ӘОЖ 004.93'11 **DOI 10.52167/1609-1817-2023-127-4-196-206**

Қ.С. Мауленов[1], С.А.Кудубаева [2], Н.М. Казиева[2], Ж.Б.Шүрен[2]
[1]А. Байтұрсынов атындағы Қостанай өңірлік университеті, Қостанай, Казақстан
[2] Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Казақстан
E-mail: k_maulenov@inbox.ru

АДАМДАРДЫҢ БЕЙНЕЛЕРІН ДЕ-ИДЕНТИФИКАЦИЯЛАУ ӘДІСТЕРІ ЖӘНЕ ОЛАРДЫ ШЕШУ ЖОЛДАРЫ

Аңдатпа. Мақалада соңғы жылдары пайда болған бетті тану жүйелерінің заманауи проблемасы қарастырылған. Бұл Fawkes технологиясының мысалында бетті де-идентификациялау процедурасынан өткен бет бейнелерін тану сияқты мәселе болып табылады. Мақалада Fawkes-ті сәйкестендіру процедурасын бет суреттеріне қолдану кезінде пайда болатын өзгерістері егжей-тегжейлі сипатталған және көрсетілген. Бет суреттеріндегі құрылымдық бұзылулардың (бұрмаланулардың) бітімдік өзгерістері мен ерекшеліктері ұсынылған және сипатталған. Оларды ресми және сандық бағалау үшін бұзылулардың көп деңгейлі параметрлік бағалау әдістері қолданылған. Resnet34 моделі негізінде терең оқыту әдістерімен де-идентификациялау рәсіміне қатысқан адамдардың бейнелерін тану бойынша эксперименттердің нәтижелері ұсынылған. CNN негізіндегі жүйенің құрылымы мен сипаттамасы ұсынылған. Жүргізілген эксперименттер нәтижесінде де-идентификация процедурасынан өткен кескіндердің терең оқыту негізінде жүйе бойынша танылмайтындығы анықталды. Терең оқыту тапсырмаларында Fawkes процедурасын орындау барысында бұзылған (бұрмаланған) адамдардың суреттерін пайдалану мүмкін емес болуының себептері түсіндірілді. Екі өлшемді косинус түрлендіруі, кездейсоқ нүктелерді генерациялау әдісі (кездейсоқ), жарықтық мәндерін есептеуге негізделген әдіс сияқты детерминделген тану алгоритмдері арқылы Fawkes-тың сәйкестендіру процедурасына ұшыраған кескіндерді тану мәселесін шешудің мүмкін жолдары антропометриялық нүктелердің координаттарын анықтау және кескіндерді тегістеу арқылы алды-ала өңдеу процедурасын қолдану ұсынылады.

Практикалық маңыздылығы. Сверткалы нейрондық желінің кірісінде Fawkes процедурасынан өткен адамдардың кескіндерін өңдеудің қарапайым әдістерін қолдану оларды жоғары тиімділікпен тануға мүмкіндік береді, сонымен қатар кескіндерге әртүрлі де-идентификациялау процедуралары қолданылатын басқа жүйелерде де қолданылуы мүмкін деп мәлімдейді.

Түйінді сөздер. Де-идентификация, бетті тану, терең оқыту, Fawkes процедурасы, детерминделген тану әдістері.

Кіріспе.

Авторлар бет-әлпетті танудың заманауи алгоритмдері әртүрлі «кедергілер» болған кезде, яғни көзілдірікті, қалпақшаларды кию, бастың бұрылуы және қисаюы кезінде жақсы жұмыс жасай біледі, бұл алгоритмдердің көпшілігі терең оқыту әдістеріне негізделген. Бірақ шын мәнінде үлкен қара көзілдірік, қалпақ, шарф немесе жай ғана қолыңызбен жабылған бет тұлғаны тануға мүмкіндік бермеуге көмектеседі. Мұның айқын мысалы - Американдық ұлттық стандарттар және технологиялар институтының (NIST) зерттеушілері жүргізген зерттеу жұмыстары. Нәтижесінде медициналық бетперде кию - тұлғаны танудың арнайы алгоритмдері арқылы адамды анықтауға кедергі келтіретіні анықталды. Зерттеу барысында 89 тұлғаны тану алгоритмдері сыналды, олар қалыпты жағдайда шамамен 0,3% жағдайда қате нәтиже береді. Алайда, алгоритмдер медициналық

бетперде киген адамдарға сыналған кезде, қателіктер саны 5% - дан 50% - ға дейін өсті [1]. Осылайша, жоғарыда аталған әдістермен тиісті түрде танудан құтылуға болады және бұл өте қарапайым. Бірақ оны үнемі пайдалану керек, ал нақты өмірде бұл қазірдің өзінде қиын мәселе болып табылады.

Мысалы: қол жетімділікті басқару, шекара өткелі немесе тұлғаны автоматты түрде тану (идентификация/аутентификация) жүйесімен жеке басын тексеретін кез-келген басқа тармақ шеңберінде бетперде киген адамды тану мәселесі тұлғадан бетпердені алып тастау сұралған кезде шешілетіні анық. Осындай сценарийлер аясында бетперде және/немесе бетті жабатын кез-келген басқа заттарды алып тастау міндетті болып табылады. Қазіргі заманғы тану жүйелері үшін анағұрлым күрделі мәселесі жасанды интеллект негізіндегі бет бейнелерін анықтаудың жаңа революциялық шешімдерінен туындайды [2, 3], олардың бірі - Fawkes процедурасы.

