

səviyyəsinə əsasən təsnifatına gətirir. Bunu etmək üçün müəyyən bir yol yoxdur, lakin dörd səviyyəli ISO 27001 məlumat təsnifatı yaxşı bir başlanğıc nöqtəsi ola bilər. Sonra, hər bir məlumat növünün məlumatların qorunması, ehtiyat nüsxəsi və şifrələməsi və ötürülməsi baxımından necə işlənəcəyi təsvir edilir.

Informasiya təhlükəsizlik siyasəti yazmaq hekayənin yalnız yarısıdır. Ön çox yayılmış kibertəhlükəsizlik təhdidlərinə, şirkətin təmiz masa prinsiplərinə, IT resurslarından məqbul istifadəyə və təhlükəsizlik pozuntusu zamanı atılacaq addımlara diqqət yetirən məlumatların mühafizəsi protokolları üzrə təlim sessiyaları təşkiləlməlidir.

Sonra, şəbəkə, cihaz və məlumat təhlükəsizliyi, siyasətin həyata keçirilməsi, təhsil, habelə insidentlərin hesabatı və cavab tədbirləri ilə bağlı gündəlik işçilərin vəzifələrini müəyyənləşdirilir.

Nəticə

Son yarım əsr ərzində təşkilatlar öz biznes proseslərini idarə etmək üçün informasiya sistemlərini tətbiq ediblər. Bu informasiya sistemləri indi daha çox müəssisə informasiya sistemləri kimi tanınan sistemlərə çevrilmişdir. Təşkilatda müəssisənin informasiya sisteminin tətbiqinin vacib tərəfi biznes prosesləri üçün informasiya sistemi daxilində təhlükəsizliklə bağlı məsələlərin işlənilməsi və hazırlanmasıdır. Informasiya təhlükəsizlik siyasəti mühüm prosesdir. Budur ki, məlumatların icazəsiz girişdən qorunması, müəssisənin təhlükəsizliyinin təmin edilməsi baxımından təhlükəsizlik siyasəti mükəmməl vasitədir. Informasiya təhlükəsizliyi siyasəti vasitəsi ilə kibertəhlükəsizliyə ümumi yanaşmanı müəyyən etmək, istifadəçilərə təhlükəsizliklə bağlı aydın və müvafiq təlimat təklif etmək və effektiv, təhlükəsiz informasiya idarəçiliyi üçün məsuliyyət, vəzifə və rolları bölmək mümkündür.

Ədəbiyyat

- [1] <https://tresorit.com/blog/how-to-create-an-enterprise-information-security-policy-and-make-it-stick-the-2022>
- [2] <https://www.upguard.com/blog/information-security-policy#toc-0>
- [3] <https://blog.rssecurity.com/what-is-the-purpose-of-an-enterprise-information-security-policy/>
- [4] <https://itsecurity.uiowa.edu/policies-standards-guidelines/compliance/enterprise-information-security-program>
- [5] <https://www.ekransystem.com/en/blog/information-security-policies>
- [6] <https://www.caiso.com/NewEmployeeDocuments/EnterpriseInfoSecurityPolicy.pdf>
- [7] <https://www.coskunuz.com.tr/yonetim-sistemleri/politikalar/bilgi-guvenligi-politikasi.html>
- [8] <https://www.elsisan.com/sites/default/files/page/2021-03/BILGI%20GUVENLIGI%20POLITIKASI.pdf>
- [9] <https://www.domainhizmetleri.com/bilgi-guvenligi-politikasi/>
- [10] <https://www.celebiaviation.com/tr/bilgi-guvenligi-politikasi>

ŞƏXSİYYƏT İDARƏÇİLİYİNİN GƏLƏCƏYİ: ÜZ TANIMA SİSTEMLƏRİNİN TƏDQIQI **Rəhimova Nazilə, Əsgərov Nihad** **Azərbaycan Dövlət Neft və Sənaye Universiteti**

Xülasə:

