

ӘОЖ 004.93'11

DOI 10.52167/1609-1817-2025-138-3-274-284

Қ.С. Мауленов¹, Н.М. Казиева², Б.Ж. Жарлыкасов¹

¹Baitursynuly University, Қостанай, Қазақстан

²L.N. Gumilyov Eurasian National University, Астана, Қазақстан

E-mail: k_maulenov@inbox.ru

ДЕ-ИДЕНТИФИКАЦИЯ ПРОЦЕДУРАСЫНАН ӨТКЕН БЕТ-ӘЛПЕТТЕРДІ ТАНУ МӘСЕЛЕСІН ШЕШУ ТӘСІЛІ РЕТІНДЕ ДЕТЕРМИНИРЛЕНГЕН АЛГОРИТМДЕРДІ ҚОЛДАНУ

Аңдатпа. Мақалада бет-әлпетті тану жүйелерінің дәлдігіне елеулі әсер еткен 2019-2021 жылдар аралығындағы заманауи мәселелер егжей-тегжейлі талданады. Бұл мәселелердің қатарында COVID-19 пандемиясы кезінде кеңінен таралған маска киюге байланысты бет-әлпетті тану қиындығы және жаңа Fawkes процедурасын пайдалану арқылы жасалған де-идентификацияланған суреттерді тану мәселелері бар. Мұндай мәселелер шекаралық қауіпсіздік, шекаралық бақылау және басқа да маңызды салаларда тұлғаны дұрыс тану қажеттілігі туындағанда ерекше маңызды болып табылады. Мақалада осы мәселелерді шешу жолдарына ерекше назар аударылып, Fawkes процедурасымен өңделген суреттерде пайда болатын текстуралық өзгерістер мен құрылымдық бұзылуларды талдау жүргізілді. Бұл өзгерістерді формалды және сандық бағалау үшін көпдеңгейлі параметрлік әдістер қолданылды. Нәтижесінде, Fawkes процедурасынан өткен бет-әлпет суреттерінің терең оқыту жүйелерімен дұрыс танылмау себептері анықталды, және мұндай суреттерді дәстүрлі, терең оқытуға негізделмеген әдістерді қолдану арқылы сәтті тануға болатыны дәлелденді. Сонымен қатар, зерттеу барысында маска кию сияқты бет-әлпетті тануға кедергі келтіретін факторларға қатысты ұсынылған әдістердің тиімділігі көрсетілді. Бұл әдістер тек Fawkes процедурасымен өңделген суреттерді ғана емес, сонымен қатар маска киген беттерді де сенімді тануға мүмкіндік береді.

Практикалық маңыздылығы. Қарапайым алдын-ала өңдеу әдістерін қолдану арқылы Fawkes процедурасынан өткен суреттерді терең оқыту жүйелерінде тану нәтижелілігін арттыруға болатындығы атап көрсетілген. Бұл әдістер, маска киюге байланысты бет-әлпетті танудағы мәселелерді шешуде де пайдалы болуы мүмкін. Осылайша, бұл зерттеу ұсынылған әдістердің жоғары тиімділігі мен болашағын көрсетеді.

Түйінді сөздер. Де-идентификация, бет-әлпетті тану, детерминирленген алгоритмдер, Fawkes технологиясы, терең оқыту, екі өлшемді косинус- түрлендіру.

Кіріспе.

Заманауи бет-әлпетті тану алгоритмдері көзілдірік, қалпақ және басын бұру сияқты әртүрлі кедергілер кезінде жоғары тиімділікті көрсетеді. Бұл алгоритмдердің көпшілігі терең оқыту әдістеріне негізделген және таза деректер жағдайында тамаша нәтижелер көрсетеді. Алайда, шынайы өмірде үлкен қара көзілдірік, қалпақ, шарф сияқты аксессуарларды кию немесе бетті қолмен жабу тану процесін айтарлықтай қиындатады.

АҚШ Ұлттық стандарттар және технологиялар институты (NIST) жүргізген зерттеу медициналық маска кию бет-әлпетті тану алгоритмдерінің тиімділігін айтарлықтай төмендететінін көрсетті. 89 алгоритмді тестілеу кезінде, әдетте, қате

нәтижелер тек шамамен 0,3% жағдайларда байқалады, бірақ маска киген беттерді тану кезінде қателер саны 5%-дан 50%-ға дейін өсті [3]. Бұл бет-әлпетті танудан түрлі әдістер арқылы құтылуға болатынын көрсетеді, алайда мұндай әдістерді үнемі қолдану күнделікті өмірде қиындық тудырады.

Маска кию немесе басқа аксессуарларды қолдану мәселелері қол жеткізу бақылауында, шекаралық бақылауда немесе масканы уақытша шешуді қажет ететін басқа жағдайларда шешілуі мүмкін. Алайда, жасанды интеллектке негізделген бет-әлпетті де-идентификациялау суреттерінің жаңа әдістері қазіргі бет-әлпетті тану жүйелері үшін әлдеқайда күрделі мәселе болып табылады. Мұндай әдістердің бірі - Fawkes процедурасы, ол бет-әлпет суреттерін өзгертіп, оларды қазіргі тану алгоритмдері үшін танымастай етеді.

Маска кию және бет-әлпет суреттерін де-идентификациялау мәселелерін шешу өте өзекті болып отыр. Қазіргі бет-әлпетті тану жүйелерінің дәлдігі мен сенімділігін сақтау үшін әсіресе қауіпсіздік пен қол жеткізуді бақылау контекстінде бар алгоритмдерді бейімдеу және жақсарту қажет.