Зерттеудің мақсаты - Fawkes бет кескіндерін анықтау процедурасын зерттеу, Fawkes процедурасынан кейін бет кескіндеріндегі құрылымдық өзгерістер мен құрылымдық бұзылулардың (бұрмаланулар) ерекшеліктерін зерттеу, Fawkes сәйкестендіру процедурасынан өткен адамдардың кескіндерін тану мәселесін шешудің жолдарын іздеу.

Материалдар мен тәсілдерді.

Көп деңгейлі параметрлік бағалау, формальды және сандық бағалау, терең оқыту әдістері, детерминделген тану әдістері.

2020 жылдың тамызында Чикаго университетінің компьютерлік инженерлері құрған Fawkes деп аталатын тұлғаны анықтаудың заманауи әдісі белгілі болды.

Fawkes процедурасы, бет бейнесін түрлендіруді жүзеге асырады және оларды терең оқыту технологиясында қолдануға жарамсыз етеді (Deep Learning, DL) [4]. Бұл процедураны әзірлеушілер Fawkes-түрлендіру кезінде бет бейнелері айтарлықтай бұрмаланбайды, бірақ CNN (Convolutional Neural Network) оқыту тапсырмасына қажетсіз болуы үшін өзгертіледі (жасырылады немесе жойылады) және танылмайды, - деп санайды. Fawkes фотосуретті пиксель деңгейінде өзгертуге, бет кескіндерін түрлендіруге немесе зерттеушілер айтқандай, оны «жасыруға» — бетті тану жүйелері тәуелді болатын кейбір ерекшеліктерді болмашы өзгертуге бағытталған. Мұндай «жасыру» көзге көрінбейді, бірақ бетті тану жүйелері енді деректерді дұрыс өңдей алмайды.

Тестілеу аясында Чикаго университетінің әзірлеушілері Fawkes көмегімен Amazon, Microsoft, сондай-ақ қытайлық Megvii компаниясының бет-әлпетін тану жүйелерін алдай алды. Facebook әлеуметтік желісінің бетті тану жүйесіндегі сынақтар жасырын нұсқаның ТИ-ын танымады.

Бұл құралдың суреттерді өзгертуде үш режимі бар: төмен, орта, жоғары. Режим неғұрлым жоғары болса, соғұрлым кескін бұрмаланады және сенімді қорғауды қамтамасыз етеді. 1-суретте АҚШ-тың бұрынғы президенті Барак Обаманың үш режимдегі (төмен, орта, жоғары) кескінін бұрмалау нәтижелері көрсетілген, фотосурет Fawkes әзірлеушілерінің ресми деректемесінен алынған.

1 сурет - Төмен, орта, жоғары - үш режимдегі Fawkes процедурасының нәтижелері [4]

Бұл мысалда түпнұсқамен салыстырғанда ешқандай айырмашылық болмаса да, көптеген пайдаланушылар өзгерістердің жоғары параметрімен (mod high) көзге көрінетін елеулі өзгерістер болды деп шағымданды. Әйелдер бетінің өзгертілген суреттерінде бет шаштары, көгерулер және басқа өзгерістер байқалады. Әзірлеушілер Fawkes мүмкіндіктерін жетілдіруді жалғастыруда.

2-суретте цифрлық түпнұсқа кескіндерді жасырудың ең жоғары параметрі-mode = « high_ cloaked кезіндегі Fawkes-түрлендіру нәтижелерімен салыстыру көрсетілген, мұнда жеке цифрлық фотосуреттер бастапқы деректер (түпнұсқа кескіндер) ретінде пайдаланылады. 2, а -суретте беттің бастапқы түсті бейнесі және 2, б - суретте максималды режимде Fawkes процедурасынан өткендегі бейнесі.

a *b*

2 сурет - Түпнұсқа (а) және Fawkes –түрлендіру нәтижесі (b)

Шынында да, Fawkes-трансформация процедурасынан кейінгі беттердегі өзгерістер жай көзбен байқалады, әсіресе қас, мұрын және жоғарғы ерін, көз деңгейіндегі беттің сопақ шекаралары, сондай-ақ бастың сыртқы контуры - осының барлығын 2, б-суреттен көруге болады.

Нәтижелер.

