

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ. И. Сәтбаев атындағы
Қазақ ұлттық техникалық университеті

Б. С. Ахметов
А. И. Иванов
Т. С. Картбаев
А. Ю. Малыгин
В. А. Фунтиков

ТҰЛҒАЛАРДЫҢ БИОМЕТРИЯЛЫҚ АУТЕНТИФИКАЦИЯСЫ НЕГІЗДЕРІ

Университеттің Ғылыми-әдістемелік кеңесі
оқу құралы ретінде ұсынған

Алматы 2014

ӘОЖ 004 (075.8)
КБЖ 32.973-018.2 я 73
Т 85

Пікір жазғандар:

Джурунтаев Д. З. – техн., ғыл., док-ры., профессоры, Қ. И. Сәтбаев атындағы ҚазҰТУ;
Төкеев У. А. – техн., ғыл., док-ры., профессоры, Әл-Фараби атындағы ҚазҰУ;
Өтепбергенов И. Т. – техн., ғыл., док-ры., профессоры, АЭЖБУ.

T85

Ахметов Б. С., Иванов А. И., Картбаев Т. С., Малыгин А. Ю., Фунтиков В. А.
Тұлғалардың биометриялық аутентификациясы негіздері: Оқу құралы. –
Алматы: Қ.И. Сәтбаев атындағы ҚазҰТУ, 2014. – 155 б.

Сурет 71. Кесте 4. Библиогр. – 98 атау.

ISBN 978-601-228-698-4

Оқу құралында заманауи биометриялық технологиялардың дамуы мен қалыптасу тарихы қарастырылған. Жеке тұлғаның биометриялық параметрлерінен мәліметтерді алу процедуралары баяндалған. Қолданылып жатқан статикалық және динамикалық биометриялық бейнелердің жетістіктері мен кемшіліктері көрсетілген.

Биометриялық параметрлер мен нейрожелілік биометрия-код түрлендіргіштердің айқын емес экстракторлары талданған. МЕСТ Р 52633.0-2006 сәйкес нейрондық желілерді жасанды үйретудің ерекшеліктері берілген. Бірнеше нейрожелілік контейнерлердің қауіпсіз бірігу мультибиометриясының механизмдері мен ашық әрі қорғалған нейрожелілік контейнерде нейрондық желімен үйретілген мәліметтерді жсайғастыру интерфейсі сипатталады.

МЕСТ Р 52633.1-2009 бойынша «Өзім» және «Бөгде» сынақ қорын қалыптастыру мен биометриялық бейнелер сынақ қорының көлемін көбейту кезінде «Бөгде» биометриялық бейнелерінің көбею генетикалық алгоритмі, МЕСТ Р 52633.3-2011 бойынша сынақ жүргізу сұрақтары қарастырылған.

Әртүрлі нейрондардың бірдей байланысынан іздеу арқылы нейрондық желілердің шығындалуына Г. Маршалко шабуылы мен шабуылға қарсы әрекет жолдарын қарастыру талқыға салынып отыр. Жеке биометриялық мәліметтерді көп шекті кванттау функциясы бар нейрондар мен қорғау процедуралары берілген.

Оқу құралы ынтымақтастық туралы Меморандумға сәйкес Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті мен Пенза мемлекеттік университетінің шығармашылық ұжымы дайындаған.

«Есептеу техникасы және бағдарламалық қамтамасыз ету», «Ақпараттық қауіпсіздік жүйелері», «Ақпараттық жүйелер» мамандықтарының бакалаврлары, магистранттары және докторанттарына, сонымен қатар, тұлғаларды аутентификациялау және ақпаратты қорғау жаңа биометриялық құралдарын құру қызықтыратын барлық мамандарға арналады.

ӘОЖ 004 (075.8)
КБЖ 32.973-018.2 я 73

Қазақстан Республикасы Білім және ғылым министрлігінің 2014 жылғы басылым жоспары бойынша басылды.

ISBN 978-601-228-698-4

© Ахметов Б.С., Иванов А.И.,
Картбаев Т.С., Малыгин А.Ю., Фунтиков В.А.
© Қ.И. Сәтбаев атындағы ҚазҰТУ, 2014

КІРІСПЕ

Адамның жеке басын қорғау және социумды ұжымдық қорғау – әрқашан биометрия негізінде құрылған. Кішкентай бала өз ата-анасын мүлтіксіз таниды. Әкесі мен анасы өз баласының бейнесін жақсы біледі және көптеген балалардың арасынан оны ажырата алады. Ана, әке, әпке, аға бейнелері адам түйсігінде (бас миының тереңдігінде) орналасады және адамдарға біршама қауіпсіз балалықты қамтамасыз етеді.

Ер жете келе, біз танитын адамдарымызға яғни көршілер, туыстар, таныстар мен қызметтестерімізге анағұрлым сенімділікпен қарай отырып, өз ұжымдық қауіпсіздігімізді құрамыз. Биометрия немесе таныс адамдардың бейнелерін тани алуымыз – социумдардың ұжымдық қауіпсіздігін қамтамасыз ету тетігінің рөлін орындай бастайды.

Қоғамның дамуы қарқынды жүріп жатыр. Оның негізі, адамдар арасындағы ақпарат алмасу болып табылады. Адамдардың ақпаратты адамдар арасында тасымалдауы үшін құрған күрделі жоғары ақпараттық тілдері бірінші ақпараттық революция болып табылатын секілді. Келесі ақпараттық революция – ауызекі тілді жазбаша түрде көрсетуі болып табылады. Қағаздағы немесе басқа да ақпарат тасымалдаушысындағы әріптер (таңбалар, иероглифтер) – бұл адам ауызекі тілінің цифрлық формадағы кодталуы.

Адамдардың қазақ, орыс, ағылшын табиғи тілдері күрделі объектілерді, соның ішінде сол немесе басқа адамның анағұрлым күрделі биометриялық бейнелерін сипаттай алады. Бірақ табиғи тілдер әдетте адамның өте күрделі сипаттамасын береді. Мемлекеттік есепке алу мақсатынан мемлекет пен қалалар рөлінің күрделенуінен адамдардың сипаттамасының қажеттілігі де күрделенеді. Мемлекет кез келген уақытта адамның шыққан тегін осы адамды танитын адамдарға сүйене отырып қалпына келтіруі мүмкін, бірақ бұл технология көлемі кіші мекендерде ғана тиімді. Үлкен аудандар мен қала тұрғындарының құқығын есепке алу үшін төлқұжат – жасын,

құқығын, статусын, азаматтың биометриясын көрсететін биометриялық құжат қажет. Төлқұжатқа деген қажеттілік әдетте адамның өз отбасынан, өз мекен-жайынан яғни өзін барлығы танытын жерден басқа танымайтын жерге қоныс аударғанында пайда болады.

Оқу құралы – қалайша адамның жеке ақпаратын өзінің жеке криптографиялық кілті мен жасырын биометриялық бейнесін қолдану арқылы биометриялы-криптографиялық қорғанысты дұрыс құруды және қолдануды үйретуге бағытталған.

Оқу құралы Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университетінің және Пенза мемлекеттік университетінің авторлық ұжымы бірлестігімен №753.МОН.ГФ.13.13 «Медициналық мекемелер үшін науқастардың электрондық тарихын биометриялық жасырын көрсету ON-LINE жүйесінің қолданыстағы зертханалық үлгісін іске асыру нұсқаларын зерттеу және өңдеу» ғылыми жобасын орындау барысындағы ынтымақтастық меморандумына сәйкес дайындалды.

1. БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫҢ ПАЙДА БОЛУ ЖӘНЕ ДАМУ ТАРИХЫ

Төлқұжаттар (жеке куәлік) 19 ғасырдың аяғы мен 20 ғасырдың басында мемлекеттер тарапынан беріле бастаған болатын. Заманауи төлқұжаттар адамның қолтаңбасы, фотосуреті тағы сол сияқты жынысы, шаш түсі, көзінің түсі, бойы тағы да басқа биометриялық мәліметтерінен тұруы мүмкін. Қағаз түріндегі төлқұжат – лауазымды адамдар тарапынан адам тұлғасының биометриялық идентификациясының процедурасын жүргізуге құжат түрінде негіз болуына қызмет етеді. Тексеруші тұлға ең алдымен қағаз тасымалдаушысындағы төлқұжат баспабегінің шынайылығын тексеруі қажет. Осыдан кейін өз көру органдарының көмегімен төлқұжаттағы фотосуретті тексерілуші бет-бейнесімен салыстыруы қажет. Бұл процедура едәуір күрделі болып табылады. Мұндағы мәселе – адам бет-бейнесінің жасына байланысты өзгеруінде, сонымен қатар, фотосурет жазық, ал бет-бейне көлемді. Осындай салдардан тексеруші қателіктерге бой алдыруы мүмкін. Мұның себебі төлқұжатта адам туралы биометриялық мәліметтердің шектеулі болуында. Пайда болған анықталмағандықты бірнеше әдіспен шешуге болады. Біріншіден, тексеруші тексерілушіден оның қол қоюын өтініп, оны төлқұжатта қойылған қолтаңбамен салыстыруына болады. Екіншіден, тексеруші тексерілушіні жақыннан танитын бірнеше адамның пікіріне сүйенуіне болады.

Жалпы алғанда тұлғаның органлептикалық (көру органдарының көмегімен) төлқұжаттық тексеруі едәуір күрделі, әрі айтарлықтай қателіктер ықтималдығымен түйіндес процесс болып табылады. Сонымен қатар, 100-ден артық әртүрлі мемлекеттерде төлқұжат санының көп болуы оның шынайылығын тексеруді екінші маңызды мәселе етеді. Мұның барлығы 21 ғасырдың басында халықаралық төлқұжаттарға деген сенімнің төмендеуіне әкелді. 2001-жылдың 11 қыркүйегіндегі Нью-Йорктегі оқиға АҚШ-тың қағаз тасымалдаушысындағы халықаралық төлқұжатқа деген шүбәсін ушықтыра түсті. 20 ғасырдың аяғында АҚШ күдіксіз

ақпараттық көшбасшы ретінде өзіне органлептикалық биометрияны қайталайтын тұлғаның автоматтандырылған бақылауына бағытталған 50 ұлттық биометриялық стандарт жиынын құрды.

11 қыркүйектегі оқиғадан кейін АҚШ тексерілетін адамның биометриялық мәліметтері орналастырылған радио оқымалы микросұлбасы бар жаңа ұрпақтық биометриялық төлқұжатты құру бастамасымен шығуда. Сонымен бірге, төлқұжат микросұлбасындағы биометриялық мәліметтердің ақиқаттығы олардың нөмірінің төлқұжаттағы нөмірмен және мәліметтердегі электронды сандық қолтаңбамен сәйкес келуімен кепілденеді деп болжанады. Қазіргі кезде электронды сандық қолтаңбаны қолдан жасау қорғаныс элементтері бар жасанды төлқұжат баспабеттеріне қарағанда әлде қайда қиын деп есептеледі. Жасанды төлқұжат баспабетін шығаруды ретке келтірген қаскүнем өз шабуылының таралымын көбейтуді көздеуі мүмкін. Полиграфиялық қорғанысты толықтыратын, криптографиялық қорғанысты енгізу жасанды төлқұжаттарды көбейтуден қаскүнемнің бастартуына әкеліп соқтырады. Микросұлбаның электронды мазмұнындағы электронды сандық қолтаңбаны әрбір уақытта қайта бұзуға тура келеді. Бұл тұрғыдан, төлқұжат микросұлбасындағы биометриялық мәліметтер және басқа да жеке мәліметтер бүтіндігінің криптографиялық қорғанысы жаңа кезең халықаралық биометриялық төлқұжаттарына деген сенімді айтарлықтай жоғарылатады.

Биометриялық технологияларды криптографиялық қолдау биометриялық төлқұжаттық мәліметтерге немесе басқа да биометриялық мәліметтерге деген сенімді қамтамасыз ететін маңызды тұсы болып табылады. Биометриялық технологияларды криптографиялық қолдаудың жүзеге асуының формасы әртүрлі болуы мүмкін, бірақ криптографиялық қолдаусыз заманауи биометрия мүмкін болмайды. Мұның барлығы Ғаламторда және басқа да ашық ақпараттық кеңістікте биометрияны қолданғанда анық көрінеді. Ашық ақпараттық кеңістікте криптография бірден-бір тиімді қорғаныс тәсілі болып табылады. Яғни биометрияның криптографиямен тиімді

байланысын жүзеге асыру қажет. Мәселен, бұл ашық биометриялық бейнені ашық криптографиялық кілтпен және адамның жасырын биометриялық бейнесін оның жасырын (жеке) кілтімен байланыстыру жолымен жасалуы мүмкін. 1.1-суретінде адамның бет-әлпет геометриясымен ассиметриялық криптография ашық кілтімен байланыстырудың нейрожелілік нұсқасы және адамның қолжазба құпиясөзін оның жеке криптографиялық кілтімен байланыстырудың нейрожелілік нұсқасы көрсетілген.



1.1-сурет. Қолданушының жеке басын биометриялық авторландыруды жүзеге асыратын автоматтарға арналған ашық және жабық электронды куәлік құрылымы

Егер биометрияны кілтпен байланыстырудың осы және басқа да нұсқасын электронды қолтаңбамен қамтыса, онда біз ғаламтор желісі мен басқа да ашық ақпараттық кеңістікте қолдануға болатын ашық және жабық электронды куәліктің екі нұсқасын аламыз. Ғаламтор ортасы үшін қауіпсіз биометриялық паспорттарды және басқа да куәліктерді жасау тапсырмасы өзекті мәселе.

Бүгінгі күнгі барлық биометрияны шартты түрде екі тармаққа бөліп қарастыруға болады. Бірінші тармақ – бұл адамның ашық биометриялық бейнесін қолдану тармағы. Әдетте бұл – төлқұжаттық-визалық құжаттар мен қылмыскерлер туралы биометриялық деректер қорының полициялық биометриясы.

Барлығына ашық адамның биометриялық бейнесін қолдана отырып, сол адамның анонимдігін қамтамасыз ету мүмкін емес.

Биометрияның екінші тармағы биометриялық бейненің жасырындығы негізінде жасалады. Мұнда биометрияның жасырындығын қалай қамтамасыз ету маңызды емес. Маңыздысы адамның жасырын бейнелерінің биометриясы әдеттегі ашық бейнелер биометриясынан анағұрлым күштірек болып табылады. Мұның себебі, қаскүнем жасырын бейне биометриясына қалай шабуыл жасау керектігін білмейді. Ол әртүрлі адамдарға тиісті кездейсоқ биометриялық бейнелерден тұратын көлемді қор құруға мәжбүр болады және оларды әрі қарай адамның жеке кілтін сақтайтын биометриялық программалық роботқа ұсынуы қажет. Ашық биометриялық бейнелер – бұл жай биометрия, жасырын биометриялық бейнелер – бұл белгісіз тұлға қолжазбалық құпиясөзі, дыбыстық құпиясөзі, саусақ таңбасы «жасырынына» көбейтілген биометрия.

Ұсынылып отырған оқу құралы адам жеке ақпаратын оның жеке криптографиялық кілтін және жасырын биометриялық бейнесін қолдану арқылы қалай биометриялық-криптографиялық қорғауды дұрыс құруға және қолдануға болатындығына бағытталған.

1.1. Негізгі түсініктер және анықтамалар

1.1.1. Бірінші және екінші текті қателіктер ықтималдығы

Кез келген биометриялық қорғау «Өзім» бейнесін жақсы тануы және сенімді түрде «Бөгде» («барлығы Бөгде») бейнелер жиынын ерекшелеуі негізінде құрылады. Биометриялық қорғау құралдарының (биометриялық аутентификация) қателесуі мүмкін екені анық. Биометрия үшін негізгі мәселе (№1 тапсырма) болып «Өзім» биометриялық бейнесі донорының кіруге рұқсат беруін қамтамасыз етуі болып табылады. Бұл тапсырманы орындаудағы қателік бірінші текті қателік ретінде қарастырылады. Биометриялық аутентификация құралдары

жұмысы тиімділігінің негізгі сипаттамасы болып бірінші текті қателіктің пайда болу ықтималдығы – P_1 болып табылады.

Биометриялық аутентификация құралдарының екінші тапсырмасы болып, «Бөгде» бейнесі донорының кіруіне тосқауыл қою болып табылады. Биометриялық құралдардың екінші маңызды сипаттамасы қарастырылып отырған белгілердің (биометриялық параметрлердің) мүмкін болатын «Өзім» және «Бөгде» бейнелерінің коллизиясынан пайда болатын P_2 – екінші текті қателіктің пайда болу ықтималдығы болып табылады.

P_2 – екінші текті қателік ықтималдығы қаншалықты аз болса, қандай болса да биометриялық аутентификация құралдар соншалықты көп биометриялық параметрлерді қабылдайды. Тек қана жүздеген немесе мыңдаған биометриялық параметрлерді талдайтын биометриялық құралдарды жоғары сенімділікті деп атауға болады. Сонымен қатар, шабуылдаушы теріп жатқан биометриялық бейнесін білмеген жағдайда ғана биометрия жоғары сенімділікті.

Бүгінгі күні ең үздік жоғары сенімділікті биометриялық аутентификация құралдары бір миллиардтық және одан төмен деңгейдегі екінші текті қателік ықтималдығын қамтамасыз етеді. Яғни, биометриялық қорғауды бұзушы қаскүнем миллиардтаған әртүрлі биометриялық бейнелерді (мәселен, миллиардтаған қолжазбалық құпиясөзін өз қолымен жазуы қажет) ұсынуы қажет. Егер бір қолжазбалық құпиясөзді жазуға 10 секунд кететін болса, онда қаскүнемге 10 миллиард секунд қажет, бұл шамамен 321 жыл үздіксіз еңбек. Бұл бір адамның өмірінен анағұрлым көп.

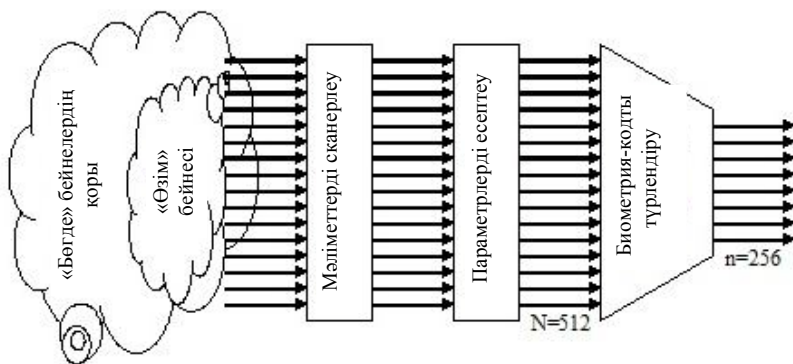
1.1.2. Жүйеге кіру кілтінің кодына биометриялық бейнелерді түрлендіру

Биометриялық қорғауды қолдану үшін «өзім» бейнесі биометриялық мәліметтерінің көп өлшемді континуумын кіру криптографиялық кілтінің кодына түрлендіруді білу қажет. Ол үшін ұсынылған биометриялық бейнені сканерлеп, бақыланатын биометриялық параметрлерді есептеу қажет. Әрі қарай, 1.2-

суретінде көрсетілгендей биометриялық параметрлерді биометрия-код түрлендіргіші кірісіне ұсыну керек.

Биометрияны кодқа түрлендіргіштің өзі әртүрлі технологиялармен орындалуы мүмкін. Мәселен, «айқын емес экстракторлар» және [1-3] қолданылуы мүмкін. «Айқын емес экстракторлар»-ды құру жолымен негізінен ағылшын зерттеушілер келуде. Орыс тіліндегі әдебиеттерде «айқын емес экстракторлар» бойынша жарияланымдар аз [4, 5].

Ресей және Қазақстанда биометрия-код түрлендіргіштері жасанды нейрондық желілерді қолдану арқылы құрылады [6,7]. Алдын ала жасанды нейрондық желілер байланыстарының құрылымын таңдау қажет, ал осыдан соң оны «өзім» биометриялық бейнесінің үлгісі түрлендіргіш шығысында Ресей немесе Қазақстан азаматының жеке криптографиялық кілтінің кодын беретіндей, ал «бөгде» бейнелерінің үлгісі үшін түрлендіргіш шығысында кездейсоқ кодтық комбинация пайда болатындай етіп үйретуі қажет [8-12].



1.2-сурет. Кілт кодына биометриялық параметрлерді түрлендіру

Қандай технология қолданылатынына қарамастан биометрия-код түрлендіргіш әрқашанда биометриялық мәліметтер шығысына қарағанда (криптографиялық кілт шығысы ұзындығына қарағанда) кірісі көбірек болады. Осылайша, 1.2-суретте түрлендіргіш $N=512$ биометриялық параметр кірісіне және тек

кана $n=256^1$ криптографиялық кілттің шығыс разрядына ие. $N > n$ шарты әрқашан биометриялық мәліметтердің төмен ақпараттылығынан орындалады. Бір биометриялық параметр криптографиялық кілттің бір битін алуға жеткіліксіз. Міндетті түрде, биометриялық параметрлердің артық санын «айқын емес экстракторлар»-дағы кодтау қателіктерін түзету немесе түрлендіргіште кіріс биометриялық мәліметтерді нейрондық желілер көмегімен «жетілдіру» қажет.

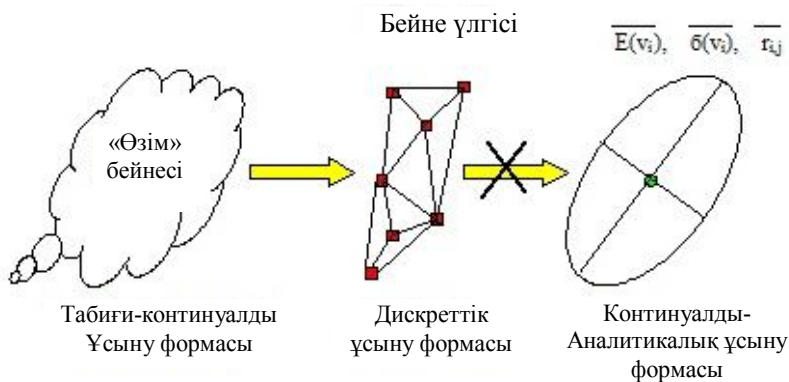
1.1.3. Биометриялық бейнелер көп өлшемді континуумын аз дискреттік үлгілер санымен ұсыну

Биометриялық аутентификация қиындығының негізгі себебінің бірі тапсырма өлшемінің жоғарылығы болып табылады (512 және одан да жоғары «жаман» биометриялық параметрлерді есепке алуға тура келеді). Осы себепті, классикалық сызықты алгебра және көп өлшемді статистика аппаратын қолдану мүмкін емес болып табылады. Биометрия-код түрлендіргішін үйретуші іріктемесіндегі аз санды үлгілер негізінде үйрету (баптаумен) жағдайы қиындай түседі.

Биометриялық аутентификация құралдарын үйретуде қолданушы 10-нан 20 дейін «өзім» биометриялық бейне үлгілерін ұсынуы қажет. Бірақ олардан 100 немесе 200 үлгі ұсынуды өтінсек, бұл жұмыс қолданушы тарапынан жағымсыз қабылданады. Бүгінгі күні қолданушылар өз биометриялық программалық роботын (биометрия-код түрлендіргішін) үйретуге айтарлықтай күш салуға дайын емес. Соңғысы, 512 өлшемді «өзім» бейнесі параметрлері континуумы үлестірілуі үшін біз параметрлердің әрқайсысынан бар жоғы 20 үлгі ұсынуға тиістіміз дегенді білдіреді. Біз 20 үлгілі «Өзім» графасының ішкі көлемі арқылы «Өзім» бейнесінің мәліметтері ұсынған 512 өлшемді көлемдегі табиғи-континуалды формасын көз алдымызға елестетуге талпына аламыз, бірақ бұл өте әлсіз жақындау болады. Бұл оқиға 1.3-суретінде бейнеленген.

¹ Ресей стандарты бойыншы электронды сандық қолтаңбаны шифрлау және қалыптастыру үшін криптографиялық кілт ұзындығы 256 битті құрайды.

Бар болғаны 20 үлгіні қолданып, $E(v_i)$ – биометриялық параметрлердің математикалық болжамын, $\sigma(v_i)$ – олардың орташа квадраттық ауытқуын және r_{ij} – параметрлер арасындағы корреляция коэффициенттерін есептеу мүмкін емес. 20 үлгіден тұратын үйретуші іріктеуде, математикалық болжамды бағалау салыстырмалы қателігі 0-ден $\pm 25\%$ дейін, орташа квадраттық ауытқу салыстырмалы қателігі 0-ден $\pm 50\%$ дейін, корреляция коэффициенттерін бағалаудағы салыстырмалы қателік 0-ден $\pm 100\%$ дейін болуы мүмкін. Осындай нақты емес мәліметтерден «өзім» бейнесінің мәліметтерін үлестіру көп өлшемді аналитикалық моделін құру мүмкін емес.



1.3-сурет. Аз санды үлгімен «өзім» көп өлшемді бейнесін ұсыну (7 үлгімен)

Егер биометриялық параметрлердің мәнін қалыптандырылған қалыпты үлестіру гипотезасы аумағында жұмыс жасауға тура келсе, олар үшін 512 өлшемді корреляциялық матрица құру қажет. «Бөгде» бейнелерінен «Өзім» бейнесін бөліп тұрған гиперэллипстің жоғарғы жағын есептеу үшін 512 өлшемді матрицасын² өзгертуге тура келеді. Себебі гиперэллипстер

² Гиперэллипстердің жоғарғы жағы жоғарғы өлшемнің кері ковариациялық (корреляциялық) матрицасы кіретін сызықты алгебраның квадраттық пішіндерімен сипатталады.

формасында жоғарыны бөліп тұрушы талдамалы сипаттама құру техникалық тұрғыдан мүмкін емес, 1.3-суреттің бірінші көрсеткішінің асты сызылған.

Жоғарыда сипатталған жағдай «өлшем қарғысы» деген атауға ие болды. Қосымша биометриялық параметрлерді есепке алу анағұрлым анық нәтижелерге алып келуі қажет еді, бірақ барлығы керісінше жүреді. Шешіліп отырған тапсырманың өлшемін үлкейтуге әрекет еткен сайын ол нашарлай береді. Нашар шарттылық немесе есептеу қателіктерінің шоғырлану әсері пайда болады. Дәл осы биометриядағы өлшем «қарғыс»-ының себебінен сызықтық алгебра және классикалық көп өлшемді статистикамен қолдану мүмкін емес. Бірақ жасанды нейрондық желілер және «айқын емес экстракторлар» осы «қарғыс» мәселесін әлсіретуге немесе толығымен шешуге көмектеседі.

Кейінірек көрсетілетіндей, егер автоматты түрде үйрету алгоритмін қолдансақ, 512 кірісі және 256 шығысы бар үлкен жасанды нейрондық желілерді автоматты түрде сапалы үйрету үшін «өзім» бейнесінің 20 үлгісі жеткілікті [8]. Қазіргі сәтте тек Ресей стандартының алгоритмі [8] ғана биометриялық деректердің дискреттелу шуларына шамасы келуде, бұл «өзім» бейнесінің табиғи көп өлшемді-континуалды түрде ұсынылуының орнын, бар болғаны 20 үлгіден тұратын жақындату басатындығымен негізделеді. Қашанда үздіксіз функция (континуум) аз санды күймен (үлгімен) ұсынылғанда өте үлкен дискреттелу қателіктері пайда болады. Олар есептеулер кезінде (нейрондық желілерді үйретуде) жинақталу мүмкіндігіне ие. Үйрету алгоритмі [8] бірінші болып табылады, бірақ бірден-бір абсолютті тұрақты көп өлшемді деректерді орташалау (көп өлшемді кеңістіктегі олардың интегралдануы³) арқылы құрылған алгоритм емес. Шешілетін тапсырманың өлшемі қаншалықты үлкен болса, соншалықты оның жұмысы

³ Біз уақыт өлшемінің 512 санау интеграциясына үйренгенбіз, сонымен бірге интеграция операциясы есептеудің дәлдігін жоғарылатады. Уақыт бойынша интеграциялаудың орнына көп өлшемді жүйе үшін әртүрлі кеңістіктегі 512 бойынша мәліметтерді орташаландыруға болады, бұл табиғи қателерді тиімдірек басып, оларды тұрақтырақ жасайды.

жақсы болады. Өлшем «қарғысы» әсеріне кері әсер туындайды. Бұл кері әсерді жоғары және аса жоғары өлшемділіктің «сәті түсуі» деп атауға болады.

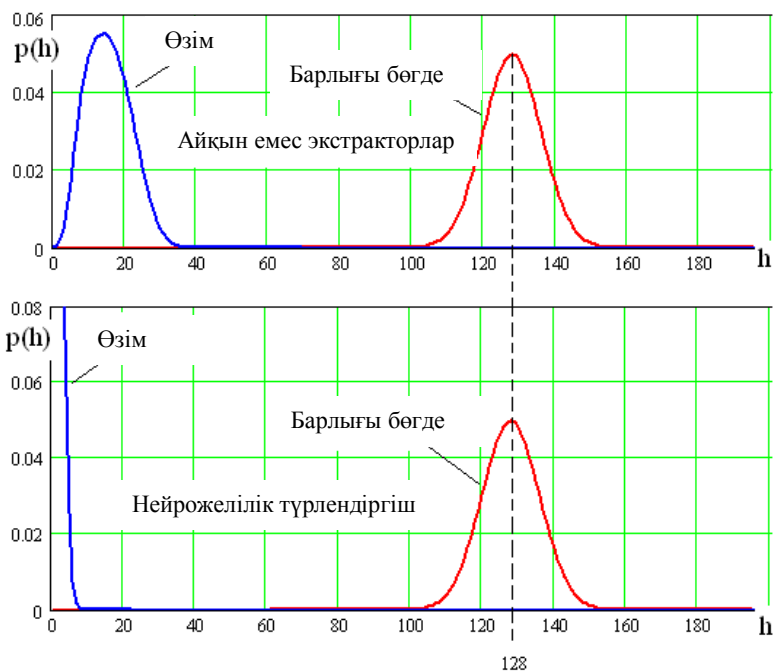
1.1.4. Хэмминг арақашықтығы кеңістігіне өту

Кіріс биометриялық деректер, әдетте континуалды (үздіксіз), ал түрлендіргіштің шығыс коды дискретті. Кодтың мүмкін күйінің саны әрқашанда шекті. Кез келген биометрия код түрлендіргіші бұл көп өлшемді континуумның берілген ұзындықтағы код күйінің ақырғы санына мүмкін болған көрінісінің бірі. Сәйкесінше, оның шығыс кодтарын зерттеу үшін Хэмминг арақашықтығын қолдануға болады. Ұзындықтары бірдей екі код үшін Хэмминг арақашықтығын есептеу үшін оларды разрядтары бойынша салыстырады, осыдан кейін сәйкес келмейтін разрядтарының санын санайды. Егер алынған шығыс кодты «0» және «1» разрядтар жағдайлар жиынынан тұратын $\bar{X}$ векторы түрінде берсек, онда «өзім» кодына дейінгі Хэмминг арақашықтығы – $\bar{c}$ келесі өрнекпен есептеледі:

$$h = \sum_{i=1}^{256} x_i \oplus c_i \quad (1.1)$$

мұндағы 256 – салыстырылатын кодтың ұзындығы, i -салыстырылатын разряд нөмірі, $\oplus$ - екі модулі бойынша қосу амалы.

«Бөгде» және «өзім» шығыс кодтарының арасындағы Хэмминг арақашықтығы битпен өлшенеді және статистикалық зерттеулер үшін өте ыңғайлы метрика болып шықты [11 – 17]. Бұл метриканы «айқын емес экстракторлар» мен биометрия-код нейрожелілік түрлендіргіштеріне қолдану «өзім» және «барлығы бөгде» бейнелері үшін айтарлықтай өзгеше үлестіруді береді. «Айқын емес экстракторлар» бейненің биометриялық параметрлерін сапаландыруға дейін кванттайды. Осы себепті «өзім» бейнесінің коды тұрақсыз және Хэмминг арақашықтығының мәндері айтарлықтай кең үлестірілуге ие (1.4-суреттің жоғарғы бөлігі).



1.4-сурет. 256 бит ұзындықтағы кодтар үшін «айқын емес экстракторлар» және нейрожелілік түрлендіргішке арналған Хэмминг арақашықтығының үлестірілуі

Нейрожелілік түрлендіргіштердің «өзім» бейнесінің биометриялық деректерінің сапасын жақсарту алуына байланысты «өзім» кодтары үшін Хэмминг арақашықтығы сығылады (1.4-суреттің астыңғы бөлігінде координаттар жүйесінің «нөлдік» осіне жақын орналасады).

1.4-суреттің жоғарғы бөлігінде бейнеленгендей, «айқын емес экстракторлар»-дың шығыс кодын басқара отырып, Хэмминг арақашықтығынан бастап нақты «өзім» кодына дейінгі 40 биттен кем кодтар жиынын «өзім» коды сияқты қабылдауы қажет. Нейрожелілік биометрия-код түрлендіргішінің шығысында «өзім» кодтары 7 битке дейінгі анағұрлым аз тұрақсыздыққа ие болады.

«Барлығы бөтен» кодтарының Хэмминг арақашықтығының маңызды ерекшелігі ол мәндерді тарату қалыпты заңымен өте жақсы сипатталатындығы болып табылады. Осы себепті деректерді үлестірудің математикалық болжамы, $p(h(x))$ үлестірілуі және оның орташа квадраттық ауытқуын есептеуге мүмкін болады. Осы екі статистикалық жағдай бойынша айқын емес экстракторлар, сондай-ақ нейрожелілік түрлендіргіштер үшін болжанатын екінші текті қателік ықтималдығын есептеуге болады:

$$P_2 \approx \frac{1}{\sigma(h(x)) \cdot \sqrt{2\pi}} \int_0^{\max(h(c))} \exp\left\{-\frac{(E(h(x)) - u)^2}{2 \cdot \sigma^2(h(x))}\right\} \cdot du \quad (1.2)$$

мұндағы $\max(h(c))$ – «өзім» кодтары Хэмминг арақашықтығының максималды мүмкін мәні;

$E(h(x))$ – «Бөтен» кодтары Хэмминг арақашықтығының математикалық болжамы;

$\sigma(h(x))$ – «бөтен» кодтары арақашықтығының орташа квадраттық ауытқуы.