Üz tanıma sistemləri təhlükəsizlik, şəxsiyyətin yoxlanılması və fərdiləşdirilmiş xidmətlərin mənzərəsini yenidən formalaşdıran təməlqoyma texnologiyası kimi ortaya çıxdı. Süni intellekt (AI) və maşın öyrənməsi (ML) ilə təchiz edilmiş mürəkkəb alqoritmlərdən istifadə etməklə, bu sistemlər üz xüsusiyyətlərini əlamətdar dəqiqliklə aşkarlaya, təhlil edə və müqayisə edə bilər. Onların tətbiqləri səmərəlilik və istifadəçi rahatlığı üçün innovativ həllər təklif edərək hüquq-mühafizə orqanları,

pərakəndə satış, səhiyyə və fərdi cihazların təhlükəsizliyi daxil olmaqla müxtəlif domenləri əhatə edir. Bununla belə, sifətin tanınmasının geniş şəkildə tətbiqi məxfilik, etik mülahizələr və alqoritmik qərəzlik ətrafında müzakirələrə səbəb oldu. İcazəsiz nəzarət, avtoritar rejimlər tərəfindən potensial sui-istifadə və sistemlərin ədalətli olması ilə bağlı narahatlıqlar onların tətbiqində möhkəm tənzimləmə və şəffaflıq tələb edir. Bu çətinliklərə baxmayaraq, sifətin tanınması texnologiyası inkişaf etməyə davam edir və süni intellektdə perspektivli irəliləyişlər zəif işıqlı mühitlərdən mürəkkəb kütlələrə qədər müxtəlif ssenarilərdə təkmilləşdirilmiş performansını təmin edir.

Açar Sözlər: Üz tanıma sistemləri, süni intellekt (AI), maşın öyrənməsi (ML), biometrik autentifikasiya, məxfilik və etika, müşahidə texnologiyası, alqoritmik qərəz, şəxsiyyətin yoxlanılması, gələcək tendensiya, Əşyaların İnterneti (IoT)

Giriş : Rəqəmsal dövrdə üz tanıma sistemləri fərdlərin və təşkilatların şəxsiyyətin yoxlanılması, təhlükəsizlik və fərdiləşdirilmiş xidmətlərə yanaşma tərzində inqilab edərək ən əhəmiyyətli texnoloji irəliləyişlərdən biri kimi ortaya çıxdı. Bu sistemlər gözlər arasındakı məsafə, çənə konturları və ya burun forması kimi unikal üz xüsusiyyətlərini təhlil edərək fərdləri müəyyən etmək və yoxlamaq üçün mürəkkəb süni intellekt (AI) və maşın öyrənməsi (ML) alqoritmindən istifadə edir. Bir vaxtlar elmi fantastikada təsvir edilən futuristik texnologiya hesab edilən texnologiya indi gündəlik həyatımıza inteqrasiya olunub və smartfonların kilidini açmaqdan tutmuş sərhədlərdə və hava limanlarında qabaqcıl təhlükəsizlik sistemlərinə qədər müxtəlif proqramları gücləndirir. Üzün tanınması texnologiyasının cəlbediciliyi onun səmərəliliyi, dəqiqliyi və rahatlığı mükəmməl şəkildə birləşdirə bilməsindədir. Unudula, oğurlana və ya saxtalaşdırıla bilən parollar, PIN-lər və ya şəxsiyyət vəsiqələri kimi ənənəvi təhlükəsizlik üsullarından fərqli olaraq, üzün tanınması qeyri-invaziv, əllər-sərbəst və istifadəçi dostu alternativ təmin edir. Onun bank işi, pərakəndə satış və səhiyyə kimi sahələrdə tətbiqi daha çox avtomatlaşdırma, fırıldaqçılığın azaldılması və təkmilləşdirilmiş istifadəçi təcrübələri üçün yol açdı. Məsələn, banklar indi əməliyyatları təsdiqləmək üçün üz identifikasiyasından istifadə edir, pərakəndə satış şirkətləri isə fərdi alış-veriş təcrübələri təklif etmək üçün ondan istifadə edir. Bütün dünyada hökumətlər milli təhlükəsizliyi gücləndirmək və dövlət xidmətlərini sadələşdirmək üçün üz tanıma sistemlərinə də böyük sərmayə qoyurlar. Məsələn, hüquq-mühafizə orqanları real vaxt rejimində şübhəliləri müəyyən etmək üçün texnologiyadan istifadə edir və hava limanları immiqrasiya proseslərini sürətləndirmək üçün ondan istifadə edir. Bu inkişaf daha təhlükəsiz və daha səmərəli mühitlər yaratmaq üçün üz tanıma sistemlərinin transformativ potensialını nümayiş etdirir. Möhtəşəm potensialına baxmayaraq, üz tanıma texnologiyası mübahisəzər deyil. Onun geniş şəkildə qəbulu məxfilik və etik mülahizələrlə bağlı gərgin müzakirələrə səbəb oldu. Tənqidçilər iddia edirlər ki, sifətin tanınmasının tənzimlənməmiş istifadəsi fərdi məxfiliyə ciddi təhlükə yaradır, çünki bu, kütləvi müşahidə və icazəsiz məlumatların toplanmasına imkan verə bilər. Tanınma dəqiqliyinin müxtəlif demoqrafik qruplar arasında fərqli ola biləcəyi alqoritmik qərəzlə bağlı narahatlıqlar da texnologiyanın ədalətliliyi və inklüzivliyi ilə bağlı müzakirələrə təkan verdi. Üstəlik, avtoritar rejimlər tərəfindən sifətin tanınmasının potensial sui-istifadəsi onun vətəndaş azadlıqlarının aşınmasındakı rolu ilə bağlı qorxuları artırır.