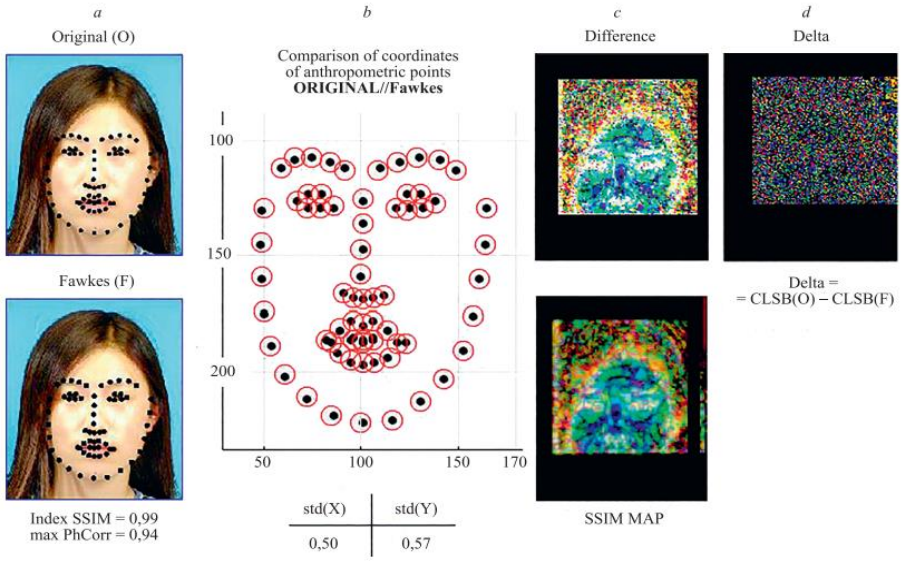
Fawkes процедурасынан өткен суреттердегі өзгерістер.

Осы өзгерістердің табиғатын зерттеу үшін осындай процедура cufs бет бейнелеу базасына да қолданылды [5], 3-сурет. Cufs бет кескінінің базасы (CUHK) бет эскиздерін синтездеу және бетті тану саласындағы зерттеулерге арналған. Fawkes процедурасынан кейінгі өзгерістер, тіпті максималды режимде де, 1-суретпен салыстырғанда аз байқалады, бірақ олар әлі де бар. Бұл кескіннің көлеміне және беттегі эмоцияға байланысты болуы мүмкін.

3 сурет - CUFFS бет суреттерінің базасы [5]

Fawkes процедурасын қолданғаннан кейін оларға негізгі (антропометриялық) нүктелердің координаттарын есептеу, құрылымдық ұқсастық индекстерінің параметрлік бағалары және фазалық корреляцияның максимумы сияқты бірқатар процедуралар

қолданылды. 4, а-суретте екі түпнұсқа кескін ұсынылған- түпнұсқа (Original) деп алынған CUFS базасындағы беттің түрлі-түсті бейнесі және оның Fawkes түрлендіруінің (Fawkes) нәтижесі.



4 сурет - Бастапқы деректер: түпнұсқа және оның Fawkes-түрлендіру нәтижесі (a), сондай-ақ олардың өзара сипаттамаларын ұсыну формалары (b, c, d) [6]

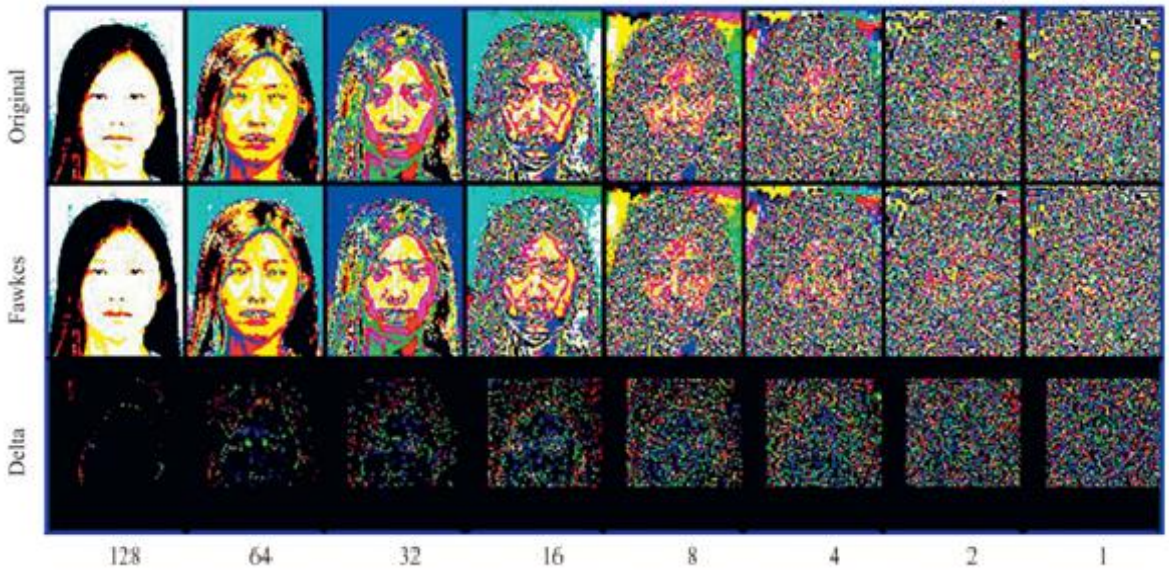
Бетке есептелген негізгі (антропометриялық) нүктелердің координаттары жазылады. Бұл суреттердің текстуралық айырмашылықтарының параметрлік бағаланулары келтірілген: құрылымдық ұқсастық индексі (Index Structural SIMilarity) [7] Index SSIM = 0,99 және максималды фазалық корреляция [8] — max Phase Correlation = 0,96. Бұл екі бағалау беттердің екі кескінінің — түпнұсқаның және оның Fawkes түрлендіруінің нәтижесінің толық ұқсастығын көрсетеді, дегенмен кейбір фазалық корреляция (0,96) текстурада бар екені анық. 4, b - суретте екі тұлғаның да негізгі нүктелерінің координаттары, сондай-ақ олардың негізгі нүктелерінің координаттарының орташа квадраттық ауытқуын бағалау ұсынылған. Бұл ауытқулар пиксельдің жартысына жуығын құрайды, оны Fawkes-бет аймағының өзгеруіне де, негізгі нүктелерді өлшеу қателіктеріне де жатқызуға болады. Осы ескертулерді ескере отырып, біз 4, а, b-суреттеріне назар аударамыз, онда Fawkes-түрлендіру процедурасынан өткен түпнұсқа және кескін құрылымы мен кескін пішіні арасында маңызды өзгерістер жоқ екені көрініп тұр. Дәл осы факт туралы Fawkes процедурасын орындаушы авторлар хабарлады. 4-суретте олардың мәндерінің 100 есе өсуі кезіндегі текстуралардың айырмашылығы (дифференциал) және бастапқы кескіндер арасындағы құрылымдық ұқсастық матрицасы (SSIM MAP [9]) келтірілген. Соңында, 4, d-суретте түпнұсқасының CLSB (O) түрлі-түсті биттік қабаттары (Color Least significant bit, CLSB) мен оның Fawkes-CLSB(F) түрлендіру нәтижесі арасындағы айырмашылық ретінде алынған «Delta» түсті кескіні ұсынылған. Бұл жағдайда CLSB : O — Original және F — Fawkes түрлі-түсті кескіндерімен ұсынылған, бастапқы матрицалар бойынша 2 модуль операциясы арқылы есептеледі