1.1.5. Биометриялық параметрлердің ақпараттылығы

«Жақсы» және «жаман» биометриялық параметрлер деп айтылып отыратын нақты емес түсініктерден ақпараттылық деп аталатын – биометриялық параметрлердің сапалық көрсеткішін көрсететін түсінікке өтейік. Осы мақсатта оқиғаны қарапайымдату үшін шешімдер қабылдаудың «өзім» - «1» және «бөгде» - «0» қарапайым ережесін қарастырайық. Мұндағы «өзім» квантталу шектерін «өзім» мәндерінің үлестірілуінің $E(v)$ математикалық болжамынан $\pm 3\sigma(v)$ арақашықтығына ауыстырамыз. Бұл жағдайда бірінші текті қателіктің ықтималдығын елемеуге болады, ал екінші текті қателік ықтималдығы әрқашанда айтарлықтай үлкен болады:

$$P_2(v) \approx \frac{1}{\sigma(\xi)\sqrt{2\pi}} \int_{\min(v)}^{\max(v)} \exp\left\{-\frac{(E(\xi) - u)^2}{2\sigma^2(\xi)}\right\} du \quad (1.3)$$

мұндағы $E(\xi)$ - ξ «барлығы бөгде» бейнелерінің биометриялық параметрлерінің математикалық болжамы;

$\sigma(\xi)$ - ξ «барлығы бөгде» бейнелері параметрлерінің орташа квадраттық ауытқуы;

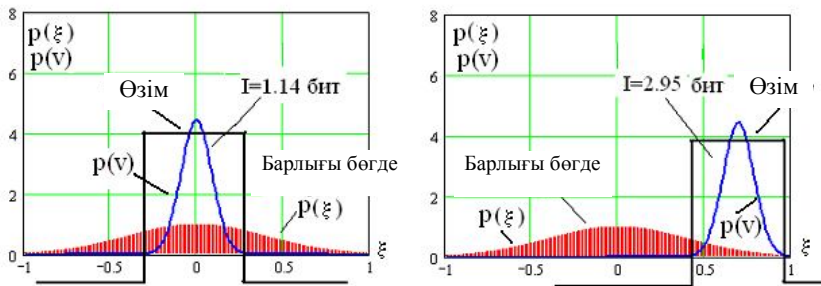
$\min(v)$ - v «өзім» бейнесі параметрінің минималды мәні;

$\max(v)$ - v «өзім» бейнесі параметрінің максималды мәні.

Бірінші текті қателіктің нөлдік ықтималдығында екінші текті қателік ықтималдығы қаншалықты кіші болса, v - биометриялық параметрінің ақпараттылығы соншалықты жоғары болады:

$$I(v) = -\log_2(P_2(v)) \quad (1.4)$$

Көрініп тұрғандай, биометриялық параметрдің ақпараттылығы биометриялық параметр ("Өзім" үлестірілуінің сығылуы) тұрақтылығының өлшеміне байланысты өседі. Сонымен бірге, "Барлығы бөгде" бейнелерінің таралуына қатынасы бойынша "Өзім" бейне мәліметтерінің таралу жағдайы ақпараттылыққа әсер етеді. Бұл жағдай 1.5-суретінде өз көрінісін табады.



1.5-сурет. Параметрдің ақпараттылығына - v "Өзім" бейнесінің үлестірілу жағдайының әсері- $p(v)$

1.5-суреттен көрініп тұрғандай, «Өзім» мәліметтерінің сол бір үлестірілуі «Барлығы бөгде» бейне мәліметтерінің үлестіру перефериясына жылжыту параметрдің ақпараттылығының айтарлықтай өсуіне алып келеді. Егер бірінші жақындауда биометриялық параметрдің ақпараттылығы бір биттен көп

болса, онда оны «жақсы» деп есептеуге болады. Осыған сәйкесінше бір биттен төмен ақпараттылығы бар биометриялық параметрді «қанағаттанарлық» деп есептеуге болады.

Биометриялық параметрлерді «жаман» деп есептеу қолданылып жатқан мәліметтерді өңдеу технологиясына байланысты. Айқын емес экстракторлары үшін «жаман» 0.5 биттен төмен ақпараттылыққа ие биометриялық параметрлер болып табылады. Жасанды нейрондық желілер үшін 0.05 биттен төмен ақпараттылыққа ие биометриялық параметрлер, «жаман» болып табылады. Айқын емес экстракторлармен өңделмейтін мәліметтердің төмен ақпараттылығын қолдануға мүмкіндік беретін биометриялық мәліметтерді нейрожелілік өңдеу тиімді.

1.1.6. Биометрия-код түрлендіргішінің энтропиясын бағалау

Кез келген биометриялық код түрлендіргішінің ең маңызды сипаттамасы «Барлығы Бөгде» бейнелерімен биометрия-код түрлендіргішіне әсер ету шарттылығында есептелген оның шығыс жағдайындағы энтропия болып табылады. Бұл көрсеткіштің маңыздылығын мәтінді шифрлау үлгісінде көрсету оңай. Қазақ немесе орыс тіліндегі мәтіндер шифрланып тасталмаса тіл тасымалдаушылар оңай оқиды. Ашық табиғи тілдің код разрядтары айтарлықтай корреляция коэффициенттеріне ие. Код разрядтарының арасындағы жұп корреляция коэффициенттерінің жоғары мәнділігіне ие болуы – бұл барлық биометриялық кодтардың және орысша әрі қазақша сөйлейтін ұжымдық биометрия кодтарының белгісі. Шифрлау жеке биометриялық кодтардың және компьютерде қолдан терілген құпиясөз кодтарының табиғи корреляциялық байланыстарын бұзады. Шифрлағаннан кейін кодтар «ақ шу»-ға айналады, «0» және «1» күйлері олардың разрядтарында тәуелсіз болады, жұп корреляциялар жоқ ($r_{ij}=0.0$ барлық $i \neq j$ үшін).

«Ақ шудың» және бір сипаттамасы мұндай кодтардың әрбір разрядының энтропиясы бір битпен дәл сәйкес келетіндігі болып табылады. Демек, «ақ» шуды көрсететін кездейсоқ кодтың шын мәніндегі ұзындығы оның энтропиясының мәнімен сәйкес келеді. 256 битті кездейсоқ кодтың энтропиясы дәл

256 битке тең келеді. Егер код кездейсоқ деп аталмаса, онда оның энтропиясы төмендейді:

$$H(256) < 256 \text{ при } |r_{i,j}| > 0.0, i \neq j$$

ең болмағанда бір жұбы үшін

(1.5)

Барлық кодтар үшін (корреляцияланған және тәуелсіз разрядтар) энтропия іріктеу шабуылының тұрақтылығының көрсеткішімен немесе екінші текті ықтималдылығымен байланысты. Егер 256 битті ұзындығы бар кілтті симметриялық шифрлау туралы сөз болса, онда мәтінді бірінші талпыныстан кездейсоқ қойылған кілтпен шифрын ашу ықтималдығы:

$$P_2=2^{256} \text{ немесе } H(256)=256=-\log_2(P_2)$$
(1.6)

құрайды. Жалпы түрде мынаны жазып алуға болады:

$$H(n) = -\log_2(P_2)$$
(1.7)

мұндағы n – биометриялық кодтың ұзындығы, P_2 – биометрия-код түрлендіргішінің екінші текті қате ықтималдығы.

Айта кететін жайт, МЕСТ Р 52633.0-2006 [6] «Бөгде» биометриялық кодтарының разрядтарындағы корреляциялық байланыстарға шектеу қояды. Осы корреляциялық байланыстардың модулінің орташа мәні 0.15 аспауы тиіс. Егер $E(|r_{i,j}|) = 0.15$ көрсеткішті жағдай болса, онда екінші текті қате ықтималдығы шамамен $P_2=2^{25.6}$ төмендейді. Шифрлаумен салыстырғанда іріктеу шабуылының тұрақтылығы шамамен 231.4 жоғалады. Жұп корреляция коэффициенттерінің үлкен мәндегі модульдері кезінде іріктеу шабуылына⁴ биометрия-код түрлендіргіш тұрақтылығының күрт төмендеуі болады. Егер біреу биометрия-код түрлендіргіш кодының разрядтары арасында жұп корреляцияларды жойып, 256 разрядты код беретіндей жасаса, онда мұндай түрлендіргіш шифрлау

⁴ Биометрия-код түрлендіргішінің тұрақтылығы оның екінші текті қате ықтималдығына кері пропорциялы.

қорғаныс тұрақтылығы мен оның кілт ұзындығына да сәйкес келетін іріктеу шабуылының тұрақтылығына ие.

Маңызды жайттардың бірі – биометриялық кодтардың шығыс кодтарын қалай есептеу керектігінде болып табылады. Шеннонның формуласы қолданып көруге болмайды:

$$H(256) = - \sum_{i=1}^{2^{256}} P_i \cdot \log_2(P_i) \quad (1.8)$$

мұндағы P_i – биокодтың i -ші жағдайының пайда болу ықтималдығы.

256 шығысы бар (жағдай саны 2^{256}) биометрия-код түрлендіргіші үшін (1.8) формуласы бойынша энтропияға баға беруді орындау техникалық тұрғыдан мүмкін емес. Биометриялық-кодтың мүмкін болған шығыс жағдайының алфавиті тым үлкен. Осы мәселеге байланысты Хэмминг арақашықтығының кеңістігінде (1.2) формуласы бойынша екінші текті қате ықтималдығын алдын ала бағалап, энтропияны тек (1.7) формуланы пайдалана отырып қана есептеуге болады.

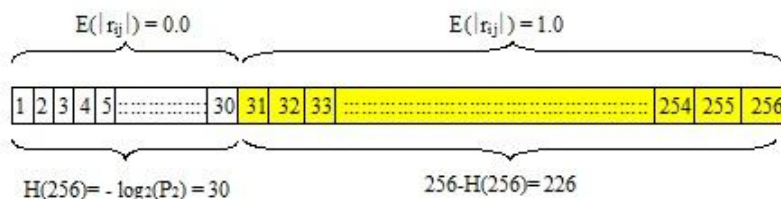
1.1.7. Шешіліп жатқан биометриялық тапсырманың өлшемін бағалау

Интеллекттің (жасанды және табиғи) мүмкіндігі оның қандай өлшемдегі тапсырманы шеше алуымен анықталады. Қарапайым математика көзқарасы бойынша кез келген тапсырманы қандайда бір көп өлшемді $F(x_1, x_2, x_3, \dots, x_n)$ функция түрінде жазуға болады, мұндағы n -өзгеруді есепке алатын сан. Көрініп тұрғандай, тапсырманың көлемі мен оның күрделілігін өзгеруші сан бойынша талдап бағалауға болады. Бұл өте тұрақталған, әрі тиімді әдіс.

Егер өзгеруші өте тәуелді болса, онда олар жоғары өлшемділік көрінісін ғана береді. Биометрия-код түрлендіргішінің шығыс жағдайының саны мен өзгерушінің кіріс санын талдап өлшеуде шешіліп жатқан тапсырма туралы талдауда ештеңе айтпайды. Биометрия-код түрлендіргішінің шешіліп жатқан

тапсырмасының шын мәніндегі өлшемі түрлендіргіштің (1.8) кодтық жағдайының шығыс энтропия мәнімен байланысты, сонымен бірге ол битпен өлшенеді.

(1.8) бойынша шығыс кодының энтропиясын есептей отырып, сонымен бірге қысқа кодты битке айналдырып және кодтың ұзындығы арасындағы ерекшелікті талдап, абсолютті корреляцияланған жағдаймен қандайда бір пайдасы жоқ үстеме сияқты қарастыра отырып, біз шығыс кодының ұзындығын тапсырманың толық өлшемдігіне дейін қысқартамыз деген сөз [10, 16-18]. Бұл жағдай 1.6-суретінде берілген.



1.6-сурет. Әлсіз корреляцияланған разрядты, 256 битті ұзындықтағы биокодтың 30 тұрақты корреляцияланбаған разрядтар мен 226 толық корреляцияланған пайдасыз разрядтар түрде ұсынылуы

Бағалаудың мұндай әдісі барысында шешіліп жатқан биометриялық тапсырма көлемінің разрядтары әлсіз корреляцияланған болса, шығыс код ұзындығының біршама кіші кезінде де өте жоғары болуы мүмкін. Код разрядтары арасындағы корреляциялық байланыстардың өсуі кезінде биометриялық қорғаныстың шешілген тапсырмасының өлшемі төмендейді. Код разрядтары кез келген ұзындықта толық корреляцияланған болса, онда оның энтропиясы 1 бит, көлемі де 1 битті құрайды.

Нейрондардың байланыс саны, нейрон қабаттарының саны, биометрия-код түрлендіргішінің кіріс саны, үйрету алгоритмі шешіліп жатқан тапсырманың көлеміне өз әсерін тигізеді.

Жоғарыда айтылған параметрлердің кез келгенінің қарапайым өсуі түрлендіргіштің шығыс кодтары энтропиясының сәйкесінше өсуісіз ақпаратты биометриялық қорғаудың шешілген тапсырмасы өлшемінің өсуіне алып келмейді [10, 16-18].

2. ЗАМАНАУИ БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАР ТАЛДАУЫ

2.1. Саусақ таңбасы суретін талдау технологиясы

Қазіргі кездегі ең көп тараған биометриялық технологиялардың бірі – саусақ терісі папиллярлық суретін (саусақ таңбаларының суреттері) талдау технологиясы болып табылады [19-22].

Сериялы шығарылатын және анағұрлым сұраныспен қолданылатын саусақ таңбалары суреттерінің оптикалық сканері және сыйымдылық сканерлері болып табылады. Кеңселік мекемелерде жұмыс жасау үшін әдетте оптикалық сканерлерді, мекемелерден тыс орындарда (банкоматтарда) сыйымдылықтық сканерлер қолданылады (2.1-сурет). Сыйымдылықтық сканерлерді, мәселен, банкоматтарда қолдану – бұл сканерлердің техникалық шарттары кең температуралық ауқымда жұмыс жасауына мүмкіндік беруімен негізделеді.



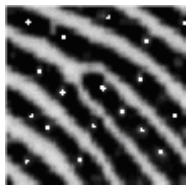
Оптикалық сканер



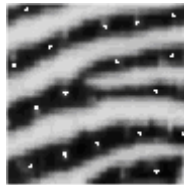
Сыйымдылықтық сканер

2.1-сурет. Саусақ таңбалары суретінің оптикалық және сыйымдылықтық сканерлері

Саусақ таңбасы папиллярлық суретін талдауда екі типтегі белгіні бөліп көрсетеді: ғалами белгілер, жергілікті белгілер. Ғалами белгілер (папиллярлық сурет орталығы, дельта) бірден-бір болып табылмайды, бірақ папиллярлық өрнек типін жіктеуге мүмкіндік береді. Жергілікті белгілер төбешік сызығының аяқталу нүктесі және төбешік сызығының тармақталу нүктесінен тұрады. Өзара орналасқан мұндай нүктелер адамды идентификациялауға болатын бірден-бір қайталанбайтын ақпарат болып табылады (2.2-сурет).



а) тармақталу

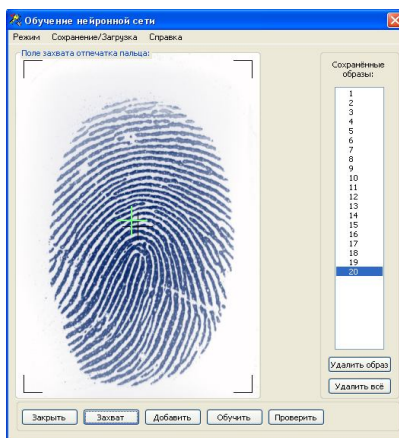


б) аяқталу

2.2-сурет. Саусақ таңбасы папиллярлық суретіндегі жергілікті белгілер ерекше нүктелерінің екі типі (тер бездері терінің кара төбешіктерінде ақ нүктелермен көрсетілген)

Әдетте тұлғаның биометрия-нейрожелілік аутентификация құралы екі жұмыс режиміне ие (2.3-сурет):

- саусақ таңбалары суретінің бірнеше үлгілерін ұсынуды талап ететін – үйрету режимі;
- верификацияланатын суретті ұсынуды талап ететін – аутентификация режимі.



а) нейрондық желіні үйрету



ә) нейрожелілік аутентификация

2.3-сурет. Іске асырылған №1 макетті программа жұмысының режимі

Егер саусақ таңбасының суретін биометриялық бақылау құралы BioAPI [23] халықаралық стандартының негізінде

жасалса және МЕСТ Р ИСО/МЭК 19784-1 – 2007 [24], сондай-ақ, МЕСТ Р ИСО/МЭК 19784-2 – 2010 [25] стандарттарына сәйкес болса, онда биометриялық дайын қалып (шаблон) ретінде МЕСТ Р ИСО/МЭК 19794-2 [26] бойынша қалыптастырылған сәйкес координаттарымен берілген ерекше нүктелер тізімі қолданылуы қажет. Саусақ таңбасы суретінің ерекше нүктелерінің тізімі түріндегі адамның жеке биометриялық мәліметтері № 152 «Жеке мәліметтер туралы» РФ ФЗ №1 класы бойынша сенімді қорғалуы қажет [27].

Егер осы жеке биометриялық мәліметтер тұлғасыздандырылған қорғалған нейрожелілік контейнерге (жүзеге асырылған №1 макетте орындалғандай) орналастырылса, онда осы жеке биометриялық ақпаратты қорғауға № 152 РФ ФЗ ерекше талаптар қоймайды.

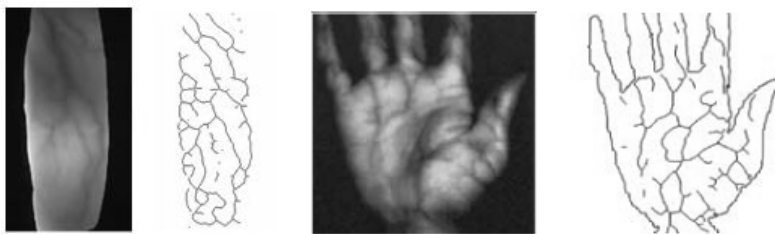
Бұл типтегі биометриялық технологиялардың бір саусақ суретін қолданғандағы екінші текті қателіктің ықтималдығы («Бөгдені» өткізу) 10^{-3} -нен 10^{-6} дейінгі аралықты құрайды. Екінші текті қателік ықтималдығы қолданылған саусақ таңбасы суретінің ақпараттылығынан өте тәуелді. Егер таңба суретіндегі ерекше нүктелер аз болса, онда ол аз ақпараттылыққа ие және оның теру шабуылдарына тұрақтылығы аз. Айта кететін жайт, егер кескінді өндеуде сурет сызықтары ерекшеліктеріне салыстырғанда тері бүкпелерінің төбешіктерінде орналасқан тер бездерінің өзінің біркелкі емес орналасуын ерекшелеп белгілеу арқылы саусақ таңбасы суретінің ақпараттылығы айтарлықтай көбейтілуі мүмкін.

Осы мақсатта, заманауи сканердің рұқсат ету мүмкіндігін айтарлықтай жоғарылату қажет және биометриялық параметрлерді алдын ала өңдейтін программалық қамтамаға түзету енгізу қажет.

2.2. Саусақ және алақан қантамырлары ағашын талдау технологиясы

Саусақ таңбалары суретінің сканерлерін қолдану практикасы шамамен 8% адамдар үшін бұл технология төмен тиімділікке ие екенін көрсетті [19]. Адамдардың бір бөлігінде саусақ терісінің папиллярлық суреті анық емес көрінеді. Әдетте,

бұл әйелдер, балалар және азиат текті адамдар. Осыған байланысты қазіргі кезде жапондық фирмалар саусақ немесе қол қантамырлары суретін талдау технологиясына бағытталған. Жапонияда қол саусағы терісінің астындағы немесе алақанның барлық аумағындағы қантамырлар таралуын талдау негізіндегі банкоматтар желісі бірнеше жылдан бері жұмыс жасауда. «Хитачи» («Hitachi») корпорациясы саусақ терісі астындағы қантамырлары суретінің сканерлерін, Футджицу» («Fujitsu») корпорациясы алақан қантамырларының суретін талдайтын сканерлер мен жүйелерді өндірумен айналысады (2.4-сурет).



2.4-сурет. Алақан және саусақ қантамырлары суретінің мысалдары

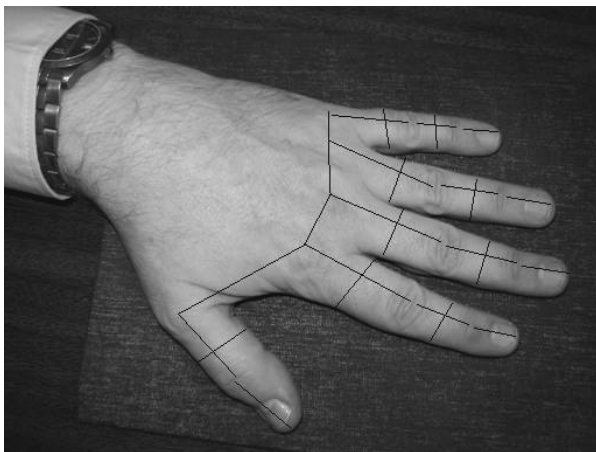
Екі типтегі де биометриялық авторизация құралдарының екінші текті қателігі 10^{-4} -ден 10^{-6} дейінгі аралықты құрайды. Қан тамырларының суретін өзгертуге болмағандықтан төлем жүргізу қызметінің операторы оның биометриялық параметрлерін құпия түрде сақтауы керек. Қорғалған биометриялық хеш-функция немесе биометриялық контейнерлер қолданылуы мүмкін. Сонымен бірге, жеке биометриялық мәліметтер қоры тұлғасыздандырылған болуы тиіс. Егер әдеттегі биометриялық үлгі қолданылып жатса, онда биометриялық үлгілердің қорғанысы 1 РФ ФЗ № 152 класы бойынша орындалуы керек.

Берілген биометриялық технология жеке есеп шотты басқару үшін қолданылатын төлем қызметі операторларының кеңселік терминалдарында және банкоматтарында қолданылуы мүмкін.

2.3. Алақан геометриясын талдау технологиясы

Қол қан тамырларын талдаумен қатар Жапон банкоматтары қолдың білезікке дейінгі бөлігінің өзге барлық геометриялық параметрлерін қосымша талдайды. Әрбір адамның саусағының ұзындығы мен ені, сонымен бірге анық көрінетін қол терісіндегі бүкпелер мен әжімдер де әр түрлі болады. 2.5-суретте қолдың сыртқы көрінісінің фотосуреті көрсетілген.

Бүгінгі күні қолдың білезікке дейінгі бөлігінің геометриялық талдауы негізінде құрылған биометриялық жүйенің екі типі бар. Бірінші типтің жүйесі әдеттегі жарықтықта алынған қолдың алақаны немесе қолдың білезікке дейінгі бөлігінің кескінін талдау негізінде құрылған. Екінші типті жүйесі қолдың білезікке дейінгі бөлігінің сыртқы көрінісі қан тамырлары ағашының тармақталуын бөліп көрсету негізінде құрылған. Қолдың өзіне қарағанда қолдың білезікке дейінгі бөлігіне құятын қан ыстықтау болады, сондықтан қан тамырларының суретін белгілеу үшін спектрдің инфрақызыл бөлігіне сезімтал болып келетін оптикалық элементтерді қолдануға тура келеді.



2.5-сурет. Қолдың білезікке дейінгі бөлігінің сыртқы фотосуреті, бұл бойынша оның салыстырмалы геометриялық параметрлерін бағалауға болады

Тері бүкпелерін ерекшелеу арқылы алынған қол алақан параметрлерінің ақпараттылығы жоғары болып табылады («өмір жолы» деп аталатын). Алақан мен білезікке дейінгі қол бөлігінің тері әжімдерінің сыртқы орналасу геометриясы биометриялық параметрлерінің ақпараттылығы өте жоғары болмақ. Бірақ ол заманауи биометриялық бақылаудың техникалық құралдары жағынан қажетті түрде толық қолданылып жатқан жоқ.

Қол геометриясы мен оларды қайта құру параметрлерінен биометриялық мәліметтерді шығару туралы толығырақ мәліметтерді МЕСТ Р ИСО/МЭК 19794-10-2010 [28] стандартынан білуге болады.

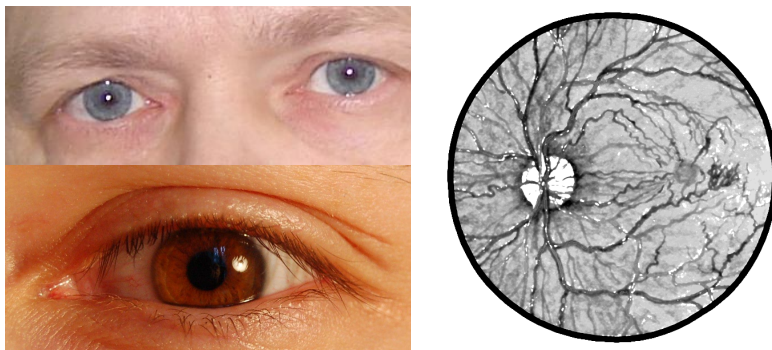
2.4. Көздің шатырша қабығы мен көз түбінің тамырларын талдау технологиясы

Әрбір адамның денесінің геометриялық параметрлері, сондай-ақ оның көздерінің параметрлері бірден-бір болып табылады. Қазіргі уақытта көз параметрлерінің өлшемі негізінде құрылған биометриялық жүйелердің екі типі белгілі. Олардың бірінші типіне көздің шатырша қабығының суретін талдау негізінде құрылған жүйелер жатады. Сонымен бірге, Даугмен [29] бойынша көздің шатырша қабығының суреттері адам генетикасынан тәуелді емес және бірұрықты егіздерде де өзгешеленеді. Екінші типке көзтүбінің (торлы қабығы) қантамырлары суретін талдау негізінде құрылған жүйелер кіреді. Әрине, бірінші және екінші жүйелерде оптикалық сипаттамалары әртүрлі болып келеді. Әртүрлі адам көздерінің торлы қабықшасының суреттеріне және көз түбінің қантамырларының бір суретіне мысал 2.6-суретте көрсетілген.

Қан тамырлары ағашының анализі де қолдың білезікке дейінгі бөлігінің қантамырлары ағашының анализі немесе адам денесінің басқа да бөліктерінің принциптері сияқты жүзеге асырылады. Дайын үлгіні (шаблонды) қалыптастыруда түбірлер, өзектер, бұтақтар болады, одан кейін олар өздерінің орналасуына және диаметрлеріне байланысты жіктеледі. 2.6-суреттің төменгі бөлігінің оң жағында барлық қантамырлар анық көрінетін жалпы түбірі анық көрсетілген. Бұл түбір

биометриялық өлшем жүргізілетін әртүрлі деңгейдегі бұтақтар мен өзектер геометриясының ортасы болып қарастырылуы қажет.

Көздің шатырша қабығы суретін талдауда оны көздің қарашығы айналасында орналасқан параллельді шоғырлас шеңбер бойынша сканерлеуді жүзеге асырады. Сонымен қатар, адам көзінің қарашығы қарастырылып отырған дене жарықтығына бейімделуіне байланысты өз өлшемін ауыстыратыны есепке алынады.

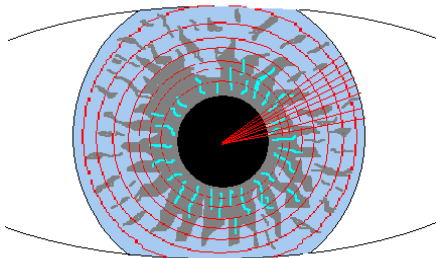


2.6-сурет. Әртүрлі адам көздерінің торлы қабықшасы суреттерінің және көз түбі қантамырлары суретінің мысалы

Осыған байланысты көздің шатырша қабығының биометриялық дайын үлгісін (шаблонын) қалыптастыру және оның суреті бойынша адамды идентификациялау бірдей жарықтықта жүзеге асқаны орынды. Бұл жағдайда қарашық диаметрі мен шатырша қабығының ішкі диаметрінің қатынасы тұрақты болып табылады және қайта есептеуді қажет етпейді.

Шатырша қабықты сканерлеуде алдын ала берілген шоғырлас шеңбер бойындағы кескіннің орташа жарық деңгейінің мәнін бағалайды. Осыдан кейін шоғырлас шеңбер берілген секторлар санына бөлінеді, мәселен, 128 сектор, және осындай әрбір сектор үшін орташа жарықтық есептелінеді. Сектордағы жоғары және төмен жарықтық орташа жарықтыққа қатынасы «1» және «0» сканерлеу кодын береді. Егер сканерлеуде 8 шоғырлас шеңберді қолданса, онда сәйкесінше сканерлеудің ақырғы коды $128 \times 8 = 1024$ бит ұзындықтағы кодқа тең болады. Мұндай кодтың мысалы 2.7-суретінде берілген.

Айта кететін жайт, шатырша қабығы жарықтығы айырмасының қорытынды кодтық қисындастыруы өте қатты корреляцияланған (тәуелді) іргелес есептеуге тең. Дегенмен, айтарлықтай корреляция көптеген биометриялық параметрлерге тән және өлшенетін мәліметтерді айтарлықтай тәуелсіз етуге көмектесетін арнайы декорреляциялық түрлендірулер қажет.



2.7-сурет. Көздің шатырша қабығы жарығының айырмасын сканерлеудегі бірнеше шоғырлас шеңберлердің қолданылуы

Офтальмологиялық биометриялық жүйелер тек қана көздің шатырша қабығының суретін талдау негізінде емес, сондай-ақ көзтүбінің қантамырларының суретін талдау негізінде де қолданылады.

Фотосуреттегі қолданылып жатқан оптиканың өте жақсы көрініске ие көздерде қанмен көз алмасын жабдықтайтын қан тамырлары ерекшеленіп тұрады. Бұл суреттер бірден-бір қайталанбас, сондықтан адам аутентификациясында және идентификациясында қолданылуы мүмкін. Бірақ, бүгінгі күні биометриялық нарықта бұл іспеттес жүйе жоқ.

Көздің шатырша қабығының офтальмологиялық биометриялық мәліметтерін өңдеу үрдісі МЕСТ Р ИСО\МЕК 19794-6 «Автоматтық идентификация. Биометриялық идентификация. Биометриялық мәліметтермен ауысу форматы. Көздің шатырша қабығы көрінісінің деректері» стандартында көрсетілген.

Көздің шатырша қабығы анализінің технологиясы банкомат қолданушыларын авторизациялау үшін, қолдануға ең қолайлысы

болып табылады. Банкоматтар үшін ең дұрысы адамның биометриялық мәліметтерін контактісіз сканерлеу әдісін қолданғаны. Қазіргі кезде көздің шатырша қабығының суретін 30-дан 50 сантиметрге дейінгі аралықта мүмкіндігінше кең көріністе сканерлеу кезіндегі видео бақылаудың техникалық құралдары бар.

Көздің шатырша қабығы анализінің биометриялық құралдарын жасаушы көшбасшылар ағылшындар болып табылмақ. Бұл технология өнертабыспен қорғалған, оның жақын арада уақыты аяқталады. Өнертабыстың биометриялық технологияларды қорғауы Ресейге, Белорусияға және Қазақстанға таралмаған.

Ағылшындардың берген деректеріне жүгінсек, көздің шатырша қабығы суретінің анализі кезінде екінші текті қате ықтималдылығы 10^{-5} –нен 10^{-11} -не дейін құрайды [29]. Бұл сандар сөзсіз жоғарылатып көрсетілген, себебі көздің шатырша қабығы суреттерінен туындайтын код разряды тәуелсіздігінің болжамы көлемінде бағаланған қателер болатын. Тәуелсіздік ерекшелігін қамтамасыздандыру үшін 0.3 астам корреляцияға ие код разрядтары серпілді.

Көздің шатырша қабығы кодтарының корреляциялану коэффициенттерінің қалдық есебі МЕСТ Р 52633.3 – 2011 төртінші бөлімнің әдісі бойынша белгілі бір дәрежеде екінші текті қате ықтималдылық бағасының төмендеуіне алып келуі керек.

Көздің шатырша қабығы статикалық биометриялық бейне болып табылады, оның эталондық параметрлері қорғалған түрде сақталуы керек. Белгілі бір адамның көз шатырша қабығы суретінің [30] параметрлерін әдеттегі хэш-функция коды түрінде немесе биометриялық хэш-функция түрінде есепке алуға бағытталған. Көздің шатырша қабығы суреттерінің эталондық мәліметтер қоры тұлғасыздандырылған болуы тиіс.

2.5. Адам беті геометриясы талдауының екі және үш өлшемді технологиялары

Негізінде адамдар бір-бірін бет әлпет ерекшеліктерінен таниды. Ереже бойынша жеке куәлік, төлқұжат, жүргізуші куәлігі өз иесінің фотосуретіне ие. Адамды бет әлпет

ерекшеліктерінен танып білу процедурасын автоматтандыру мүмкіндігі, биометриялық идентификация құралдарының екі класының пайда болуына алып келді [31-33]. Мұндай құралдардың бірінші класы адам бетінің жазық бейнесінің анализін жасайды (2D портреттері). Бұл құрылғылардың жұмысы 2.8-суретінде көрсетілген.

Жазық бейнесінің екі өлшемді анализаторлары адам «анфас» портретінде ерекше нүктелер мен арақашықтықтарды табады (2.8-суретінде):

- көз ортасының аралығы;
- мұрын ұшы мен көз сызығының аралығы;
- мұрынның ең үлкен еніне сәйкес келетін;
- иектің төменгі жағы мен қас дағаларының аралығы;
- құлақ сырғалығының төменгі аралығы;
- еріннің төменгі нүктесі мен мұрын ұшының аралығы;



2.8-сурет. Адамның жазықтағы фотосуретінде ерекше нүктелердің бөлініп шығуы мен олардың арақашықтығының әрі қарай есептелуі

Адам портретін қырынан қарағандағы екі өлшемді бейнесін анализдеу кезінде жақсы ерекшеленетін ұқсас нүктелер қолданылады, сонымен бірге бет сұлбасындағы жақсы ерекшеленген нүктелер адам құлақ қалқанының жақсы

ерекшеленген нүктелеріне дейінгі арақашықтықпен толықтырылуы мүмкін. Мәліметті өңдеу мен олардың форматтары туралы ақпаратты дәлірек МЕСТ Р ИСО/МЕК 19794-5 «Автоматтық идентификация. Биометриялық идентификация. Биометриялық мәліметтермен ауысу форматы. Бет бейнесінің мәліметтері» білуге болады.