Üz tanıma sistemləri təkamül etməyə davam etdikcə, texnoloji yeniliklər və etik məsuliyyət arasında tarazlığın yaradılması çox vacibdir. Bu məqalə üz tanıma sistemlərinin hərtərəfli icmalı təqdim etmək, onların texniki əsaslarını, müxtəlif tətbiqləri və təklif etdikləri üstünlükləri araşdırmaq məqsədi daşıyır. O, həmçinin onların təqdim etdiyi problemləri, xüsusən də məxfilik, ədalətlik və təhlükəsizlik baxımından araşdıracaq. Nəhayət, məqalə bu transformasiya texnologiyası üçün qarşıda duran yola dair fikirlər təqdim edərək, onun Əşyaların İnterneti (IoT) və genişlənmiş reallıq ilə inteqrasiyası kimi sifətin tanınması sahəsində gələcək tendensiya olaraq nəzərdən keçirəcək.

Üzün tanınmasının işləmə prinsipi: Üzün tanınması texnologiyası fərdin şəxsiyyətini müəyyənəşdirmək və ya yoxlamaq üçün üz xüsusiyyətlərinin çəkilməsini, təhlilini və müqayisəsini əhatə edən çox mərhələli prosesdir. O, dəqiqliyi və etibarlılığı təmin etmək üçün qabaqcıl kompüter

görmə üsullarını və maşın öyrənmə alqoritmlərini birləşdirir. Aşağıda üz tanıma sistemlərinin necə işləməsi haqqında ətraflı məlumat verilmişdir:

1. Üzün aşkarlanması

Proses şəkli və ya video çərçivəsində üz aşkarlanması ilə başlayır. Haar şəlalələri, Tək Atış MultiBox Detektoru (SSD) kimi alqoritmlərdən və ya YOLO (Yalnız Bir dəfə Baxırsan) kimi dərin öyrənmə modellərindən istifadə edərək sistem üzlərin yerini müəyyənləşdirir. Bu addım üz nəhiyəsinə fondan təcrid edərək əlavə təhlil etməyə imkan verir.

2. Üz xüsusiyyətlərinin çıxarılması:

- Üz aşkar edildikdən sonra sistem gözlər, burun, ağız və çənənin mövqeyi kimi unikal xüsusiyyətləri çıxarır. Tez-tez orientirlər adlanan bu xüsusiyyətlər üz şablonu və ya xüsusiyyət vektoru adlanan riyazi təsvirə uyğunlaşdırılır. Bu şablon barmaq izi kimi hər bir fərd üçün unikaldir və müqayisə üçün əsas rolunu oynayır.