$$Delta = CLSB(O) – CLSB(F), \quad (1)$$

мұндағы CLSB(O) = mod(Original, 2); CLSB(F) = = mod(Fawkes, 2)[6].

4 с, d-суреттердегі нәтижелер бойынша түпнұсқалық Original кескін мен Fawkes-кескіндерінің арасында айырмашылықтар бар екенін, олар беттің жоғарғы бөлігін қамтиды деп айта аламыз.

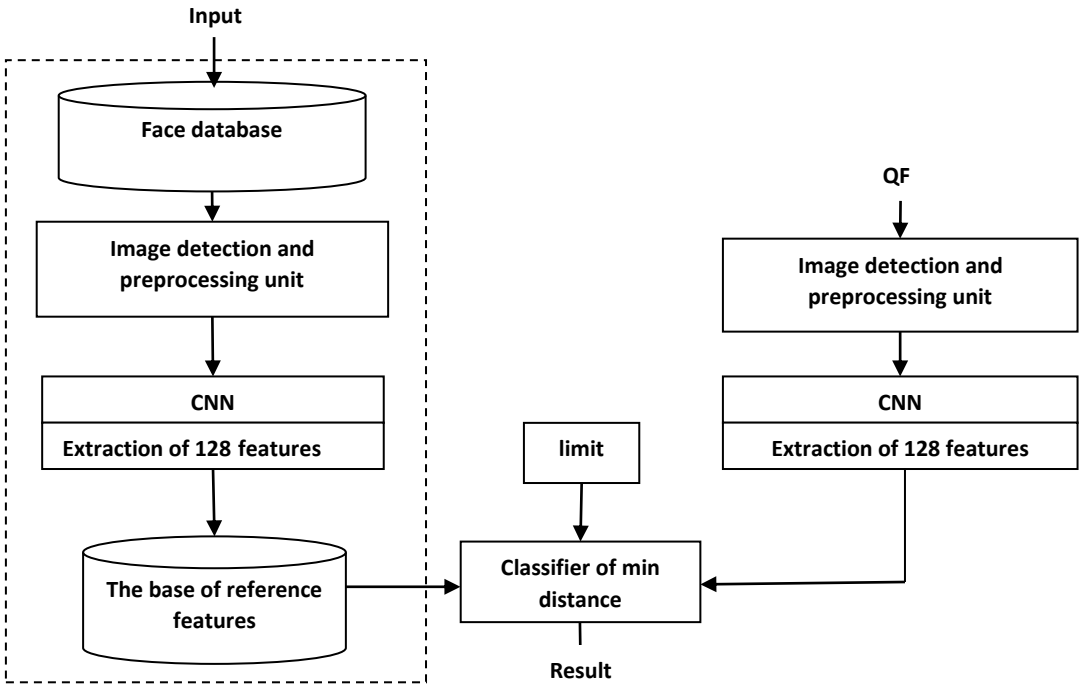
Және бұл өзгерістер бит қабаттарында, яғни 5-суретте көрсетілген Fawkes-түрлендіру процедурасынан өткен «суреттердің ішінде» орын алады.