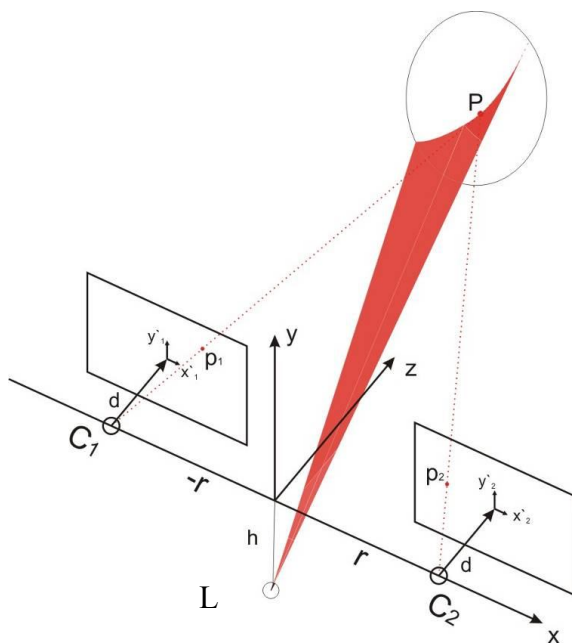
Бет әлпеттің өзара орналасқан екі өлшемді анализаторлары екінші текті қате ықтималдылығын (пропуск «Бөгде») 0.05 деңгейінде қамтамасыздандыра отырып, белгілі бір дәрежеде төмен биометриялық ақпарат алуға мүмкіндік береді. Күрделірек үш өлшемді бет геометриясына талдауға өту, алынатын биометриялық ақпарат көлемінің белгілі бір дәрежеде көтерілуіне мүмкіндік береді. Үш өлшемді көріністі алу үшін екі немесе арнайы көмескі жарығымен бір фотокамера [34, 35] қолданылуы мүмкін. Мысалы, көмескі жарық, жазықтыққа жарық беру кезінде бірқалыпты тор жасаушы, жарық сызықтарын бойлаған және көлденең жайғасқан жүйесі болуы мүмкін. Мұндай көмескі жарықта идентификация жасалып жатқан адам бетінде, жарық түсіп жатқан нүктеден фотокамераға дейінгі арақашықтағы пропорционалды деформацияланған ұяшықтар, торы пайда болады. Тор ұяшықтарының деформация белгілері бойынша көмескі жарықтар адам бет терісінің жоғарғы бөлігінің үш өлшемді биометриялық бейнесін қайта қалпына келтіруі мүмкін.

Ресейде 3D геометриясымен айналысатын «Артек групп» (www.artec3D.com) Мәскеу қаласы) ЖШҚ компаниясы әртүрлі заттардың үш өлшемді модельдерін жылдам жасау үшін онша қымбат емес қол сканерлерін жеткізумен айналысады. Қозғалмайтын затты үш өлшемді сканерлеу, камераның оны жағалай айнала отырып, әрі тоқтаусыз жарқылдауымен түсіру кезінде жүзеге асады, ал кейін үш өлшемді заттың көрші фотосуреті бойынша қайта қалпына келтіретін бағдарламалық қамтама қолданылады. Сонымен бірге, бұл компанияда адамға көрінбейтін инфрақызыл диапазонда лазер нұрынан торланған адам бетіндегі көмескі жарық кезінде қозғалыссыз камераның мәліметі бойынша адам бетін 3D сканерлеу тапсырмасын шешудің нұсқасы бар.

«Наука Техника Безопасность» ЖШҚ компаниясы зерттеліп жатқан беттен 60 см-ден 120 см-ге дейінгі арақашықтықта орналасқан қозғалыссыз камерамен адам бетінің 3D сканерін ұсынады. Көмескі жарықтың инфрақызыл торы қолданылады, A4Vision технологиясы бойынша 3D бейнесін қайта қалыпқа келтіру жүргізіледі, 5 Кбайт шамасындағы өлшемге ие биометриялық үлгіге ие.

«Пенза мемлекеттік университетінің» мәліметтері бойынша адам беті көмескі жарық лазерінің жолағын қолдану арқылы екі камера фокусировкасының міндеті 3D көру жүйесі үшін алынып тасталуы мүмкін. Патентке [36] сипаттамада ұсынылған сканерлеудің өлшеу сұлбасы өз көрінісін 2.9-суретінде тапқан.

2.9-суретінде C_1 , C_2 – HD-камералары, L – көмескі жарық құрылымының көзі (үлгісі), d – камераның фокустық арақашықтығы, r – координатадан бастап камераға дейінгі арақашықтығы, P – жазықтыққа тиісті көмескі жарық құрылымының объектітегі еркін нүктесі белгіленген.



2.9-сурет. Екі бақылау камерасының автоматты түрдегі фокусировкасын қажет етпейтін сканерлеудің өлшеу сұлбасы

Берілген әдістің артықшылығы объектке автоматты фокусталу құрылғысымен, бұйымның бағасын көтеретін әрі белгілі біл дәрежеде конструкциясын қиындататын оптикалық жүйенің жоқтығы болып табылады. Төмен баға мен көмескі жарық құрылымы көзінің кең таралғандығы сканерленіп жатқан модуль конструкциясының қарапайымдылығында.

3D моделін қайта құрудағы мақсат бұл екі фотосурет бойынша объектке тиісті нүкте координаттарын анықтау болып табылады.

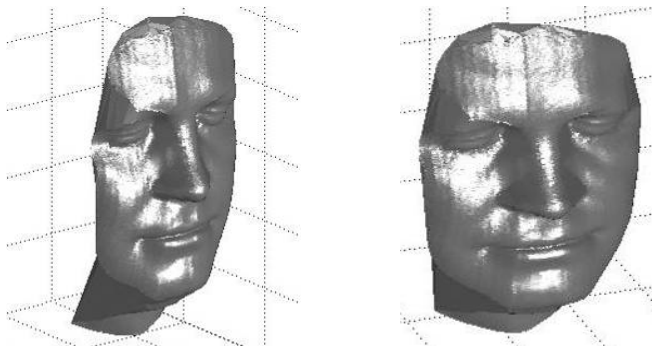
Кеңістіктегі нүкте координаттары мен оның бейнесінің координаттары арасындағы байланысты проектілік бейнелеу операторы көмегімен суреттеуге болады.

$$\begin{bmatrix} x'_1 \\ y'_1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -r \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{d} & 1 \end{bmatrix} \times \begin{bmatrix} x \\ y \\ z \\ 1 \end{bmatrix} \quad (1);$$

$$\begin{bmatrix} x'_2 \\ y'_2 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & r \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{d} & 1 \end{bmatrix} \times \begin{bmatrix} x \\ y \\ z \\ 1 \end{bmatrix} \quad (2);$$

сәйкесінше, мұндағы x, y, z – евклидтік кеңістіктегі нүкте координаттары, d – камералардың фокустық арақашықтығы, r – координаттардан бастап камераларға дейінгі арақашықтық, x'_1, y'_1 и x'_2, y'_2 – C1 мен C2 камераларындағы фотосуреттерде нүктелер бейнесі координаттары.

Жүйенің (2.1) және (2.2) екі матрицалық теңеу шешімі адам бетінде кез келген Р-нүктелерінен, көмескі жарық лазерінің жазықтығында орналасқан, үш координатты табуға мүмкіндік береді. Адамның бетінің сыртқы геометриясының үш өлшемді қайта қалпына келуінің үлгі-нұсқасы 2.10-суретінде көрсетілген.



2.10-сурет. Адамның бетінің сыртқы геометриясының үш өлшемді қайта қалпына келуінің шешімі

Пенза мемлекеттік университеті биометриялық құрылғылар мен технологияларды тестілеудің Салааралық зертханасы мен ҚазҰТУ ақпаратты қорғаудың биометриялық әдістері ғылыми-зерттеу зертханасындағы зерттеулер бойынша [37] беттің жоғарғы жағында кездейсоқ таңдалған үзінділердің 10 мм диаметрлі шеңбер аймақтарының 512 ортасын қайта құру кезінде 10^{-5} мөлшеріне дейін екінші текті қателік ықтималдығын төмендетеді. Бұл көрсеткішті саусақ танбасының суреттерін бақылау кезінде ұқсас көрсеткішпен салыстырамыз.

Беттің 3D геометрия анализі келесі ұрпақ банкоматтарының шынайы болашағы болып табылады. Бет 3D геометриясының биометриялық үлгісі, ISO/IEC JTC1 SC37 биометриялық халықаралық стандарты бойынша, адамның жақсы қабылдайтын ақпараттарын өзінде сақтап тұрғандықтан сенімді түрде қорғалған болуы тиіс. Осы биометриялық мәліметтерді орнықтыру барысында тұлғасыздандырылып қорғалған нейрожелілік контейнерге қосымша қорғаныстың қажеті жоқ.

2.6. Құлақ қалқаны геометриясын талдаудың үш өлшемді технологиясы

Адам идентификациясының ең бірінші биометриялық жүйесін жасай отырып, Альфонс Бартильон адамның құлақ қалқанының пішіні мен типін анықтауға өз назарын көбірек аударған.

Мұндай назар аударудың себебі: адамдардың құлақ қалқанының көлемі мен орналасуының вариациясы басқа дене мүшелерінің вариациясына қарағанда анағұрлым жоғары. Сонымен қатар, әр адамның құлақ қалқанының пішіні әртүрлі.

2.11-суретінде бірдей көлемде, арақатынасының нақты көлемін дәл суреттейтін, кездейсоқ алынған бес ер адамның құлақ қалқаны фотосуреті көрсетілген.

Құлақ қалқанының пішіні мен көлемінің вариациясына (өзгеруіне) қарамастан қазірге құлақ қалқанының геометриясын қолданатын тиімді биометриялық жүйелер жоқ.

Бұл үш өлшемді техникалық көрудің мәселесімен байланысты сияқты.

Екі өлшемді көру құралдары жасанды болып тұрғанда, олар күрделі үш өлшемді құлақ қалқанының пішінін жасай да, есте сақтай да алмайды. Екі өлшемді құлақ қалқанының бейнесінен (образ) белгілі бір көлемде биометриялық ақпарат алу мүмкін емес.



2.11-сурет. Бір көлемде берілген кездейсоқ алынған бес ер адамның құлақ қалқанының әртүрлі пішіндері

Құлақ қалқаны суретінің жиектік сызығын қолданудың талпыныстары жүзеге асырылады, бірақ жиектік сызығының барлық программасы көмескі жарықтың бүйіріне өте сезімтал болып табылады, әрі қозғалыссыз объектілерде ғана жақсы жұмыс істейді.

Шамамен биометриялық жүйенің интеллектуалды мүмкіндіктері бірте-бірте күшейе барады, сәйкесінше, егер құлақ қалқанының күрделі пішінінің 3D геометриясы талдауына өтсек, құлақ қалқанының күрделі геометриясының бақылауы тәжірибелік қолданыс үшін қолайлы болады.

Құлақ қалқанының геометриясын жеке ақпаратты қорғау үшін шынымен тиімді жасау оның, нейрожелілік контейнерлер мен аутентификация рәсімі (процедура) орындалып жатқан кезінде биометрия иесінің анонимдігін толық қамтамасыз етуді орналастыру арқылы, құпиялылығын сақтағанда ғана жүзеге асады.

2.7. Дауыс ерекшелігі талдауының бір және екі өлшемді технологиясы

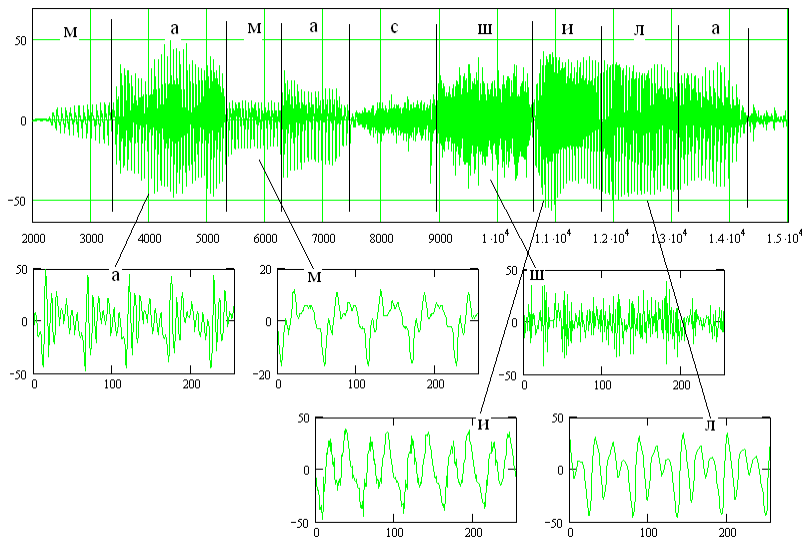
Жалпы адам баласы сөзді естуге әрі сөйлеуге туылғанынан бастап талпынады, бірақ баланың (адамдарға түсінікті) анық сөйлеуі екі немесе үш жылдан кейін басталады.

Адамдарға түсінікті дыбыс сөздерін қолдану үшін біздің әрбіріміздің екі немесе үш жылымыз дауыс желбезегін басқарып үйренуге кетеді деген сөз. Әрбіріміздің дыбыстау аппаратымыз өте күрделі (кез келген жасанды музыкалық аспаптан да күрделірек), оны бір рет игергеннен-ақ біз өмір бойы өзіміздің жеке сөйлеу ерекшеліктерімізді сақтап қаламыз.

Адам сөзі дыбыстардан құралғандықтан оның ресімделуі кезінде әріптермен теңелуі мүмкін, сәйкесінше адамның ауыз екі сөйлеуі баспа немесе қолжазба мәтіні түрінде баяндалады. Осындай теңестірілудің мысалы 2.12-суретінде келтірілген.

Суретте берілген әрбір сөз дыбысы өзіне тән сипаттағы қысымның ауытқу пішініне ие. Сөздің бір бөлік дыбысы айтылған (белгілі бір уақытты қайталанып тұрады), ал екінші бөлігі ызың болып табылады (белгілі бір уақытта қайталанып тұрмайтын).

Кезеңдік дыбыстардың бағытталуы үшін негізгі кезең (үннің негізгі кезеңі) табылған болуы мүмкін. Әдетте, адам үнінің негізгі периоды аз өзгереді. Оның өзгерісі әдетінше $\pm 20\%$ аралығына орналасады. 2.12-суретінде бейнеленген үндескен дыбыстар 8000 Гц дискретизация жиілігімен шығарылған шамамен 70 есепті негізгі үннің кезеңіне ие. Бұл үннің негізгі кезеңіне 115 Гц сәйкес келеді. Әрбір үннің негізгі кезеңінде дыбыстың (үннің негізгі кезеңінің ішінде) ішкі тербеліс байқалады.



2.12-сурет. «Мама шила» деген тіркесін дауыстап айту кезіндегі адамның дыбыс қысымының вариациясы

«А» дыбысының ішкі тербелісі ерекше жоғары жиілікке ие. 2.12-суретте берілгендей негізгі үннің «а» дыбысына бір ауытқуы 8 үдемелі ішкі тербелістен құралған, бұл сөйлеушінің дауысындағы «а» дыбысының ішкі тербелістер жиілігі, негізгі үннің жиілігінен $115 \times 8 = 920$ Гц құрай отырып, 8 есеге үлкен.

Ең аз ішкі тербелістер жиілігі «и» дыбысында (бір негізгі үннің кезеңіне екі үдемесі) байқалады.

Бұл дауыстың ішкі тербелістерінің ең аз дыбыс жиілігі, 2.12-суретіндегі, 230 Гц құрайды. Мұндағы жағдайда, көбіне ақпаратқа қатысты негізгі үннің кезеңдік толықтыру жиілігі 200-ден 1000 Гц дейінгі арақашықтығында өзгереді.

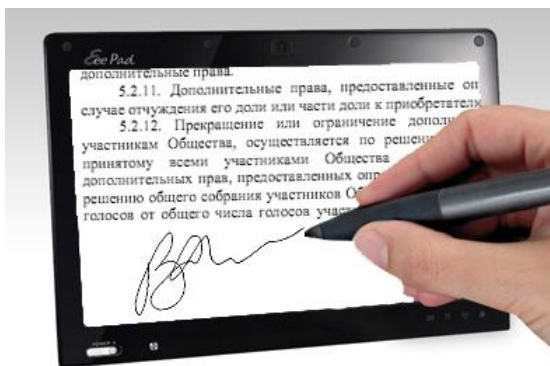
2.8. Қолжазбалық жазу динамикасы талдауының технологиясы

Қазіргі кезде жеке тұлғаның органолептикалық идентификациясы қолжазба автографы бойынша, көбіне төлем жүйелерінде, белсенді қолданылып бастаған.

Егер қайта жаңғырту процесі тексерушінің бақылауында болса, адам автографын қайта жаңғырту динамикасы бойынша жеке тұлғаның авторизация сенімділігін күшейту үшін адамның жеке тұлғасының нейрожелілік автоматты идентификациясы құралдары жеткілікті болады. Мониторда суреттелген құжатта өз ізін қалдыратын тексерушінің арнайы қаламмен құжатқа бірнеше рет қолтаңба тәртібі тиімдірек болып табылады.

Тексеруші адам өз қаламының ізін сезімтал экранда көргенде, қағазды құжатқа қолтаңбаның дәстүрлі құрастыру технологиясының ұқсас жаңа технологиясын жасағандықтан принциптік тұрғыда тәртіп қажет болып табылады.

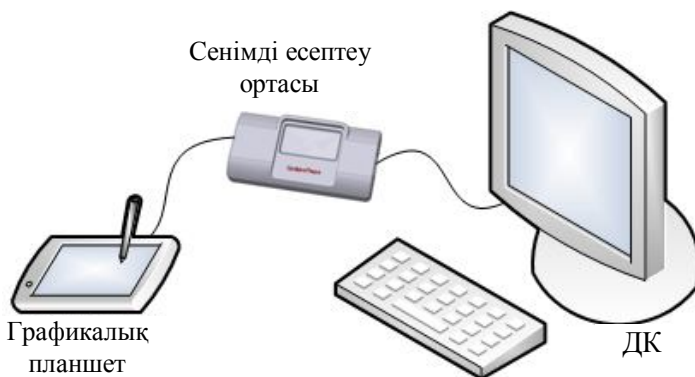
Тек қана осындай жағдайда жаңаны тартып алу психологиялық тосқауылы адам бойынан арылады. Қазіргі кезде электронды құжатқа адамның қолжазбалық қолын жүзеге асыру үшін сенімді есептеу ортасымен және сезімтал экранды планшеттік компьютерлердің пайда болуы техникалық тұрғыдан орындалатын тапсырма болып табылады. Бұл тапсырманы төлем операцияларын биометриялық қолдау типтік құралдарын өңдеу көлемінде шешу қажет. Экранда электронды құжатты жүзеге асыру мен сезімтал экранды сенімді есептеу планшетінің үлгі-нұсқасы 2.13-суретінде берілген.



2.13-сурет. Сезімтал экранда автограф қолтаңбалайтын, құрылып жатқан электронды құжатты жасаушы қызметкердің сенімді есептеу ортасы бар планшеттік компьютері

Егер аутентификация процедурасын мультибейнелі (шектеулі уақыт ішінде екі немесе үш адам автографының жасалуының қолданылуы) жасаса, адамды жеке автографы бойынша авторизациялау құралдарының сенімділігі жеткілікті дәрежеде жоғары болуы мүмкін болар еді.

Ашық биометриялық адам бейнесін оның автографы түрінде қолдану кезінде адамды өз қолтаңбасын өте жылдам қоюға мәжбүрлеу керек. Қазіргі кезде қолжазба құпиясөзі немесе құпия сөйлем бойынша шектеулі мүмкіндік жүйесінде қолтаңбалауды жүзеге асыру кезінде қандайда бір шектеу жүктелмейді. Техникалық тұрғыдан мұндай шектеуліктер енгізу қиын емес.



2.14-сурет. Төлеушінің ЭСҚ-ны қауіпсіз қалыптастыруының USB Био-токен түріндегі CEO мен графикалық планшеттің жігі

Қолжазбалық қолы бойынша жеке тұлғаны аутентификациялау тәртібінде қолжазба құпиясөзін көрсету орынды емес.

Соған байланысты биометриялық аутентификация процедурасын орындау үшін CEO стандартты графикалық планшет пен есептеу құрылғысына қосылатын, әдетте сенімсіз есептеу машинасына мүмкіндік беретін, био-токен түрінде орындалуы мүмкін. Жеке кілтте сандық қолтаңба қоюды қалыптастыру бойынша барлық операцияларды және жасырын биометриялық бейнені био-токен сенімді есептеу ортасы ішінде

жеке кілтке өзгерту бойынша операцияларды орындау қауіпсіздеу болып табылады. Қолжазба құпиясөздерінің жасырын биометриялық бейнелері мен сандық қолтаңба қоюды қалыптастырудың жеке кілті био-токеннің СЕО-тан тастап кетпеуі керек. Бұл жағдайда сандық қолтаңбаны қалыптастырудың жеке кілті мен жасырын биометриялық бейненің беделін түсіруге болмайды. Типтік графикалық планшеттің USB адаптері түрінде био-токен арқылы сенімсіз есептеу ортасымен қарым-қатынасы 2.14-суретінде бейнеленген.

Адам автографының ашық қолжазбасы бойынша авторизациялау төлемдерді қабылдау мен беру банктерінде және өзге операторларында жасалуы керек.

Банк шотымен қашықтықтан Ғаламторлық басқару арқылы жасырын биометриялық бейне бойынша авторизациялауды қолдану керек. Барлық жағдайда адамның арнайы биометриялық мәліметтерінің биометриялық контейнерлерде [30] өзін шифрлеп қорғаған немесе жеке биометриялық хэш-функцияға [38] дербес бағытталған түрінде қауіпсіз сақталуы қамтамасыз етілуі керек. Сенімді есептеу ортасынан алыну кезінде ашық қолжазба биометриялық бейнелердің динамикасы туралы биометриялық мәліметтер тұлғасыздандырылып қорғалған нейрожелілік контейнерлерде сақталуы қажет.

Сенімді есептеу ортасынан алыну кезінде жасырын қолжазба биометриялық бейнелер динамикасы туралы биометриялық мәліметтері жеке қорғалған нейрожелілік контейнерлерде сақталуына болады. Қазіргі кезде адам атын қолжазба арқылы жүзеге асыру мен автографтар түрінде ашық қолжазба бейнелері үшін 10^{-2} бастап 10^{-4} дейінгі дәрежедегі екінші текті қате ықтималдығына қол жеткізуге болады. Бес әріптен тұратын қолжазба құпия сөзін жасырын сақтаған жағдайда екінші текті қате ықтималдығын 10^{-4} бастап 10^{-8} көлеміне дейін төмендетуге болады. Мультибиометрияға (бірнеше әртүрлі қолжазба сөзін қолдануға) өту биометриялық бейнелерді қолдану санына сәйкес қате ықтималдығының дәрежесін төмендетуге мүмкіндік береді.

Жеке тұлғаның биометриялық қолжазба аутентификациясының технологиясы тек қана төлем қызмет операторларының

офистік ғимараттарда және электронды Ғаламтор сауда қызметі мен қашықтықтан басқаратын электрондық банкинг қызметтері қолданушылардың үй жағдайында қолданылады.

2.9. Мультибиометриялық қосымшаларды қолданудың болашағы

Бірнеше биометриялық технологиялардың бірігуі, нақтырақ айтсақ, мультибиометриялық бірігуі қолма-қол ақша алу немесе жеке шотпен қашықтықтан басқару жүйесіне рұқсат берілген кезінде жеке тұлғаны биометриялық авторизациялау процедурасының қауіпсіздік дәрежесін көтерудің бір әдісі болып табылады.

Мультибиометриялық бірігуді қолданудың болашағы:

- іріктеу шабуылына биометриялық жүйенің тұрақтылығының күшейтілуі.

Әртүрлі биометриялық технологиялардың тұрақтылығының арасындағы ерекшелік динамикалық биометрия мен статикалық салыстыру кезінде байқалады. Бөлек биометриялық бейнелер әрқашан сапа мен биометриялық параметрлердің санын қамтамасыз ете бермейді. Осылай, саусақтардың ізін қолдану сканерден алынатын ерекше нүктелер саны мен суреттің күрделілігі, әрі папилярлық сурет бейнесінің сапа жеткіліксіздігі қазіргі кезде екінші текті қателік ықтималдығын $10^{-4} - 10^{-6}$ кем көлеміне дейін төмендетуге мүмкіндік бермейді. Тек қана биометриялық бейне бойынша кепілдендірілген шектеулі мүмкіндік тапсырмасын шешу үшін бұл жеткіліксіз. Биометрияның бірнеше түрінің бірігуі талап етілетін екінші текті қате ықтималдығын қамтамасыз етеді.

- Биометрияның әшкерелеу қауіп катерінің төмендетілуі. Биометриялық бейненің біркелкі әшкерелеуді қолдануға рұқсат етілген тізімнен оны алып тастайды. Бұл мәселе статикалық биометрияның барлық түріне маңызды: саусақ ізі, қол немесе алақан суреті, көктамыр суреті, көздің сыртқы мөлдір қабығы, бет геометриясы т.б. Динамикалық және статикалық биометрияның мультибиометриялық бірігуі тапсырманың шешімі болуы мүмкін, бұл биометрия донорының қалауы бойынша өзгеруі мүмкін деген сөз.

- Бірнеше аутентификация нұсқасын қолдау. Аутентификацияның биометриялық технологиясының бірнеше баламасын қолдану арқылы биометрияны енгізу қабілетін уақытша жоғалтқан кезде (мысалы, саусақты тіліп немесе тамақ ауру кезінде дауыстың жоғалуы) авторизациялауды жоғалтудан қашуға болады. PIN-кодтарды немесе жасырын биометриялық бейне бөліктерін әшкерелегеннен кейін аутентификацияның қосымша нұсқасы толық көлемде ешбір шотты оқшаулаусыз операцияларды орындауға мүмкіндік береді. Бұл жағдайда банк тұтынушысы аутентификациялауды бір немесе бірнеше әдіспен орындау мүмкіндігінің жоғалуы туралы мәлімдеуі ғана жеткілікті, ал банк оларды оқшаулауы тиіс. Сонымен бірге аутентификацияның балама нұсқасы ерлі-зайыптылардың бір банк шотын бірге қолдануын жүзеге асыруға мүмкіндік береді. Қазіргі кезде карточка шотын бірлесіп қолдану бір шот үшін пластикалық картаның бірдей көшірмесін шығару арқылы жүзеге асырылады.

- Бірнеше қатысушыны қолдау. Аутентификацияның бірқатар протоколдары бір-бірінен бөлек сақталған бірнеше кілттің қолдануын қажет етеді.

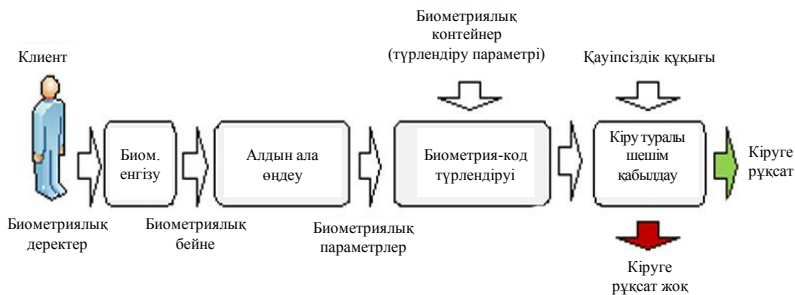
Жеке биометриялық бейнелерімен кілттің құрамдас бөліктерінің байланысы ұйым немесе үшінші біреулер жағынан рұқсат етілген бақылау мен біріктірудің әртүрлі сұлбаларын қолдануға мүмкіндік береді. Ескере кететін жайттардың бірі, бұл банктік операцияларды орындау өкілеттігін PIN-кодтар немесе электронды тасымалдаушы жүйеге кіру кодтарға бергендегі жағдайға қарағанда, биометриялық авторизациялау жағдайында беру қиындау.

- Құпияның бөлшектену сұлбасын қолдау. Биометриялық аутентификация процесінің қатысушылары арасындағы таратылған құпия бөліктерімен қажет болса биометрия көмегімен байланыс орындалуы мүмкін.

- Биометриялық мәліметтер мен шығыс кодының құпиясөзін сақтау бойынша мультибиометриялық өндегішке қауіпсіздік талаптарының сақталуы, үйретуді аяқтағаннан кейін оларды жоқ ету бойынша талаптарының сақталуы, сақталған параметрлерді қолданған ұйымдар шабуылының күрделілігі тек төлем операция қатысушыларының биометриялық авторизациялау

қосалқы жүйесін өңдеу МЕСТ Р 52633 стандарт пакетінің талаптары орындалған кезінде ғана жүзеге асады.

Жоғары сенімді биометриялық аутентификация процесі жалпы жағдайда бірнеше сатыны өз ішіне енгізеді: биометрияны енгізу, оны алдын ала өңдеу, шешім қабылдау мен биометрия-кодты қайта жасауды орындау (2.15-сурет).



2.15-сурет. Жоғары сенімді биометриялық аутентификация процесінің қарапайым сұлбасы

Биометрияны енгізу кезінде қолданушы өз биометриялық мәліметтерін биометриялық сипаттарды алатын, сонымен қатар электрлік немесе өзге сигналды сандық форматқа аударатын (биометриялық бейнеге) физикалық құрылғыға ұсынады.

Алдын ала өңдеу кезінде қалыптастырылған биометриялық бейне, талдау процедурасында және жоғары сенімді биометриялық аутентификация процесінде қолдану үшін "Барлығы Бөгде" бейнелерінің жиынынан тұтынушының "Өзім" бейнелерін ерекшелеу сапасына ие мәнді биометриялық параметрлерді ерекшелеп алуға ұшырайды.

Биометрия-кодты түрлендіру кезінде тұрақсыз, биометриялық параметрлердің жалпы жағдайында банк тұтынушысының аутентификациясы үшін қолданылатын кейбір қол жеткізу шығыс кодына түрленеді, сонымен бірге тұтынушы бейнесінің биометриясына ұсынылған жақындық индикаторларының мәніне түрленеді.

Шешім қабылдау кезеңінде банк алынған рұқсат кодын эталонды мәнімен айқын немесе айқын емес салыстыруды

жүзеге асырады, сонымен бірге индикатор мағынасын талдайды және аутентификация нәтижесі туралы шешім шығарады: мүмкіндікке рұқсат ету, мүмкіндікке рұқсат етпеу. Шешім қабылдау ережесі мен аутентификация уақытындағы тұтынушымен қарым-қатынас тәртібі банк қауіпсіздігінің саясатшыларымен анықталады.

Жоғары сенімді биометриялық аутентификацияның қандай сатыда бірігуінің орындалуына байланысты МЕСТ Р 52633.7 төмендегі мультибиометрияның түрлерін бөліп шығарады:

- мультимодальді биометриялық аутентификация. Әртүрлі енгізу құрылғыларымен байланысты бірнеше биометриялық технологиялардың қолданылуымен орындалады. Графикалық планшет пен сканер көмегімен орындалатын саусақ ізі мен қолжазбалық бейнесі бойынша биометриялық аутентификация үлгі түрінде қызмет етеді;

- мультібейнелі биометриялық аутентификация. Бір биометриялық технологияның бірнеше биометриялық бейнелерді қолдану арқылы орындалады. Оң және сол қол бірнеше саусақтарының бір сканерге қойылуы немесе бірнеше қолжазба құпиясөздерін енгізудің кезектілігімен биометриялық аутентификация үлгі түрінде қызмет етеді;

- мультисенсорлық биометриялық аутентификация. Биометриялық бейнені енгізуге арналған бірнеше құрылғының көмегімен орындалады. Кеңістікте аутентификацияланып жатқан жағдайды бақылаушы бірнеше микрофонды қолданумен дауыс сөзін енгізуі үлгі түрінде қызмет етеді. Өзге үлгісі-екі бақылау камерасын қолданумен құрылған бет көлемінің бейнесі бойынша аутентификациялау;

- мультиүлгідегі биометриялық аутентификация. Бір биометриялық бейненің бірнеше үлгісі көмегімен орындалады. Биометриялық бейненің алынып жатқан сапасы төмен болса, оларды сапаландыру қажет болғанда ғана қолданылады. Бірнеше уақыт ішінде және келесі оларды өңдеу барысында биометриялық мәліметтерді (саусақ іздері мен дене бөліктерінің бейнесі) бірнеше рет алу жолымен аутентификацияланып жатқанға сезілмей орындалуы мүмкін;

- мультиалгоритмдік биометриялық аутентификация. Бұл бойынша ақпаратты максималды алу мақсатында бір

биометриялық бейне бірнеше әр түрлі алгоритмдермен өңделеді;

- көпшілік пайдаланушы биометриялық аутентификация.

Бірнеше биометриялық бейне донорларының қатысуымен орындалады. Әртүрлі құпияны бөлу немесе ажырату сұлбасын қолдану жағдайында жүргізіледі;

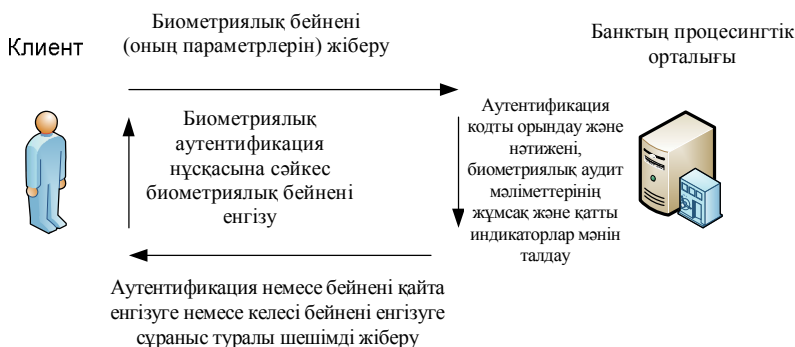
- көпнұскалы биометриялық аутентификация. "Немесе" логикалық операциясының көмегімен мультибиометриялық аутентификацияның әртүрлі түрін біріктіреді.

Жоғарыда аталып өткен мультибиометриялық аутентификацияның барлық түрі бірлесіп қолданылуы мүмкін (аралас мультибиометриялық аутентификация).

Бірнеше биометриялық технологиялар бірігуінің бұл тәсілдерінің кез келгені биометрия-код қайта жасаушыларының жоғары сенімді базасында төлем жүйесінің ақпараттық қауіпсіздігін күшейту үшін қолданылуы мүмкін. Сонымен бірге келесі жүйенің жаңғыруы жаңа биометриялық аутентификация технологиясының қосылу жолымен іске асады, олардың біреуінің іске асуы тұтынушының биометриялық аутентификациясының жалпы сұлбасын бұзбайды.