Зерттеудің мақсаты - де-идентификацияға ұшыраған бет-әлпеттерді тану мәселесін шешу үшін детерминирленген алгоритмдерді қолдану арқылы тану жүйелерінің дәлдігі мен сенімділігін арттыру.

Материалдар мен тәсілдер.

Зерттеуде алдын ала үйретілген CNN (конволюциялық нейрондық желілер) және дискреттік косинустық түрлендіру мен Random әдісі сияқты детерминирленген алгоритмдер қолданылды. Суреттерді өңдеу үшін Python кітапханаларын пайдалана отырып, оларды тегістеу әдісі қолданылды.

Маска тағылған бет-әлпетті тану.

Бет-әлпетті тану жүйелері адамның тану қабілетінен асып түсті деп айтуға болатын сияқты, және бұл саладағы міндеттер шешілгендей көрінеді. Алайда COVID-19 пандемиясы заманауи алгоритмдер, соның ішінде нейрондық желілер, адамдар маска кигенде, тұлғаны анықтау міндетін әрдайым орындай алмайтынын көрсетті.

АҚШ Ұлттық стандарттар және технологиялар институты (NIST) жүргізген зерттеу медициналық масканың бет-әлпетті тану дәлдігін айтарлықтай төмендететінін анықтады. Қалыпты жағдайда алгоритмдер 0,3% жағдайда қателеседі, ал маска киген бет-әлпеттерді тану кезінде қателер саны 5%-дан 50%-ға дейін өседі. Бұл зерттеу АҚШ Ішкі қауіпсіздік министрлігі мен Кеден қызметімен бірлесіп жүргізілді, олар қылмыскерлерді бақылау және анықтау үшін тану технологияларын пайдаланады.

Қазіргі уақытта маска тағылған бет-әлпеттерді тануға бағытталған жұмыстар көп емес. Осындай жұмыстардың бірі - авторлары Bishwas Mandal, Adaeze Okeukwu, Yihong Theis жасаған Masked Face Recognition using ResNet-50 [3] зерттеуі. Онда ResNet-50 архитектурасы қолданылды. Нәтижесінде алгоритм адамдардың 89%-ын маскасыз және 46%-ын маскамен таныды. Бұл толықтай идеалды нәтиже болмаса да, зерттеу мәселені шешудің ықтимал жолын көрсетеді.

Алайда, шекаралық бақылау контекстінде маска тағылған бет-әлпетті тану мәселесі өзекті емес, өйткені шекарадан өткен кезде масканы шешу талап етіледі. Бірақ қылмыскерлер дерекқорында маскамен түсірілген фотосуреттер болса, жүйе маскасыз бетті осындай суретпен сәйкестендіре білуі керек, бұл болашақ зерттеулердің қажеттілігін көрсетеді.

Fawkes технологиясы арқылы тұлғаны деидентификациялау.

Заманауи бет-әлпетті тану жүйелері Fawkes процедурасы сияқты жаңа де-идентификация әдістері салдарынан елеулі қиындықтарға тап болуда. Fawkes бет-әлпет

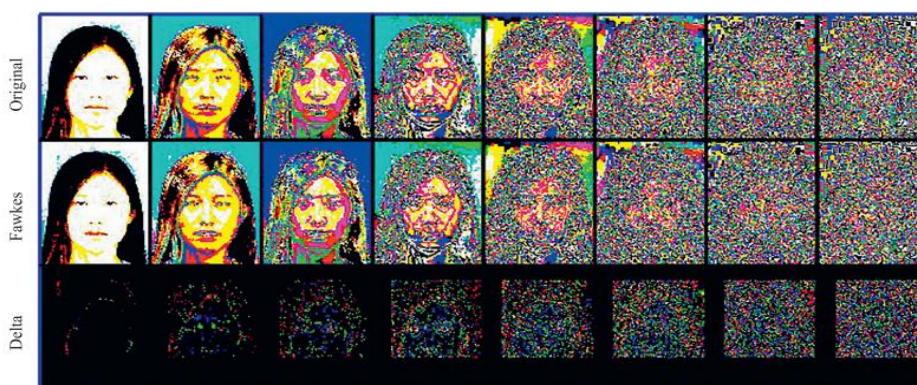
суреттерін нейрондық желілер үшін оларды оқыту және тануға жарамсыз етіп өзгертеді. Өзірлеушілер мұндай пиксел деңгейіндегі өзгерістер минималды және көзге көрінбейтінін, бірақ олар суретті заманауи тану жүйелері үшін пайдасыз ететінін айтады.



1 сурет - Fawkes процедурасынан кейінгі суреттердің мысалдары

Fawkes үш түрлі өзгерту режимін ұсынады: low, mid, high. Режим неғұрлым жоғары болса, сурет соғұрлым көбірек бұрмаланады, бұл жақсырақ қорғауды қамтамасыз етеді. 1-суретте Fawkes процедурасынан кейінгі суреттердің мысалдары көрсетілген. Бастапқы деректер ретінде өз фотосуреттеріміз және CUFS дерекқорындағы суреттер пайдаланылды [4].