5 сурет - Түпнұсқа кескін мен оның Fawkes-түрлендіру нәтижесі арасындағы айырмашылықтарды білдіретін 8 биттік қабаттар [6]

5-суретте CLSB(O)- түпнұсқалық кескіндерінің сегіз түрлі-түсті биттік қабаттары, сегіз CLSB(F) Fawkes-түрлендіру нәтижелерінің кескіндері және олардың арасындағы сегіз CLSB(Delta) айырмашылық көрсетілген. Сегіз CLSB — дің әрқайсысында екі түрлі аймақты байқауға болатындығын ескеруге болады, олар: қара және түрлі-түсті. «Delta» жолағындағы қара аймақтар нөлдік пиксель мәндерімен құрылады және түпнұсқа кескін мен Fawkes кескініндегі осы аймақтардың толық сәйкестігін анықтайды. Түрлі-түсті аймақтар - бұл Fawkes кескіндерінің түпнұсқа кескіндерден айырмашылығы. Көріп отырғаныңыздай, минималды салмағы 1-ге тең, ең үлкен өзгерістер (немесе бұзылулар) LSB қабаттарында (Least Significant Bit) болған. LSB қабаттарындағы «1» - ден «0» - ге дейінгі және кері бағыттағы өзгерістер кескін жарықтығының 1/255(максималды жарықтылыққа қатысты) шамасына өзгеруіне сәйкес келеді. LSB қабатының сол жағындағы келесі қабаттарда бұл өзгерістер жарықтылыққа 2/255 коэффициентімен, келесісінде 4/255 коэффициентімен және т.б. әсер етеді. Биттік қабаттардың ең шеткі сол жақтағы бағанында бұл коэффициент 128/255-ті немесе жарықтық диапазонының (0-ден 255-ке дейін) жартысын құрайды. Fawkes процедурасындағы осы өзгерістерді ескере отырып, биттік қабаттардағы өзгеретін аймақтардың мөлшері немесе олардағы өзгеретін пикселдердің саны LSB қабатының сол жағының бағытында қабаттан қабатқа қарай азаяды. Бұл Fawkes түрлендіру нәтижесінде көрінетін текстуралық өзгерістердің азаюына қол жеткізеді [6].

Орындалған эксперименттер аясында біз Fawkes процедурасынан өткен беттердің суреттері терең оқыту әдістері арқылы расында танылмайтынын анықтадық. Ол үшін Dlib кітапханасында [11] ResNet34 терең сверткалық нейрондық желінің (Convolutional neural network, CNN) алдын-ала дайындалған моделін енгізу негізінде тану жүйесі жасалды, ол бірнеше кезеңнен тұрды. Детектор ретінде HOG [10] пайдаланылды. Бетті тегістеу үшін 68 антропометриялық нүктені іздеу және олардың негізінде бетті орталықтандыру алгоритмі қолданылды [15]. Ерекшеліктерді анықтау әдісі ретінде CNN resnet34 моделі қолданылды. Осылайша, CNN (Recognition System with CNN - RS_CNN) негізіндегі бетті тану жүйесінің құрылымы келесі 6-суретте көрсетілгендей болды.



6 сурет - CNN негізіндегі жүйенің құрылымы
(Recognition System with CNN - RS_CNN)

Жүйенің құрылымы екі симметриялы бөліктен тұрады – сол және оң.

Сол жақ бөлікке тізбектей жалғанған блоктар кіреді: эталондық кескіндер базасы; эталондық кескінді анықтау және өңдеу блогы; әр сілтеме кескіні үшін эталондық белгілер базасында сақталатын 128 белгілер жиынтығын құрайтын CNN. Эталондық белгілер базасы жіктеуішке қосылған.

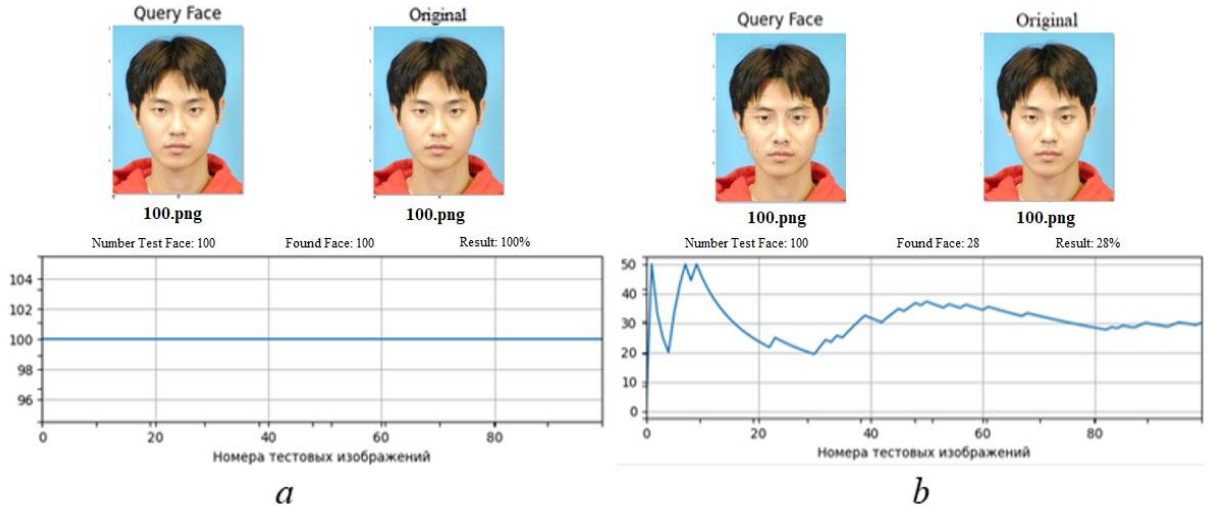
Оң жақ бөлігі сол жақтан ерекшеленеді, өйткені оның кірісіне сұраныс кескіндері (query Face - QF) келіп түседі. Оң жақ бөліктің шығысы да жіктеуішке қосылған.