3. Üz Alignment: Dəqiqliyi təmin etmək üçün aşkarlanan üz poza, işıqlandırma və ya üz ifadələrindəki dəyişiklikləri nəzərə almaq üçün normallaşdırılır. Sistemə ardıcıl müqayisələr aparmağa imkan verən üz təsvirini standartlaşdırılmış formata uyğunlaşdırmaq üçün təsvirin əvvəlcədən işlənməsi, fırlanma və miqyaslama kimi texnikalar tətbiq edilir.

4. Üz uyğunluğu: Sistem daha sonra çıxarılan üz şablonunu saxlanılan şablonların verilənlər bazası ilə müqayisə edir. Bu, oxşarlıq ölçüləri və ya üzləri təsnif etmək üçün öyrədilmiş neyron şəbəkələrindən istifadə etməklə həyata keçirilir. Doğrulama tapşırıqları üçün (məsələn, smartfonun kilidini açmaq) sistem üzü bir saxlanılan şablonla müqayisə edir. Eyniləşdirmə tapşırıqları üçün (məsələn, hüquq-mühafizə orqanları) uyğunluq tapmaq üçün üzü böyük verilənlər bazası ilə müqayisə edir.

Qərar qəbulu: Nəhayət, sistem giriş üzünün hər hansı saxlanılan şablonlara uyğun olub- olmadığını müəyyən edir. Nəticə ikili (uyğunluq/uyğunluq yoxdur) və ya ehtimala əsaslanan ola bilər, burada uyğunluq ehtimalını göstərmək üçün etimad xalı təyin edilir.

Əsas Texnologiyalar:

Süni intellekt (AI) və Machine Learning (ML):

Süni intellekt modelləri, xüsusən də konvolyusiya neyron şəbəkələri (CNN) üz tanıma sistemlərinin əsasını təşkil edir. Bu modellər üz naxışlarını öyrənmək və zamanla dəqiqliyi təkmilləşdirmək üçün böyük məlumat dəstləri üzərində öyrədilir.

Dərin Öyrənmə Alqoritmləri: Transfer öyrənmə və generativ rəqib şəbəkələr (GAN) kimi üsullar sistemlərə müxtəlif ssenarilərə uyğunlaşmağa imkan verir, çətin mühitlərdə performans artırır.

3D Üz Tanınması: Qabaqcıl sistemlər dərinliyi və konturları təhlil etmək üçün 3D xəritələmədən istifadə edir, bu da onları ənənəvi 2D üsulları ilə müqayisədə bucaq və işıqlandırmadakı dəyişikliklərə qarşı daha möhkəm edir. Üz tanıma sistemlərinin tətbiqləri: Üz tanıma sistemləri sürətlə çoxsaylı sənaye sahələrini əhatə edən tətbiqlərlə çox yönlü alətlərə çevrilmişdir. Bu sistemlər təhlükəsizlik protokollarını yenidən formalaşdırır, istifadəçi təcrübələrini təkmilləşdirir və müxtəlif sektorlarda səmərəliliyi təqdim edir. Aşağıda üz tanıma texnologiyasının əhəmiyyətli təsir göstərdiyi əsas tətbiq sahələrinin hərtərəfli tədqiqi verilmişdir:

1. Təhlükəsizlik və Nəzarət Təhlükəsizlik üz tanıma sistemlərinin qəbulunun əsas hərəkətverici qüvvəsi olaraq qalır:

- Hüquq-mühafizə orqanları: Üzün tanınması cinayət məlumat bazalarına qarşı müşahidə görüntülərinə çarpaz istinad etməklə şübhəli şəxslərin müəyyən edilməsində mühüm rol oynayır. Bütün dünyada polis idarələri bu texnologiyadan istifadə edərək soyuqqəymə hallarının həllində, itkin düşən şəxslərin müəyyən edilməsində və şübhəliyə tutulmasında uğur qazandıqlarını bildirdilər.

- Sərhəd Nəzarəti və Hava Limanının Təhlükəsizliyi: Səmişinlərin yoxlanılması, immiqrasiya və gömrük proseslərini sürətləndirmək üçün beynəlxalq hava limanlarında qabaqcıl üz tanıma sistemləri tətbiq edilir. Avtomatlaşdırılmış e-qapılar səyahət edənlərin pasportlarına uyğunluğunu yoxlamaq üçün üz məlumatlarından istifadə edərək, təhlükəsizliyi gücləndirərək gözləmə vaxtlarını azaldır.