«Адамдардың бейнелерін де-идентификациялау әдістері және оларды шешу жолдары» [2] мақаласында текстуралар арасындағы айырмашылықтарды параметрлік бағалау нәтижелері егжей-тегжейлі көрсетілген: құрылымдық ұқсастық индексі (Index Structural SIMilarity, SSIM) 0,99 нәтижесімен және фазалық корреляцияның максимумы 0,96-ға тең. Бұл көрсеткіштер Fawkes-процедурасынан кейінгі бейнелер мен түпнұсқа арасындағы дерлік толық ұқсастықты көрсетеді, дегенмен фазалық корреляция (0,96) текстураларда кейбір өзгерістердің бар екенін көрсетеді. Сондай-ақ, мақалада текстуралар айырмашылығы (Difference) және бастапқы бейнелер арасындағы құрылымдық ұқсастық матрицасы (SSIM MAP) көрсетілген. Нәтижелер Original және Fawkes бейнелері арасындағы айырмашылықтардың бар екенін және олардың негізінен беттің жоғарғы бөлігіне әсер ететінін көрсетеді. Бұл өзгерістер Fawkes-процедурасынан өткен бейненің «ішіндегі» биттік қабаттарда болады. 2-суреттің үшінші жолында Original және Fawkes бейнелері арасындағы айырмашылықтарды көрсететін 8 биттік қабат көрсетілген (Delta).

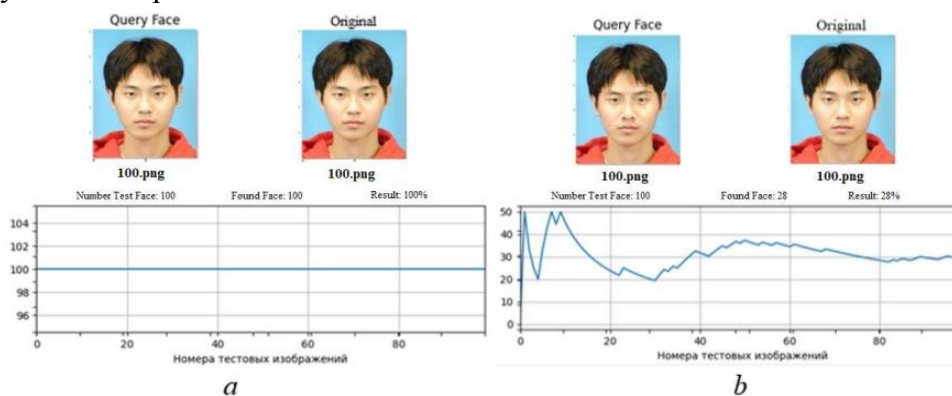


2 сурет - Оригинал кескін мен Fawkes-процедурасынан өткен нәтиже арасындағы айырмашылықтарды көрсететін 8 биттік қабат [2]

Зерттеуде сондай-ақ ResNet34 терең конволюциялық нейрондық желісі негізінде құрылған жүйенің түпнұсқа кескіндер мен Fawkes процедурасына ұшыраған

кескіндерді салыстырудағы тану дәлдігін бағалау нәтижелері көрсетілген. Мұндай кескіндердің тану үшін жарамсыз болатыны анықталды. Fawkes процедурасынан өткен кескіндер бойынша жүйенің дәлдігі 100%-дан 28%-ға дейін төмендеді. Жүйенің жұмыс нәтижелері 3-суретте көрсетілген.

Бұл факт терең оқыту әдістеріне негізделген жүйелер үшін үлкен мәселені көрсетеді. Әлі де кешенді зерттеулерді, әртүрлі деректер базалары мен нейрондық желілер модельдерімен тәжірибелерді жүргізу қажеттілігі бар болса да, бірдей деректер базасында визуалды түрде дерлік бірдей кескіндерде дәлдіктің 100%-дан 28%-ға дейін төмендеуі аландатарлық сигнал болып табылады.



3 сурет - CNN негізіндегі жүйені тану нәтижелері
(Recognition System with CNN - RS_CNN) [2]

Бұл қазіргі бет-әлпетті тану жүйелері үшін үлкен қауіп төндіретінін көрсетеді.

Нәтижелер.

Эксперименттер барысында Fawkes процедурасына ұшыраған бет-әлпет суреттерін детерминирленген алгоритмдермен сәтті тануға болатындығы анықталды, бұл алгоритмдер терең оқыту әдістері контекстінде қолданылған жоқ [5, 6]. Егер Fawkes процедурасымен өзгертілген суреттерді өңдеу үшін конволюциялық емес алгоритмдерді қолдансақ, өзгерген биттік қабаттарда сезімтал емес ерекшеліктер жиынтығын алуға болады. Бұл Fawkes процедурасымен масқаланған суреттермен жұмыс істей алатын қарапайым бет-әлпет тану жүйелерін (Simple Face Recognition Systems — Simple FaReS) жасауға мүмкіндік береді.

Simple FaReS модельдері [5, 6] келесі компоненттерді қамтиды:

- бет-әлпет суреттерінің параметрлерімен деректер базасы;
- үш функционалдық элемент: бет-әлпет суреттерін алдын ала өңдеу алгоритмі; ерекшеліктерді алу әдісі, суреттердің бастапқы өлшемдерін және ерекшелік кеңістігінің өлшемділігін қамтитын; ерекшеліктерді таңдау алгоритмі және соңғы ерекшеліктер саны;
- классификатор түрі (мысалы, қашықтықтың минимумын қолданатын классификатор — KMP), қолданылатын метрика және нәтижені бағалау рейтингі.