Мультибиометриялық аутентификацияны қолданудың ерекшелігі бірнеше биометриялық бейнелердің бір кезде немесе кезектесіп енгізілу қажеттігі болып табылады. Бұл процесті бірегейлендіру бойынша жұмыс 4 қадам бойынша (2.16-сурет) қарым-қатынас процедурасын сипаттауға мүмкіндік берді, бұл тұтынушыны қашықтықтан аутентификациялау, тұтынушыны банкомат (терминал) арқылы аутентификациялау, банк бөлімшесінде жеке өзінің қатысуымен аутентификациялау кезінде жүзеге асуы мүмкін. Мультибиометриялық аутентификация кезінде тұтынушыға қолданылған аутентификация сұлбасына сәйкесінше дәйекті түрде биометриялық бейне үлгілерін енгізуді орындау ұсынылады. Әрбір енгізілген бейне процессінгілік банк орталығына бағытталады. Мұнда нәрсенің жеткіліктігіне биометриялық бейнелерді енгізудің кезектегі бірізділігі аутентификация кодын жасау үшін және олардан күтілетін сипаттаманың сәйкестенуі үшін талданады. Сонымен бірге танып-білу үшін тұтынушы аутентификациясының коды мен биометрия шабуылына биометрия ұсынған биометриялық аудит

пен сапа индикаторының мәндер бағасы қолданылады. Алынған қорытынды негізінде, тұтынушыға бағытталған, аутентификация процесінің жалғасуы немесе дұрыс яки бұрыс нәтижелі шешіммен тоқтатылуы туралы шешім қабылданады. Банк таңдаған аутентификация саясатына байланысты ақпараттық қауіпсіздік қауіп-қатерінің шешілуі мен мультибиометриялық аутентификациясы процедурасын практикалық қолданудың қолайлығы арасындағы келісімге және қауіпсіздіктің талап еткен дәрежесіне қол жеткізуге болады.



2.16-сурет. Мультибиометриялық аутентификация кезінде биометрияны ұсынудың тәртібі

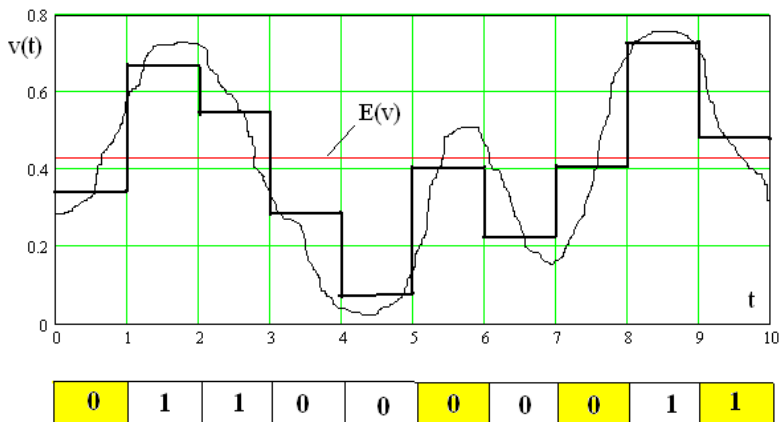
Төлем жүйесі қолданушыларының мультибиометриялық аутентификацияға өтуі белгілі бір дәрежеде жеке тұлғаның биометриялық аутентификациясының сенімділігін жоғарылатады да, сонымен бірге қолданушылар үшін аутентификация процесін қиындатады. Мультибиометриялық аутентификацияны қолданушыға жеңілдету үшін ол эталлондыға биометриялық мәліметтер ұсынылған қауіпсіз жақындық индикаторларымен жабдыкталуы керек. Қауіпсіз жақындық индикаторлары МЕСТ Р 52633.6 «Ақпаратты қорғау. Ақпаратты қорғау техникасы, биометриялық мәліметтер «Өзім» бейнесіне ұсынған жақындық индикациясына талаптар» талабына сай орындалуы керек.

3. БИОМЕТРИЯЛЫҚ ПАРАМЕТРЛЕРДІҢ АЙҚЫН ЕМЕС ЭКСТРАКТОРЛАРЫ

Қазіргі кезде АҚШ пен Еуроодақтың елдері адамның биометриялық мәліметтерін оның криптографиялық кілттерімен "айқын емес экстракторлар" деп аталмыш қолданыс арқылы байланыстыру жолында жүр [39 – 51]. Сонымен бірге, «айқын емес экстракторлар» биометриялық мәліметтердің дәлме-дәл қайта жаңғыртудың мүмкіндігі болмағандықтан пайда болған қателікті өтеуге қабілетті және шуылды жағдайындағы биометриялық мәліметтерден кездейсоқ тегіс таратылған биттер тізбегін ерекшелейтін алгоритмдер есебінде қарастырылады. Кілттерді оларға жүгіну арасында сақтаудың қажеттісіз генерациялау үшін «айқын емес экстракторларды» қолдануға болады. Негізінде «айқын емес экстракторлар» «шикі» биометриялық мәліметтерінің бинарлық кванттау және қатені табушы классикалық шығыс кодтар арқылы әрі қарай кванттау қателіктерін түзету жолымен жасалады.

3.1. Биометриялық мәліметтерді кванттаудың қарапайым нұсқасы

Биометриялық технологиялар үшін бақыланатын биометриялық параметр уақыт аралығында өзгеруші қандай да бір қызмет сияқты ұсынылуы мүмкін. Мысалы, бұл көздің сыртқы мөлдір қабығы аумақтарын радиалды сканерлеу кезінде жарықтығын өзгерту болуы мүмкін, бұл дыбыс толқынының ауытқу амплитудасының өзгеруі болуы мүмкін, бұл қолжазба құпиясөзін жасау кезінде қаламның ауытқу координаттары болуы мүмкін. 3.1-суретінде осындай ауытқулардың бірінің үлгісі көрсетілген.



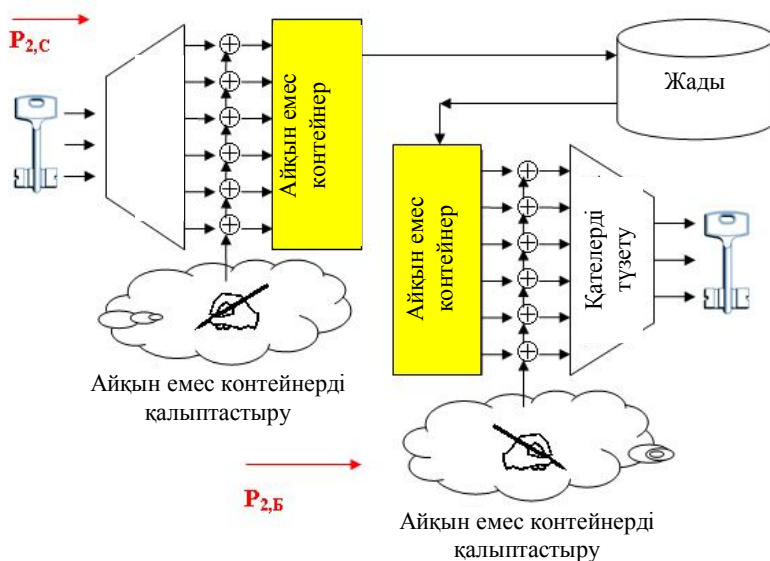
3.1-сурет. Біршама орта мәндегі $v(t)$ биометриялық параметрдің өзгеру қисығының квантталуы

Биометриялық мәліметтердің өзгеру қисығы квантталуының қарапайым нұсқасы уақыттың алдын ала қойылған интервал санының бөлінуіне алып келеді (3.1-суретінде 10 интервал қолданылды). Әрбір кванттау интервалында $v(t)$ параметрінің орташа мәні есептеледі де, $E(v)$ –бақылаудың барлық интервалы бойынша орташа мәнімен салыстырылады. Егер параметрдің орташа мәні интервалда $E(v)$ -дан үлкен болса, биокодтың бұл дәрежесі «1» жағдайы беріледі. Егер параметрдің орташа мәні интервалда $E(v)$ -дан кіші болса, биокодтың бұл дәрежесіне «0» жағдайы беріледі. 3.1-суретінің төменгі жағында жасалған биокодтың дәрежелері берілген. Кванттау аумағына шамамен бірдей болымды және болымсыз $v(t)$ қисық көріністері түскендіктен, биокод дәрежесінің шамамен жартысының мұндай бейнеде қалыптасуы тұрақсыз болып табылады. Биокодтың тұрақсыз дәрежелері 3.1-суретінде қара түспен белгіленген. Іс жүзінде биокодтың көптеген тұрақсыз дәрежелерін (80% дейін) жасырады, ал қалған 20% тұрақсыз дәрежелердегі қателерді тауып, түзететін кодтарды қолдану арқылы жөндейді.

3.2. Гамманы салу арқылы ақпаратты жасырып ұстайтын «айқын емес экстрактор»

Егер биокодтар сенімді есептеу ортасында сақталып әрі өңделетін болса, жеке тұлғаның биометриялық аутентификациясын тексеріліп жатқан адам биокоды мен биокод үлгісін қарапайым салыстыру арқылы орындауға болады. Мұндай технологиямен биокодтың ашық үлгілері мәліметтер қорында сақталуы тиіс. Биометриялық үлгілер қорының көлемі өскен сайын оның құны да өседі, сәйкесінше биометриялық кодтар қорының ұрлану қаупі де өседі.

Адам биокодын қорғау әдістерінің бірі – бұл оларды гаммалау [52-59] болып табылады. Бүгінгі күні көптеген «айқын емес экстракторлар» 3.2-суретінде көрсетілген сұлба бойынша гамманы алу және шығарумен жеке тұлға биокодын гаммалаудан құрылған.



3.2-сурет. Айқын емес контейнерді қалыптастыру кезінде гамманы салу мен аутентификация процедурасы кезінде оны алу

3.2-суретінде көрініп тұрғандай, қорғаныс гамма айналаға белгісіз адамның жеке криптографиялық кілтінен жасалады. Гамманы қалыптастыру кезінде таңдалған өзін-өзі түзететін кодтың қателерінің синдромын есептеу жүргізіледі. Қателер синдромын өзін-өзі түзететін кодтың артық бөліміне қосып болған соң, әрі оны өзін-өзі түзететін кодтың ақпараттық бөлімімен байланыстырған соң алынған гамманың ұзындығы қорғаушы биокодтың ұзындығына сәйкес келуі керек.

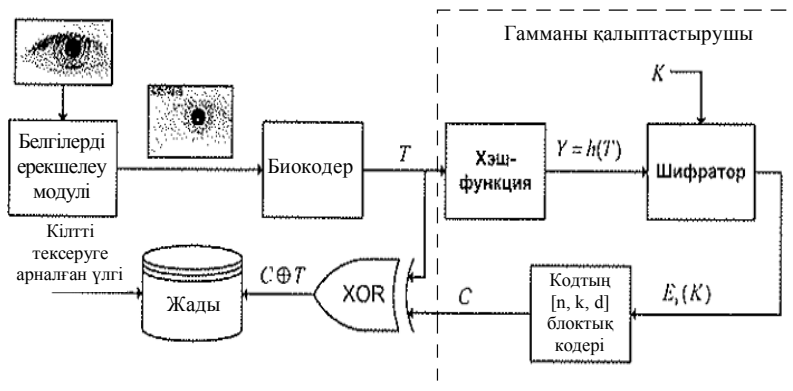
3.2-суретінде берілгендей қолданушының жеке кілтінің ұзындығы әрқашан оның биокодының ұзындығынан кіші. Биокод пен жеке кілттің ұзындығының арақатынасы биокодтағы түзетілуші қателер санына байланысты таңдалады. Егер өзін-өзі түзететін кодты 100% артықшылығымен қолданса, онда биокодтағы қателердің шамамен 4% түзетуге болады. Бұл жағдайда жеке криптографиялық кілттің ұзындығы айқын емес контейнер немесе биокодтың жарты ұзындығын құрауы тиіс.

Биометриялық аутентификация кезінде кері процесс болады, жаңа ғана қалыптасқан биокод екі айқын емес контейнер модулі бойынша құралады. Сонымен бірге биокод гаммасын қорғаушы толығымен дерлік алынып тастау жүргізіледі. Гамма биокодтың қате биттерінде ғана алынып тасталмайды. Биокодтың қате биттері өзін-өзі түзететін кодпен басқарылады да, қолданушының жеке кілті қайта құрылады, сонымен бірге криптографиялық аутентификация протоколында қолданылады.

«Айқын емес экстракторлардың» бір қызық жері бұл олардың биокодтың криптографиялық қорғаныс тұрақтылығын бақылаудан, ал биометриялық қорғау тұрақтылығын «Бөгде» кездейсоқ бейнелерді алмастырып қою шабуылынан анық түрде бөлуге мүмкіндік береді. Криптографиялық қорғаныс тұрақтылығы жеке кілттің ұзындығына пропорциялы болады ($P_{2,c}$ екінші текті қате ықтималдығына қарсы пропорциялы, бірінші талпыныстан жеке кілтті табуға шарттасқан). Қорғаныстың биометриялық тұрақтылығы биокодтың ұзындығына және оның дәрежелерінің тұрақтылық көрсеткіштеріне пропорционалды.

3.3. Гамманы салу және биокодты хэштеу мен «айқын емес экстракторлар»

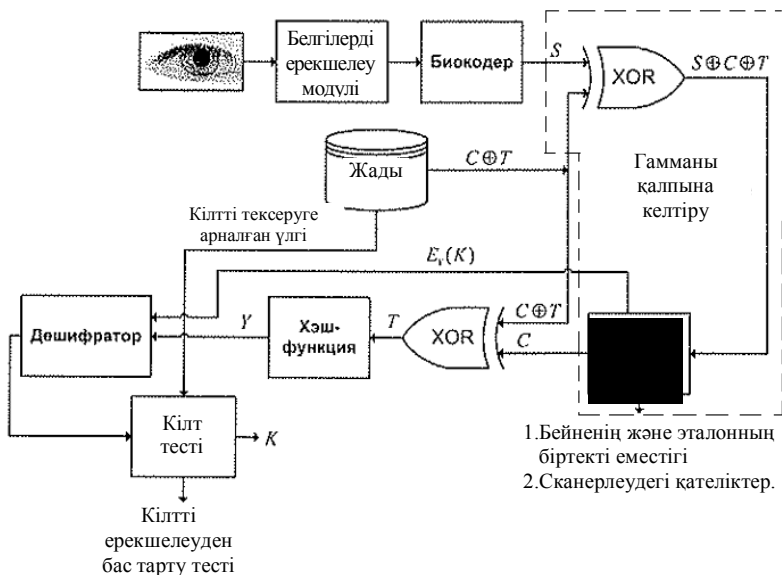
Биокодты [55, 56] алдын ала хэштеуді қолдану қорғаныс гаммасын қалыптастырудың және бір әдісі. 3.3-суретінде гамманы қалыптастырудың екінші әдісінің блок-сұлбасы берілген.



3.3-сурет. «C» гамманы қалыптастырудың екінші әдісі мен хэштеуді қолдана отырып, айқын емес контейнер жасау

Екінші әдіс бойынша биокод оны хэштеп болған соң кілтті – K шифрлайды. Әрі қарай, алынған шифрмәтінді өзін-өзі түзететін кодпен жабады және алынған гаммамен биокодты жабады. Осындай бейнеде қалыптасқан айқын емес контейнерді мәліметтер қорында қауіпсіз сақтауға болады.

Биометриялық аутентификация кезінде гамманы алып тастау кері процесін жүзеге асырады, оның блок-сұлбасы 3.4-суретінде берілген.



3.4-сурет. «С» қайта құрылып жатқан гамманы қайта хэштеуден және шифрды жай жазуға айналдырушы кілтті қайта құрудан алдын қалыптастыру

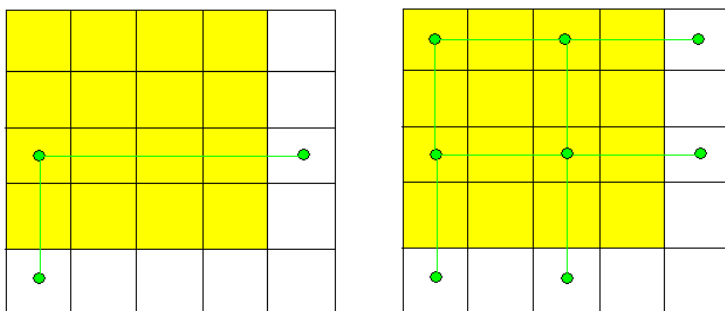
3.4-суретінде көрініп тұрғандай гамманы алып тастау дәл өзге айқын емес экстракторлардағыдай болып жатыр. Мәлімет қорының айқын емес контейнері жаңа ғана алынған биокодтан модуль екі бойынша құрастырады. Сонымен бірге биокодтың сенімді биттерінен гамманы толық алып тастау болады. Биокодтың қате биттері алдын ала енгізілген шығынның есебінен түзетіледі. Бірінші әдістің екінші әдістен ерекшелігі (3.2-суретінде) қайта құрылған биокодты хэштеу операциясының толықтырылуыннан және одан да күрделірек шифрлау кілтінің қайта құру операциясынан құралады.

3.4. «Айқын емес экстракторлардағы» қолданылатын өзін-өзі түзететін кодтарды таңдау

«Айқын емес экстракторлар» биокод дәрежелерінің тұрақтылығын жасырын түрде (маскирование) дәрежесін 5%-дан

10%-ға дейін қате пайда болғанша арттыруға тырысады. Кейін қатені табу мен түзету классикалық кодтарымен қателерді басқарады. Негізінде классикалық өзін-өзі түзететін кодтар [57-59] ешбір қиындықсыз 10% қатеге дейін басқара алады.

Қалыпты кедергіге қарсы тұратын кодтау теориясы белгілі бір дәрежеде күрделі. Бірнеше оншақты жеткілікті дәрежеде тиімді кодтар құрылған, олардың әрбірі айқын емес экстрактордарда қолданылуы мүмкін. Барлық классикалық кедергіге қалыпты қарсы тұратын кодтардың басты кемістіктерінің бірі олардың артықшылығында, олар биокодтың бір бөлігін классикалық өзін-өзі түзететін кодтарды артықшылықпен толтыруға сарп етуді талап етеді. Мұны қарапайым жұптық бақылау блок кодтарда үлгі-нұсқамен сипаттайық. Мұндай кодтардың ақпараттық және артықшылық бөлімдерін қалыптастырудың принциптері 3.5-суретінде сипатталады.



3.5-сурет. Ақпараттық өріс матрицасының тармақ және бағана жұптық бақылау қарапайым блок кодтары

3.5-суретінде блок кодтың ақпараттық матрицасы бояумен боялып белгіленген, ал матрицаның оң және төменгі жолдары кодтың артықшылық бөлімін жасайды. Бағанның оң өрісі мен код матрицасының төменгі бөлімінде, сәйкесінше ақпараттық матрицаның жолы мен бағанында мәліметтердің жұптық биттерін жазады. Ұяшықтың төменгі оң жағында, блок кодтың артықтық бөлімінде ақпараттың жұптық биттері жазылады.

Кодты ақпараттық құраушы код матрицалары мен жұптық тармақтардың көрсеткішін кодтың артықтық бөлімінде олардың жұптық биттерімен салыстыру арқылы тексереді. 3.5-суретінің сол жағында блокта бір қате пайда болғанда олар 25 бит, бұл қате қате бағаны мен қате тармағының қиылысында ақпаратты инверттеумен оңай табылып, жөнделеді жағдайы суреттелген. Бұл қаралып жатқан блокты код бір қатені блокқа жөндеуге қабілетті, ал блокта шамамен 8 қатені табады. Кодтың артықтықтығы 56% кезінде ол $P=1,0$ ықтималдығымен жалғыз қателерді жөндейді немесе шамамен бір-біріне қатынасы бойынша қателердің таралуы 4%.

Егер әрбір блокқа 2 қатеден тура келсе, бұл код 0.5 ықтималдығымен барлық қателерді басқарады. Бұл жағдай 3.5-суретінің оң жағындағы көрінісінен көрініп тұрғандай өңдеуге болатын 4 жер табылып тұр. Блок кодының тек қана екі битін жөндеу қажет. Шамамен 8% - 12% қатені бірдей басқару үшін 100%-дан 200% дейін артықтықты күрделірек кодтауды (мысалы, БЧХ кодтарын немесе Рид-Соломон кодтарын) қолдану қажет. 200% артықтықты классикалық кедергіге қалыпты қарсы тұратын кодты қолдана отырып іс-жүзінде ақпараттық бөлімінде тек қана $1/3$ дәрежесін қалдыру қажет. Биокод қателерінің көбірек санын түзету талпынысы биокодтағы ақпаратты одан да көбірек жоғалтуға алып келеді.

Биокодта 20% қатені жөндеу кезінде биокод негізінің ақпараттық құраушысы негізгі ұзындығынан $1/5$ дейін және $1/10$ дейін төмендейді.

Биокодтардың ақпараттық бөлімінің апатты сығылуының салдарын егер, кеңейтілген ақпараттық матрицаның 128×64 [60, 61] тармақтары мен бағандары бойынша есептеліп, биокілттің ең кіші 16×16 ақпараттық матрицасынан кездейсоқ таңдалған мәліметтер кестесі болатын хэш-функцияның дәрежелер бөлімінің жұптық бақылауынан мәндік бақылауына өтсе жоюға болады. Техникалық әсері тармақтар мен бағандар хэш-функциясының кіші дәрежелерін (1,2 немесе 3 дәрежелерін) криптографиялық хэш-функциялардың кері айналып келмейтіндігінен ашық сақтауға болатындығынан құралған. Жалғыз қателер қарапайым жұптық бақылаулы блок кодтарда

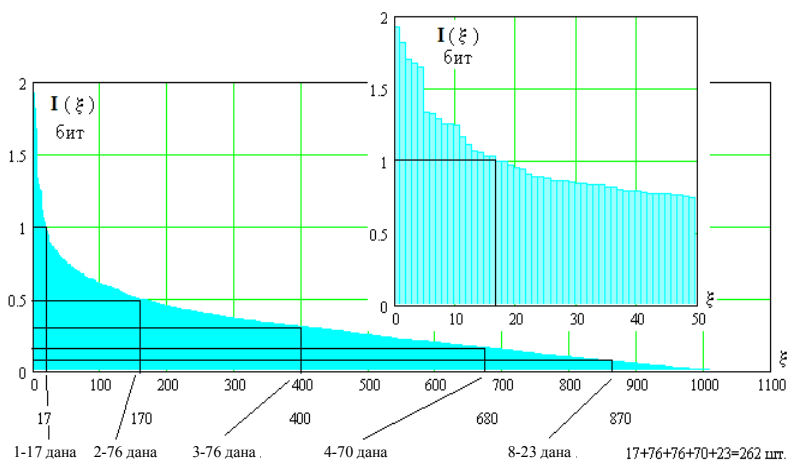
орналасқандай орналасады. Топтық қателер хэш-функция жағдайының артылуы болып табылады, сәйкесінше эталонды дәрежесінің «дұрыс» жағдайы да тура солай. Қысқартылған хэш-функцияның бақыланып жатқан дәрежелерінің ұлғаюы кезінде экспоненциалды түрде қайта кодтауға жұмсалатын уақыт өседі, бірақ сонымен бірге жөнделген қателер саны полиномал түрде өседі [61].

4. БИОМЕТРИЯ-КОДТЫ НЕЙРОЖЕЛІЛІК ТҮРЛЕНДІРГІШ

4.1. Дара нейронның (персептрон) итерационды үйрету алгоритмі

«Жақсы емес» биометриялық параметрлердегі ақпараттар бір биометриялық параметрден сенімді шешім қабылдау жеткіліксіз. Міне осыған байланысты «айқын емес экстракторлар» биокодтың бір ғана дәрежесін қарастырып қоймай биокодты толығымен қарастырып, ондағы қателерді басқарады. Биометриялық мәліметтерді кванттауға дейін оларды нейрожелілік байытуды жүзеге асыру тиімдірек өзге бір техникалық тәсіл болып табылады.

Нейрожелілік байыту кезінде барлық биомәліметтерді қолданбай, олардың топтарын қолданады. Сонымен бірге мәліметтер қаншалықты жаман болса, соншалықты көптеген мәліметтер бір нейронмен сапаландырылатын бір топқа бірігуі керек. Егер талданып жатқан биометриялық параметрлердің ақпараттылығы есептелсе, байытуға қажет нейрондар санын жақыннан бағалауға болады (4.1-сурет).



4.1-сурет. Биометриялық мәліметтерді байыту үшін қажет
нейрондар санын шамамен бағалау

Биометриялық параметрлердің ақпараттылығын тарату көрсеткішінен көрініп тұрғандай (4.1-сурет) ақпараттылықтың ең жоғарғы көрсеткіші тек қана 17 биометриялық параметрге ие, олардың әрбірін кванттағаннан кейін өз алдына қолдануға болады. Ақпараттылығы 1 биттен 0.5 битке дейін «қанағаттандырылғы» сапалы биопараметрлер – 152, олар екі кірісті 76 нейронды жасауға қолданылуы мүмкін.

Осындай 76 нейроннан 3 кірісті де жасалады, бұл кезде әрбір кірістің ақпараттылығы 0.5 биттен 0.35 битке дейінгі арақашықтықта болады. Биомәліметтердің одан да аз ақпараттылығын 70 нейронды 4 кіріспен ал шамамен 23 нейронды 8 кіріспен байытуға тура келеді. Жалпы барлығы шамамен 262 нейрон қайталанбайтын кірістермен болады, мұндағы әрбір нейронның шығысы биокілттің бір тұрақты дәрежесін береді. Жоғарыда берілген бағалар өте жақын болып табылады, себебі «Өзім» бейнесі параметрлерінің арасындағы қуатты корреляциялық байланысты ескермейді. Іс жүзіндегі биометриялық жүйелердегі нейрондардың кіріс саны, жоғарыда келтірілген бағаларға қарағанда, шамамен екі-үш есеге көп болуы керек.

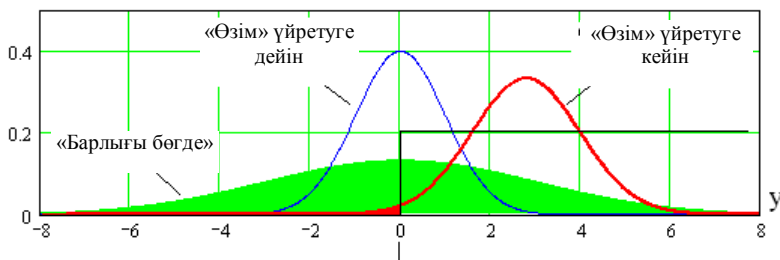
Биомәліметтердің нейрожелілік байытуын пайдалану үшін жасанды жалғыз нейрондарды үйретіп білу қажет. Жасанды нейрондар мен желілерді үйрету бойынша кең түрде суреттелген орыс тіліндегі әдебиеті [62-66] бар. Жасанды нейронды үйретудің жүздеген алгоритмдері мен нейрондарды қоздыру (өршіту) функцияларын орындайтын көптеген нұсқалары бар.

Биометрия тапсырмасының [67-70] шешілуіне сәйкес көбіне нейрондарда персептрондағы [70, 71] сияқты сатылы тақ өршіту (кванттау) функциясы қолданылады. Кванттаудың сатылы жұп функциясы сирек қолданылады, 3 немесе одан да көп шығу жағдайы бар [66, 72] бірқалыпты емес кванттау функциялы нейрондардың айтарлықтай болашағы бар. «Персептрон» атауы тек қана сумматор шығыс мәліметтерінің қарапайым кванттау функциясымен нейрондарға бекітілген, осыған байланысты «персептрон» термині мәтін ішінде «нейрон» терминімен параллельді түрде қолданылады.

Тарихқа көз жүгіртсек, бірінші болып орташа квадратталған кателерді итерациялы барынша азайтуда құрылған, нейрондар шешімін қабылдайтын, үйрету алгоритмі жасалды.

Орташа квадраттау қате минимумының өлшемін қарастырмай дәстүрден шегінейік, себебі ол биометрияда сирек қолданылады. «Өзім» «Все Чужие» таралуларының бөліну сапасы деп аталатын белгісін биометрияда қолдану ең тиімді болып табылады.

Биометриядағы нейрожелілік қосымшалардың негізгі функциясы «Өзім» бейнесінің таралуын «Барлығы Бөгде» бейнесінің таралуынан итеріп шығарып тастау. Бұл жағдай 4.2-суретінде суреттелген.



4.2-сурет. Нейрон сумматоры шығысында «Өзім» бейнесі мәліметтерінің таралуын «Барлығы Бөгде» мәліметтерінің таралуынан итеріп шығарудың нәтижесі

Үйретуден алдын нейрон сумматорының салмақ коэффициенттері кездейсоқ беріледі, нәтиже жағынан ықтималды болып табылатын жағдайлардың бірі — бұл нейрон сумматор шығысындағы «Өзім» бейнесінің таралу күйі «Барлығы Бөгде» таралу бейнелерінің ортасында болуы. Биометриялық параметрдегі нейронды кванттаудың шығыс функциясы әрқашан «Барлығы Бөгде» бейнелерін таралуының ортасында жұмыс істеуге бағытталады. Нәтижесінде үйренілмеген нейронның шығысында «Өзім» бейнелерінің таралуы тұрақсыз болады (шамамен теңдей ықтималдылық жағдайымен «0» және «1» береді). Егер нейрон шығысында «1» жағдайын «Өзім» бейнесі үшін алғымыз келсе, «Өзім» бейнесін таратуды «Барлығы Бөгде» бейнелерді таратудың ортасынан оңға қарай итеріп шығара отырып нейронды үйрету керек болады. Нейрон жұмысының сапасы «Өзім» бейне таралуын қаншалықты алысқа итеріп тастауымызға байланысты. Осы үйретудің сапалылығы үшін келесі сапа көрсеткіші қолданылады:

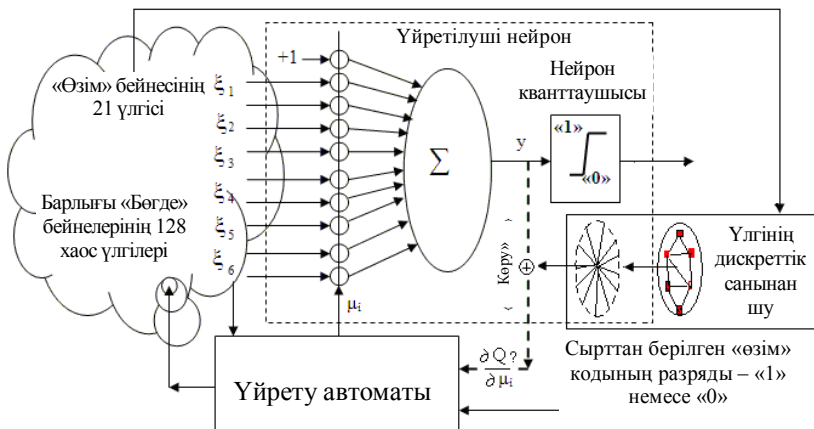
$$Q = \frac{|E(y_v) - E(y_\xi)|}{\sqrt{\sigma_v \cdot \sigma_\xi}} \quad (4.1)$$

мұндағы $E(y_v)$ – «Өзім» үлгілерінің математикалық болжалы, $E(y_\xi)$ – «Барлығы Бөгде» үлгілерінің математикалық болжалы, σ_v – «Өзім» үлгілерінің орташа квадраттық үйлеспеуі, σ_ξ – «Барлығы Бөгде» үлгілерінің орташа квадраттық үйлеспеуі.

Математикалық болжам арасындағы айырмашылық қаншалықты көп болса, сапа көрсеткіші соншалықты жоғары болады. Егер көпшілікті бөлетін орталықтың арасындағы арақашықтық белгіленген болса, көпшілікті бөлетін орташа квадратталған орташа геометриялық арақашықтық азайтылып, сапа көрсеткіші тағы өседі.

Сапа көрсеткішін (4.1) қолдана отырып, сапаны көтеру жағына қарай қозғалыс критериясы бойынша нейронды (4.3-сурет) үйретудің итерациялық процедурасын құруға болады. Бұл мақсат

үшін сапа үйретуі бойынша $\frac{\partial Q}{\partial \mu_i}$ жеке туындыны есептеу қажет.



4.3-сурет. Итерациялық алгоритммен дара нейронды үйрету сапасының максимумын іздеуге үйрету

Егер туынды болымды болса, онда реттемелі салмақ коэффициентінің мінін - μ көтеруге тура келеді. Сапа туындысы болымсыз болса, онда реттелмелі салмақ коэффициентін азайту қажет.

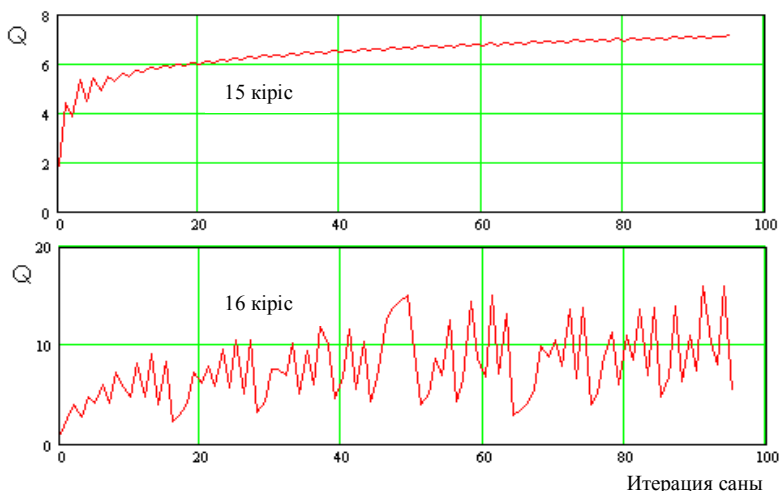
Сапаны үйрету бойынша жеке туындыны есептеу барысында интерациялық үйретудің автоматын құру оңай сияқты. Егер биометриялық мәліметтердің «жақсы» сапасымен аз санды кірісті нейрондарды үйрету туралы сөз болса, бұл шынымен солай болады. Егер олай болмаса, көп санды кіріс нейрондарын үйрету қиынға соғады. Негізгі мәселе, «Өзім» үйрету үлгілерінің аз дискреттік санмен шарттасқан, үйрету процедурасының ішкі шуыннан құралған. «Барлығы Бөгде» үлгілерінің жеткілікті санын алдын ала жасау техникалық тұрғыдан қиын емес. «Өзім» бейнесі үлгілерінің ондаған немесе жүздегенін жасай отырып, қолданушыларды өз күшін сарыптауға мәжбүрлеу қиындау. Үйретудің есептеу проблемасы

$\frac{\partial Q}{\partial \mu_i}$? сапалы жеке туындыны «Өзім» үлгілерінің аз саны

кезінде есептеудің тұрақсыздығында. «Өзім» үлгілерінің аз болғандығынан $\frac{\partial Q}{\partial \mu_i}$? туындыларды есептеу кезінде пайда

болатын $\Delta E(y_v)$, $\Delta \sigma(y_v)$ кемшіліктері күшейеді де, компонентке пайдалы қозғалыс бағытын тах $\{Q\}$ жағына қарай «ығыстырады». Үйретудің максимум сапасына қарай бағытталған қозғалыс орнына қателердің көп өлшемді шегі бойынша орынсыз адасушылық пайда болады. Бұл жағдай 4.4-суретінде суреттелген.