- Təhlükəsiz Obyektlərdə Giriş Nəzarət: Üzün tanınması hökumət binaları, tədqiqat laboratoriyaları və hərbi qurğular kimi həssas yerlərə girişi təmin etmək üçün açar kartları, PIN-lər və parollar kimi ənənəvi metodları əvəz edir. Üz biometriklərinin ötürülməzliyi daha yüksək səviyyədə təhlükəsizliyi təmin edir.

2. Şəxsi Cihazın Autentifikasiyası

Üzün tanınması istifadəçinin rahatlığını və təhlükəsizliyini artıraraq şəxsi elektronika standart funksiyaya çevrilir:

- Smartfonlar və Planşetlər: Apple-ın iPhone X ilə birlikdə təqdim etdiyi Face ID, təhlükəsiz üz identifikasiyası üçün meyar təyin etdi. Oxşar texnologiyalar Android cihazları tərəfindən qəbul edilmişdir ki, bu da istifadəçilərə telefonların kilidini açmağa, ödənişlərə icazə verməyə və proqramlara təhlükəsiz şəkildə daxil olmağa imkan verir.

- Noutbuklar və fərdi kompüterlər: Microsoft cihazlarında integrasiya olunmuş funksiya olan Windows Hello problemsiz, parolsuz giriş təcrübəsi təmin etmək üçün üz tanımadan istifadə edir. Bu yanaşma kibertəhlükəsizliyi artırır və mürəkkəb parolların yadda saxlanması əngəlini aradan qaldırır.

3. Bank və Maliyyə xidmətləri

Maliyyə sektoru təhlükəsizliyi, müştəri təcrübəsini və fırıldaqçılığın qarşısının alınmasını təkmilləşdirmək üçün üz tanıma sistemini mənimsəmişdir:

- Rəqəmsal əməliyyatlar: İndi bir çox banklar icazəsiz girişin minimuma endirilməsini təmin edərək yüksək dəyərli onlayn əməliyyatlar və ya həssas hesab dəyişiklikləri üçün üz identifikasiyası tələb edir.

- Fırıldaqçılığın qarşısının alınması: Müştərilərin üzlərini fırıldaqçılar məlumat bazası ilə müqayisə edərək, maliyyə institutları real vaxt rejimində potensial fırıldaq fəaliyyətlərini qeyd edə bilərlər.

ATM integrasiyası: Bir neçə ölkədəki banklar PIN kodlara və fiziki kartlara ehtiyacı aradan qaldıraraq, üz tanıma sistemi ilə təchiz edilmiş bankomatları yerləşdirməyə başlayıblar. Müştərilər sadəcə olaraq maşına yaxınlaşır və onların şəxsiyyəti biometrik olaraq yoxlanılır. Üz tanıma sistemlərinin üstünlükləri: Üz tanıma sistemlərinin qəbulu onların müxtəlif domenlər üzrə təklif etdiyi əhəmiyyətli üstünlüklərdən irəli gəlir. Bu üstünlüklər onların gücləndirilmiş təhlükəsizlik, əməliyyat səmərəliliyi və istifadəçi rahatlığı təmin etmək qabiliyyətindən irəli gəlir. Aşağıda üz tanıma sistemlərinin tətbiqinin əsas üstünlüklərini araşdırırıq:

1. Artan Əməliyyat Effektivliyi

Üz tanıma sistemləri prosesləri sadələşdirir, əl ilə identifikasiya və ya yoxlama üçün tələb olunan vaxtı və resursları azaldır:

- Tapşırıqların avtomatlaşdırılması: Davamiyyətin izlənməsi, giriş nəzarət və müştərilərin qeydiyyatı kimi proseslərin avtomatlaşdırılması vaxt və səylərə qənaət edərək əl ilə nəzarət ehtiyacını aradan qaldırır.

- Problemsiz Integrasiya: Üz tanıma təhlükəsizlik kameraları və ya müştəri idarəetmə proqramı kimi mövcud sistemlərlə integrasiya oluna bilər və əsas infrastruktur dəyişiklikləri tələb etmədən onların funksionallığını artırır.