Қарастырылып отырған тапсырмада Simple FaReS-ті екі өлшемді косинус түрлендіру (2D DCT) [7] негізінде тиімді қолдануға болады. Бұл тәсілдің негізгі идеясы — сурет деректерін олардың дискретті түрлендіру коэффициенттері түрінде ұсыну. Бұл әдіс суреттің пикселдері арасындағы корреляцияны бір ғана бағытта емес, екі бағытта да есептеуге мүмкіндік береді. Осыған байланысты суреттерді қысу әдістері екі өлшемді косинус түрлендіруді қолданады. Оның формуласы:

$$G(i, j) = \frac{1}{\sqrt{2n}} C_i C_j \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} p_{xy} \cos \left[\frac{(2y+1)j\pi}{2n} \right] \cos \left[\frac{(2x+1)i\pi}{2n} \right], \quad (1)$$

бұнда $0 \leq i, j \leq n - 1$. Сурет $n \times n$ өлшемді пиксель блоктарына бөлінеді және теңдеулер әр блок үшін G_{ij} коэффициенттерін табу үшін қолданылады. Трансформация коэффициенттері олардың маңыздылығына сәйкес реттеледі, мысалы, ақпараттық мазмұнға қосқан үлесіне байланысты. Ақпараттық мазмұны төмен трансформанттарды өткізіп жіберуге болады (түзету), бұл 4-суретте көрсетілген.

Суретте оң жақтағы сол жақ жоғарғы бұрышта қызыл үшбұрышпен белгіленген жерде ең жоғары ақпараттық мазмұны бар коэффициенттер орналасқан. Барлық басқа трансформанттар ақпараттық мазмұнға аз үлес қосатын коэффициенттерді өткізіп жіберуге болады.

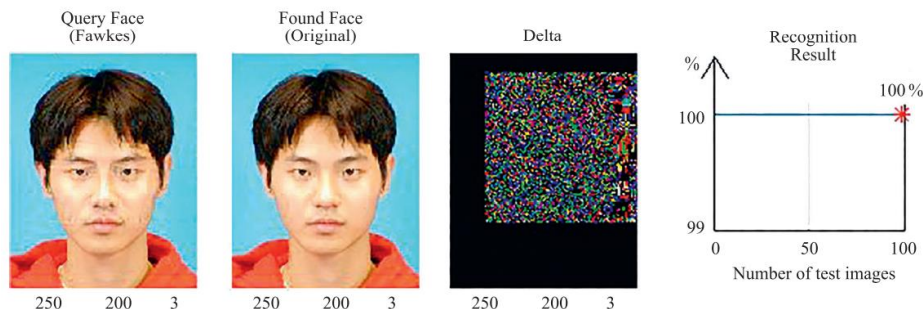


4 сурет - Трансформация коэффициенттері олардың маңыздылығына сәйкес реттеледі

DCT (дискретті косинус түрлендіру) оның базалық функциялары сандық суреттердің үлкен жиынтығы үшін есептелген жеке функцияларды жақсарту үшін оңтайлы болатынына негізделген. Осылайша, бастапқы суреттерді алдын ала өңдеу кезеңін толықтай жоюға болады. Косинус түрлендіру беттерді кішкене санды сипаттамалар — спектралды компоненттерді пайдаланып дәл беруге мүмкіндік береді. Бетті тану және қалпына келтіру үшін тек 20 кеңістіктік спектралды компоненттер жеткілікті, олар түрлендіру матрицасының сол жақ жоғарғы бұрышында шоғырланған. Мысалы, 250×200 өлшемді сурет үшін (50 000 нүкте) тек 210 нүкте қажет, бұл бастапқы сипаттамалар кеңістігінің 1% -ынан азы. Zigzag әдісін қолдану арқылы ең маңызды компоненттерді бөліп көрсетуге болады, бұл жүйенің дәлдігін арттырады [8].

Бұл әдістің тиімділігін түпнұсқа суреттер мен олардың Fawkes түрлендірілген нұсқалары арасындағы косинус-кеңістіктегі қашықтықтар көрсетеді. Эксперименттерде біз L1 метрикасы мен қашықтық классификаторы бойынша нормаланбаған қашықтықтарды алдық. 1-ші және 2-ші рангтар үшін келесі параметрлер үштіктер алынды: {0,19; 0,67; 2,0} және {19; 34; 82} сәйкесінше. Fawkes процедурасы арқылы бұзылған 100 бет суреттері үшін дұрыс танылған беттер үшін қашықтықтар (1-ші ранг) сурет 5a-де, ал 2-ші ранг үшін — сурет 5b-де көрсетілген. Алынған нәтижелер косинус түрлендіруі Fawkes процедурасына ұшыраған суреттерді 100% тануды қамтамасыз ететінін көрсетеді [6]. Бұл біздің экспериментіміздің нәтижелерімен расталады, ол 5-ші суретте көрсетілген.

5 суретте Delta бейнеленген екі бастапқы бет-әлпет суреттерінің түсті биттік қабаттары арасындағы айырмашылық, Query Face суретінің Fawkes-процедурасынан өткенін тексеруге арналған. Query Face суретінде бет-әлпеттің текстуралық бұрмаланулары көрінеді.



