (sayt). URL: https://en.wikipedia.org/wiki/Gait_analysis#Applications. (Murojaat vaqti: 30.11.2020).

110. CASIA harakatga asoslangan autentifikatsiya bazasi(sayt). URL:http://www.cbsr.ia.ac.cn/english/Gait%20Databases.asp. (Murojaat vaqti: 30.11.2020).

111. OU-ISIR harakatga asoslangan autentifikatsiya bazasi (sayt). URL: http://www.am.sanken.osaka-u.ac.jp/BiometricDB/GaitLP.html. (Murojaat vaqti: 30.11.2020).

112. TUM-IITKGP harakatga asoslangan autentifikatsiya bazasi (sayt). URL: https://www.mmk.ei.tum.de/verschiedenes/tum-iitkgp-gait-database/. (Murojaat vaqti: 30.11.2020).

113. Husnixat xususiyatiga asoslangan autentifikatsiya usullari (sayt). URL: http://www.biometric-solutions.com/keystroke-dynamics.html. (Murojaat vaqti: 30.11.2020).

114. Husnixat xususiyatiga asoslangan autentifikatsiya bazasi (sayt). URL: http://www.vmonaco.com/keystroke-datasets. (Murojaat vaqti: 30.11.2020).

115. NEC yuz tasviriga asoslangan autentifikatsiya tizimi (sayt). URL: http://www.nec.com/en/global/solutions/safety/face_recognition/index.html. (Murojaat vaqti: 30.11.2020).

116. COGNITEC yuz tasviriga asoslangan autentifikatsiya tizimi (sayt). URL: http://www.cognitec.com. (Murojaat vaqti: 30.11.2020).

117. Neurotechnology yuz tasviriga asoslangan autentifikatsiya tizimi (sayt). URL: http://www.neurotechnology.com. (Murojaat vaqti: 30.11.2020).

118. Qo'l geometriyasi asosida identifikatsiya tizimlari (sayt). URL: http://www.futuremarketinsights.com/reports/hand-geometry-biometrics-market. (Murojaat vaqti: 30.11.2020).

119. Qo'l geometriyasi asosida identifikatsiya bazasi (sayt). URL: http://bosphorus.ee.boun.edu.tr/hand/Home.aspx. (Murojaat vaqti: 30.11.2020).

QISQARTMA SO'ZLAR RO'YXATI

2D - 2-dimensional.
3D - 3-dimensional.
AAM - Active Appearance Model.
AdaBoost – Adaptive Boosting.
AMS - Approximate median significance.
AR - Aleix Robert.
ArcFace - Additive Angular Margin.
ASM - Active Shape Model.
BAA – Birlashgan Arab Amirliklari.
CACD - Cross-Age Celebrity Dataset.
CASIA - Institute of Automation of Chinese Academy of Sciences.
CCL - Center for Creative Leadership.
CESG - Canada Education Savings Grant.
CMU - Carnegie Mellon University.
CNN - convolutional neural network.
Cosface – Cosine face.
CPU - central processing unit.
CSI/FBI - Computer Security Institute/ Federal Bureau of Investigation's.
DCT - Discrete Cosine Transform.
DL – Deep Learning.
DNA - deoxyribonucleic acid.
DoS - Denial of Service.
FDLib – Face detection library.
FERET - Facial Recognition Technology.
FSDK – Face software development kit.
FVC - Fingerprint verification competition.
GAN - Generative adversarial network.
GPU - graphics processing unit.
IAFIS FBI - Integrated Automated Fingerprint Identification System.
ICA - independent component analysis.
ID – Identifier.
IIT - Intellectual information technology.
ILSVRC - ImageNet Large Scale Visual Recognition Competition.
IP – Internet protocol.
JPEG - Joint Photographic Experts Group.

LDA - Linear Discriminant Analysis.
LFW - Labeled Faces in the Wild.
LLC - Limited Liability Company.
LPB - Local Binary Patterns.
MF - matrix factorization.
MS-Celeb – Microsoft Celebration.
NEC - Nippon Electric Corporation.
NIST - National Institute of Standards and Technology.
NLPR - National Laboratory of Pattern Recognition.
OCV – OpenCV.
OpenCV - Open Source Computer Vision Library.
ORL - Oracle Research Laboratory.
OU-ISIR - Osaka University - Institute of Scientific and Industrial Research.
PCA - principal component analysis.
PIN - Personal Identification Number.
RCG - Resources Cooperation Group.
ReLu - rectified linear unit.
ResNet - Residual Network.
RFID - Radio Frequency IDentification.
RGB – Red Green Blue.
SAE - Social Adaptive Ensemble.
SDK - software development kit.
SENet - Squeeze-and-Excitation Networks.
SIF - Source Input Format.
SIFT - scale-invariant feature transform.
SIM - Subscriber Identification Module.
SNT – Svyortkali neyron tarmoq.
SVM - Support vector machine.
TATU – Toshkent axborot texnologiyalari universiteti.
Universitet_MB – Universitet Ma'lumotlar Bazasi.
Uzb_MB – O'zbek Ma'lumotlar Bazasi.
VGG - Visual Geometry Group.

Mundarija

K.A.Tashev,
Z.T.Xudoyqulov, Sh.Z.Islomov

YUZ TASVIRI ASOSIDA SHAXSNI IDENTIFIKATSIYALASH VA AUTENTIFIKATSIYALASH JARAYONINING SAMARADORLIGINI OSHIRISH

(MONOGRAFIYA)

Toshkent – «NIHOL PRINT» OK – 2021

Muharrir: A.Tog'ayev
Tex. muharrir: F.Tog'ayeva
Musavvir: B.Esanov
Musahhiha: O.Muxammadiyeva
Kompyuterda sahifalovchi: G.Tog'ayeva

9323

№ 7439-765f-47f1-7ea1-a683-4648-1314.
Bosishga ruxsat etildi: 1.03.2021. Bichimi 60x841 /16.
Shartli bosma tabog'i 8,0. Nashr bosma tabog'i 7,75.
Adadi 20. Buyurtma № 7.

«Nihol print» Ok da chop etildi.
Toshkent sh., M. Ashrafiy ko'chasi, 99/101.