- Daha sürətli emal vaxtları: Hava limanının təhlükəsizliyi və ya hadisələrin qeydiyyatı kimi tətbiqlərdə sifətin tanınması şəxsiyyətin yoxlanılmasını sürətləndirir, darboğazları azaldır və istifadəçi təcrübələrini yaxşılaşdırır.

2. Uzunmüddətli dövrdə xərc-effektivlik

İlkin quraşdırma xərcləri yüksək ola bilsə də, üz tanıma sistemləri zamanla çox vaxt sərfəli olur:

- Azaldılmış personal xərcləri: Avtomatlaşdırma personalın şəxsiyyət yoxlamaları, davamiyyətin idarə edilməsi və ya müştərinin yoxlanılması kimi tapşırıqları yerinə yetirmək ehtiyacını azaldır.
- Aşağı Baxım: İtki və ya zədələnmə səbəbindən tez-tez dəyişdirilməsini tələb edən kart əsaslı sistemlərdən fərqli olaraq, üz tanıma sistemləri tətbiq edildikdən sonra minimum texniki xidmət tələb edir.

3. Gələcəyə Hazır Texnologiya

Üz tanıma sistemlərinin tətbiqi təşkilatları texnologiyada gələcək irəliləyişlərə hazırlayır:

- Süni intellekt və Əşyaların İnterneti ilə integrasiya: AI və IoT ekosistemləri genişləndikcə, üz tanınması daha ağıllı, bir-biri ilə daha çox əlaqəli sistemlərin yaradılmasında mühüm rol oynayacaq.
- Yeni istifadə hallarına uyğunlaşma: Texnologiyanın uyğunlaşması bizneslərin emosiyaların tanınması və ya multimodal biometrik sistemlər kimi gələcək təkmilləşdirmələri asanlıqla integrasiya edə bilməsini təmin edir.

Sifətin tanınması sistemlərinin üstünlükləri təhlükəsizlik, səmərəlilik, rahatlıq və davamlılığı əhatə edir. Bu sistemlər təkcə cari çağırışları həll etmir, həm də sənayeləri rəqəmsal transformasiyanın gələcəyi üçün yerləşdirir.

Üz Tanıma Sistemlərinin Çətinlikləri və Məhdudiyyətləri: Üz tanıma sistemlərinin çoxsaylı üstünlüklərinə baxmayaraq, onların tətbiqi problemsiz deyil. Məxfilik, etika, texnoloji məhdudiyyətlər və cəmiyyətin qəbulu ilə bağlı məsələlər əhəmiyyətli müzakirələrə səbəb olub. Bu problemləri başa düşmək narahatlıqları həll etmək və texnologiyadan məsuliyyətli istifadəni təmin etmək üçün vacibdir.

1. Məxfilik Narahatlığı

- Üz tanıma sistemlərinin ən çox müzakirə olunan aspektlərindən biri onların şəxsi məxfiliyə potensial təsiridir:
- İcazəsiz məlumatların toplanması: Bir çox üz tanıma sistemləri açıq razılıq olmadan üz məlumatlarını toplayır və saxlayır. Məsələn, ictimai yerlərdə təhlükəsizlik sistemləri belə monitorinqdən xəbəri olmayan şəxslərin üzlərini skan edə və qeyd edə bilər.
- Məlumatların saxlanması və təhlükəsizlik riskləri: Toplanmış üz məlumatları çox vaxt mərkəzləşdirilmiş verilənlər bazalarında saxlanılır. Bu verilənlər bazası oğurlanarsa, bu, şəxsiyyət oğurluğu da daxil olmaqla ciddi məxfiliyin pozulmasına səbəb ola bilər.
- Davamlı Nəzarət: Xüsusilə hökumətlər tərəfindən sifətin tanınması sisteminin ictimai tətbiqi kütləvi nəzarət məsələsini gündəmə gətirir. Tənqidçilər xəbərdarlıq edirlər ki, bu cür texnologiyalar fərdi azadlıqları poza bilər və insanların daim nəzarətdə olduqlarını hiss etdikləri mühitlər yarada bilər.
- Qeyri-adekvat hüquqi çərçivələr: Bir çox yurisdiksiyalarda biometrik məlumatların toplanması, istifadəsi və saxlanması tənzimləyən aydın qanunlar yoxdur. Bu tənzimləmə çatışmazlığı potensial sui-istifadə üçün yer buraxır.