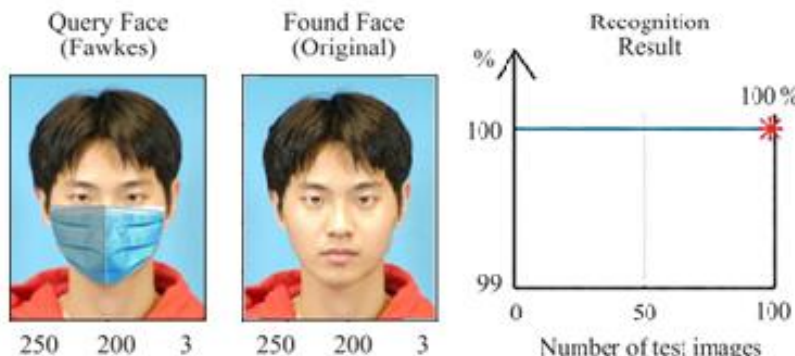
5 сурет - DCT негізіндегі тану жүйесінің жұмысының скриншоты

Жүйенің моделі:

$$\text{GUFS}(100/1/100) \{2\text{DDCT}:250 \times 200 \rightarrow 15 \times 15/\text{zigzag}(119)\} [\text{KMP}/\text{L1}/\text{rank} = 1], (2)$$

мұнда $\text{GUFS}(100/1/100)$ — 100 бастапқы бет-әлпет суреттері (әр классқа 1 эталон) және 100 Fawkes процедурасынан өткен тестілік суреттерді қамтитын GUFS1 бейнелер базасы; $\{2\text{DDCT}:250 \times 200 \rightarrow 15 \times 15/\text{zigzag}(119)\}$ — 250×200 өлшеміндегі суреттерді екіөлшемді косинус-түрліндіру алгоритмімен өңдеу, Zigzag әдісімен спектральды белгілерді таңдау [9], спектрдің 15 диагоналі бойынша жалпы саны 119 мәнмен (суреттің орташа жарықтылық мәнін есептемегенде); $[\text{KMP}/\text{L1}/\text{rank} = 1]$ — арақашықтықты минимизациялау классификаторы, L1 метрикасы және 1 рангімен [8].

Осы модель Simple FaReS 2DDCT негізінде маскадағы бет-әлпеттерді тану мәселесін шешу үшін де жарамды екенін атап өту керек. Маскадағы бет-әлпеттер үшін осы жүйенің скриншоты 6-шы суретте көрсетілген.



6 сурет - Маскадағы бет-әлпеттер үшін модельдің (формула (2)) жүйесінің жұмысы

Келесі екі Simple FaReS моделдері де Fawkes-процедурасының нәтижесіндегі биттік қабаттардағы өзгерістерге сезімтал емес белгілер жиынтығына негізделген. Осы Simple FaReS модельдерінің түрлері келесідей:

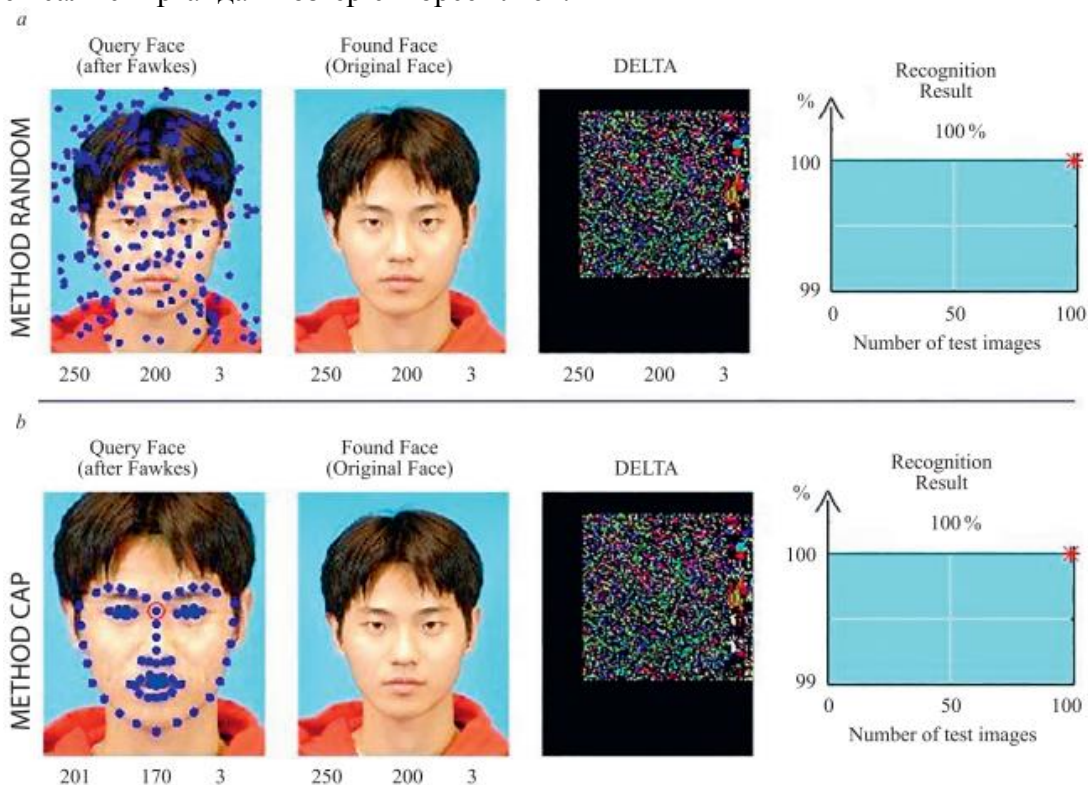
$$\text{GUFS}(100/1/100) \{\text{Face}:250 \times 200 \rightarrow \rightarrow \text{Random}(\text{NUM})\} [\text{KMP}/\text{L1}/\text{rank} = 1]; (3)$$

$$\text{GUFS}(100/1/100) \{\text{Face}:250 \times 200 \rightarrow \rightarrow \text{CAP}(\text{NUM})\} [\text{KMP}/\text{L1}/\text{rank} = 1], (4)$$