4.4-суретінен көрініп тұрғандай нейрон 15 кірісті кезінде итерациялық үйрету тұрақтырақ болады, бірақ нейронның кіріс саны 16 дейін көбейткен кезде итерационды үйретудің тұрақтылығы жоғалады. Үйрету сапасының көптеген жергілікті максимумы мен минимумы пайда болады, бұл «Өзім» бейнесі мәліметтерінің континуум үлгілерінің соңғы санымен шарттасқан есептеу процедурасының өз шуын күшейту болып табылады.



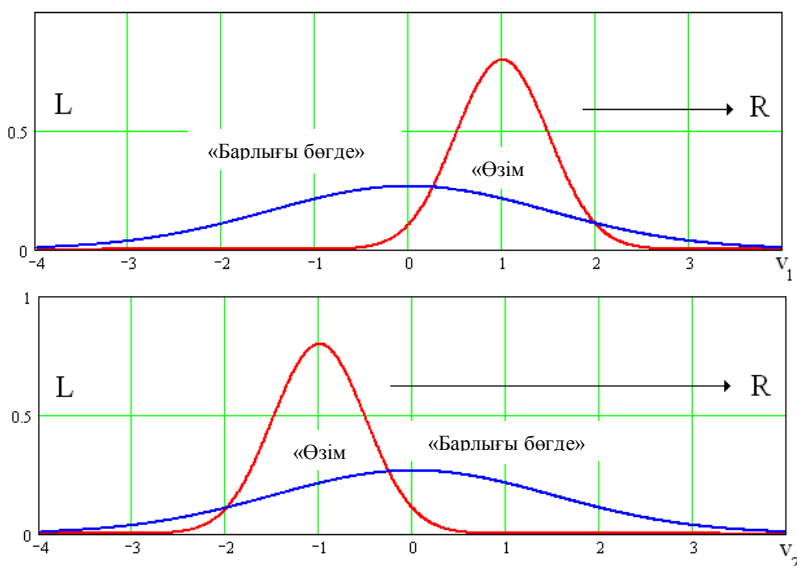
4.4-сурет. Бір нейронды итерационды үйрету процедурасының тұрақтылығын жоғалтып алу

4.2. Нейронды үйретудің абсолют тұрақты итерациялық емес алгоритмі

Биометриялық қосымшалардың нейрондарын үйретудің проблемасы адам бұл процесте қатыспауы тиіс. Нейронды кепілдік бере отырып үйрететін абсолют тұрақты үйрету автоматы болуы қажет. МЕСТ Р 52633.5 – 2011 итерациялық емес үйрету алгоритмдерін қолдануды ұсынады. Бұл типтес алгоритмдер үшін жеке туындыларды есептеудің қажеті жоқ, әрі олар бойынша кері байланыс ілмектері толығымен үзіледі (4.3-сурет). Бұл типтес алгоритмдер «болжау», яғни тосып отырған шешімді салмақ коэффициенттері кезінде ерекше ықтималды белгілерді болжау арқылы және салмақ коэффициенттерінің мәнін болжаудан құралған. Әрине белгілі бір дәрежеде үйретудің сапасы төмендейді, бірақ есептеудің жоғарғы тұрақтылығының әсері пайда болады. Осылайша үйретіліп жатқан нейронның кірісі қаншалықты көп болса, есептеудің тұрақтылығы соншалықты жоғары болады.

«Қарғысқа ұшыраған» өлшем бірлігі орнына қарама-қарсы жоғары және аса жоғары өлшем бірліктерінің «сәтті» әсері пайда болады.

Нейронның салмақ коэффициенттері белгісін автомат болжау бір кіріске дейін сумматордың құлдырау жорамалына құрылған болуы мүмкін. Бірақ одан алдын үйрету автоматы «Өзім» бейнесін қай жаққа (R – оң жаққа немесе L – сол жаққа) итеріп шығару шешімін қабылдауы тиіс. «Барлығы Бөгде» бейнелерінің көпшілігінен «Өзім» бейнесін R-итеріп тастау бізді қызықтырады деп есептейік. Берілген жағдай 4.5-суретінде көрсеткішпен көрсетілген.



4.5-сурет. «Барлығы Бөгде» бейнелерінің көпшілігінің ортасынан «Өзім» бейнелерінен R итеріп тастауы туралы шешімі

4.5-суретінен көрініп тұрғандай, көп өлшемді тапсырма (нейронның сумматорында тек қана бір кіріс) шешімінен белгілі бас тарту бір кірісті салмақ коэффициентінің белгісін таңдау тапсырмасын ешбір пайдасыз (тривиалды) жасайды. Міне осылай суреттің жоғарғы жағындағы салмақ коэффициентінің

белгісі болымды болуы керек, себебі математикалық болжал- $E(v_2)$ болымды болып табылады. Суреттің төменгі жағында кері жағдай суреттелген, математикалық болжау $E(v_2)$ болымсыз болып табылады.

«Өзім» бейнесінің R итеріп шығаруының тиімділігі үшін сумматордың екінші шығыс салмақ коэффициентінің белгісін ауыстыру қажет. Қорыта келе, R итеріп шығару үшін үйретіліп жатқан нейронның салмақ коэффициентінің белгісін болжау процедурасы пайда болады:

$$\text{i-ші таңбаның R-ші болжамы} \quad \begin{cases} + \mu_i & \text{if } E(\xi_i) \leq E(v_i); \\ - \mu_i & \text{if } E(\xi_i) \geq E(v_i). \end{cases} \quad (4.2)$$

Егер «Барлығы Бөгде» бейнелер көпшілігінен солға қарай «Өзім» бейнесін кері итеріп тастау мақсатын қойса, онда R қағида инверсиясы пайда болады (4.2):

$$\text{i-ші таңбаның L-ші болжамы} \quad \begin{cases} + \mu_i & \text{if } E(\xi_i) \geq E(v_i); \\ - \mu_i & \text{if } E(\xi_i) \leq E(v_i). \end{cases} \quad (4.3)$$

Негізінде көптеген шығысты үйретіліп жатқан нейронның салмақ коэффициентінің ол немесе бұл белгісін дәл көрсету қиын. Бұл белгіні дәл есептеу мүмкін емес, сонымен бірге ол итерациялық үйрету процесінде бірнеше рет өзгеруі мүмкін, бірақ (4.2) және (4.3) мағынасын қолдану арқылы нейрон салмақ коэффициентінің белгісін шамамен болжауы мүмкін. Нейрон салмақ коэффициентінің белгісін дұрыс болжау ықтималдығы қаншалықты жоғары болса, нейронды үйрету соншалықты тұрақты болады. Салмақ коэффициентінің белгісін болжаудың тиімді бағасын үйретілген нейрон салмақ коэффициентінің белгісімен (4.2) және (4.3) формулалары бойынша есептеу шешімінен алынған белгілерді салыстыру арқылы беруге болады. Санаулы сынақ көрсетуі бойынша белгінің қате ықтималдылық болжамын 0.11-ден 0.27-ге дейін құрайды. Бұл салмақ коэффициенті белгісінің болжам процедурасы минимум

73% жағдайында дұрыс шешім, максимум 89% жағдайында дұрыс шешім береді. Дәл осы жағдай жасанды нейронның желілік бөлімін үйретудің жылдам итерациондық емес алгоритмдерді жасау үшін алғышарт болып табылады.

Егер нейронды үйрету итерациондық алгоритмі тұрақсыз екені және нейронды артығымен үйретуге алып келу мүмкіндігі, сонымен бірге нейронды толық үйретілмегені белгілі болса, онда «Өзім» және барлығы «Барлығы Бөгде» кіріс мәліметтерінің статистикасына сүйене отырып нейрондарды салмақ коэффициенттері мәнін болжауды үйрену кажет болады. Салмақ коэффициенттерінің мүмкін болған мәндерін болжаудың ең қарапайым әдісі «Өзім» бейнесі мәліметтерінің тұрақсыздығын есепке алу болып табылады. Мұндай болжауды қалыптастырудың идеясы коэффициенттер арқылы тұрақсыз биометриялық параметрлердің әсерінің әлсізденуінен құралған:

$$|\mu_i| = \frac{1}{\sigma(v_i)} \quad (4.4)$$

4.4 формуласы бойынша коэффициенттерді таңдау кезінде $b(v_i)$ үлкен мәнді тұрақсыз коэффициенттері аз дисперсиялы тұрақтырақ коэффициенттеріне қатынасы бойынша шешімге шамамен 2-3 есе аз әсер етеді. Егер жоғары бірегейлікке ие биометриялық параметрінің әсерін күшейтсек, «Барлығы Бөгде» бейнелерінен «Өзім» бейнесін одан да тиімдірек итеріп шығаруға болады. Яғни салмақ коэффициенттері төмендегі формулалар бойынша есептелуі керек:

$$|\mu_i| = \frac{|E(\xi_i) - E(v_i)|}{\sigma(v_i)} \quad (4.5)$$

Тәжірибе көрсетіп отырғандай, (4.5) формуласы бойынша салмақ коэффициенттерін есептеу «Барлығы Бөгде» бейнелер перефериясына «Өзім» бейнелерін жылдам итеріп тастау мүмкіндігін береді. Есепке алынған биометриялық параметрлердің санын көбейту есебінен теориялық тұрғыдан $n \rightarrow \infty$ үйретілген сумматордың шығысында «Өзім» бейнесін

мүмкіндігі болғанша алысқа итеріп тастауға болады. Бірақ барлығы бөгде бейнелерінен «Өзім» бейнесін өте қатты алысқа итеріп тастауға болмайды, себебі биометриялық егіздердің іздеу шабуылы жүзеге асуы мүмкін.

4.3. Нейрондар желілерін үйрету мен қалыптастыру. Нейрожелілік контейнерлер

Биокодтың кіру кілтін алу үшін кілттің ұзындығына тең шығыс санымен нейрондар желісін жасау қажет. Нейрондық желінің кірісі мен шығысы қаншалықты көп болса, соншалықты қабылданатын шешімнің сапасы жоғары болмақ. Мұндай байланыстың қаншалықты күштілігін 1-кестеден көруге болады.

1-кесте

Жасанды нейрон желісінің кіріс және шығыс сандарына байланысты шешім сапасының өсуі

Нейрожелінің кіріс саны	Нейрожелінің шығыс саны	«Өзім» бейнесін кіргізбеу ықтималдығы	«Бөгде» бейнесін кіргізу ықтималдығы
5 кіріс	1 шығыс, 2 классты	$P_1=0,1$	$P_2=0,17$
48 кіріс	1 шығыс, 2 классты	$P_1=0,1$	$P_2=0,03$
480 кіріс	1 шығыс, 2 классты	$P_1=0,1$	$P_2=0,005$
480 кіріс	256 шығыс, 2^{256} классты	$P_1=0,1$	$P_2=0,000000001$
480 кірісті және 256 шығысты нейрожеліні үйрету МЕСТ Р 52633.5-2011 алгоритмімен «Бөгде» бейнелерінің 128 үлгісі және «Өзім» бейнесінің 20 үлгісімен жүргізілді.			

1-кестеден көрініп тұрғандай, есепке алынған биометриялық параметрлердің кіріс санының өсуі тиімді емес. Нейрон желісінің кіріс сандарына параллельді түрде оның шығыс сандарын да көбейту маңыздырақ. Бірдей кіріс сандары кезінде

(480 кіріс) 1-ден 256 дейін шығыс сандарын көбейту нейрондық желінің шешіміне миллиард есе (қосымша алты нөл пайда болады) ұтыс алып келеді. Сонымен бірге уақыт пен басқа да есептеу ресурстарының шығындары 100 есеге көбейіп кетеді, жасанды интеллект көлемінің экспоненциалдық байланысы мен олардың қабылдап жатқан шешімінің сапасы көрініп тұр.

Қолданылып жатқан нейрондық желінің құрылымын таңдау ең маңызды мәселелердің бірі. Жасанды нейрондар желілері бойынша желілерді әдебиетте бір қабатты, екі қабатты, үш қабатты деп бөледі, сонымен бірге желілерді нейрондардың үш санынан да көбірегіне бөледі. Нейрондық желілердің құрылымының соншалықты кең әралуандығы биометрия үшін маңызды емес. МЕСТ Р 52633.5 – 2011 не бір қабатты нейрондық желіні, не екі қабатты нейрондық желіні қарастырады. Екі қабатты нейрондық желі үшін бірінші және екінші қабат қызметі бөлінген. Бірінші қабаттың нейрондары биометриялық мәліметтерді байыту мен сапаланған мәліметтерді кванттау қызметін атқарады. Егер байытудың сапасы жеткіліксіз дәрежеде болса, онда нейрондардың екінші қабаты бірінші қабат нейрондарының биокод қателерін басқарады.

Ескере кететін жайттардың бірі, нейрондардың екінші қабатын әрқашан қатені іздеп табушы және жөндеуші қарапайым классикалық кодтармен ауыстыруға болады, бірақ қателерді нейрожелілік түзету ұтымды. Нейрожелілік түзетуді қолданудың ұтымдылығы «Өзім» биокодтар үлгісімен екінші қабатты үйрету кезінде биокодтың әрбір дәрежесінің нақты тұрақтылық көрсеткішін бағалау болып табылады.

Тәжірибе бойынша, биокод дәрежелерінің басым көпшілігі жоғары тұрақтылыққа ие, тұрақсыз болып қалатындары тек қана анық белгілі қалыптағы бөлек код дәрежелері.

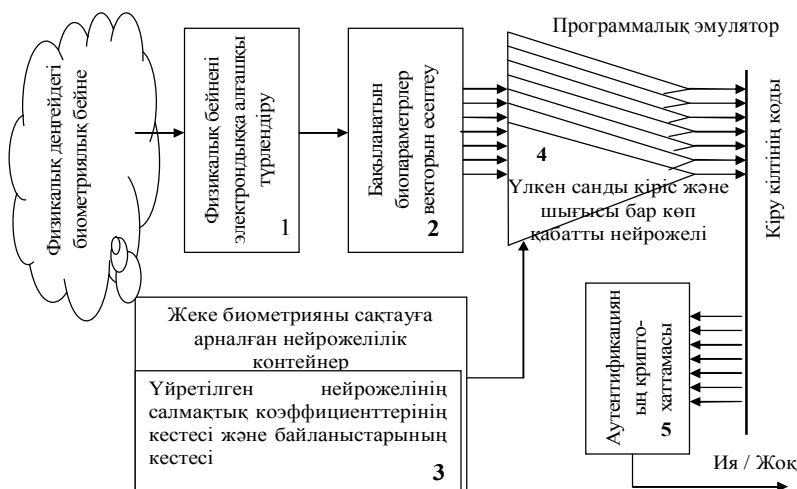
Нейрондардың екінші қабаты тұрақсыз дәрежелерді түзетуді, сонымен қатар тұрақты әрі тұрақсыз дәрежелер ретінде хэштеуді үйренеді. Қателерді іздеп табушы әрі жөндеуші барлық классикалық кодтар, код дәрежелері арасында қателерді таратудың тең ықтималдығы туралы болжам жиегінде, керісінше құралған. Міне дәл осы үшін, «Өзім» биокод тұрақтылық көрсеткіштерін нақты таратуды үйрету кезінде

есепке алатын нейрожелілік қателерді түзетушілерден классикалық өзін-өзі түзетуші кодтар жеңіледі.

Нейрон желілерінің қабат санынан басқа әрбір нейронның шығыс сандарын таңдау және желі кіріс нөмірлерімен кіріс байланысын беру қажет. Егер барлық нейрожелі 480 кіріске ие болып, кірістің орташа ақпараттылығы 0.3 битті құраса, онда 1-ден 18-ге дейінгі кіріс санды нейрондарды қолдану қажет болады (нейрон қолданып жатқан биометриялық параметрлер сапасына және олардың арасындағы түзетуге байланысты). Қажет кіріс сандары тек нейронды үйрету кезінде ғана табылуы мүмкін. Сондықтан алдын ала кірістің аз ғана сандарына кездейсоқ таңдау берілгеннен кейін, егер шешім сапасы тапсырысқа дейін жетпесе, онда нейронның кіріс сандарын көбейтеді. Қорыта келгенде, бір қабатты нейрон желісі пайда болады, мұндағы әрбір нейрон барлық желі кірістеріне кездейсоқ қосылған өз кіріс санына ие болады. Үйретуден кейін әрбір нейронның кірісінің байланысуы үшін салмақ коэффициенттерінің кестесі қосымша болады.

Ресми мойындалып үйретілген желі нейрон байланыстары кестелерін және салмақ коэффициенттері кестелерінде сипатталады. Егер желі екі қабатты болса, онда нөмірлер байланыс кестесі мен салмақ коэффициенттерінің кестесі әрбір нейрон қабаты үшін жасалуы қажет. Нейрон қабаттары кезекті түрде үйретіледі. Нейронның бірінші қабатын үйретуден кейін нейрон желісінің кірісінен нейронның шығысына «Барлығы бөгде» және «Өзім» желілерінің үлгілерін тарату жүргізіледі, биокод үлгілерін алып, олар бойынша екінші қабаттағы нейрондарды үйретеді.

Үйретілген нейрондардың нейрондық желі байланыс кестесі мен салмақ коэффициенттер кестесі нейрожелілік контейнерлерді жасайды (құрастырады). Программалық үйретілген нейрожеліні криптографиялық кіру кілтінің кодына адамның биометриялық мәліметтерін түрлендіруді қажет кезінде қосу үшін нейрожелілік контейнерде ақпараттар жеткілікті. Аутентификацияның процедурасы нейрожелілік контейнерді қолданумен құрылған.



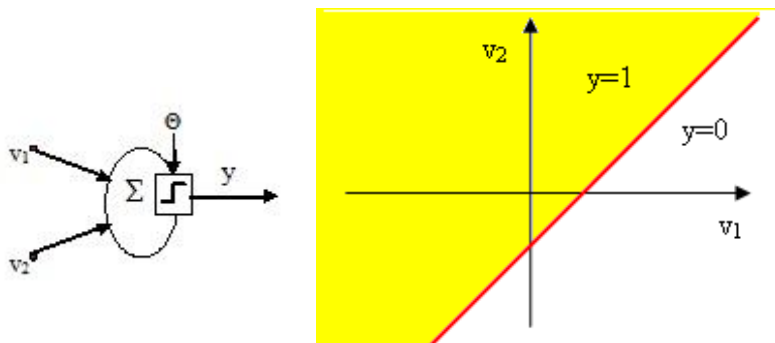
4.6-сурет. Нейрожелілік контейнерді қолданған биометриялық аутентификацияның блок-сұлбасы

МЕСТ Р 52633.4 - 2012 стандартында адам биометриясы мен олардың өзара әрекеттесу интерфейстерін сақтау үшін нейрожелілік контейнерлерді қолдану мен қалыптастыру берілген [73]. Бірнеше әртүрлі биометриялық технологияларды (мультибиометриялық аутентификация) қолдануға тура келсе, онда бірнеше нейрожелі контейнерлерінің биометриямен өзара қарым-қатынасы МЕСТ Р 52633.7-2013 талабына сәйкес жүзеге асырылады [74].

4.4. Жасанды нейрондардың екі қабатты желісінің әмбебаптығы

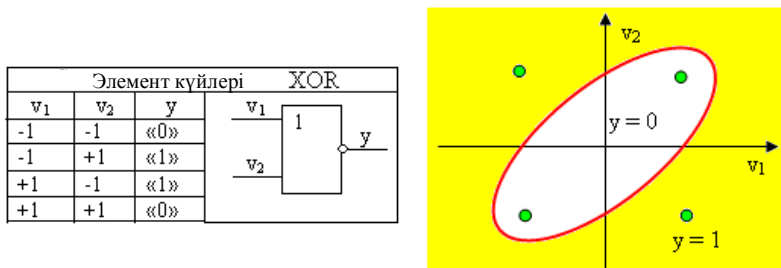
МЕСТ Р 52633.5-2011 нейрондардың екі қабатты желісін таңдағандағы шарты, бұл нейрожелілік құрылымының жан-жақтылығы мен барлық тапсырманы шеше алуында. М. Минский мен С. Пейперт [75] дара персептрон жан-жақты емес екенін көрсетті. Персептронбиометриялық параметрлердің көп өлшемді кіріс кеңістігін екі кең көлемдегі жазықтыққа

«0» және «1» шығыс жағдайына сәйкес бөлуді жүзеге асырады. Мұны көп өлшемді кеңістік үшін суреттің екі өлшемді графикасымен кітапта көрсету мүмкін емес. Екі өлшемді персептрон жағдайын ғана суреттеп көрсетуге болады (4.7-сурет).



4.7-сурет. Кеңістікті екі өлшемді нейронмен «0» және «1» екі бөлікке бөлу

Персептронның сызықтығы оның сызықтық емес қызметін орындауына мүмкіндік бермейді, мысалы, «НЕМЕСЕ жоққа шығарушы» қарапайым қызметін жүзеге асыру. Төменде «НЕМЕСЕ жоққа шығарушы» жағдай кестесі берілген және бұл жағдайлардың графикасы бейнеленген:



4.8-сурет. Эллипстік бастапқы функциясымен радиалды «нейронмен» жақындауы және (XOR) «НЕМЕСЕ жоққа шығарушы» логикалық қызмет жағдайының кестесі

«НЕМЕСЕ жоққа шығарушы» сызықты емес логикалық қызметін персептронмен жақындау мүмкін еместігіне көз жеткізу үшін персептронға сәйкес келетін теңсіздік жүйесімен оның жағдайын жазып аламыз:

$$\begin{cases} -1 \cdot \mu_1 - 1 \cdot \mu_2 - \theta < 0; \\ -1 \cdot \mu_1 + 1 \cdot \mu_2 - \theta > 0; \\ +1 \cdot \mu_1 - 1 \cdot \mu_2 - \theta > 0; \\ +1 \cdot \mu_1 + 1 \cdot \mu_2 - \theta < 0; \end{cases} \quad (4.6)$$

Жүйенің бірінші теңдеуінен (4.6) осы жүйенің екінші теңдеуін, ал үшінші теңдеуден төртіншіні есептеп шығарсақ, үйлеспейтін жүйе аламыз:

$$\begin{cases} -2 \cdot \mu_2 < 0; \\ -2 \cdot \mu_2 > 0; \end{cases} \quad (4.7)$$

Жүйенің үйлеспеуі (4.7) персептронды қарапайым сызықты емес функцияны орындай алатындай етіп үйретуге болмайды деген сөз. Сызықты алгебраның көлемінде отырып-ақ біз квадраттық пішінді қолдана аламыз:

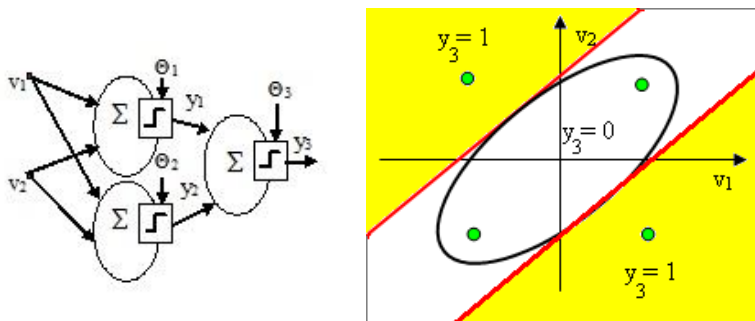
$$e^2 = (E(\bar{v}) - \bar{v})^T \cdot R^{-1} \cdot (E(\bar{v}) - \bar{v}) \quad (4.8)$$

мұндағы R^{-1} – биометриялық параметрлердің кері корреляциялық матрицасы, $(\sigma(v_i) = 1)$. Биометриялық параметрлердің орташа квадраттық ауытқу бойынша мөлшерленген вектор - $\bar{v}$

(4.8) формуласы екі биометриялық параметрдің бақылау жағдайында дәл осы эллипсті сипаттайды. Квадраттық пішін кейбір шегімен- Θ (4.8) бойынша есептелгенді салыстыра отырып, біз «0» және «1» жағдайын қабылдаушы эллипстік бөлу функциясын аламыз (4.8-сурет).

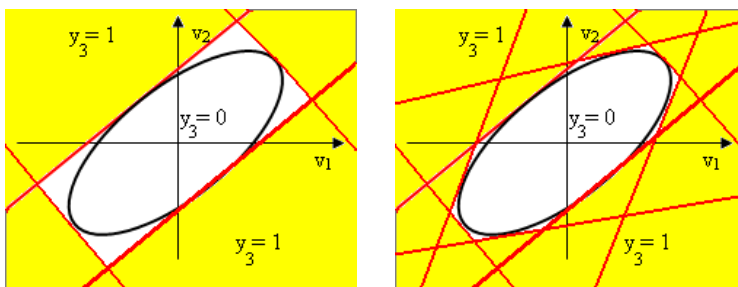
Дара нейрон (персептрон) тіпті шек қойылған сызықтық бөлу қызметін орындай алады, бірақ біз персептронның екі қабатты желісін қолдансақ, онда кез келген күрделі бөлу қызметін жүзеге асыра аламыз. Мысалы, егер біз желінің бірінші қабатында екі персептронды желіні және желінің екінші қабатында бір

персептронды желіні қолдансақ, онда біз екі түзу параллельді түрінде «жөкке шығарушы НЕМЕСЕ» жақындауын аламыз.



4.9-сурет. Бірінші қабатта екі персептронмен, ал екінші қабатта бір персептронмен «НЕМЕСЕ жөкке шығарушы» тапсырманың шешілуі

4.9-суретінің бірінші бөлімінен көрініп тұрғандай, екі кеңістікті бөлуші түзулер белгілі бір дәрежеде анық емес «НЕМЕСЕ жөкке шығарушы» қызметтерін жақсы жуықтайды. Қарапайым логикалық функциялардың екі қабатты персептрондармен жақындатылуы өз алдына теориялық мәнге ие емес, әрі шектеулі жалғыз персептронның ыңғайлы суреттелуі ғана болып табылады. Мұның бәрі М. Минский мен С. Пейперттің қаланған дәстүрі [75]. Эллипстік бөлу функция персептрондарының желілермен жақындатылуы теория мен тәжірибе үшін көбірек мәнге ие. Мұндай бірінші қабаттағы 4 және 8 персептронды сызық-тілімдеріне ұқсас желілік жақындатылудың екі үлгісі 4.10-суретінде көрсетілген.



4.10-сурет. Бірінші қабаттағы 4 және 8 персептронды эллипстік шешуші функциялы желілік жақындатылу тапсырмасының шешімі

Бірінші қабатта персептрондар қаншалықты көп болса, эллипстік бөлуші функцияның сызық тілімдерінің жуықтауы соншалықты дәлірек болады. Кез келген сызықты емес бөлуші функцияның жақындатылудағы кемшілігі бірінші қабаттағы нейрондар санына пропорциялы болады. Қайта жаңғыртылатын сызықты емес бөлуші функцияның саны екінші қабаттағы нейрондардың (персептрондардың) санына байланысты. Жақындатылу кеңістігінің өлшемі бірінші қабат нейрондарының кіріс санына байланысты.

Нейрожелілік шешуші қағидалардың артықтығының маңыздылығы тәжірибеде жоғары өлшемді (4.8) квадраттық пішіндермен қолдануға болмайды. «Өзім» бейнесінің 20 үлгісі бойынша кез келген өлшемдегі корреляциялық матрицаны техникалық тұрғыдан есептеуге болады:

$$R_2 = \begin{bmatrix} 1 & r_{1,2} \\ r_{2,1} & 1 \end{bmatrix}, \quad R_3 = \begin{bmatrix} 1 & r_{1,2} & r_{1,3} \\ r_{2,1} & 1 & r_{2,3} \\ r_{3,1} & r_{3,2} & 1 \end{bmatrix}, \dots, \\ R_n = \begin{bmatrix} 1 & r_{1,2} & \dots & r_{1,n} \\ r_{2,1} & 1 & \dots & r_{2,n} \\ \dots & \dots & \dots & \dots \\ r_{n,1} & r_{n,2} & \dots & 1 \end{bmatrix} \quad (4.9)$$

Сонымен бірге 2-ден 4-ке дейінгі кіші тәртіптегі корреляциялық матрицалар белгілі бір дәрежеде жақсы айналады, міне осыны пайдаланып эллипстік бөлуші функцияны жасауға болады. 5-ші және одан да үлкен тәртіптегі корреляциялық матрицалар шағын үйретуші іріктемеде қос корреляцияның дәл есептеу коэффициентінің төмендігінен айналмайды. Сызықтық алгебра квадраттық пішіндер түрінде жұмыс істеуден қалады.

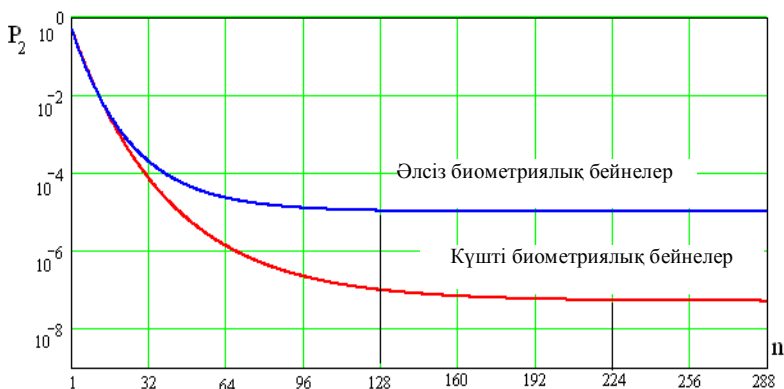
Квадраттық пішіндердің нейрожелілік жақындауына тоқтасақ, олар өз жұмысын кез келген тәртіпке дейін жалғастыра береді. МЕСТ Р 52633.5 – 2011 бойынша іс жүзінде

жасанды нейрондарды үйрету, нейрондардың кіріс сандарын көбейтсек, одан әрі тұрақтай түседі. Дәл осы себепті үлкен нейрондық желілер үйретілгеннен кейін көп өлшемді статистиканың классикалық алгоритмдерінен және сызықтық алгебрадан да беріктеу жұмыс істейді. 480-өлшемді гиперэллипс түріндегі квадраттық шешуші ережені құру техникалық тұрғыдан мүмкін емес кезінде, осы гиперэллипстің жуықтауын 480-өлшемді параллелепидтермен құру (бірінші қабаттағы 480 кірісті 4 персептрон) толық мүмкін. Нейрондардың екі қабатты желісі келесі ізіндегі криптографиялық аутентификацияның сандық автоматымен қосындысында жан-жақты. Бұл қосынды биометриялық ақпаратты қорғаудың кез келген қосымшасын жасауға мүмкіндік береді. Желі қабаттарында нейрондар санын көбейту (бірінші және екінші) өте тиімді техникалық амал болып табылады.

4.5. Нейрожелілік түрлендіргіштердің биокод ұзындығын ұтымды таңдауы

Егер бізге келесі криптографиялық аутентификация үшін кілт ұзындығына 256 бит қажет болса, онда нейрожелілік түрлендіргіш биометрия-код 256 шығысқа ие болуы қажет. Егер нейрожелілік түрлендіргіш бір қабатты болса, онда бірінші қабат 256 нейронға ие болуы тиіс. Жоғарыда айтылып өткендей, криптографиялық қорғаныс құпия сөз қорғанысы мен биометриялық қорғанысқа қарағанда едәуір күштірек. Мұны біз бірінші қабаттағы нейрондар санын өзгерткенде жақсы көре аламыз. Бірінші жақындауда $P_{2,B}$ биометриялық қате ықтималдығы қолданылған нейрондар санының өсуімен азайтылады, сәйкес келуші қисық төмендеу 4.11-суретінде бейнеленген. Бірақ тұрақтылықтың жылдам өсуі ($P_{2,B}$ ықтималдығының жылдам төмендеуі) үздіксіз бола бермейді. Әдетте $P_{2,B}$ ықтималдығының сызықтық төмендеуі тек қана нейрондар саны өсуінің бастапқы аумағында байқалады. Кейін өсу көрсеткішінің баяулауы болып, біраздан кейін екінші текті қате ықтималдығы мүлдем төмендемей қояды. Екінші текті қате ықтималдығының төмендеуі тоқтаған мезет «Өзім» биометриялық бейнесінің ақпараттылығына байланысты. 4.11-суретінде

аутентификацияны құраушы биометриялық қате ықтималдығының екі қысық төмендеуі көрсетілген.



4.11-сурет. Бір қабатты нейрондық желі шығыс санының екінші текті қате ықтималдығының мәніне әсері

4.11-суретінен көрініп тұрғандай, «әлсіз» аз ақпаратты биометриялық бейне ($P_{2,b}=10^{-4,7}$) қате ықтималдығына көп мән береді, бұл бейненің толығыуы кілт ұзындығы 128 битке жеткен кезде болады. Демек, егер шығыс кодының ұзындығы 256 бит болса, біз ешбір ауыртпалықсыз қатені табу мен жөндеуге жұмсалатын 50% код шығынына ие боламыз. «Күштірек» биометриялық бейне ($P_{2,b}=10^{-7,1}$) дәрежелі 224-тен асатын ұзындықтағы код үшін толықтыру аумағына ие. Демек, бұл код шығыны 12,5% құрайды. Сонымен бірге бұл шығын классикалық өзін-өзі түзетуші кодтардың қателерді жөндеу мен табу үшін қолданылуы мүмкін. Егер бұл шығын жетпесе, онда биокод шығысының ұзындығын қажетінше көбейтуге тура келеді.

Кейбір жағдайларда кілт ұзындығы биометрико-нейрожелілік қорғаныстың толықтыру аумағының басына дейінгі ұзындықтан кіші болуы мүмкін. Бұл жағдай екінші жағдайға, яғни кілтке қажет 128 бит кезіндегі «күшті» биометрияны қолдануға, сәйкес келеді. Ресми түрде біз нейрондық желінің бірінші қабатында 128 нейронмен

шектелуімізге болады, бірақ бұл белгілі бір дәрежеде сапа көрсеткішін жоғартуға алып келеді.

