ӘОЖ 654.01

БЕТ БИОМЕТРИЯСЫН ҚОЛДАНА ОТЫРЫП, ЖЕКЕ ДЕРЕКТЕРДІ РҰҚСАТСЫЗ ҚОЛ ЖЕТКІЗУДЕН ҚОРҒАУ

Тоқтау Д.С[1]., Шүрен Ж.Б[2].
dinarats11@mail.ru
[1]Л.Н.Гумилев атындағы ЕҰУ, «Радиотехника, электроника және телекоммуникациялар» кафедрасының магистранты, Нұр-Сұлтан, Қазақстан
[2]Л.Н.Гумилев атындағы ЕҰУ, «Радиоэлектрондық аппаратураны жобалау және құрастыру» кафедрасының оқытушысы, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Казиева Н.М.

Қоғам дамуының қазіргі кезеңі ақпараттандыру мен телекоммуникациялық технологияларды жетілдірудің үздіксіз процесімен сипатталады. Осының арқасында байланыс және есептеу жүйелерін енгізу саласы үнемі кеңейіп, қоғам өмірінің барлық жаңа аспектілеріне әсер етеді. Осыған байланысты, ақпараттық қауіп-қатерлердің көрінісі жағдайында олардың тиімді жұмыс істеуі үшін осы жүйелердің жеткілікті дәрежеде қорғалуын қамтамасыз ету маңызды міндет болып табылады, ол үшін өз кезегінде ақпараттық тәуекелдерді талдау мен басқарудың әдісі болуы қажет. Бұл мақалада бет биометриясын қолдана отырып, ақпаратты қорғау жүйесін дамытуға қатысты мәселелер қарастырылған. .

Түйінді сөздер: биометрия, ақпаратты қорғау жүйесі, бет биометриясы, бет суреті, рұқсатсыз қол жеткізу, ақпараттық қауіпсіздік.

Қазіргі таңда автоматтандырылған жүйелер мен процестерді енгізбестен адамның, кәсіпорынның жұмысын ұйымдастыруды елестету қиын. Сонымен қатар, әр әзірлеуші өз жүйесін қарапайым және ыңғайлы етуге тырысады, өйткені бұл нарықтағы бәсекелестік өте үлкен. Жыл сайын ақпараттық технологиялар саласы тез дамып келеді. Әр түрлі өндірістік процестер автоматтандыруғ.а көбірек ұшырайды. Сондай-ақ, интернетті пайдаланушылар саны тұрақты өсуде. Әрине, қазіргі уақытта ұйым, тіпті ең кішкентай болса да, қол жеткізуді басқару жүйелерін, тіпті қарапайым, жергілікті есептеу жүйелерін, интернет ресурстарын және басқа да заманауи ақпараттық-коммуникациялық құралдарды пайдаланбай жұмыс істемейді. Осы себепті сыртқы және ішкі қауіпсіздік тақырыбының өзектілігі айқын болады. Сондықтан, бұл мақалада ақпаратты, жеке деректерді қорғау үшін қолданылатын тәсілдердің бір түрі бет биометриясы туралы қарастыратын боламыз.

Биометриялық сәйкестендіру – бұл пайдаланушының бірегей биометриялық параметрін ұсынуы және оны барлық қол жетімді мәліметтер базасымен салыстыру процесі. Мұндай жеке деректерді алу үшін биометриялық оқырмандар қолданылады.

Биометриялық қол жетімділікті басқару жүйелері пайдаланушылар үшін ыңғайлы, өйткені ақпарат тасымалдаушылары әрқашан олармен бірге болады, жоғалмайды немесе ұрланбайды. Қол жеткізудің биометриялық бақылауы неғұрлым сенімді болып саналады, өйткені сәйкестендіргіштерді үшінші тұлғаларға беруге, көшіруге болмайды.

Биометриялық сәйкестендірудің негізгі әдістерін салыстырмалы талдау жүргізе отырып, кез-келген жүйені бағалау үшін екі параметр керек екендігі анықталды:

FAR (False Acceptance Rate) - жалған өткізу коэффициенті, яғни жүйеде тіркелмеген пайдаланушыға жүйеге кіруге рұқсат беретін жағдайлардың туындау пайызы.

FRR (False Rejection Rate) - жалған бас тарту коэффициенті, яғни жүйенің нақты пайдаланушысына қол жеткізуден бас тарту.

Екі сипаттама да математикалық статистика әдістері негізінде есептеу арқылы алынады. Бұл көрсеткіштер неғұрлым төмен болса, объектіні тану дәлірек болады. Биометриялық сәйкестендірудің ең танымал әдістері үшін FAR және FRR орташа мәндері 1-кестеде көрсетілген.