мұндағы $\text{Random}(\text{NUM})$ — бет немесе бүкіл фотопортрет аймағында біркелкі таралған NUM пиксел координаттарын генерациялау әдісі [9,10]. Осы өзгермейтін координаттарға негізделген түрде әрбір оригинал (эталон) және барлық Fawkes-суреттер үшін жарықтық белгілер векторы есептеледі. Кейін жүйе осы жарықтық белгілер векторларын салыстырып, олардың классификациясын жүргізеді; $\text{CAP}(\text{NUM})$

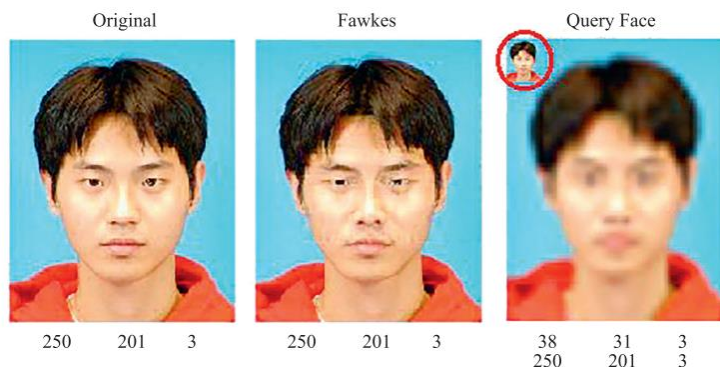
— антропометриялық нүктелердің (Coordinates of the Anthropometric Points, CAP [11]) NUM координаттарын таңдау әдісі, бұл нүктелер бойынша жарықтық белгілер векторлары есептеледі. Бұл векторлар әрбір жеке бет-әлпет суретін (оригинал және оның Fawkes-процедурасынан кейінгі нәтижесі) жеткілікті дәлдікпен көрсетеді, соның негізінде олардың тану әдісі құрылады.

Модельдердің (3) және (4) жүйесінің жұмысын көрсететін скриншоттар сурет 7-де көрсетілген. Simple FaReS (3) демонстрациялық болып табылады және Fawkes-процедурасынан өткен бет-әлпет суреттерін танудың ең қарапайым әдісі ретінде Random [9, 10] идеяларын көрсетеді. Simple FaReS (4) CAP негізінде, өйткені жарықтық белгілер бет аймағын жазық айналдыру, үлкейту, кішірейту және/немесе жылжыту кезінде өзгеріссіз қалады. Мысалы, сурет 7-де Query Face суретінің өлшемінің эталон суретімен салыстырғандағы өзгерісі көрсетілген.



7 сурет - Fawkes процедурасымен жасалған бет-әлпет суреттерін тану жүйелерінің жұмысын көрсететін скриншоттар: модельдер 3 (формула (3)) (a) және 4 (формула (4)) (b)

Соңында, біз QF (Query Face) бейнесін алдын ала өңдеуге негізделген әдісті ұсынамыз. Бұл алдын ала өңдеу процедурасы кез келген бола алады, бірақ оның мақсаты Fawkes процедурасымен бұзылған бейнедегі бет аймағындағы «күшті бұрмаланған ақпаратты қалпына келтіру» болып табылады. Мысалы, бұл екі кезеңде орындалуы мүмкін: бірінші кезеңде бейне кішірейтіледі, сосын бастапқы өлшеміне қайта оралады. Бірінші кезеңде Fawkes процедурасымен өзгертілген аймақтар қысқарады және орташа алынады, нәтижесінде жұмсарады. Екінші кезеңде CLSB аймақтарын интерполяция арқылы кеңейту жүзеге асырылады, бұл бет текстурасындағы бұрмаланған ақпаратты жұмсартады. Бұл өзгерістердің мысалдары 8-ші суретте көрсетілген [6].



8 сурет - Fawkes-процедурасымен өңделген бейнені алдын ала өңдеудің кезеңдері

Суретте көрсетілген: бастапқы сурет; Fawkes түрлендіргеннен кейінгі нәтиже (бет текстурасының айқын бұрмалануы); кішірейтілген сурет (шеңбермен бөлінген); нәтижесінде алынған — сұрау бетінің тегістелген суреті. Соңғы сурет кез келген жоғарыда көрсетілген жүйе арқылы 100% дәлдікпен танылуы мүмкін.

Талқылау.

Көрсетілгендей, детерминирленген алгоритмдер негізіндегі әзірленген жүйелер Fawkes процедурасынан өткен бет-әлпет суреттерін тану мәселесін табысты шешуде, бұл теориялық негізделген және практикалық түрде расталған. Бұл жетістік мәселені шешуде маңызды қадам болып табылады, бірақ әрі қарайғы кешенді зерттеулер қажет болып табылады. Әртүрлі деректер базалары мен нейрондық желілер модельдерімен қосымша тәжірибелер жүргізу маңызды, өйткені әрбір модель ерекше және Fawkes процедурасынан өткен суреттермен әртүрлі деңгейде жұмыс істей алады.

Қандай нейрондық желілердің архитектуралары мен олардың конфигурациялары осындай суреттерді тануда ең тиімді болуы мүмкіндігін анықтау қажет, ал қайсысы керісінше, аз нәтиже береді [12]. Сондай-ақ, ұсынылған детерминирленген әдістерді қазіргі терең оқыту модельдерімен интеграциялау мүмкіндіктерін қарастыру керек. Бұл де-идентификацияланған суреттерді сенімдірек тануға қабілетті гибридік жүйелерді жасау перспективаларын ашады.