Жіктеуіш «біреуден көпшілікке» дейтін сценарий бойынша орындалған. Мұнда біреуі QF, ал көпшілігі эталондар жиынтығы болып табылады. Жіктеуіш мына критерий бойынша жүзеге асырылады, яғни минималды қашықтық (Minimum Distance Criterion) l2 метрикасында және дәрежесі 1-ге тең, оны келесі (MDC/L2/rang1) модельмен ұсынуға болады. Жіктеуіштің міндеті - эталондық кескіндердің барлық белгілерімен QF бейнелейтін белгілер жиынтығы арасындағы қашықтықты есептеу және олардың арасынан берілген шекті мәнмен минималды қашықтыққа сәйкес келетін анықтамалық кескінді іздеу. Сонымен қатар, қабылданған жіктеуіш моделіне сәйкес, бұл минимум бірінші орында тұруы керек.

RS_CNN жұмысы эталондық кескіндерді жинаудан, оларды өңдеуден және олар бойынша эталондық белгілерді есептеуден басталады. Бұл тіркеу кезеңі (стандарттар) деп аталады. Сондықтан жүйенің сол жағы тек бір рет қолданылады. Тіркеу аяқталғаннан кейін ғана жүйенің оң жағы қосылады. Әрі қарай, ол QF кескіндерінің кірісіне қарай тану режимінде жұмыс істейді. Тану режимін сәйкестендіру, іздеу, аутентификация ретінде жүзеге асыруға болады. Жүйенің сол және оң жағындағы CNN блогы бірдей екенін ескеру керек.

Жүйенің сол және оң жағындағы түпнұсқа CUFS(O) базасында, яғни CUFS(O) беттерінің «таза» кескіндер базасында және кескін жүйесінің кірісінде эксперименттер жүргізу кезінде -сұраулар (query Face-QF), яғни CUFS(O) нәтиже 100% болды, барлық кескіндер танылды (7, а-сурет). Ал сол жағында және кескін жүйесінің кірісінде CUFS(O)

базасымен ұқсас эксперименттер жүргізген кезде - сұраулар (query Face - QF) Fawkes CUFS(F) процедурасынан өткен кескіндер жүйе танылған кескіндердің 30% - дан төменін шығарды.



7-сурет. CNN негізіндегі жүйені тану нәтижелері
(Recognition System with CNN - RS_CNN)

Fawkes-түрлендіру процедурасы бет кескіндерін CNN-ді танудан қорғауға мүмкіндік беретіні сөзсіз. Fawkes технологиясының авторлары атап өткендей:» ... Fawkes мінсіз болмаса да, ол адамдарға бұрын болмаған құралдарды ұсынады және бет-әлпетті қажетсіз танудан қорғауды қамтамасыз ете алады» [5].

Талқылау.

Мүмкін болатын шешімдер.

Fawkes процедурасының өзі жасанды интеллект негізінде жасалғандықтан, терең оқыту әдістерінен тыс, мысалы кеңінен танымал және бұрын қолданылған детерминделген тану алгоритмдері арқылы шешім іздеуге болады [8].

2DDCT косинус- түрлендіруі.

Біз қарастырып отырған тапсырмада 2DDCT косинус-түрлендіру (Two-dimensional Discrete Cosine Transform) негізінде Simple FaReS тиімді пайдалануға болады [8,12,13,16]. Бұл тәсілдің негізгі идеясы - кескін деректерін олардың дискретті түрлендіру коэффициенттерімен (трансформаторлармен) ұсыну болып табылады. Екі өлшемді DCT формуласы келесі үлгідей болады:

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

Бұл $0 \leq i,j \leq n-1$ кезінде орын алады. Кескін n × n өлшемді пиксел блоктарына бөлінеді және теңдеулер әрбір пиксел блогы үшін Gij коэффициенттерін табу үшін қолданылады. DCT cos-түрлендірудің негізгі функциялары сандық кескіндердің жалпы жиынтығы (үлкен жиынтықтар) үшін есептелген меншікті функцияларды жуықтау үшін ең тиімді (минималды шығын мағынасында) болып табылатындығына негізделген. Осы фактіні ескере отырып, бастапқы кескінді өңдеу кезеңін толығымен алып тастауға болады. Сонымен қатар, cos-түрлендіру DCT спектрлік компоненттерінің белгілері аз беттермен бастапқы кескінді дәл көрсетеді.

Random.

Fawkes-түрлендіру нәтижесінің биттік қабаттарындағы өзгерістерге сезімтал емес тағы бір модель Random әдісіне негізделген жүйе болуы мүмкін. Random – бұл бет немесе бүкіл фотопортрет аймақтарына біркелкі бөлінген пиксел координаттарын жасау әдісі [8,14]. Бұл өзгермейтін координаттар әрбір түпнұсқа және барлық Fawkes танылатын кескіндер үшін жарықтық белгілерінің векторын есептейді. Әрі қарай, тану жүйесі жарықтылық белгілерінің векторларын салыстырады және оларды жіктейді.