Техникалық тұрғыдан криптографиялық кілттегі шығыс ұзындығынан нейрондар санының көп болғаны тиімдірек (мысалы, $224 > 128$), сондықтан кейбір жағдайларда биокодты хэштеуді жүзеге асыруға тура келеді. Хэштеуден кейін хэш-функцияны қажетінше кесіп тастап, оны кілт есебінде пайдалану керек.

Кілттер биометриялық қосымшалардан тысқары жасалған жағдайда хэш-функцияның мәнін қосымшасы бар екінші модуль бойынша құрастырсақ, берілген мәнге келтіру мүмкін болады. Қажет болса, «Өзім» биокодының хэштеуін «тұзбен»⁵ орындайды. «Тұз» және хэш-функцияны толықтыруды ашық түрде сақтайды.

Ескере кететіні, жоғарыда сиппатталған әдіс тек қана кілт ұзындығын қысқартып қоймай, оның ұзындығын үлкейтуге де қолдануға болады. Бұл «Өзім» біршама «әлсіз» биометриялық бейне үшін 128 желілі жасанды нейрондармен ғана биокод ұзындығын хэштеу арқылы 128-ден 256-ға дейін амалдауға болады деген сөз. Мұндай амал есептеу ресурстарын үнемдеу қажет болғанда орынды. Әдетте криптографиялық хэштеу жасанды нейрондық желінің бағдарламалық эмулядеуіне қарағанда шамамен 1000 есеге жылдам орындалады.

4.6. Нейронның екінші қабатымен биокодты нейрожелілік түзету

Егер классикалық өзін-өзі түзетуші кодтар тым көп ақпараттық жоғалтулар алып келсе, МЕСТ Р 52633.5-2011 бірінші қабат нейрондары жіберген катені түзету үшін екінші қабат нейрондарын қолдануға ұсыныс жасайды. Екінші қабат нейрондарын жөнге салудан алдын стандарт әрбір «Өзім» биокод дәрежесінің тұрақтылығын бағалауды ұсынады. «Өзім»

⁵ «Тұз» түрінде қолданылып жатқан хэш-функцияның ұзындығына салыстырмалы ұзындықтағы кездейсоқ санды қолданады. «Тұзды» қолдану хэш-функция айналымының кестесін жасауда шабуыл жасаушыға қиындық туғызады.

бейнесінің тесттік үлгілерін осы мақсат үшін беріп, $P_{1,i}$ – әрбір дәрежесі бойынша бірінші қабатты қате ықтималдығын есептейді. Әрі қарай әрбір дәреженің тұрақтылық көрсеткіштерін есептейді:

$$\gamma_i = 2 \cdot |P_{1,i} - 0.5| \quad (4.10)$$

мұндағы i -дәрежелі γ_i – тұрақтылық көрсеткіші, абсолюттік тұрақты дәрежелер үшін 1.0 мәнін қабылдаушы мен тұрақсыз дәрежелер үшін «0» және «1» теңдей ықтималдық жағдайымен 0.0 мәні.

Екінші қабат нейронын жөндеу кезінде тұрақтылық көрсеткіштеріне пропорциялы түрде оның салмақ коэффициенттерін қою қажет (4.10). Салмақ коэффициентінің белгісі кездейсоқ таңдалады. Түзетуші нейрондардың кірістерін биокодтың дәрежелеріне кездейсоқ қосады да, биокод дәрежелерінің мәнін түрлендіруді жүзеге асырады: «0» жағдайын -1 жағдайына түрлендіру, «1» жағдайына +1 мәнін иемдету. Салмақ коэффициенттерінің кездейсоқ белгілерімен ± 1 биокод дәрежелерінің кездейсоқ жағдайларын нейронның сумматор шығысында көбейтсек, нөлге жақын жағдай пайда болады.

Нейронды жөнге салу қос шығыстарда белгілерді кездейсоқ циклдік орын ауыстыруына алып келіп соғады. Әлбетте, 64 кірісті нейронның максималды мүмкін болған шығыс жағдайы +64 шамасына жақын, ал минималды мүмкін болған мәні -64 жақын болады. Егер жөнге салынып жатқан нейрон 1 қатені басқарып, «1» жағдайын берсе, онда +2 жақын «Өзім» үлгілеріне баға берудің максималды мәніне жету қажет болады. Егер жөнге салынып жатқан нейрон 1 қатені басқарып, «0» жағдайын берсе, онда -2 жақын «Өзім» үлгілеріне баға берудің максималды мәніне жету қажет болады. Нейрон жөндеген қателер саны әрқашан шамамен «Өзім» үлгілерінің максималды баға беру модулінен бірге кем болуы тиіс. Нейрондардың екінші қабаты екі қызметті орындайды. Біріншіден ол нейрондардың алдыңғы қабатының биокод қателерін басқарады, екіншіден «Бөтен» кодтарының мәліметтерін екінші қабат нейрондар сумматорлары хэштейді.

4.7. Екінші қабат нейрондары орындайтын «Бөгде» мәліметтерін хэштеу

Мінсіз биометрия-код түрлендіргіш «Өзім» кодтарының екіұштылығын (неопределенность) толық жоққа шығару керек және «Бөтен» кодтарының энтропиясын максимал күшейтуі керек. «Өзім» бейне үлгілерінің үздіксіз мәліметтерінің кіріс энтропиялары мен «Бөтен» бейнесінің үлгілері салыстырмалы:

$$H_{480}(\bar{v}) \approx H_{480}(\bar{\xi}) \quad (4.11)$$

Нейрожелілік түрлендіру жүзеге асқаннан кейін жағдай өзгереді:

$$\begin{cases} H_{256}(c) \approx 0; \\ H_{256}(x) \approx 256; \end{cases} \quad (4.12)$$

Істің мәні бойынша «Өзім» кодтарының энтропиясы қаншалықты аз болуы мен «Бөтен» кодтар энтропиясының қаншалықты 256 бит шекті мәніне жақындығы нақты түрлендірудің мінсізге жақындығын анықтайды.

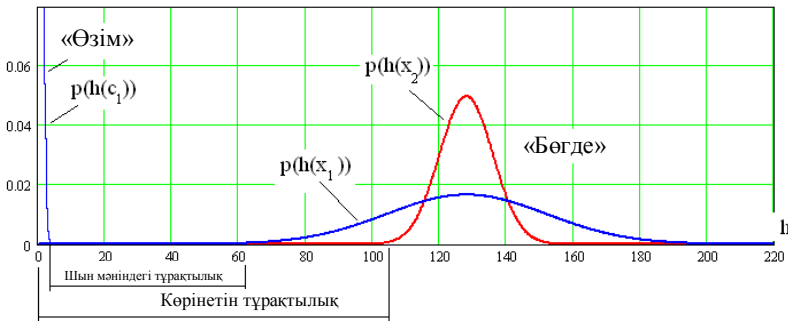
Екі қабатты нейрожелі қабаттан қабатқа өз ерекшеліктерін жақсартып барады, мұндағы бірінші қабат кодтарын 1 индексімен белгілеп, ал екінші қабат 2 индексімен жазып алуға болады:

$$\begin{cases} H_{256}(c_1) \rangle H_{256}(c_2) \approx 0; \\ H_{256}(x_1) \langle H_{256}(x_2) \approx 256; \end{cases} \quad (4.13)$$

Бұл жағдай «Өзім» кодтары мен «Бөтен» кодтары Хэмминг арақашықтығын сәйкесінше таратуда көрінеді.

4.12-суретінде берілгендей бірінші қабат нейрондарының шығысында биокод іріктеу шабуылына шамамен 56 бит тұрақтылығына ие («Өзім» және «Бөтен» Хэмминг арақашықтығын таратудың шеттері арасындағы арақашықтық). Екінші қабат нейрондары қателерді түзеткеннен кейін көпшілік арасындағы көрініп тұрған арақашықтық 100-ден артығырақ

битті құрайды, бірақ бұл күмән келтіретін (көтеріңкі) тұрақтылық. Алдын келіскен екінші қабат нейрондары тек қана «Өзім» биокодын басқарып қоймай, сонымен бірге «Бөтен» кодын да хэштейді. Екінші қабат нейрондарын хэштеуші ерекшеліктерді нейрожелілік шығыстағы «Бөтен» кодтар энтропиясына бірінші қабат нейрондарының шығысындағы биокод энтропиясының қарым-қатынасы сияқты бағалауға болады.



4.12-сурет. Нейрондардың ерекшелігін хэштеу себебінен екінші қабат нейрондарының шығысында Хэмминг арақашықтығын таратуды сығу

Желілердің екінші қабат нейрондары жеткілікті дәрежеде күшті хэштеуші ерекшеліктерге ие, бұл салмақ коэффициенттері белгілерінің кездейсоқ қойылуымен және олардың орындап жатқан суммалаудың шешімін дөңгелектендіру операциясымен түсіндіріледі. Кодтың кілтін кішірейтуге алып келетін кез келген бір бағытталған операция қысқа шығыс кодтарынан бастапқы мәліметтерді қайта қалыптастыруға болмағандықтан, кейбір хэштеуші қасиеттерге ие. Біздің жағдайда нейрон кодын жөндеуші суммалаудың шешімі 64-дан +64-дейінгі интервалда өзгере алады, ал оның шығыс коды тек «0» мен «1» екі мәніне ие. Мұнда 9 дәрежелі код ұзындығын 1 дәрежеге дейін қию операциясы қатысады.

5. БИОМЕТРИЯЛЫҚ МӘЛІМЕТТЕР ҚОРЫН ҚАЛЫПТАСТЫРУ МЕН НЕЙРОН ЖЕЛІЛЕРІН ҮЙРЕТУ САПАСЫН СЫНАУ

5.1. Шағын сынақ сұрыптамасында бірінші текті қатенің пайда болу ықтималдылығының бағасы

Биометрия-код жаңғыртушысын сынау кезінде [76] және бір маңызды сипаттаманың бірі бірінші текті қателік ықтималдығы болып табылады ("Өзім" бейнелерінің донорына кірудегі жаңылыс бас тарту). Осыған байланысты МЕСТ Р 52633.0-2006 негізгі ұлттық стандарты әрбір үйретуден кейін жетіскен нейрожелілік шешімдерді қабылдау сапасының сынағын жүзеге асыруды талап етеді.

"Өзім" бейнесінің биометриялық кодының шегіне жеткен биокодтың жұп дәрежелері мен нөлдік энтропиясын бірден-бір корреляциялауға сәйкес келетін жағдайын сипаттауға тән:

$$\begin{cases} E(|r_{i,j}|) \approx 1.0; \\ H_{256}(c) \approx 0.0; \end{cases} \quad (5.1)$$

Мұндай шегіне жеткен жағдайда барлығына ұнайтын мәліметтердің тәуелсіздігінің болжамы мүлдем жұмыс істемейді, шығыс кодының барлық дәрежелері өте мықты корреляцияланған [77 – 81]. Егер бұл болжам жұмыс істегенде, биокод мәндерінің биноминалды таралу заңына ие болар едік. Сондықтан шартты орындау кезінде биноминалды заң қандай шегіне жеткен таралуға ұмтылып жатқанын білуіміз қажет (5.1).

Жүргізілген зерттеулердің көрсетуінше, χ^2 биноминалды заң шегіне жеткен таралу болып табылады, бұл таралу бостандық дәрежесінің нөлдік санына дейін дерлік:

$$P(256, h, P_1 \rightarrow 0.0, |r| \rightarrow 1.0) \rightarrow \chi^2(\omega \approx 0), \quad (5.2)$$

мұндағы ω – k тәжірибесінде "Өзіме" бірінші бас тарту кезінде табылған Хэммингтің мөлшерленген арақашықтығын сипаттаушы, бірінші жақындаудағы бостандық дәрежесінің саны:

$$\omega = \frac{h}{k} \quad (5.3)$$

Егер k тәжірибесін өткізу кезінде Хэмминг таралуының нөлдік мәнге ие бірнеше қателері табылған болса, онда χ^2 таралуының бостандық дәрежелер саны Хэммингтің орташа ара қашықтығы түрінде есептеледі:

$$\omega = E(h) \approx \frac{1}{k} \sum_{i=1}^k h_i \quad (5.4)$$

k тәжірибесінен тұратын бірнеше сынау жүргізгеннен кейін кіруден бас тарту дерегі анықталған жоқ, бостандық дәрежелерінің сандық есебі болжам нәтижесінде жүзеге асады, бұл келесі $(k+1)$ санауда бір биттік минималды қате табылады деген сөз:

$$\omega = \frac{1}{k+1} \quad (5.5)$$

сынақтың уақытын (сынақ сұрыптамасының көлемі) үштен 10 дейін қысқарту үшін бірінші текті қате ықтималдығының бағасын мына формула бойынша орындаған жөн:

$$P_1 \approx \int_1^{\infty} \frac{1}{2^{\frac{\omega}{2}} \cdot \Gamma\left(\frac{\omega}{2}\right)} \cdot x^{\frac{\omega}{2}-1} \cdot e^{-\frac{x}{2}} \cdot dx, \quad (5.6)$$

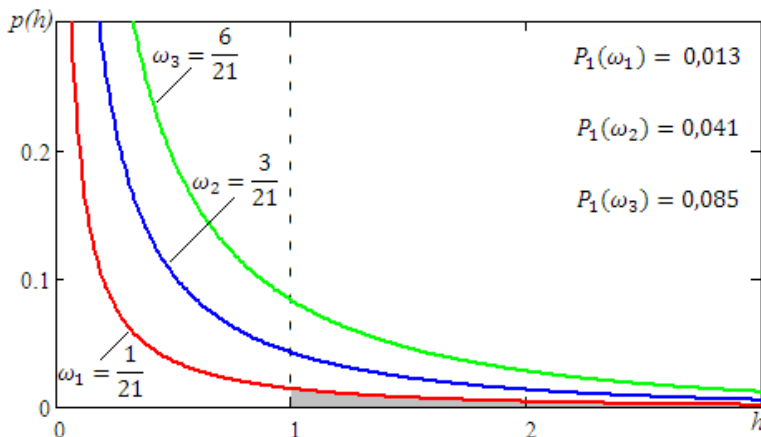
мұндағы $\Gamma(\cdot)$ – гамма функциясы.

(5.6) формуласы бойынша бірінші текті қате ықтималдығы бағасының үлгілері 5.1-суретінде келтірілген.

"Өзім" кодтарының дәрежелерінің арасындағы корреляцияның орташаланған көрсеткішін есептеу келесі формула бойынша жасалады:

$$r \approx \left(1 - \frac{2 \cdot E(h)}{n}\right) \quad (5.7)$$

яғни $n=256$ биометриялық код ұзындығы тек қана биометриялық мәліметтер арасындағы корреляцияның коэффициенттер модулін орташа бағалау кезінде белгілі бір рөл ойнап бастайды. (5.7) формуласы дәрекі жақындау болып табылады, сондықтан корреляцияның коэффициенттер модулінің жеткілікті түрде үлкен мәндеріне жұмыс істейді. Дәлірек есептеу кезінде Хэммингтің орташа квадраттық арақашықтық ауытқуын қосымша есепке алу қажет [77].



5.1-сурет. Бостандық дәрежелерінің шағын көрсеткіштер санымен хи-квадрат тарату бойынша бірінші текті қате ықтималдығы бағасының үлгілері.

Жоғарыда сипатталған жақындауды бірінші талпыныс кезінде жоғары ықтималдылықпен «Өзіме» қол жеткізуді ұсынатын биометриялық қорғаныстың жоғары қолжетімді құралдарына сынақ жүргізу кезінде қолдану керектігін айрықша айту қажет. Тек қана осы жағдайда бірінші текті қате ықтималдығын сынақ жасау проблемасы туындайды. Мысалы, бірінші талпыныстан 0.999 қол жеткізу ықтималдығы берілген болса, онда оның биязы бағасына 10 000 сынақ үлгісі қажет. Дәл осы жағдайда Хэммингтің «Өзім» өлшемдерінің таралу жақындығын бостандық дәрежесінің саны нөл көрсеткішімен хи-квадрат таралуымен қолданған жөн.

Егер бірінші текті қате ықтималдығы жоғары болса (мысалы, $P_1 \approx 0.1$), онда оның бағасы үшін 20 сынақ үлгісі жеткілікті. Бірінші текті қате ықтималдығы үлкен кезінде сынақ проблемалары олардың мәндері болмайды. Осы кезде бұл жағдай биометриялық аутентификация қосымшасының көпшілігіне тән. Заманауи биометриялық аутентификация қосымшалары бір сеанс кезінде «Өзім» бейне ұсынысының шешілген талпыныс санының ұлғаюы есебінен жоғарғы қолжетімдік проблемасын шешеді. Егер ақпараттық қауіпсіздік қамтамасыздандыру аяласы бойынша тұтынушыға «Өзім» биометриялық бейнесінің үш ұсыныс талпынысын қолдану рұқсат етілген болса, онда 1,2,3 талпыныстан рұқсат алу ықтималдығы $P_{1,1}=0.1$, $P_{1,2}=0.01$, $P_{1,3}=0.001$ құрайды. Тұтынушыға біреуінің орнына үш талпыныс беру қол жеткізу ықтималдығын 0.9-дан 0.999-ға дейін көтереді.

5.2. Екінші текті қате ықтималдығын бағалау проблемалары, биометриялық бейнелердің үлкен қорларын қалыптастыру қажеттілігі

МЕСТ Р 52633.5-2011 [82] ұлттық стандартын іске енгізіп өңдегеннен кейін әртүрлі типтегі нейрожелілік «биометрия-код» жаңғыртуларын ақпаратты қорғау құралдарының әртүрлі нарық салаларында өндіру мүмкіндігі ашылды. Сонымен бірге мұндай құралдарды тұтынушы өз жеке ақпаратының биометриялық қорғанысының анау немесе мынау құралдардың сапасына сенімді болуы керек. Егер мұндай құрал ішкі ақпаратты криптографиялық қорғау құралымен (АКҚҚ) қатар өндірілсе, онда тұтынушы биометрияның өзінің, АКҚҚ, сонымен бірге олардың түйісуінің жоғарғы сапасына сенімді болуы керек.

Программалық бөлімнің кодтарын зерттеу мен АКҚҚ құралдарын сертификаттау жақсы өңделген болып табылады. Керісінше, программалық бөлімнің кодтарын зерттеу процедурасы мен ақпаратты өте сенімді биометриялық қорғау құралдарын сертификаттау қазіргі кезде төмен зерттелген. «Өзім» биометриялық бейнелерінің әр түрлі ақпараттылығы мұндай жағдайдың негізгі себептерінің бірі болып табылады.

АКҚК-да тек қана шифрлау алгоритмі мен кілттің ұзындығы іріктеу шабуылына криптографиялық қорғаныс тұрақтылығын анықтайды. Факторлардың едәуір көп санына байланысты іріктеу шабуылының тұрақтылығы биометрияның жоғары сенімділігі артады. Осылай оған әсерін тигізеді:

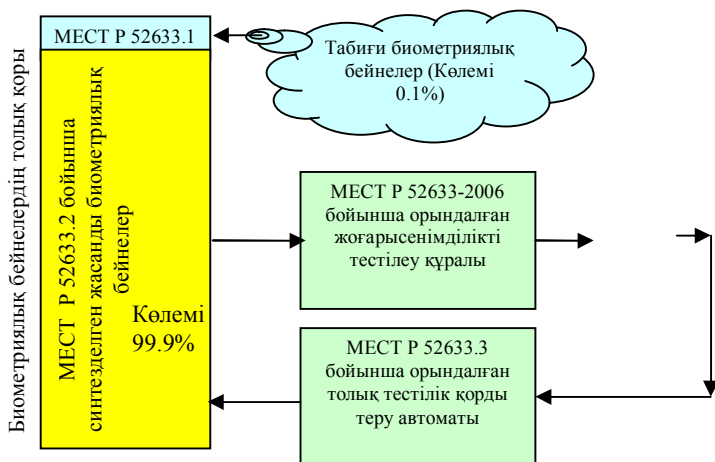
- «Өзім» биометриялық бейнесінің параметрлерінің тұрақтылық көрсеткіші;
- «Өзім» биометриялық бейнесінің параметрлерінің бірегей көрсеткіші;
- үйрету кезінде қолданылған «Өзім» бейне үлгілерінің саны;
- үйретудің алгоритмін жүзеге асыру сапасы;
- ақпаратты биометриялық қорғау құралдарымен (АБҚК) ескерілген биометриялық параметрлер саны;
- АБҚК шығыс кодының ұзындығы;
- ішкі бақылаушыдан АБҚК параметрлерін қорғау үшін тұтынушы қолданған өзін-өзі шифрлау алгоритмі немесе хэштеу.

Өзара ықпал етуші факторлардың соншалықты көптеген санының сыпайы аналитикалық есебі бүгінгі күні мүмкін емес. Осыған байланысты үйретілген нейрожелілік биометриялық-код жаңғыртушысын тәжірибелік сынақтан өткізуді ұйымдастырудың рөлі артады. Өкінішке орай, бұл зерттеудің бағыты үлкен көлемдегі биометриялық бейнелердің сынақ қорын дайындауға көптеген материалдық шығындармен кездеседі.

Жоғарыда айтылғанды 1 000 000 000 талпыныс көлемінде іріктеу шабуылына тұрақтылығымен «биометрия-код» жаңғыртушысын сынақтан өткізу үлгісін көрсетейік. Бұл мақсатқа жету үшін «Бөгде» [83, 84] кездейсоқ бейнелерінің 1 000 000 000 үлгісінен құралған сынақ қорына ие болу қажет. Егер «биометрия-код» жаңғыртушысы қолжазба бейнелерімен жұмыс істесе, онда сынақ қоры да «Бөгде» қолжазба бейнелерінің 10^9 ие болуы керек. Осындай қолжазба бейнесінің біреуін жазуға 5 секундтай уақыт қажет. Демек миллиард қолжазба бейнесін бір адамның жазуына 5×10^9 секунд немесе үздіксіз хат жазудың 160 жылы қажет болады. Егер жазушы тәулігіне 8 сағат жұмыс істесе уақыт үш есеге артады да 480 жылды құрайды. 1000 адамды жұмысқа жұмылдыру кезінде

сынақ бейнелерінің қажетті қорын шамамен жарты жылда жинап алуға болады. 1000 адамнан құралған ұжымның жарты жыл шамасында үздіксіз жұмысы өте көп материалдық шығынды қажет етеді. Осыған байланысты МЕСТ Р 52633.2-2010 [85] стандарты биометриялық бейнелердің табиғи қорын табиғидан алынған синтетикалық биометриялық бейнелермен толықтыруды ұсынады. Тәжірибенің көрсетуі бойынша қос табиғи биометриялық бейнелер аталық морфингімен және мутациямен алынған синтетикалық бейнелерді қосқандықтан биометриялық бейнелер қоры 1000 есеге өсуі мүмкін.

Осындай сынақтың блок-сұлбасы 5.2-суретінде бейнеленген.



5.2-сурет. Миллиард бейнелер ішінен толық қорды сақтаумен «Бөгде» биометриялық бейнелерін іріктеудің классикалық сұлбасы бойынша сынақ жүргізудің блок-сұлбасы

Биометриялық бейнелер қорын қалыптастыру үшін шығынды 1000 есеге төмендету проблеманы шешіп сынақты стандарт бойынша жүзеге асырады деп ойлауға болады, бірақ бұл олай емес. 10^6 табиғи биометриялық бейнелерді сақтау үшін 32 000 Гб жады қажет болады. Бүгінгі күнге мұндай жадылы сервер таңсық емес, бірақ бүкіл осы жадыны кезектегі оқу мен ақпараттан алынған кезектегі нейрожелілік өңдеу процедурасы

машиналық уақыттың бірнеше аптасын алады. Осыған байланысты сынақ тапсырмасын шешуде есептеу қаржысы мен уақыт шығынын аз жұмсайтын арнайы шара қабылдаған жөн.

«Дөрекі күшпен» толық іріктеудің классикалық әдісінен бас тартудың қажеттілігі, бұл әдістің тек қана дискреттік криптографияға пайдасымен байланысты, әрі биометрияның анық бағасына кепілдік бермейді. Дискреттік криптографиялық кілттің болуы мүмкін жағдайдың жазықтығы реттелген, әрине сонымен бірге ол тегіс тығыздығына ие, сондықтан мұндай жағдайда оны толық іріктеу тапсырмасын қарастырған дұрыс. «Өзім» үздіксіз биометриялық бейнелерінің болуы мүмкін қалпының жазықтығы шексіз және шындыққа жататын бейнелердің жайғасу тығыздығы бойынша бір текті емес. Жазықтықты толық іріктеуден өткізу үшін қажет:

- 1) «Бөгде» биометриялық бейнелерін өзара реттеу;
- 2) Сынақ қоры «Бөгде» бейнелерінің орналасу тығыздығының «Өзім» бейнесін іздеп табушы ауданында сиректеу ауытқуына ие емес екендігіне кепілдікке ие болу;
- 3) «Өзім» бейнесіне шағын арақашықтықта «Бөгде» бейнелерінің жақындау дерегін анық бейнелеуші берік жұмсақ индикаторларға ие болу.

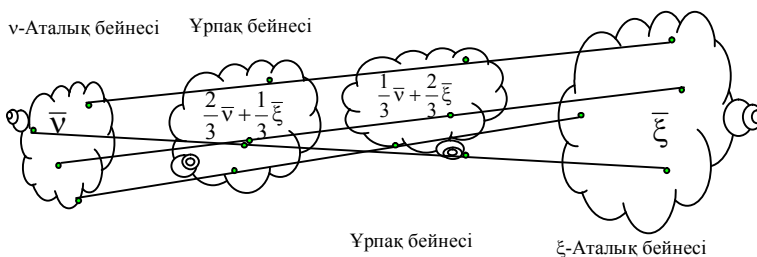
Жоғарыда айтып өтілген бірде-бір тапсырма бүгінгі күні шешілген жоқ, сондықтан «Бөгде» толық биометриялық бейнелер қорының сенімді іріктелуін ұйымдастыру бүгінгі күні мүмкін емес. Кілтті толық іріктеуді ұйымдастыру үшін тек қана криптографияда қолданылатын күшті есептеу құрылғысына ие болу қажет. «Өзім» жасырын биометриялық бейнелеріне қолданылатын күшті есептеу құрылғыларының бары жеткіліксіз: биометриялық бейнелердің жеткілікті дәрежедегі және дұрыс қалыптасқан үлкен қорына, сонымен бірге жоғарыда айтылған өз шешімін таппаған үш тапсырманың қанағаттанарлық шешіміне ие болу қажет.

Ертелі-кеш жоғарыда айтылған тапсырмалардың қанағаттанарлық шешімі табылған жағдайда ғана сынақ қорын толық «күшпен» іріктеу санаулы эксперименті жүзеге асуы мүмкін. Мұндай санаулы эксперимент көптеген материалдық және уақыт шығынына алып келеді, дегенмен бұл шығындар ақыр аяғында

өзін-өзі ақтайды. Тек қана тікелей санаулы эксперимент анау немесе мынау фирманың орындауында жеке ақпаратты «Өзім» жасырын бейнесімен биометриялық қорғау өте сенімді болып табылатындығына сенімді дәлел бола алады. Тек қана «Бөгде» биометриялық бейнелердің толық сынақ қорын тікелей іріктеу «күшпен», іріктеу шабуылына, анау немесе мынау «биометриялық-код» жаңғыртуының тұрақтылығын бағалаудың жеңілдетілген әдістерін растауы немесе жоққа шығаруы мүмкін.

5.3. Биометриялық бейне үлгілерінің тоғысуы арқылы көбеюі

Техникалық тұрғыдан табиғи биометриялық бейнелер қорын жасау қиын болғандықтан, кейбір табиғи биометриялық бейнелер қорының ядросын қалыптастыру мүмкіндігін беретін және оны қажет кезінде керекті көлемге дейін көбейтетін технологияға ие болуы қажет. Әрі қарай көбею дегенде биометриялық ұрпақтар-бейнелері параметрлерінен биометриялық аталық-бейнелері параметрлеріне сызықты көшіру процедурасын түсінеміз. Мұндай жақындық биологиядан алынған, сондықтан «генетикалық алгоритмдер» атауын алды [77, 85]. 5.3-суретінде $\bar{v}_i$, $\bar{\xi}_i$ биометриялық параметрлердің үлгілері векторлармен көрсетілген биометриялық ұрпақтар-бейнелерімен екі биометриялық аталық-бейнелерінің тоғысу жолымен генетикалық көбею технологиясы бейнеленген.



5.3-сурет. Екі биометриялық аталық бейнелері үлгілерінің морфингпен көбеюі

$\bar{V}_1, \bar{V}_2, \bar{V}_3, \dots, \bar{V}_{20}$ биометриялық параметрлердің k векторымен ұсынылған аталық-бейнесі- v басынан бастап 20 үлгіден және де сонша $\bar{\xi}_1, \bar{\xi}_2, \bar{\xi}_3, \dots, \bar{\xi}_{21}$ биометриялық параметрлердің қайтадан сол k векторымен ұсынылған аталық-бейнесі-- ξ бар деп болжап көрейік. Біз екі биометриялық аталық- бейнесінен екі ұрпақ-бейнесін алуымыз қажет. Егер бірдей қашықтықтағыларды өзара және ұрпақ-бейнесін ең жақын аталығымен синтездесек, онда бірінші ұрпақ-бейнесін синтездеу кезінде v - бейне үлгісінің $2/3$ бөлігімен ξ -бейне үлгісінің $1/3$ бөлігін қолдану қажет.

$$v'_{i,k} = \frac{2}{3}v_{i,k} + \frac{1}{3}\xi_{j,k}, \quad (5.8)$$

мұндағы i - v -Аталық бейнесінің үлгі нөмірі сонымен бірге ұрпақ-бейнесінің үлгі нөмірі;

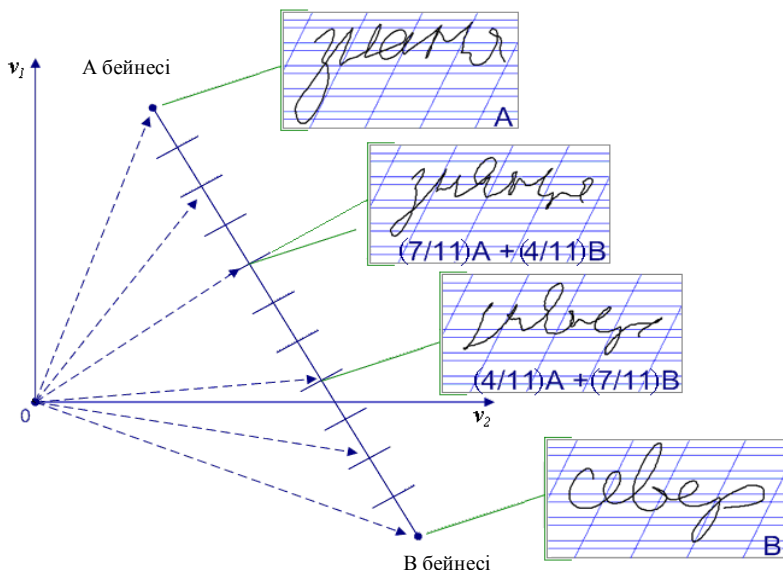
k - биометриялық параметрдің есепке алынған нөмірі;

j - ξ - аталық бейнесінің үлгі нөмірі.

ξ - аталық-бейнесіне жақындау екінші ұрпақ-бейнесінің вектор үлгілері параметрлерімен ұқсас есептеледі:

$$\xi'_{j,k} = \frac{2}{3}\xi_{j,k} + \frac{1}{3}v_{i,k} \quad (5.9)$$

Егер екі ұрпақ-бейнелерінің синтезі жеткіліксіз болса, онда олардың санын аталық-бейнесі параметрлерінің арасындағы арақашықтығын көптеген сан бөліктеріне бөлу арқылы көбейтуге болады. 5.4-суретінде екі бейненің биометриялық параметрлерінің арасындағы арақашықтықты 11 ұрпақ-бейнесін алу үшін 11 бөлікке бөлу үлгісі келтірілген.



5.4-сурет. Биометриялық қолжазба бейнелерінің екі нұсқасы
«знамя» және «Север»-дің морфингпен көбею үлгісі

Жоғарыда сипатталған тәсілмен ұрпақ-бейне өте көп үлгілерінің санын синтездеуге болады. Әрбір аталық-бейнелері үлгілерінің мүмкін болған жұбы ұрпақ бейнелерінің әр түрлі үлгілерін береді. Сондай-ақ v -аталық бейнесінің 20 үлгісі бір ғана ξ -аталық бейнесінің үлгісін қолдану кезінде әр бір ұрпақ-бейнелерінде 20 үлгіден тудырады (ξ -аталық бейнесінің 21 үлгісіне ғана иеміз). Демек, қажет кезінде әрбір екі ұрпақ-бейнесінің үлгілері $20 \cdot 21 = 420$ дейін алуға болады.

Негізінде ұрпақ-бейнелері үлгілерінің көбеюі арқылы морфинг-көбеюінің маңызды қасиеті, бұл олардың өз аталығының бейнесін барлық статистикалық сәттерін мұраға алуы болып табылады. Сонымен бірге математикалық болжал векторларының, биометриялық параметрлердің арасындағы өзара байланысының корреляциялық матрицасы мен орташа квадраттық ауытқу векторларының мұралануы болады. Осы статистикалық сәттердің барлығы өте қажет сипаттама

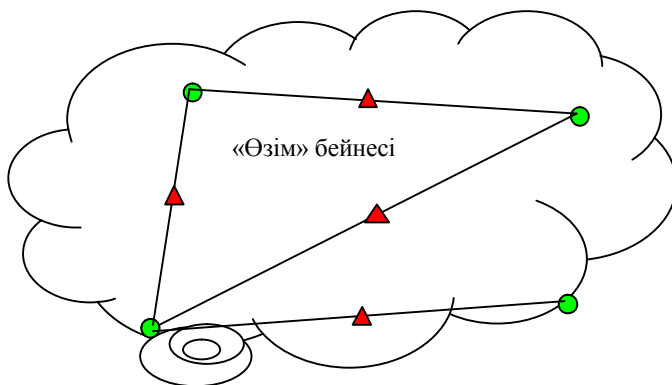
болып табылады және синтезделген биометриялық бейнелердің дұрыстығына олардың жаңғыруысыз сенімді болуға болмайды.