Бұл зерттеу бағыты қазіргі қауіпсіздік пен деректердің құпиялылығы мәселелерінің аясында ерекше маңызға ие. Fawkes сияқты де-идентификация әдістерінің белсенді дамуы жағдайында бет-әлпетті танудың тиімді шешімдерін әзірлеу тек ғылыми мәселе емес, әртүрлі салалардағы қауіпсіздікті қамтамасыз ету үшін маңызды қажеттілік болып табылады.

Қорытынды.

Мақалада соңғы жылдарда бет-әлпетті тану жүйелерінде пайда болған өзекті мәселелер қарастырылады. Негізгі назар бет-әлпетті тану мәселесіне аударылады, әсіресе Fawkes процедурасымен де-идентификацияланған суреттерде. Бұл процедура терең оқыту әдістеріне негізделген қазіргі жүйелер үшін күрделі сынақ болып табылады, себебі ол бет-әлпет суреттерінің текстуралары мен құрылымдық бұзылыстарына үлкен өзгерістер енгізеді.

Біздің зерттеуіміз көрсеткендей, детерминирленген алгоритмдер, мысалы, екі өлшемді косинус-түрлендіру (2D DCT) және қарапайым ерекшеліктерді шығару әдістері, Fawkes процедурасынан өткен суреттерді тану мәселесін тиімді шешуге қабілетті. Бұл алгоритмдер Fawkes енгізген айтарлықтай бұзылыстарға қарамастан, жоғары тану дәлдігін қамтамасыз етеді. Олардың тиімділігінің теориялық және

тәжірибелік растауы, дәстүрлі терең оқыту әдістері жеткіліксіз болған жағдайда, оларды идентификация жүйелерінде табысты қолдану үмітін береді.

Дегенмен, жетістіктерге қарамастан, қосымша кешенді зерттеулер жүргізу қажет. Мысалы, нейрондық желілердің түрлі модельдері мен олардың архитектураларының Fawkes процедурасынан өткен суреттермен жұмыс істеудегі тиімділігін зерттеу керек. Сондай-ақ, детерминирленген әдістерді нейрондық желілермен біріктіру мүмкіндіктерін қарастыру маңызды, бұл жүйелердің тану дәлдігін арттыруға ықпал етуі мүмкін. Бұл зерттеу бағыттары қазіргі идентификация жүйелерінің сенімділігі мен қауіпсіздігін қамтамасыз ету үшін маңызды болып табылады және бет-әлпетті тану технологияларының әрі қарай дамуы үшін өзекті және маңызды болып табылады.

Қаржыландыру. Бұл зерттеуді ҚР Ғылым және жоғары білім министрлігі қаржыландырды, № AP19678000 гранты.

ӘДЕБИЕТТЕР

[1] Shan S., Wenger E., Zhang J. et al. Fawkes: Protecting privacy against unauthorized deep learning models // *Proceed. 29th USENIX Security sympos.* – Boston, 2020. – P. 1589-1604.

[2] Maulenov, K. et al. METHODS OF DE-IDENTIFICATION OF FACIAL IMAGES AND WAYS TO SOLVE THEM. *KazATC Bulletin* (2023)., 127(4), 196–206. <https://doi.org/10.52167/1609-1817-2023-127-4-196-206>

[3] NISTIR 8311 Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms Mei Ngan Patrick Grother Kayee Hanaoka. This publication is available free of charge from: <https://doi.org/10.6028/NIST.IR.8311>

[4] CUHK Face Sketch Database (CUFS). [Электронный ресурс]. <http://mmlab.ie.cuhk.edu.hk/archive/facesketch.html> (дата обращения: 20.05.2022)

[5] Kukharev G. A., Maulenov K., Shchegoleva N. L. CAN I PROTECT MY FACE IMAGE FROM RECOGNITION? *Proceedings of the 9th International Conference "Distributed Computing and Grid Technologies in Science and Education" (GRID'2021)*, Dubna, Russia, July 5-9, 2021

[6] Kukharev, G.A., Maulenov, K.S., Shchegoleva, N.L. Protecting facial images from recognition on social media: Solution methods and their perspective // *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2021, 21(5), pp. 755–766. doi: 10.17586/2226-1494-2021-21-5-755-766

[7] Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P. Image quality assessment: from error visibility to structural similarity // *IEEE Transactions on Image Processing*. 2004. V. 13. N 4. P. 600–612. <https://doi.org/10.1109/TIP.2003.819861>

[8] Kukharev G.A., Kamenskaya E.I., Matveev Yu.N., Shchegoleva N.L. Methods of processing and recognizing facial images in biometrics problems. *St. Petersburg: Polytechnic*, 2013. 388 p.

[9] De Vel O., Aeberhard S. Line-based face recognition under varying pose // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1999. V. 21. N 10. P. 1081–1088. <https://doi.org/10.1109/34.799912>

[10] K. S. Maulenov, S. A. Kudubayeva and A. A. Uvaliyeva, "Studying a Face Search Method Based on the Idea of Sparse Data Representation by Generating Random Points," 2021 IEEE International Conference on Smart Information Systems and Technologies (SIST), 2021, pp. 1-6, doi: 10.1109/SIST50301.2021.9465986.