Üz Tanıma Sistemlərində Gələcək Trendlər və İnnovasiyalar: Üz tanıma sistemləri süni intellekt, aparat imkanları və proqram təminatının optimallaşdırılması sahəsində irəliləyişlərlə sürətlə inkişaf edir. Yaranan tendensiyalar və yeniliklər cari məhdudiyyətləri aradan qaldırır, tətbiqləri genişləndirir və daha geniş tətbiq üçün yol açır.

1. AI Təkmilləşdirmələri vasitəsilə Təkmilləşdirilmiş Dəqiqlik

Dərin Öyrənmə Modelləri: Konvolyusiya neyron şəbəkələri (CNN) və transformator əsaslı modellər kimi qabaqcıl dərin öyrənmə arxitekturalarının integrasiyası sifətin tanınması dəqiqliyini əhəmiyyətli dərəcədə yaxşılaşdırmışdır. Bu modellər hətta zəif işıq, müxtəlif bucaqlar və ya qismən tıxanma kimi çətin şərtlərdə belə xüsusiyyətləri müəyyən etməkdə üstündür.

- Köçürmə Öyrənməsi: Əvvəlcədən hazırlanmış modellərdən istifadə böyük verilənlər toplusundan əldə edilmiş bilikləri məhdud verilənlərə malik yeni domenlərə tətbiq etməklə daha sürətli inkişafa və təkmilləşdirilmiş dəqiqliyə imkan verir.

- Real Zamanlı Emal: Süni intellektə əsaslanan optimallaşdırma üz məlumatlarının sürətli işlənməsini təmin edir, izdihamlı ictimai yerlər və ya sürətlə hərəkət edən nəqliyyat vasitələri kimi dinamik mühitlərdə ani tanınmağa imkan verir.

2. Təkmil Canlılığın Aşkarlanması

Spufinq cəhdləri ilə mübarizə aparmaq üçün canlılığın aşkarlanmasında əhəmiyyətli yeniliklər ortaya çıxır:

- 3D Üz Xəritəçəkmə: Yüksək ayırdetmə qabiliyyətinə malik kameralar və infraqırmızı sensorlar dərinliyi aşkar etmək və canlı obyektin mövcudluğunu təmin etmək üçün üzlərin 3D modellərini yaradır.
- Davranış biometrikası: Göz qırpması və ya dodaq hərəkəti kimi incə hərəkətlərin təhlili əlavə təhlükəsizlik qatını əlavə edir.
- Termal Görüntü: İstilik imzalarını aşkar etmək üçün termal kameralardan istifadə yalnız canlı insan üzlərinin təsdiqlənməsini təmin edir.

Yekun olaraq, üz tanıma texnologiyası müxtəlif sənayelərdə dəqiqlik, təhlükəsizlik və tətbiqlərdə əhəmiyyətli təkmilləşdirmələrlə sürətlə inkişaf edir. Süni intellektlə idarə olunan alqoritmlər, kənar hesablamalar, multimodal biometrikalar və məxfiliyi qoruyan texnikalar mənzərəni yenidən formalaşdırdıqca, texnologiyanın səhiyyə, pərakəndə satış, nəqliyyat və ağıllı şəhərlər kimi sektorlarda inqilab etmək potensialı eksponent olaraq artır. Bununla belə, sifətin tanınmasının geniş şəkildə tətbiqi eyni zamanda balanslaşdırılmış yanaşmanı, etik problemlərin həllini, məlumatların məxfiliyinin təmin edilməsini və etimadı və inklüzivliyi gücləndirmək üçün qərəzləri yumşaltmağı tələb edir. Güclü idarəetmə və məsuliyyətli inkişafa diqqət yetirməklə, sifətin tanınması fərdi hüquqları qoruyarkən daha təhlükəsiz, daha fərdiləşdirilmiş təcrübələrin yaradılmasında mühüm rol oynaya bilər.