Антропометриялық нүктелердің координаттары (Coordinates of the Anthropometric Points, CAP).

Сондай-ақ, кездейсоқ нүктелерді генерациялаудан қарағанда жетілдірілген әдісті қарастыруға болады, бұл антропометриялық нүктелердің координаттарының жарқын мәндерін есептеуге негізделген әдіс. Беттің антропометриялық нүктелерінің координаттарын таңдау әдісі бойынша (антропометриялық нүктелердің координаттары, CAP [15]) жарықтық белгілерінің векторлары есептелінеді. Бұл векторлар беттің әрбір жеке бейнесін оларды тану әдісі негізделген (түпнұсқа және оның Fawkes-түрлендіру нәтижесі) жеткілікті дәлдікпен көрсетеді.

Тегістеу.

Соңында, QF (Query Face) кескінін алдын-ала тегістеуге негізделген алдын ала өңдеу процедурасын жасауға болады. Тегістеу процедурасы кез-келген түрде болуы мүмкін, бірақ оның міндеті-Fawkes процедурасы өзгерткен суреттегі бет аймағына «қатты бұрмаланған ақпаратты қайта құру». Мысалы бұған екі қадаммен қол жеткізуге болады: алдымен суретті кішірейтіп, содан кейін оны бастапқы өлшеміне қайтарыңыз. Бірінші қадамда Fawkes процедурасымен өзгертілген аймақтар сығылып, орташаланған кезде тегістеледі. Екінші қадамда CLSB сығылған аймақтарының кеңеюі (интерполяция арқылы) жүреді, бұл бет құрылымындағы бұрмаланған ақпаратты тегістеуге әкеледі.

Қорытынды.

Мақалада терең нейрондық желіге негізделген бетті тану жүйелерінің (CNN) заманауи мәселесі қарастырылады. Оған мысал: Fawkes процедурасынан өткен бетті тану – терең оқытуға негізделген жеке тұлғаны анықтау технологиясы. Fawkes процедурасы ең жоғары mode параметрімен қолданылған кезде CNN оқытқан бет кескінін танудың төмен нәтижесін растайтын эксперимент нәтижелері берілген. Бастапқы бет суреттерімен Fawkes процедурасынан өткен кескіндерді салыстырмалы талдау негізінде құрылымдық бұрмаланулардың текстуралық өзгерістері мен графикалық ерекшеліктері көрсетілген. Осы талдаудан басқа, осы бұрмаланулардың көп деңгейлі параметрлік бағаланулары берілген және олардың негізінде терең оқыту және тану тапсырмаларында Fawkes процедурасынан өткен беттердің кескіндерін пайдалануды қиындататын себеп нақтыланған. Цифрық құралдар ретінде құрылымдық ұқсастық индексі (Index SSIM) және фазалық кескін корреляциясы (Phase Correlation) қолданылады. Терең оқытудан тыс әдістермен Fawkes процедурасынан өткен беттерді тануды шешу жолдары ұсынылған. CNN кірісінде бет кескіндерін (Fawkes процедурасынан өткен) өңдеудің қарапайым әдістерін қолдану олардың жоғары өнімділікпен танылуына әкелуі мүмкін деп саналады.

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

ӘДЕБИЕТТЕР

[1] 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

[2] Wu Y., Yang F., Xu Y., Ling H. Privacy-protective-GAN for privacy preserving face de-identification // Journal of Computer Science and Technology. 2019. V. 34. N 1. P. 47–60. https://doi.org/10.1007/ s11390-019-1898-8

[3] Nousi P., Papadopoulos S., Tefas A., Pitas I. Deep autoencoders for attribute preserving face de-identification // Journal Signal Processing: Image Communication. 2020. V. 81. P. 115699. https://doi. org/10.1016/j.image.2019.115699

[4] Shan S., Wenger E., Zhang J., Li H., Zheng H., Zhao B.Y. Fawkes: Protecting privacy against unauthorized deep learning models // Proc. 29th USENIX Security Symposium. 2020. P. 1589–1604.

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

[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 Opticsthis. 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] Kuharev G.A., Kamenskaja E.I., Matveev Ju.N., Shhegoleva N.L. Metody obrabotki i raspoznavanija izobrazhenij lic v zadachah biometrii. CPb.: Politehnika, 2013. 388 s.

[9] De Vel O., Aeberhard S. Line-based face recognition under varying pose. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1999, vol. 21, no. 10, pp. 1081–1088. https://doi.org/10.1109/34.799912

[10] Maulenov Қ.S., Kudubaeva S.A. COMPARATIVE ANALYSIS OF FACE DETECTORS HAAR, HOG, CNN. // NEWS of the National Academy of Sciences of the Republic of Kazakhstan. Volume 5, Number 339 (2021), 74–82 https://doi.org/10.32014/2021.2518-1726.87

[11] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun. Deep Residual Learning for Image Recognition. https://doi.org/10.48550/arXiv.1512.03385

[12] Chao-Hsing Hsu, Zhen Guo, Kang Yen. Comparison of Image Approximation Methods: Fourier Transform, Cosine Transform, Wavelets Packet and Karhunen-Loeve Transform. Department of Electrical Engineering Florida International University 10555 W. Flagler St.Miami Fl 33174

[13] Ziad M. Hafed, Martin D. Levine. Face Recognition Using the Discrete Cosine Transform. Sivakasi, India. ISBN: 978-1-4577-2149-6

[14] Maulenov K. S., Kudubayeva S. A., and Uvaliyeva A. A. «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.