[11] Kazemi V., Sullivan J. One millisecond face alignment with an ensemble of regression trees // Proc. 27th IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2014. P. 1867– 1874. <https://doi.org/10.1109/CVPR.2014.241> 13. Evtimov I., Sturmfels P., Kohno T. FoggySight: A Scheme for facial lookup privacy // Proceedings on Privacy Enhancing Technologies. 2021. V. 3. P. 204–226. <https://doi.org/10.2478/popets-2021-0044>

[12] Serengil, Sefik & Ozpinar, Alper. (2024). A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules. Bilişim Teknolojileri Dergisi. 17. 95-107. [10.17671/gazibtd.1399077](https://doi.org/10.17671/gazibtd.1399077).

Kalybek Maulenov, PhD, senior Lecturer, Baitursynuly University, Kostanay, Kazakhstan, kmaulenov@inbox.ru

Nazym Kaziyeva, candidate of technical sciences, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, kaznaz@list.ru

Bakhtiyar Zharlykasov, master, senior lecturer, Baitursynuly University, Kostanay, Kazakhstan, bakhtiy@mail.ru

THE USE OF DETERMINISTIC ALGORITHMS AS A SOLUTION TO THE PROBLEM OF RECOGNIZING FACES THAT HAVE UNDERGONE DE-IDENTIFICATION

Abstract. This paper provides a detailed analysis of the contemporary issues in facial recognition systems that emerged between 2019 and 2021, significantly affecting recognition accuracy. Among these issues are the challenges of recognizing faces obscured by masks, which became widespread during the COVID-19 pandemic, as well as the challenges of recognizing images de-identified using the new Fawkes procedure. These issues are particularly crucial in scenarios requiring accurate personal identification, such as in border security, border control, and other critical areas. The article focuses on solutions to these problems and analyzes the textural changes and structural distortions that occur in images processed using the Fawkes procedure. Multilayer parametric methods were applied for the formal and quantitative assessment of these changes. As a result, the reasons why facial images processed by the Fawkes procedure are not recognized by deep learning systems were identified, and it was proven that such images can be successfully recognized using traditional methods that do not rely on deep learning. Furthermore, the study demonstrated the effectiveness of the proposed methods in addressing factors that impede facial recognition, such as wearing masks. These methods allow for reliable recognition of not only images processed by the Fawkes procedure but also faces obscured by masks.

Practical Significance. The use of simple preprocessing methods can improve the recognition of images processed by the Fawkes procedure in deep learning systems. These methods may also be useful in addressing issues related to recognizing faces in masks. Thus, this study demonstrates the high efficiency and potential of the proposed methods.

Keywords: de-identification, facial recognition, deterministic algorithms, Fawkes technology, deep learning, two-dimensional cosine transformation.

Қалыбек Мауленов, PhD, старший преподаватель, Baitursynuly University, Костанай, Казахстан, kmaulenov@inbox.ru

Назым Казиева, к.т.н., L.N. Gumilyov Eurasian National University, Астана, Казахстан, kaznaz@list.ru

Бахтияр Жарлыкасов, магистр, старший преподаватель, Baitursynuly University, Костанай, Казахстан, bakhtiy@mail.ru

ИСПОЛЬЗОВАНИЕ ДЕТЕРМИНИРОВАННЫХ АЛГОРИТМОВ В КАЧЕСТВЕ СПОСОБА РЕШЕНИЯ ПРОБЛЕМЫ РАСПОЗНАВАНИЯ ЛИЦ, ПРОШЕДШИХ ПРОЦЕДУРУ ДЕ-ИДЕНТИФИКАЦИИ

Аннотация. В статье подробно анализируются современные проблемы систем распознавания лиц, возникшие в период с 2019 по 2021 год и существенно повлиявшие на точность распознавания. Среди этих проблем рассматриваются трудности распознавания лиц в масках, которое стало широко распространенным в период пандемии COVID-19, а также распознавания изображений, де-идентифицированных с помощью новой процедуры Fawkes. Эти вопросы особенно важны в ситуациях, когда необходимо точно идентифицировать личность, например, в сфере пограничной безопасности, контроля и других критически важных областях. В статье уделяется особое внимание решениям данных проблем, а также проводится анализ текстурных изменений и структурных искажений, возникающих на изображениях, обработанных с помощью процедуры Fawkes. Для формальной и количественной оценки этих изменений применялись многослойные параметрические методы. В результате выявлены причины, по которым изображения лиц, прошедшие процедуру Fawkes, не распознаются системами глубокого обучения, и доказано, что такие изображения могут успешно распознаваться с использованием традиционных методов, не основанных на глубоком обучении. Кроме того, в ходе исследования продемонстрирована эффективность предложенных методов на изображениях лиц в масках. Эти методы позволяют надежно распознавать не только изображения, обработанные процедурой Fawkes, но и лица, скрытые под масками.

Практическая значимость. Использование простых методов предобработки может повысить эффективность распознавания изображений, прошедших процедуру Fawkes, в системах глубокого обучения. Эти методы также могут быть полезны для решения проблем, связанных с распознаванием лиц в масках. Таким образом, данное исследование демонстрирует высокую эффективность и перспективность предложенных методов.

Ключевые слова: де-идентификация, распознавание лиц, детерминированные алгоритмы, технология Fawkes, глубокое обучение, двумерное косинусное преобразование.

Қабылданған күні: 2024 жылғы 20 тамыз
Рецензиядан өткен күні: 2025 жылғы 12 ақпан
Мақұлданған күні: 2025 жылғы 11 сәуір