Биометриялық бейнелердің үлгілерін тоғыстырумен көбею технологиялық амалы тек ұрпақ-бейнелерін қалыптастыру кезінде ғана ұтымды емес. Бұл амал жасанды нейрондық желілерді үйрететін кіші сұрыптауларда үйрету кезінде де өте тиімді болып табылады. Әдетте биометриялық жүйелерді қолданушылар «Өзім» биометриялық бейнелерінің 12-ден 16-ға дейін үлгілерін ұсынуы қажет.

Бұл 12-ден 16-ға дейінгі кіріс нейрондары бар, нейрондарды тұрақты түрде үйретуге мүмкіндік береді. Көп санды кіріс нейрондарын тұрақты үйрету үшін, үйретуші сұрыптаудың көлемін үлкейту қажет.

Егер қолданушы жоқ болса немесе қосымша биометриялық бейнелерді қалпына келтіру қажеттігін жағымсыз қабылдаса, онда «Өзім» биометриялық бейнелер үлгілерінің көбею процедурасы морфинг арқылы қолданылуы әбден мүмкін.

«Өзім» бейнесі үлгілерінің көбею процедурасының суреттемесі 5.5-суретінде берілген, мұндағы дөңгелекпен бастапқы төрт биометриялық үлгі белгіленген, ал үшбұрышпен синтезделген үлгілер берілген. «Өзім» бейнесінің қосымша үлгісінің синтездеу алгоритмі екі үлгінің іздеуінде, өзара максималды Евклидтік арақашықтық векторларына ие j және m нөмірлерімен олардың биометриялық параметрлері тұр:



5.5-сурет. «Өзім» бейнесі үлгілерінің морфингпен көбеюі

$$\max \sqrt{\sum_{i=1}^k (v_{j,i} - v_{m,i})^2} \quad j \neq m \text{ үшін.} \quad (5.10)$$

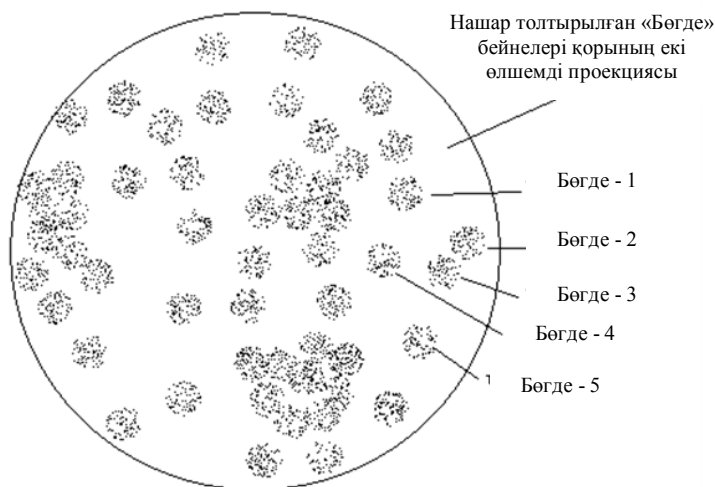
Осы суреттен көрініп тұрғандай белгісіз параметрлердің азғантай саны жеткілікті дәрежеде тез теріп алынады: машиналық уақыттың бірнеше минутында. Теріп алынатын кіріс сандарының артуы алдында бар болған үлгілерді теру уақытының өсуімен «Өзім» бейне үлгісін терудегі қажетті санының өсуіне алып келеді. Әрбір жаңа үлгімен толықтырылған сұрыптау үшін өзара ұқсамайтын ерекше жұп үлгілер қайта табылады, сонымен бірге бұл аталық-үлгілері тең мөлшерде тоғыстырылады.

5.4. «Барлығы бөгде» көп өлшемді кеңістігін біркелкі толықтыратын биометриялық бейнелер қорының синтезі

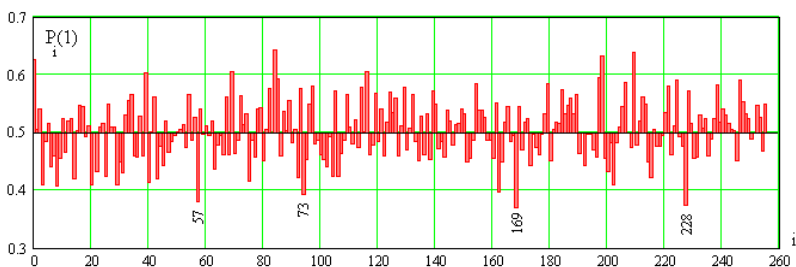
Биометриялық бейнелердің табиғи қорын қалыптастыру кезінде әдетте бар мәліметтер (жинап үлгерілген мәліметтер) қолданылады. Егер қорды толықтыру қажет болса, онда оны кездейсоқ адамдарды таңдап олардан кездейсоқ бейнелерді ала отырып толықтырған дұрыс (биометриялық құпия сөздерді немесе қолжазба құпия сөздерін жинау жағдайында бұл әбден болуы мүмкін). Кездейсоқ алынған «Бөгде» биометриялық бейнелерімен «Барлығы бөгде» көп өлшемді кеңістігін біркелкі толықтыруға кепілдік беруге болмайды. Демек, қорды сынақ жүргізу үшін қолданбастан алдын ең кем дегенде көп өлшемді қорды оның бастығын толықтыра отырып, тегістеу қажет. «Бөгде» бейнесі қорының «нашар» толықтырылған екі өлшемді кескіні 5.6-суретінде берілген.

Қорды толықтырудың біркелкі еместігін бағалау үшін кез келген «Өзім» биометриялық-кодтың үйретілген нейрожелілік жаңғыртушысын алсақ жеткілікті, әрі қарай оның кірісіне барлық тегістеу қорының бейнелерін берген жөн. «Бөгде» көп өлшемді кеңістігінің жақсы толықтырылған көріністері шығыс кодының сәйкес келетін дәрежелерінде «0» және «1» тең ықтималды

жағдайларын беруі тиіс. Керісінше, биометриялық мәліметтердің дұрыс емес теңдестіруімен көп өлшемді кеңістіктің бөлімдері «0» және «1» жағдайларының елеулі біркелкі еместігін беруі керек. 5.7-суретінде «Бөгде» қорының барлық бейнелері көріп шығуынан алынған биокод дәрежелерінде «1» жағдайының пайда болу ықтималдығының таралу үлгісі берілген.



5.6-сурет. «Бөгде» биометриялық бейнесінің тесттік қорын толықтырудың біркелкі еместігі



5.7-сурет. «Бөгде» қорының барлық бейнелері көріп шығуынан алынған биокод дәрежелерінде «1» жағдайдың пайда болу ықтималдығының таралуы

5.7-суретінен көрініп тұрғандай, 57, 73, 169, 228 дәрежелеріндегі «1» жағдайдың пайда болу ықтималдығы ең кішісі. Бұл биометриялық бейненің жетіспеуінің салдары болып табылады. Осылай болмағанда ол бұл дәрежелерде «1» жағдайын берер еді. Ол үшін аталық бейнелерін табу қажет, сонда ғана айтып өтілген барлық дәрежелерде жетіспейтін «1» жағдайын берер еді. Әрі қарай осындай аталық бейнелерінің екеуін тандап олардан ұрпақ бейнесін алу қажет. Қажетті қасиетке ие аталық бейнелері жеткілікті түрде көп (барлық «Бөгде» бейнелерінен $1/32$) болғандықтан оларды іздеу мәселесі туындамайды. Синтезделген ұрпақ-бейнесі сиректетілген көп өлшемді «Бөгде» қорының кеңістігіне түседі.

Әлбетте, жетіспеген мәліметтерге бола және де олардан ұрпақтар-бейнесін ала отырып, аталық бейнесін жүйелі түрде іздеуді қайталай бергеннен біз «Бөгде» бейнелерінің қорындағы сиректетілуді біртіндеп толықтыра бастаймыз. Жоғарыда сипатталған процедураны «Бөгде» биометриялық бейнелердің сынақ қоры қажет көлемге ие болғанша жүргізу керек. Нейрондық желі таңдаған «Өзім» тудыратын бір тексіздікті жоққа шығару үшін, қорды толтыру кезінде бірнеше үйретілген жасанды нейрондық желілерді «Өзім-1», «Өзім-2», «Өзім-3», ... қолдану қажет.

Егер биометриялық бейнелердің үлкен сынақ қорларын жасау қажет болса, онда әрбір дәрежедегі «0» және «1» жағдайының біркелкілігі жеткіліксіз болады. Бұл жағдайда дәрежелердің өз бетінше таңдалған жұбында жағдайдың пайда болу біркелкілігін бақылауға өту қажет. «00», «01», «10», «11» жағдайларының пайда болу тең ықтималдылығын бақылаған жөн. Сонымен бірге жетіспейтін жағдайлардың қорғаушысы болып табылатын аталықтарды көбейту керек.

5.5. Жұп корреляциялық байланыстардың орташаланған модулі бойынша іріктеу шабуылына тұрақтылықты жылдам бағалау

«Бөгде» биометриялық кодтарының толық тәуелсіздігі кодтардың бірізділігіне «ақ шу» береді. Мұндай бірізділіктер биометриялық кодтың ұзындығына дәл сәйкес келетін энтропияға ие болады:

– өзге шегіне жеткен жағдайда, яғни кодтардың барлық дәрежелері абсолютті түрде корреляцияланған жағдайда жалғыз ғана «Бөгде» кодының энтропиясы кодтардың ұзындығынан тәуелсіз болады:

$$\begin{cases} E(|r_{ij}|) = 1; \\ H(n) = 1; \end{cases} \quad (5.11)$$

Жалпы жағдайда «Бөгде» кодтарының шығыс энтропиясы үш өлшемді функциямен сипатталады:

$$H(n, E(|r|), E(P_{2,i})) = (\beta(n, E(|r|), E(P_{2,i})) \cdot (n - 1) + 1) \cdot H(1) \quad (5.12)$$

мұндағы $H(1)$ – барлық шығыс код дәрежелерінің бір өлшемді энтропиясының орташа мәні,

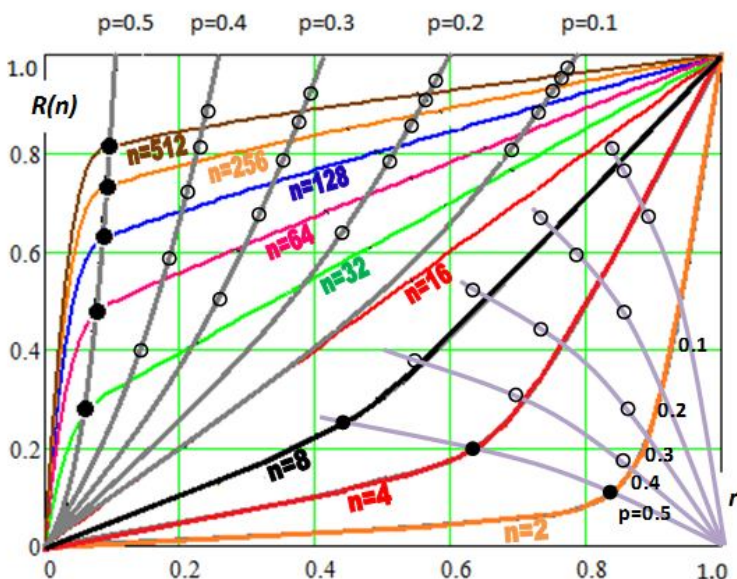
$P_{2,i}$ – «Бөгде» код i -дәрежесі үшін екінші текті қатынастың ықтималдығы.

(5.12) сипаттамасының формасының қолайлылығы бұл оның биометриялық-кодтың әрбір шығыс дәрежелерінен бір өлшемді дара энтропиясының орташа мәндегі және көп өлшемді энтропия байланысының үш өлшемді мультипликативті дерлік коэффициентін құрауында. Маңыздырақ $E(P_{2,i})=0.5$ жағдай үшін екі өлшемді мультипликативті дерлік коэффициент байланысының номограммасын құрдық [77, 86]. Бірақ бұл амал нәтижелі болмады, себебі осы сияқты қисық номограммалар өте күрделі аналитикалық тәуелдікпен сипатталады. Көп өлшемді энтропияның және бір сипаттау жолы көп өлшемді корреляциялық функцияға сүйене отырып құралған. Функцияның бұл типі энтропияның көп өлшемді функциясының қарым-қатынасы арқылы енгізіледі:

$$R(n) = \left\{ 1 - \frac{H(n)}{n \cdot H(1)} \right\} = \left\{ 1 - \frac{H(n)}{\sum_{i=1}^n H_i(1)} \right\} \quad (5.13)$$

мұндағы $H_i(1)$ – i дәрежелі бір өлшемді энтропия.

Қарапайым екі өлшемді r корреляция $R(2)$ сәйкес келеді. Жоғары өлшемдіктің мәнділігі үшін r мен $R(n)$ өзара 5.8-суретінде келтірілген номограммамен байланысты. 5.1-кестесінде келтірілген мәліметтер бойынша құрылған номограмма.



5.8-сурет. r - қарапайым корреляциялық функция модульдерінің орташаланған мәнді $R(n)$ корреляциясының жоғары көлемдік мәндер байланысының номограммасы

5.1-кесте

$P = 0.5$ параметрі үшін 1-сурет қисық мәндері

		Көп өлшемді корреляция мәні $R(n)$											
		Екі өлшемді корреляция											
		0,00	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00	
N өлшемді	2	0,00	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,09	0,30	1,00	
	4	0,00	0,03	0,05	0,08	0,11	0,13	0,18	0,32	0,53	0,76	1,00	
	8	0,00	0,06	0,10	0,15	0,23	0,33	0,43	0,57	0,71	0,86	1,00	
	16	0,00	0,10	0,21	0,32	0,42	0,51	0,62	0,71	0,82	0,90	1,00	
	32	0,00	0,32	0,39	0,47	0,55	0,62	0,70	0,77	0,85	0,92	1,00	
	64	0,00	0,50	0,56	0,62	0,67	0,73	0,78	0,84	0,89	0,95	1,00	
	128	0,00	0,63	0,68	0,72	0,77	0,81	0,84	0,88	0,92	0,96	1,00	
	256	0,00	0,74	0,77	0,81	0,84	0,86	0,89	0,92	0,95	0,97	1,00	
	512	0,00	0,81	0,84	0,87	0,89	0,91	0,93	0,95	0,96	0,98	1,00	

5.8-суретінен көрініп тұрғандай, r - қарапайым корреляциялық функциясы модульдерінің орташаланған мәнді $R(n)$ корреляциясының жоғары көлемдік қисық байланысы айтарлықтай маңызды сызықты бөлімдерге ие. Бұл мағыналы функцияның екінші номограммасымен байланыстыратын біртектілікпен байланысты. Энтропия-корреляция номограммасының күрделілігінің себебі оның әртекті параметрлерді байланыстыруында [77]. 5.8-суретінен көрініп тұрғандай, қисықтың маңызды бөлімдері айтарлықтай сызықты функциялардан құралған (қисықтар сызықты көріністердің сплайн тоғысуының сызықты-тілім жақындауымен жақсы сипатталады). Сызықты бөлімдердің сплайн қиысуы параболада орналасуы өте ыңғайлы болып табылады (5.8-суретінде нүктелер қара түспен белгіленген). Басқа параболалар мен өзге сплайн қиысу нүктелері қосымша шарттың әрбірі үшін $P=0.4$, $P=0.3$, $P=0.2$, $P=0.1$ пайда болады. Бұл мәліметтер 5.2-кестесінде келтірілген.

5.2-кесте

Әр түрлі параболаларда орналасқан сызықты бөлімнің
сплайн қиысу нүктелерінің координаттары

Координаталар (r; R(n))						
		p параметрі				
		0.5	0.4	0.3	0.2	0.1
N өлшемді r параметрі	2	(0.84;0.12)	(0.86;0.18)	(0.85;0.28)	(0.86;0.48)	(0.88;0.68)
	4	(0.63;0.21)	(0.71;0.32)	(0.73;0.43)	(0.78;0.61)	(0.86;0.77)
	8	(0.44;0.25)	(0.54;0.38)	(0.63;0.52)	(0.73;0.66)	(0.85;0.82)
	32	(0.05;0.28)	(0.14;0.40)	(0.26;0.50)	(0.43;0.63)	(0.68;0.80)
	64	(0.06;0.48)	(0.18;0.59)	(0.32;0.67)	(0.51;0.78)	(0.72;0.89)
	128	(0.07;0.63)	(0.22;0.71)	(0.35;0.78)	(0.54;0.84)	(0.75;0.92)
	256	(0.08;0.73)	(0.23;0.81)	(0.38;0.86)	(0.56;0.91)	(0.76;0.96)
	512	(0.09;0.82)	(0.24;0.89)	(0.39;0.92)	(0.57;0.95)	(0.77;0.98)

Барлық қиысу нүктелерінің координаттары параболааның екі типінде жатыр. 16-дан жоғары өлшем үшін параболалар 1-суреттің төменгі сол бұрышында орналасқан жалпы нүктеден (нүктесі $R(n)=0$, $r=0$) құралады. төмен өлшемділік үшін параболалар 1-суреттің төменгі оң бұрышында жалпы нүктеге ие (нүктесі $R(n)=0$, $r=1$). Бірінші және екінші параболааның мәліметтері 5.3-кестесінде жинақталған.

5.3-кесте

Сызықты бөлімдер қиысу нүктелерінің орналасуын сипаттаушы
параболалар

Көп өлшемді корреляция полиномы $R(n)$		
Параметр	Екі өлшемді корреляция r	
	Өлшем $n=32, 64, 128, 256, 512$	Өлшем $n=2, 4, 8$
p=0.5	$56.19r^2 + 1.59r$	$-0.42r^2 + 0.15r + 0.27$
0.4	$5.86r^2 + 2.12r$	$-1.19r^2 + 0.98r + 0.20$
0.3	$2.54r^2 + 1.01r$	$-1.02r^2 - 0.11r + 1.13$
0.2	$1.47r^2 + 0.58r$	$-4.17r^2 + 4.51r - 0.33$
0.1	$0.83r^2 + 0.59r$	$-62.5r^2 + 112.5r - 50$

Жоғарыда айтылғандардың барлығынан көріп тұрғанымыздай, $n = 16$ өлшемділігі ерекше рөл ойнайды, ол 16 өлшемді және 2 өлшемді корреляцияның арасындағы сызықтық байланысына ие:

$$R(16) = r \quad (5.14)$$

16-ға дейін және кейінгі өлшемділігі кезінде энтропия мен корреляциялар әр түрлі иілген (дөңес) байланысқа ие. $n = 16$ өлшемділігі – шекара, қарапайым көп өлшемді жаңғырту мен жоғары мөлшерлі жаңғыртуды бөлетін шекара (шекараның дәл мәні $n=15.471$).

Жоғарыда айтылған амалдың артықшылығы шығыс биометриялық кодтарының көп өлшемді энтропиясын есептеу уақытын айтарлықтай тездетуден құралған. Сонымен бірге бұл көп өлшемді корреляция әдісі табиғи тілдер (орыс, қазақ, ағылшын) энтропиясын бағалау үшін қолданылуы мүмкін [77, 87]. Сондай-ақ берілген әдіс энтропияны табиғи тілдер мәтіндерінің байланысқан ұзын кодтарына 256 әріпке дейін бағалауға мүмкіндік береді. Жанында тұрған 256 әріптің бірізділігі үшін орыс тілі энтропиясын есептеу кезінде әдісті қолданғанда 10^{104} есе (104 дәрежесінде он) есептеу жылдамдығына жетісуге болады. Бұл өте сирек кездесетін жағдайлардың пайда болуын күтудің қажеті жоқтығының салдары. Жоғарыда көрсетілген номограммалар кодтардың ең кіші көлемдерін талдай отырып, сирек кездесетін жағдайлардың пайда болуын болжауға көмек береді. Болжап табу ықтималдық көрсеткішінің және корреляция модулінің мәнін орташа есептеу үшін 200-ден 10 000-ға дейінгі кодтан құралған кіші сұрыптау жеткілікті.

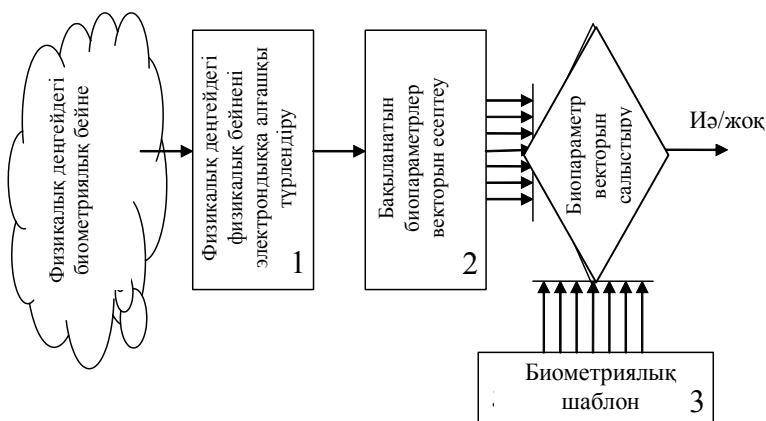
6. БИО-МӘЛІМЕТТЕРДІҢ КРИПТОГРАФИЯЛЫҚ ҚОРҒАНЫСҚА ИЕ ЕМЕС АҚПАРАТЫНА ҚОЛ ЖЕТУДЕН БИОМЕТРИЯЛЫҚ ҚОРҒАЙТЫН ҚҰРАЛДАРҒА ТӨНЕТІН ҚАУІПТЕР ЖӘНЕ ОСЫ ҚАУІПТЕРДІ ЖҮЗЕГЕ АСЫРУШЫ ШАБУЫЛДАР

6.1. «Соңғы» битке шабуыл арқылы ақпаратты қорғау программасының модификациясына төнетін қауіп

Әдетте ақпаратты криптографиялық емес қорғау құралдары программалық және аппараттық болып бөлінеді. Ақпаратты криптографиялық емес қорғау аппараттық құралдары сенімдірек болып есептеледі, себебі оларда орналасқан программалық камтамасыздандыру зерттеу мен модификациялау үшін қолжетімсіз.

Ақпаратқа қол жеткізу қорғаныс құралдары соның ішінде биометриялық қорғаныс құралдары программалы орындалғанда мүлдем өзге жағдай туындайды. Программалық қорғаныс көшірілген болуы мүмкін және әрі қарай оны зерттеп, модификация жасалуы мүмкін. Әдетте программалық қорғанысқа бұзушылар тек оны көптеген адамдар қолданған жағдайда ғана шабуыл жасайды да программалық қорғанысты бұзғаннан кейін жетістікті таралымға шығару мүмкіндігі пайда болады. Программалық қорғанысты бұзудың ең қарапайым әдісі ережені шешетін «соңғы» битті іздеу болып табылады. Ережені шешетін «соңғы» битті биометрикалық-нейрожелілік қорғанысты жүзеге асыратын үлгісі 6.1-суретінде келтірілген.

Көрініп тұрғандай, биометриялық қорғаныс кері функциясын («Бөгделерді» өткізеді де, «Өзімді» тоқтатады) орындауы үшін, ережені шешуші «соңғы» битті инвертациялау жеткілікті. Биометриялық үлгі ауысқанда немесе биометриялық параметрлердің өзгеруі мүмкін шекаралар кеңейгенде модификация шабуылының нұсқалары жетілдірілген болуы мүмкін. Осы шабуылдардың барлығы жетістікке алып келеді, бірақ олардың жағымсыз жері бұл олардың оңай таралымға шығуында. Дәл осы себептен программалық қорғаныс аппараттыққа қарағанда әлсіз деп есептеледі.



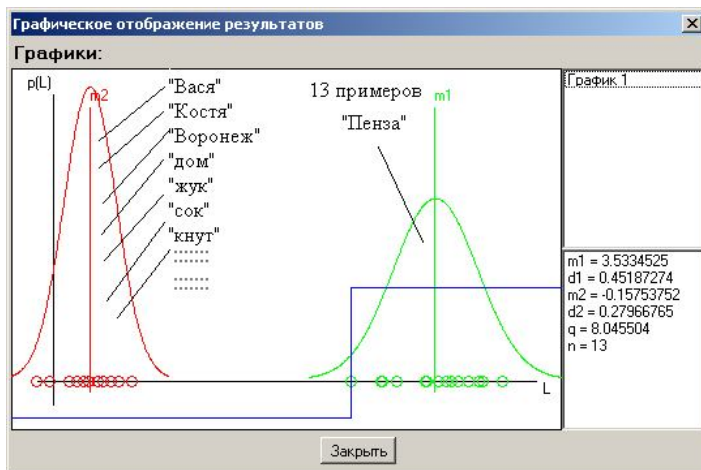
6.1-сурет. Ережені шешуші «соңғы» биті бар биометрикалық-нейрожелілік қорғаныс

Биометриялық программаларды модификациялаудан қорғау екі әдіспен жүргізіледі. Біріншіден программаны қоспастан алдын оның бүтіндігін қадағалаушы сенімді есептеу ортасын қолдануы мүмкін. Екіншіден «соңғы» биттің біреуінің орнына «соңғы» биттің 256 қолданылуы мүмкін. Бұл жағдайда мүмкін болған 256 бит жағдайларының барлығын іріктеу есептік жақтан өте қиын. Қорғаныстың осы екінші жолына берілген кітап арналған.

6.2. «Бөгде» бейнелерінің үлкен қорын іріктеу шабуылы арқылы биометриялық егіздерді іздеу қауіпі

«Бөгде» бейнелер қорынан биометриялық егіздерді іздеу және бір тиімді қауіп болып табылады. Біз егіздерді көрген кезімізде олардың соншалықты ұқсастығының себебінен шатыстырамыз. Биометриялық егіздерді ажырата алмайтын биометриялық автоматтар да тура осы жағдайға түседі. Осы жағдайды қаскүнемдер пайдалануы мүмкін. Шабуыл жасап отырған биометрияны білетін олар шабуыл жасаушы егізді тауып, «Бөгде» бейнелерінің үлкен қорынан пайдалануы

мүмкін. «Өзім» (суреттің сол жағы) бейне үлгілерінің таралуы мен «Бөгде» (экрандық пішіннің сол бөлігі) бейнелерінің таралуы берілген бұл жағдай 6.2-суретінде бейнеленген.



6.2-сурет. «НейроҮйретуші» модельдеу ортасында нейронды үйрету шешімдері қорытындысының экрандық пішіні

Сурет деректері барлық нейрондық желілерді екі классқа бөлетін классикалық алгоритмдермен сипатталатын жағдайды қамтып көрсетеді. Суреттен көрініп тұрғандай функция шегі «Бөгде» бейнелерінің таралу ортасынан алыста «Өзім» таралуының шекарасында іске қосылады. Осы себептен шабуыл жасаушының «Өзім» бейнесіне жақын «Бөгде» үлкен қорында «айтарлықтай» немесе «толық» егіз болып табылатын бейнелерді табу мүмкіндігі пайда болады. Биометриялық егізді анықтағаннан кейін оны «шынайы» биометрия донорының орнына жіберуге болады. Биометриялық автомат биометриялық егіздердің арасындағы ерекшелікті байқамайды.

Егіздерді іздеу шабуылына МЕСТ Р 52633.0 -2006 және МЕСТ Р 52633.5 – 2011 талаптарына сәйкес «Бөгде» бейнелері таралуының ортасында ереже шешушінің орналасуы ең тиімді қарсы әрекет болып табылады. Сонымен бірге шабуыл жасаушы рұқсат кілтінің кодын білмей тұрып, егізді таба алмайды. Егер

шабуыл жасаушы рұқсат кілтінің кодын немесе шабуыл жасаушы биометриялық бейнені дәл білсе ғана, ол биометриялық егізді таба алады. «Бөгде» көпшілігінің ортасындағы нейрожелідегі барлық нейрондарды кванттау функциясын ауыстыру шегінің орналасуы мен нейрондардың көпшілігін қолдану биометриялық егіздерді табу шабуылынан тиімді қорғанысты жасаудың алғышарты болып табылады.

6.3. Биометриялық қорғаныс автоматының мүмкін болған кіріс және шығыс жағдайын іріктеу қауіпі

Биокодтың ұзын шығыстарын қолданған жағдайда (мысалы, ұзындығы 256 бит) кодтың мүмкін болған жағдай саны 2^{256} үлкен болады. Жағдайдың соншалықты үлкен санын іріктеудің еш мәні жоқ. Бұзушылар тапсырманың криптографиялық қиындықтарымен кездескенде қорғанысты еш шабуылдамайды, оның орнына өзге бір осалдығын табуға тырысады.

Бұл да көбірек биометриялық акпараттарды сканерлеудің бастапқы тетіктері жағынан биометриялық қорғанысқа шабуыл жасау талпынысына жатады. Мұны саусақ ізі суретін сканерлеу үлгісінде көрсетейік. Жарықтың (8 дәрежелі) 256 градациясын есепке алу мүмкіндігімен 320×480 (500 dpi) ұлғаюына ие. Мұндай тетіктің қисындастыру санының мүмкіндігі $2^{1\,228\,800}$ құрайды. Соншалықты мүмкін болған жағдайдың көлемді сандарын іріктеудің еш мәні жоқ.

Суретте саусақ іздерінің ерекше нүктелерін бөлу алгоритмін орындау кезіндегі алдын ала өңдеу кезеңінде 153 600 өлшемділігіне ие 1 және 0 дискреттік мәнді вектор пайда болады. Бұл жағдайда биометриялық мәліметтердің жалпы саны $2^{153\,600}$ құрайды. Жағдайлардың саны айтарлықтай төмендеді, бірақ қарапайым іріктеу үшін тиімсіз болып қала береді.

Келесі үздіксіз параметрлердің бақылауына дискреттік мәліметтердің екі өлшемді түрленуі олардың өлшемділігін 256 дейін қысқартады. Жасанды нейрондық желілер кірісіндегі көптеген үздіксіз параметрлердің шектелмеген мәндері

континууммен суреттеледі және оны тура көрсетуде шек қойылады. Егер үздіксіз биометриялық параметрдің біреуін кодтауға 4 бит (ол 16 жағдаймен көрсетілуі мүмкін) қолданылса, онда биометрия-код түрлендіргішінің кірісіндегі биометриялық параметрлер мәнінің қисындастыру саны 2^{1024} құрайды. Бұл өндірушілердің ресми мәлімдеген 10^8 немесе 2^{26} іріктеу шабуылының биометриясының тұрақтылығына қарағанда айтарлықтай көп. Демек, «Бөгде» биометриялық бейнелерінің 2^{26} немесе 10^8 биометрия-код түрлендіргішінің кірісіне қою арқылы биометрияны шабуылдау ұтымдырақ. Бұл амал биометриялық мәліметтерінің мүмкін болған кіріс жағдайын іріктеуге және криптографиялық кілтінің шығыс жағдайын іріктеуге қарағанда ұтымдырақ.

Тура осындай жағдай өзге биометриялық технологияларды қолданған кезде туады. Мысалы, дауыс биометриялық қорғанысының типтік құралы ұзындығы 4 секундтық құпия сөз орамын қолданады («Невероятный сильный мороз» сөз орамы). Оны 8 кГц 8-дәрежелілік АСҚ жиілігімен сандастыру кезінде 32 000 8-көлеміндегі мәлімет. Алғашқы мәліметтер мәнінің қисындастырылуының мүмкін болған саны $2^{256\,000}$ құралған. Фурье түрлендіргішінің бір өлшемді 512 коэффициентін шығару және оларды 4 дәрежеге дейін дөңгелектеу кезінде мүмкін болған қисындастырылу саны 2^{2048} дейін қысқарады. Жағдайдың бұл саны өндірушілер мәлімдеген 10^6 немесе 2^{20} іріктеу шабуылының тұрақтылығынан көбірек. Бұл жағдайда да шабуыл жасау биометрия-код түрлендіргішінің кірісіне кездейсоқ биттік бірізділікке қарағанда дауыс құпия сөздерін қою арқылы ұтымдырақ.

6.4. Нақ бейнені дайындау шабуылы, биометриялық бейнені қағып әкету қауіпі

Биометриялық бейненің нақ бейнесін дайындаудағы қағып әкету ең тиімді шабуылдардың бірі болып табылады. Бұл шабуылға тек қана техникалық-ұйымдастырылған іс-шаралар қарсы тұра алады. Осылай өз жеке мәліметтерін суреттегі саусақ ізімен қорғайтын қолданушы сканердің әйнегінде өз тері

майының ізін қалдырады. Егер бұл ізді жоймаса, онда заңды қолданушыдан кейін келген оның биометриялық мәліметтерін алады. Қажетті саусақ ізінің суретімен нақ бейнені дайындау өте қиын техникалық тапсырма болып табылады.

Мұндай қағып алуға тек қана қолданушыны өзінің соңынан сканердің папиллярлық саусақ терісінің суретін сүртіп отыруы немесе сезімтал кеңістікті сүртетін автоматтық сканер алу арқылы қарсы тұруға болады.

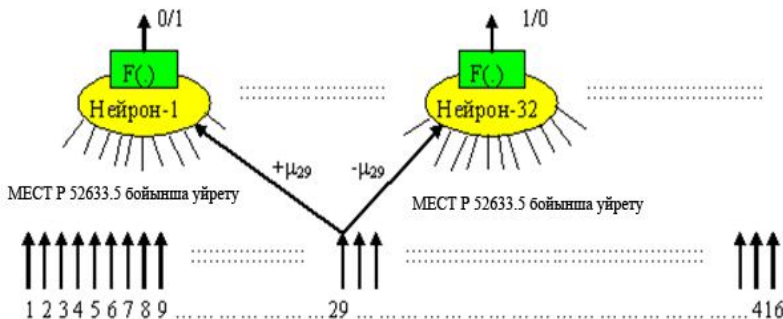
Қорғалып жатқан ақпараттың тұлғасыздандырылуы техникалық ұйымдастырылған іс-шаралардың бірі болып табылады. Егер шабуыл жасаушы адамның атын және қандай биометриялық технологиямен қолданғанын білмесе, онда саусақ іздері маңызды биометриялық қорғаныс болып табылады. Бұл электронды тұлғасыздандырылған төлемдер кезінде, мысалы, провайдер төлеушінің IP адресін жасырғанда және өзінің IP адресінен транзакция жасағанда жүзеге асуы мүмкін. Мұндай жағдайда шабуыл жасаушы IP адресіті білуі керек, сонымен бірге төлеушінің үйіне кіріп, оның жеке заттарынан саусақ іздерін алуы керек. Егер шабуыл жарамсыз болса, онда басып алушы биометриялық қол жеткізудің дауыс құпия сөзін қағып алатын жасырын тыңдау құрылғыларын немесе қолжазба құпия сөзінің графикасын қағып алатын бейне камерасын орнатуы қажет болады.