Ədəbiyyat

- [1] Chen, J., & Weng, S. (2019). Deep Learning for Face Recognition: A Critical Review. IEEE Transactions on Neural Networks and Learning Systems, 30(7), 2000-2012.
- [2] Elakkiya, R., & Ramaraj, S. (2020). Hybrid Multi-Biometrics for Security: Combining Face, Iris, and Voice Recognition. Pattern Recognition Letters, 136, 13-22.
- [3] Gonzalez, M., & Chang, L. (2019). Edge Computing for Face Recognition: A Review and Future Directions. Journal of Computational and Theoretical Nanoscience, 16(8), 3209-3219
- [4] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer Science & Business Media.
- [5] Khan, A., & Zaheer, M. (2020). A Survey of Face Recognition Algorithms for Human Identification in Real-Life Applications. Journal of Engineering Science and Technology, 15(2), 850-872.
- [6] Li, S. Z., & Jain, A. K. (2011). Handbook of Face Recognition (2nd ed.).
- [7] Springer. Masi, I., Chen, W., & Goecke, R. (2018). The Challenge of Face Recognition in the Wild: A Survey of Recent Advances and Future Directions. Computer Vision and Image Understanding, 167, 1-29.
- [8] Menczer, F., & O'Rourke, S. (2018). Artificial Intelligence and Ethics: Challenges and Future Directions in Face Recognition Technology. IEEE Computer Society.
- [9] Prabhakar, S., & Jain, A. K. (2003). The Effect of Aging on Face Recognition. Proceedings of the International Conference on Biometrics.
- [10] Raj, A., & Muneer, R. (2019). Privacy-Preserving Face Recognition Using Blockchain Technology. Future Generation Computer Systems, 92, 541-550.
- [11] Sarkar, S., & Liao, X. (2020). Recent Advances in Face Recognition: A Survey. IEEE Access, 8, 185917-185944.
- [12] Vargas, J. R., & Patiño, L. M. (2020). Face Recognition Systems in Healthcare: Applications and Challenges. IEEE Access, 8, 123543-123561.

- [13] Wang, X., & Tang, X. (2018). Face Recognition in the Era of Deep Learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(6), 1193-1210.
- [14] Yin, L., & Zhai, M. (2020). Liveness Detection in Face Recognition Systems: A Survey. *International Journal of Computer Vision*, 128(6), 1342-1360.
- [15] Zhang, Z., & Song, H. (2019). Improving Face Recognition with Deep Learning Techniques: A Survey. *Journal of Computer Science and Technology*, 34(4), 741-758.
- [16] Zhao, W., & Chellappa, R. (2018). Face Recognition: A Literature Survey.
- [17] *ACM Computing Surveys*, 51(5), 1-34.

BIG DATA ECOSYSTEM

Inara Abasova

Teacher of Computer Engineering department

ABSTRACT

The ecosystem of working with Big Data allows manufacturing companies to optimize the production and sales function, minimizing the gaps between production and sale of products through the automatic generation of predictive models of demand, purchasing and production by product groups and units of output. The system allows you to develop internal models for analyzing existing data in a graphical interface, enrich them with external sources (OSM, Rosstat data, etc.) and implement the results obtained in planning and decision-making systems.

Key words: big data ecosystem, OSM, internal models, graphical interface.

Introduction

The big data ecosystem includes the following groups of tools [1]:

- distributed file systems (Distributed File Systems - DFS);
- deployment tools;
- NoSQL and NewSQL databases;
- data integration tools;
- machine learning tools;
- service programming tools;
- planning tools;
- benchmarking tools; security tools.

To store large amounts of data, distributed file systems are used, which have the following differences:

- the ability to store files larger than the size of a separate storage server disk;
- stored files are automatically replicated on storage servers, which allows parallel processing and the creation of redundancy to ensure reliable operation of the cluster;
- the system can be easily scaled using the principle of horizontal scaling.

The most common distributed file system is the Hadoop File System. Examples of DFS are also: Red Hat ClusterFS, QuantCast File System, Ceph File System. Storing big data requires database systems and data access tools. Due to known limitations, the use of classic relational databases, such as Oracle SQL, DB2, is impossible. Storing big data requires database systems and data access tools. Due to known