[15] 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

[16] Aimbetova D.T., Zharlykasov B.Zh., Muslimova A.Z. «Raspoznavanie izobrazhenij lic dlja identifikacii». Aktual'nye nauchnye issledovanija v sovremennom mire // Obshhestvennaja organizacija» Institut social'noj transformacii». 2017, 12-1, s. 164-168.

Kalybek Maulenov, master's degree, senior lecturer, A.Baitursynov Kostanay Regional University, Kostanay, Kazakhstan, k_maulenov@inbox.ru

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

Zhazira Shuren, master's degree, senior lecturer, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Saule Kudubaeva, candidate of technical sciences, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, saule.kudubayeva@gmail.com

METHODS OF DE-IDENTIFICATION OF FACIAL IMAGES AND WAYS TO SOLVE THEM

Abstract. The article considers the modern problem of facial recognition systems that has appeared in recent years. This is such a problem as the recognition of faces subjected to the procedure of de-identification of persons, using the example of Fawkes technology. The article describes in detail and demonstrates the changes that occur when applying the Fawkes de-identification procedure to facial images. Textural changes and features of structural damage in facial images are presented and described. Multilevel parametric damage estimates are applied for their formal and numerical evaluation. The results of experiments on recognizing images of faces subjected to the de-identification procedure by deep learning methods based on the ResNet34 model are presented. Presented the structure and description of the CNN-based system. As a result of the experiments, it was found out that images that have undergone the de-identification procedure are not recognized by the system based on deep learning. Explained the reasons for the impossibility of using images of faces destroyed during the Fawkes procedure in deep learning tasks. Possible ways of solving the problem of recognizing images subjected to the Fawkes de-identification procedure by deterministic recognition algorithms such as two-dimensional cosine transformation, random point generation method, a method based on calculating the brightness values of the coordinates of anthropometric points and applying a preprocessing procedure by smoothing images subjected to the de-identification procedure are proposed.

Practical significance. It is argued that the use of simple methods of preprocessing images of persons subjected to the Fawkes procedure at the input of a convolutional neural network can lead to their recognition with high efficiency, and can also find application in other systems where various de-identification procedures are applied to images.

Keywords. De-identification, face recognition, deep learning, Fawkes procedure, deterministic recognition methods.

Қалыбек Мауленов, магистр, старший преподаватель, Костанайский государственный университет им. А.Байтурсынова, Костанай, Казахстан, kmaulenov@inbox.ru

Назым Казиева, к.т.н., и.о. доцента, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, kaznaz@list.ru

Жазира Шурен, магистр, старший преподаватель, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

Сауле Кудубаева, к.т.н., ассоцированный профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, saule.kudubayeva@gmail.com

МЕТОДЫ ДЕ-ИДЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ ЛИЦ И ПУТИ ИХ РЕШЕНИИ

Аннотация. В статье рассмотрена современная проблема систем распознавания лиц, появившийся в последние годы. Это такая проблема как распознавание лиц, подвергнутых процедуре де-идентификации лиц, на примере технологии Fawkes. В статье подробно описывается и демонстрируются изменения, которые происходят при применении процедуры де-идентификации Fawkes к изображениям лиц. Представлены и описаны текстурные изменения и особенности структурных разрушений в изображениях лиц. Применены многоуровневые параметрические оценки разрушений для их формальной и численной оценки. Представлены результаты экспериментов по распознованию изображений лиц подвергнутых процедуре де-идентификации лиц методами глубокого обучения, на базе модели ResNet34. Представлена структура и описание системы на базе CNN. В результате проведенных экспериментов было выяснено что изображения, прошедшие процедуру де-идентификации, не распознаются системой на основе глубокого обучения. Объяснены причины невозможности использования изображений лиц, разрушенных в процессе выполнения процедуры Fawkes, в задачах глубокого обучения. Предложены возможные пути решения проблемы распознавания изображений, подвергнутых процедуре де-идентификации Fawkes, детерминированными алгоритмами распознавания такими как двумерное косинус-преобразование, метод генерации случайных точек (Random), метод основаный на вычисления яркостынх значений координат антропометрических точек и применение процедуру предобработки путем сглаживания изображений, подвергнутых процедуре де-идентификации.

Практическая значимость. Утверждается, что использование простых способов предобработки изображений лиц, подвергнутых процедуре Fawkes, на входе сверточной нейронной сети может привести к их распознаванию с высокой результативностью, а также могут найти применение в других системах, где к изображениям применены различные процедурам де-идентификации.

Ключевые слова. Де-идентификация, распознавание лиц, глубокое обучение, процедура Fawkes, детерминированные методы распознавания.

****