Кесте 1

FAR және FRR орташа мәндері

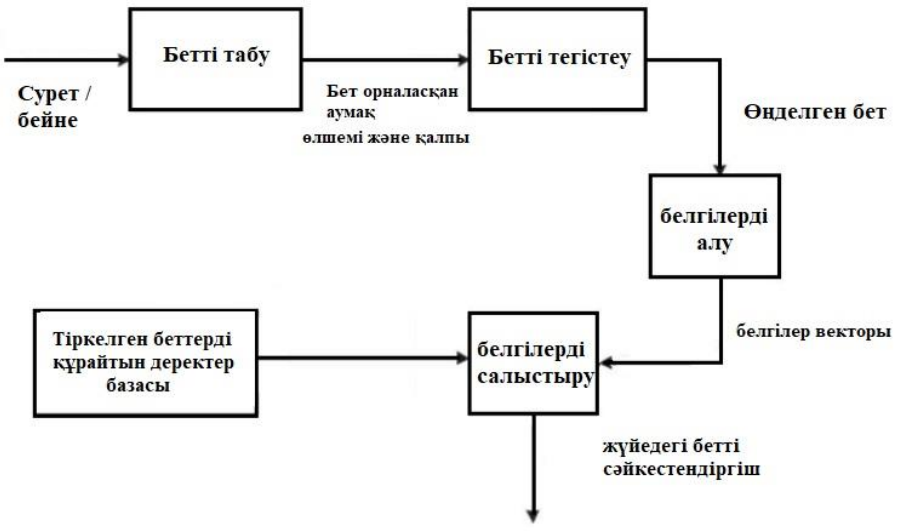
Биометриялық ҚББЖ пайдаланады:	**FAR**	**FRR**
Саусақ ізі	0,001%	0,6%
Бетті тану 2D	0,1%	2,5%
Бетті тану 3D	0,0005%	0,1%
Көздің шатырша қабығы	0,00001%	0,016%
Көздің ішкі тор қабығы	0,0001%	0,4%
Көктамыр суреті	0,0008%	0,01%

Ақпаратты қорғауды ең сенімді әдісіне бет-әлпетті тануға негізделген әдіс, оның ішінде суретте немесе бейнеде адамның бетін автоматты түрде локализациялау және қол жетімді мәліметтер базасы негізінде адамның жеке басын сәйкестендіру жатады. Қазіргі уақытта бетті танудың төрт негізгі әдісі бар:

– «Eigenfaces».
– «Айрықша белгілерді» талдау.
– «Нейрондық желілер» негізінде талдау.
– «Бет суретін автоматты түрде өңдеу» әдісі.

Соның ішінде ең тиімді деп «нейрондық желілер» тәсілін қолдануға болады. Себебі, нейрондық желіге негізделген әдісте тіркелген және тексерілетін екі адамның да сипаттамалары сәйкестікке салыстырылады. «Нейрондық желілер» тексерілетін адамның бет-әлпетінің бірегей параметрлері мен дерекқордағы шаблон параметрлерінің сәйкестігін анықтайтын алгоритмді қолданады, сондай-ақ параметрлердің ең көп саны қолданылады. Салыстыру шарасы бойынша тексерілетін тұлға мен деректер базасындағы шаблон арасындағы сәйкессіздіктер анықталады, содан кейін тиісті салмақ коэффициенттерінің көмегімен тексерілетін тұлғаның деректер базасындағы шаблонға сәйкестік дәрежесін анықтайтын механизм іске қосылады. Бұл әдіс қиын жағдайларда тұлғаны сәйкестендіру сапасын арттырады.

Қолданыстағы алгоритмдердің алуан түрлілігіне қарамастан, бетті тану процесінің жалпы құрылымы өзгеріссіз қалады. Ол келесі суретте көрсетілген.



Сурет 1 – Тану процесінің жалпы құрылымы

Бірінші кезеңде суреттегі бетті детекторлау және локализациялау жүзеге асырылады. Тану кезеңінде бет бейнесі тегістеледі (геометриялық және жарықтылық), белгілерді есептеу және тікелей тану – есептелген белгілерді дерекқорға енгізілген эталондармен салыстыру.

Биометриялық әдістерді факторлардың жиынтығы бойынша салыстыру жоғарыда айтылған Қазақстан нарығының ерекшеліктерін ескере отырып, бетті тануға негізделген 2D әдісінің артықшылықтарын көрсетеді. Бірқатар кемшіліктерге қарамастан, бірінші және екінші типтегі қателіктердің салыстырмалы түрде жоғары дәрежесі (FAR, FRR) және соның салдарынан бұрмалау мүмкіндігі, сондай-ақ айтпақшы сыртқы факторларға сезімталдықты бақылауға болады. Бетті тануға негізделген әдіс 2D, өте жоғары аутентификация жылдамдығына, алыс қашықтықтағы қозғалыс кезінде байланыссыз аутентификация мүмкіндігі, маңызды факторлар болып табылатын пайдаланушының жоғары жайлылығына ие. Әрине, төмен шығындар мен қажетті жабдықтардың қол жетімділігін атап өту керек. Орташа көрсеткіштері бар web-камералар да жеткілікті.

Қолданылған әдебиеттер тізімі

1 ҚР СТ 1699-2007 «Қол жеткізуді бақылау және басқару жүйелері. Жалпы техникалық талаптар»

2 ҚР СТ 1073 – 2007 Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар.

3 Акишев К., Дарибаева Г. Стандарттау, метрология және сәйкестікті бағалау: Оқулық. - Астана: Фолиант, 2008. - 256 бет.

4 Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов по специальности 230201 «Информационные системы и технологии» // В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стер. - М.: Академия, 2009. – 330 с. (гриф)

5 Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для вузов по направлению 230100 (654600) «Информатика и вычислительная техника» // П. Б. Хорев. - 4-е изд., стер. - М.: Академия, 2008. – 254 с. (гриф).

6 «Мемлекеттік құпияларды техникалық қорғау жөніндегі қызметті лицензиялау ережесін және оған қойылатын біліктілік талаптарын бекіту туралы» Қазақстан Республикасы Үкіметінің 2007 жылғы 18 маусымдағы № 505 Қаулысы

7 Компьютерлік ақпаратты қорғаудың құралдары мен тәсілдері: Әдістемелік нұсқау. – Ақтау қ. КМТжИУ, 2010, 46 бет.