6.5. Нейрожелідегі артық байланыстарының бар болғандығынан биокодтың біртіндеп әшкерелену қауіпі, Маршалко шабуылы

Жасанды нейрондық желілер бастапқы кедей биометриялық мәліметтерді байытуға әрі оларды байытып болғаннан кейін кванттауды жүзеге асыруға қабілеттілігімен «айқын емес экстракторлардан» ерекшеленеді. Биометриялық әртүрлі мәліметтерді біріктіре отырып, нейрондардың көлемді санын алуға болады.

Осыған орай нейрондардың біраз бөлігі көршілес нейрондармен сәйкес кірістік байланыста болады. Мұндай артықшылық (нейрондардағы кіріс байланыстарды жабу)

биокодтың беделін түсіру үшін қолданылуы мүмкін. Шабуылдың бұл түрін алғаш рет Г.Б. Маршалко [88] жазды. Маршалко шабуылының мәні 6.3-суретінде бейнеленген.



6.3-сурет. Жасанды нейрондық желілердің артықшылығына бағытталған Маршалконың шабуылы

6.3-суретте нейрон-1 мен нейрон-32-де ортақ кіріс байланысы (барлық нейрон желілерінің 29 кірісі) табылғаны берілген. МЕСТ Р 52633.5 үйретудің нақты алгоритмін береді, оң нәтижелер қатарында теріс нәтижелерде туындайды, нейрон-1 мен нейрон-32-нің салмақтық коэффициенттері модулі бойынша бірдей болады. Осы салмақтық коэффициенттердің белгілерін салыстыра отырып, биокод разрядтарының 1 мен 32 жағдайлары жөнінде тұжырым жасауға болады. Егер салмақтық коэффициенттердің белгілері бірдей болса, шығыс разрядтарының жағдайлары да бірдей болады. Егер салмақтық коэффициенттердің белгілері әртүрлі болса, онда 1 мен 32 инверсиямен байланысты.

Сандық модельдеу Маршалко шабуылының әсері жоғары екендігін көрсетеді. Оны жүзеге асыра отырып, 256 биттің жалпы санынан 200 битті байланыстыруға болады. Яғни биокодтың қалған тұрақтылығы небары 56 күшті корреляцияланған битті құрайды. Мұндай тиімді шабуылға үш тәсілмен қарсы тұруға болады [89]:

1-тәсіл. Нейрондардың кірістік байланыстарын жабуды толығымен болдырмау (Маршалко шабуылына қарсы тұрудың бірінші нұсқасы);

2-тәсіл. Қиылысатын байланыстары бар нейрон мәліметтерін өзін-өзі шифрлаумен қорғау (Маршалко шабуылына қарсы тұрудың екінші нұсқасы);

3-тәсіл. Жалпы байланыстары бар нейрондарды үйретудің итерациялық алгоритміне жиі оралу және анықталған 50% нейрондардың жалпы кірістік байланыстары үшін МЕСТ Р 52633.5 кері алгоритмінің салмақтық коэффициенттерінің белгісін беретін басқа да сапалы нейрожелілік шешімдерді табу.

6.6. Кілттің шығыс кодын білу кезіндегі нейрожелілік функционалдар матрицасының қатынау шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі

Сызықты алгебра жақсы тексерілген фундамент болып табылады. Егер сызықты алгебраның үйреншікті формаларымен қолданып көрсек, онда біз «Бөгде» бейнесінің i -ші үлгілерінің биометриялық параметрлері үшін - $\bar{\xi}_i$ және «Өзім» бейнесінің i -ші үлгілерінің биометриялық параметрлерінің векторлары үшін - $\bar{v}_i$ матрицалық теңдеулерді жазып ала аламыз:

$$\begin{bmatrix} \text{ПБК} \\ N \times n \end{bmatrix} \cdot \bar{v}_i = "c" \quad (6.1),$$

$$\begin{bmatrix} \text{ПБК} \\ N \times n \end{bmatrix} \cdot \bar{\xi}_i = "x_i" \quad (6.2)$$

(6.1) вектордың және (6.2) матрицалық теңдеулерінің сол және оң бөлігі әр түрлі табиғатқа ие. Вектордың әрбір компонентінің оң жағындағы - бұл код дәрежелері, вектор теңдеуінің сол жағы континуалды (кейбір интервалдарда үздіксіз) компоненттерге ие. Оң және сол жақты биометрия-код түрлендіргішінің (БКЖ) сызықты емес нейрожелілік функционалдарының матрицасы байланыстырады.

Әрбір биометрия-код түрлендіргіші үшін нейрожелілік функционалдар матрицасы әрқашан нақты, атап айтқанда бір қабатты нейрондық желі үшін осы матрицаның функционалдарын жекешеленген нейрондармен орындаушы функция түрінде жазып алуға болады. Сонымен бірге нейрондық

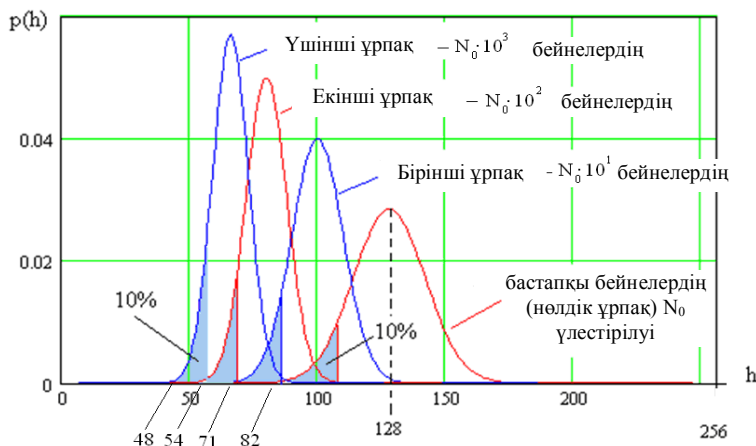
желілердің ішіндегі байланыстар өте күрделі болуы мүмкін және олар көпшілік кестелердің өзара байланысымен сипатталуы керек (нейрондардың әрбірі сипатталуы үшін кем дегенде екі кесте қажет: нейрон кірісі салмағының кестесі мен нейрон кірісі байланысының кестесі).

Біздің нейрожелілік функционалдарының матрицасы туралы білетініміз, оны қолданудан баптау өте қиын. Біз үйретілген нейрожелілік функционалдарының анау не мынау матрицаның қабылдаған шешім сапасын бағалай аламыз, бірақ басқасының бәрінде сызықтық емес матрицаның осы сияқты қасиеті жаман үйренілген болады. Атап айтқанда, сызықтық емес матрицалық (6.1) мен (6.2) тендеулерді кері түрлендіруді жүзеге асыру мүмкін бе деген сұрақ ашық қалады. «Өзім» кодын «с» біле тұра және «Бөгде» бейнелерінің үлкен сынақ қорына ие бола тұра «Өзім» бейнесін БКЖ нейрожелілік функционалдарының матрицасы бойынша қайта қалыптастыруға бола ма.

Жүргізілген зерттеулер көрсеткендей, бұл тапсырма тек қана академиялық қызығушылық емес, сонымен бірге сынақ жүргізу практикасына да, биометрия-код түрлендіргіштерінің нейрожелілік тұрақтылығының бағасына да маңызды. Негізінде бұл тапсырманың шешімін нейрожелідегі әрбір нейрон үшін құрылған түр теңсіздігінің сызықтық жүйесі шешімінде құруға болады (4.6), бірақ мұндай амалдың тиімділігі аз болады. Сызықты программалаудың әдістері өз шектеулеріне ие, сондықтан үлкен және тым үлкен жасанды нейрондық желілер үшін жұмыс істемейді. Хэмминг арақашықтығының кеңістігіндегі генетикалық алгоритмдер іріктеуі мен аталық бейнелерін келесі тоғыстыруы тиімдірек болып табылады. Генетикалық селекцияға бағытталған процедураның жалпы мағынасы 6.4-суретінде суреттелген.

Алгоритм жұмысы «Бөгде» бейнелер қорының бастапқы күйін селекционды материалдың нөлдік бастапқы күйінің ұрпағы деп қарастырудан басталады. Әрі қарай зерттеліп жатқан биометриялық код түрлендіргішіне «Бөгде» бейнелерінің үлгілерін береді де, олардың үн қатуының биокодын алады. Әрі қарай «Бөгде» биокодтарын «Өзім» кодымен салыстырып, нөлдік ұрпағы үшін Хэмминг арақашықтығының таралуын алады. Осыдан кейін «Өзім» бейнесіне Хэммингтің арақашықтығы бойынша

жақынырақ «Бөгде» бейнелерінің 10% таңдайды (6.4-суретінде жақынырақ арақашықтық қара түспен белгіленген).



6.4-сурет. «Өзім» биометриялық бейнесіне жақындау аталық - бейнелерінің селекциясына бағытталған генетикалық алгоритмдер

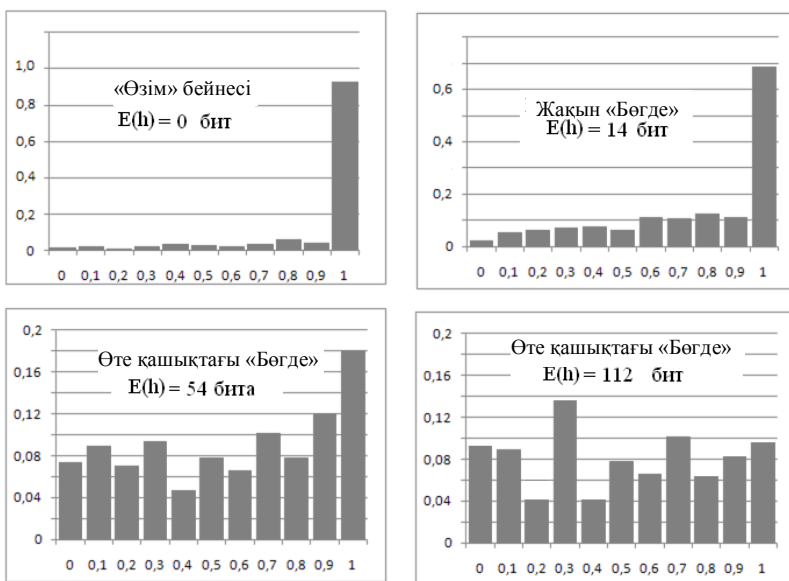
Бейнелердің келесі ұрпақтарын алу үшін мутацияны қолдана отырып, белгіленген бейнелерді өзара тоғыстырады (аталық бейнелерін тоғыстырған биометриялық параметрлерге кездейсоқ шуды енгізе отырып). Бірінші ұрпақтың саны бастапқы нөлдік ұрпақ санына жеткенше көбеюді жүзеге асырады. Әрі қарай жаңа ұрпақта «Өзім» бейнесіне жақынырақ аталық бейнелерінің селекция процедурасын қайталайды. «Өзім» белгісіз бейнесінің параметрлерін қалпына келтіру жағына ақырын жылжи отырып процедураны көп рет қайталайды. Мұндай машина уақытының бірнеше минутында есептеу «Өзім» бейнесінің биометриялық параметрлерінің векторын 80%-дан 90% дейін эшкерелеуге мүмкіндік береді. Демек, ең жақын биометриялық бейнелердің соңғы ұрпағы «Өзім» бейнесінің биокодына 80%-дан 90% дейін сәйкес келетін кодтар береді.

Осындай типтегі шабуылға қорғаныс нейрожелілік биометриялық-код түрлендіргішке қатенің көбею механизмін қою арқылы құрылады, мысалы, мұндай механизм осыдан алдыңғы нейрондардың шығыс жағдайларынан қалыптасқан

кілт кодында келесі нейрондар мәліметтерін шифрлау арқылы құрылуы мүмкін. Қателерді көбейту механизмін қосқанда Хэмминг арақашықтығының бақылаушылары «соқыр» болады, биокодтағы кез келген қате келесі нейрондардың мәліметтерінің шифрларын қате ашады (келесі нейрондардың барлығын оқымаған жасайды).

6.7. Биокод дәрежелерінің тұрақтылық параметрлері бойынша генетикалық іріктеу жолымен нейрожелілік функционалдар матрицасының қатынауы шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі

Қауіп «Өзім» кодының шығыс дәрежелерінің өте тұрақтылығынан құралады. «Бөгде» кодтарының дәрежелерінің тұрақтылығы «Өзім» бейнесінен «Бөгде» бейнесінің жоқ болуына байланысты төмендейді. Бұл жағдай 6.5-суретінде бейнеленген.



6.5-сурет. «Бөгде» кодтарының дәрежелерінің тұрақтылығы «Өзім» бейнесінен «Бөгде» бейнесінің жоқ болуына байланысты төмендеуі

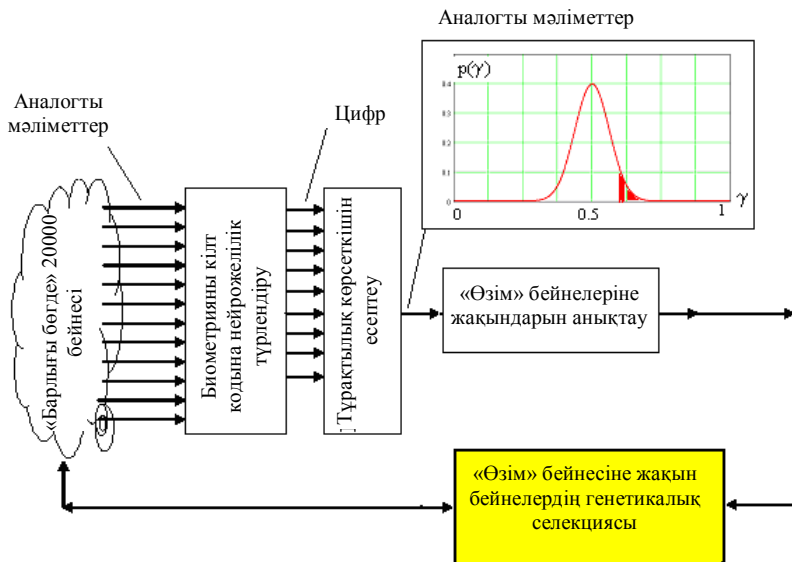
Шығыс код дәрежелері тұрақтылық көрсеткіштерінің таралу гистограммасы бойынша «Өзім» бейнесіне дейін Хэмминг арақашықтығын бағалауға болатынын 6.5-суретінде көрсетілген. «Бөгде» кодтарының бұл қасиеті «Өзім» шығыс биокодын білмей олардың Хэмминг арақашықтығын жанама бағалауға мүмкіндік береді. Өз кезегінде, бұл, тұрақтылық көрсеткіштеріне сүйене отырып, «Өзім» бейнесін біртіндеп әшкерелеу бойынша генетикалық селекция шабуылын ұйымдастыруға мүмкіндік береді. 6.6-суретінде осындай шабуылдың блок-сұлбасы берілген.

6.6-суретіндегі блок-сұлбаға сәйкес зерттеліп жатқан БКТ-не «Бөгде» бейнелер қорының мәліметтері беріледі, сонымен бірге шығыс биокодтары пайда болады. «Бөгде» бейнесінің әрбірі үшін тұрақтылық көрсеткіштерін есептейді және осы көрсеткіш бойынша Хэмминг арақашықтығын болжайды. Бұл алдыңғы параграфта сипатталған «Өзім» биометриялық бейнесін біртіндеп қайта қалыптастыру мен БКТ матрицасының генетикалық айналу алгоритмін іске қосуға мүмкіндігін береді.

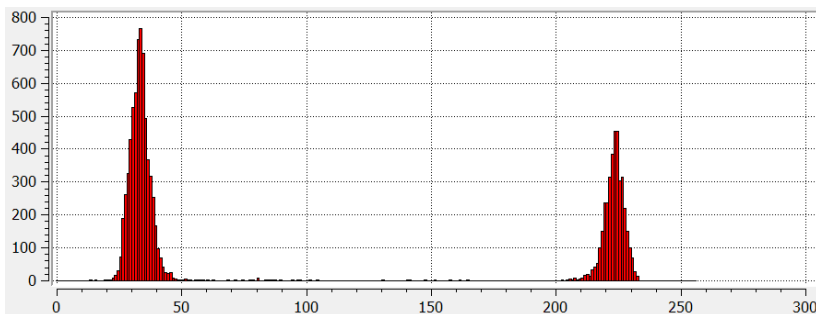
БКТ матрицаның айналу екі алгоритмінің түбегейлі ерекшелігі Хэмминг арақашықтығының метрикасы мен биокод дәрежелерінің тұрақтылық метрикасының табиғаты әртүрлі болып табылады. Осы себептен Хэмминг арақашықтығының минимумдасу алгоритмдері (6.4-сурет) $p(h)$ қалыпты таралудың сол жағында орналасқан мәліметтерді таңдауда құрылған. Тұрақтылықтың максимумдау алгоритмі $p(\gamma)$ қалыпты таралудың оң жағындағы тұрақтырақ аталық-бейнелерін таңдауды қарастырады (6.6-суретін қараңыз).

Бұл тапсырманың шешімі екеу екендігі нейрожелілік функционалдар генетикалық матрицасының айналу алгоритмдерінің және бір ерекшелігі болып табылады. «Өзім» бейнесіне жақын бейнелер мен «Өзім» бейнесінің инверсиясына⁶ жақын биометриялық бейнелер қайта қалыптастырылады. Нәтижесінде генетикалық селекцияның 64 ұрпағынан кейін Хэмминг арақашықтығының таралу тығыздылығы екі серпілге ие жоғары тұрақтылықты бейнелер пайда болады. Бұл 6.7-суретінде көрсетілген.

⁶ Инверсияланған «Өзім» бейнелері инверсияланған биометриялық мәліметтер кірісі мен инверсияланған шығыс кодына ие.

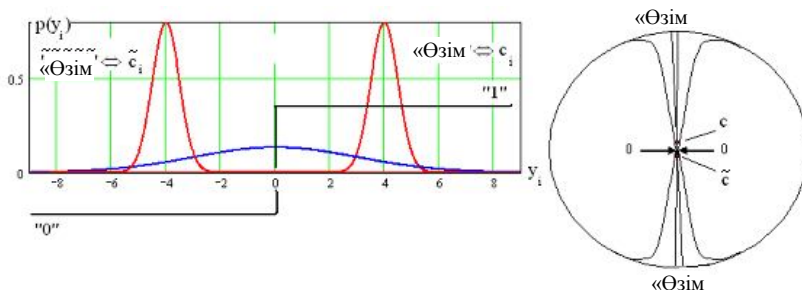


6.6-сурет. «Бөгде» кодтарының тұрақтылық көрсеткіштерін бақылау жолымен «Өзім» бейнесін біртіндеп әшкерелеу мен нейрожелілік функционалдар генетикалық матрицасының айналу шабуылын ұйымдастыру



6.7-сурет. Тұрақтылық көрсеткіштерін максимумдау критериясы бойынша генетикалық селекцияның 64 ұрпағынан алынған тұрақты бейнелердің Хэмминг өлшемдерінің нәтижелі таралуы

6.7-суретінен көрініп тұрғандай, тұрақтылық көрсеткіші бойынша селекцияны жүргізу кезінде Хэмминг арақашықтығымен бір-біріне қатынасы бойынша жақын екі топ бойынша аталық бейнелерін сұрыптау қажет. Мұның барлығы бинарлық нейрондардың «Өзім» бейнелеріне және оның инверсиясына қарым-қатынасы бойынша симметрияға ие болуы салдарынан болып табылады (6.8-сурет).



6.8-сурет. БКТ шығыс кодтардың жоғары мәнді энтропиясының гиперсферасы «Өзім» коды мен оның инверсиясы үшін энтропия өте төмен мәндегі екі сәтсіздікке ие

Мұндай симметрияның бар болуы биокод энтропиясының жоғары мәндегі гиперсферасы нөлдік мәнге дейінгі энтропия сәтсіздігіне ие (6.8-суретінің оң жағы). Тура және инверсиялық кодтар энтропиясының сәтсіздіктерінің бар болуы нағыз осал жер болып табылады. Кілт кодына қол жеткізуді біртіндеп қалпына келтіру шабуылын ұйымдастыру үшін қолданылуы мүмкін.

Жоғарыда сипатталған «Өзім» бейнесін және оның инверсиясын іріктеуге бағытталған шабуылдан қорғаныс нейрожелілік биометриялық код түрлендіргішінің құрамына қателерді көбейту механизмін енгізу арқылы орындалуы мүмкін. Мұндай жағдайда Хэмминг арақашықтық байланысының бірқалыптылығы мен дәрежелердің тұрақтылық көрсеткіштері бұзылады. Қателерді көбейту механизмін қосқан кезде тура және инверсиялық жоғары мәндегі энтропия гиперсферасының сәтсіздіктері өте тар тесіктерге айналады (6.8-суретінің оң жағында).

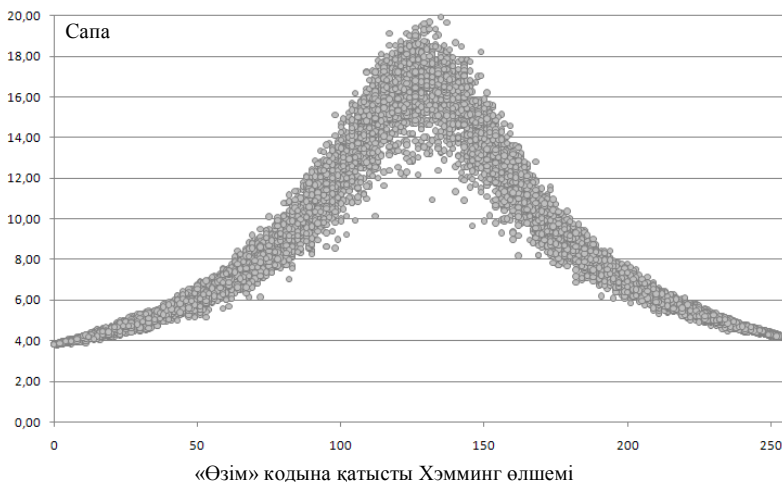
6.8. Шығыс биокодтың және минимум энтропияға ие оның инверсиясын біртіндеп әшкерелену қауіпі

БКТ шығыс кодтарының жоғары мәндегі энтропиясының (6.8-суретінің оң жағында) сферасында екі симметриялық тесіктің барына байланысты нейрожелілік биокод контейнерлерінен рұқсат кілтін шығарып алу бойынша шабуыл ұйымдастырылуы мүмкін. Мұндай шабуыл нейрожелілік биометрия-код түрлендіргішінің кірісіне «Барлығы бөгде» көпшілігіндегі сияқты орташа квадратталған ауытқу мен нөлдік математикалық болжамды қалыпты шу генераторынан кездейсоқ мәліметтер берілуімен құрылады. Осы кездейсоқ әсерлерден БКТ шығысында кодтар пайда болады. Кездейсоқ «Бөгде» алынған кодтардан қорды құрады да, барлық өзге кодтардың алфавиттеріне қатынасы бойынша әрбір кодтардың энтропиясын есептейді.

Код энтропиясын есептеуді Шеннон бойынша жүргізуге болмайды, себебі есептеу жағынан үлкен шығынға алып келетін процедура. Энтропияны есептеуді Хэмминг арақашықтық кеңістігіндегі жылдам процедуралармен жүзеге асыру керек. Бұл есептеулер кезінде энтропиясы бағаланған әрбір код «Өзім» коды сияқты қаралуы керек, әрі оған қатысты Хэмминг арақашықтығының таралуы құрылуы керек.

Нәтижесінде код энтропиясының таралуының мәні «Өзім» коды мен оның инверсиясының нағыз мәніне дейінгі Хэмминг арақашықтығының кейбір функциясы түрінде келіп шығады. 6.9-суретінде осы мәліметтер бейнеленген.

6.9-суретінен көрініп тұрғандай, энтропияның минималды мәнді кодын таңдағаннан (сапа көрсеткіші) біз қайтадан кодтардың екі тобын аламыз. Бір тобы «Өзім» кодына жақын, ал екінші топ «Өзім» инверсия кодына жақын. Биокодтың қолжетімді кілтін қалпына келтіру үшін осы кодтарды екі топқа бөліп, бір топтағы кодтың мәндерін инвертациялап, әрбір код дәрежесінде «0» немесе «1» жағдайларының ықтималдырақ мәнін шығару жеткілікті.



6.9-сурет. Код үшін сапа (энтропия көрсеткіштері)
көрсеткіштерінің таралуы, олардың БКТ кірісіне кездейсоқ
әсер етуден алынуы

Дәрежелердің бір бөлігі жоғары дұрыстықпен, ал қалған бөлігі аз дұрыстықпен қалпына келтіріледі. Код рұқсатын табу үшін аз дұрыстықпен қалпына келтірілген код дәрежелерін толық сұрыптау қажет болады. Мұндай шабуыл «Өзім» кодын 85% дейін қалпына келтіруге мүмкіндік береді. Демек, биокод ұзындығы 256 бит кезінде шамамен 40 битті сұрыптау қажет болады. Мұндай айтарлықтай толық әшкереленген биокод кілтінге қол жеткізудегі қалдықты тұрақтылық, алдыңғы қатарлы өндірушілер мәлімдеген, нейрожелілердің биометрия-код түрлендіргішінің тұрақтылығымен салыстырмалы.

Нейрожелілік контейнерлерден «Өзім» биокодын шығару шабуылынан қорғаныс келесі бөлімде толық сипатталатын қателерді көбейту механизмін оларға ендіру арқылы жүзеге асады.

6.9. Хэммингтің өлшенген метрикасының минимизацияланған іріктеу жолымен нейрожелілік функционалдар матрицасының қатынау шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі

Айта кететін жайт, шабуыл құрылымының принциптері бойынша шабуылды анықтау – бұл қандай да бір бөліп байланыстыру түрдегі осы шабуылдардан қорғау тапсырмасы, жасанды амал. Өмірде бәрі өзгеше, шабуыл жасаушы бірден бірнеше шабуыл нұсқасын қолданып, қарсылық аз жолымен жүреді. Демек, жоғарыда сипатталған шабуылдарға тиімді амалдар қарастыру қажет.

Өте тиімді шабуылдардың бірі Хэмминг метрикасында да тұрақтылық метрикасында да бір кезде құрылған шабуыл болып табылады [90, 91]. Андреевтің қиыстыру метрикасының идеясы ($E(\gamma) \approx 1.0$) бірлігіне жақын тұрақтылық көрсеткішті детерминдендірілген кодтар үшін Хэмминг метрикасы жақсы жұмыс істеуінде түзілген. биометриялық үстемелерде метрика тұрақтылығы мен Хэмминг метрикасы бір-бірін толықтырып тұрады. Мысалы, «Өзім» кодтары үшін Хэмминг арақашықтығы минималды ($h=0.0$), ал тұрақтылыққа максималды ($E(\gamma) \approx 1.0$). «Бөгде» алыс кодтары үшін барлығы керсінше, Хэмминг арақашықтығы максималды ($E(h) \approx 128$), ал тұрақтылық көрсеткіштері минималды ($E(\gamma) \approx 0.0$). Осы қасиеттерді қолдана отырып, Хэмминг өлшемін құруға болады. Оның дәрежелерінің тұрақтылық көрсеткіштері бойынша өлшенген өлшемін құруға болады. Өлшеу кезінде Хэммингтің қалыпты өлшемімен қолданған ыңғайлы:

$$h_{Re} = \frac{1}{n} \sum_{i=1}^n c_i \oplus x_i \quad (6.3)$$

және оны толықтырумен:

$$h_{lm} = \sqrt{(1 - h_{Re}^2)} = \frac{1}{n} \sum_{i=1}^n \tilde{c}_i \oplus x_i = \frac{1}{n} \sum_{i=1}^n c_i \oplus \tilde{x}_i \quad (6.4)$$

Сәйкесінше Хэммингтің өлшенген метрикасы анықталады

$$\begin{cases} \gamma_{h_{re}} = \frac{1}{n} \sum_{i=1}^n \gamma(c_i) \cdot c_i \oplus \gamma(x_i) \cdot x_i; \\ \gamma_{h_{lm}} = \frac{1}{n} \sum_{i=1}^n \gamma(c_i) \cdot c_i \oplus \gamma(x_i) \cdot \tilde{x}_i; \end{cases} \quad (6.5)$$

Метриканың күдікті (6.4) бөлігін енгізудегі қажеттілік бұл өлшенген метрика (6.5) салыстырмалы кодтардың сәйкес келмейтін дәрежелерінің, сонымен бірге кодтардың сәйкес келетін дәрежелерінің тұрақтылық көрсеткіштерін де есепке алуы керектігінде шарттастырылған.

Хэмминг өлшенген метрикасын тәжірибе қолдану, оның жоғары тиімділігін көрсетті. Оған өту кезінде әшкерелеуге бағынбайтын код бөлігінің ұзындығын жарты есеге төмендетуге мүмкіндік бар.

Хэмминг өлшенген метрикасының қорында қателерді көбейту механизмін нейрожелілік биометрия-код түрлендірушісіне енгізу арқылы шабуылдан қорғаныс құрылады.

7. НЕЙРОЖЕЛІЛІК КОНТЕЙНЕРЛЕР ҚҰРАМЫН КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ

7.1. Құпиясөздерді және жүйеге қолжеткізу биометриялық кодтарын хэштеу арқылы жеке мәліметтерді классикалық қорғау

Жеке тұлғаның классикалық құпиясөздік аутентификациясы операциялық жүйеде құпиясөздің өзі сақталмауымен, құпиясөздің криптографиялық хэш-қызметі жады ұяшығында сақталуымен, оның мекенжайы пайдаланушының ашық атымен (логин) байланысты болады. Өкінішке орай, қосымша бөлікке арналған құпиясөздік қорғау жеткіліксіз болып қалып жатыр, адамдар екі регистрдің кездейсоқ таңбаларынан ұзын құпиясөзді сөйлемдерді есте сақтағысы келмейді. Есте сақтау үшін қысқа мағыналы құпиясөзді сөйлемдер таңдап алған ыңғайлы, олар шабуылдарға төзімді болмайды. Адамдарға ыңғайлы қысқа құпиясөздік тізбектер сөздіктері жасалған, олардың көмегімен жүйелік администратор әлсіз құпиясөздерді тез тауып алады.

Адам өте үлкен көлемді мәліметтерді қарапайым құпиясөздік тізімдер арқылы ала алады, міне биометрия осы жағынан өте ыңғайлы. Биометрикалық қорғаулардың тұрақтылығы құпиясөздік сөйлем мағыналы ма, жоқ па, оған байланысты емес. Пайдаланушы графикалық планшетте құпиясөздік сөзді қолымен енгізгенде адамның жазуы бірден-бір, қайталанбайтын рөл атқарады. Біздің әрқайсымыз әріпті өздігімізше, әртүрлі жазамыз, мұнда алдыңғы әріп қандай болды, екіншісі қалай жазылды, міне осыған көп нәрсе байланысты. Екі және үш әріп рөл атқарады. Егер биометрикалық құпиясөз 5 қолжазба әрпінен тұрып әшкереленіп қалса, оның іріктеу шабуылына табандылығы аз, 10^2 -нен 10^3 -не дейін болады. Әшкереленбеген 5 әріптен құрылған қысқа қолжазба құпиясөзі 10^5 -нен 10^{12} -не дейінгі теру шабуылдарына тұрақтылығын қамтамасыз етеді, бәрі қолжазбаның бірқалыпты және бірден-бірлігіне болуына байланысты. Биометриялық құпиясөзді жасырын сақтау өзінің ықпал етуі бойынша биометрияның өзінен анағұрлым күштірек болады.

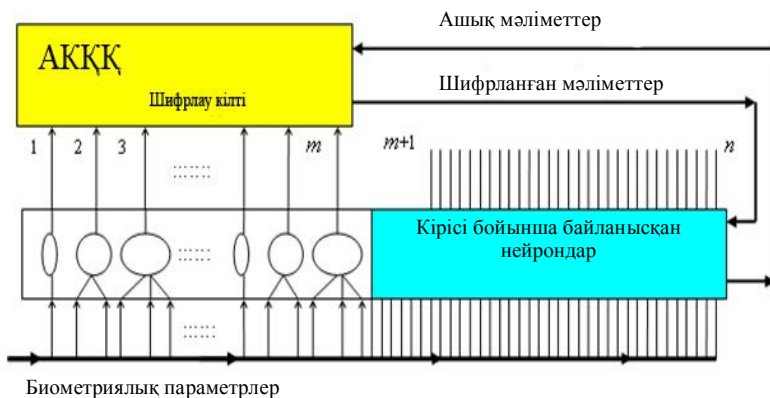
Әрине, операциялық жүйедегі биометриялық қолжеткізу кодын ашық сақтауға болмайды. Біз құпиясөздің хэш-функциясын қалай сақтасақ, биометрикалық кодтың хэш-функциясын да солай сақтауымыз керек. Егер жеке тұлғаның бірлескен құпиясөздік-биометрикалық аутентификациясы қарастырылса (болжанса), онда құпиясөз конкатенациясының хэш-функциясын және биометрикалық кодтарды бірге сақтау қауіпсіз болады.

Арнайы құрастырылған криптографиялық хэш-функцияларды пайдаланғанда құпиясөздердің хэш-функциясы мен қолжеткізу биокодтарын сақтау қауіпсіз болып саналады. Нақты криптографиялық хэш-функцияларды қайтымсыз етіп қарастыруға болады. Басқаша айтқанда, олардың тікелей есептелуіне уақыт аз кетеді, ал бастапқы деректердің хэш-функциясының мәнісі бойынша іздеудің кері міндеті іс жүзінде орындалмайтын тапсырма (егер хэштелетін мәліметтердің ұзындығы хэш-функцияның ұзындығынан артық немесе тең болса) болып табылады.

Windows операциялық жүйесіндегі құпиясөздерді хэштеуді қолдану тәжірибесі – шығыс коды 128 бит ұзындықты MD-5 хэш-функциясын қолдануда құрылады. Шартты түрде таңдау талпынысы 2^{128} деңгейіндегі кері тапсырманың күрделілігі туралы айтуға болады, осындай қорғау 2^{40} таңдауындағы шабуылға табандылық танытатын құпиясөздер мен биокодтар үшін толығымен жеткілікті болады. Осындай тәжірибе - қазіргі кезде жалпы қабылданған тәжірибе, б.а. қорғау үшін қолданылатын криптографиялық хэш-қызметі жекелей немесе қосып алғандағы құпиясөздер мен биокодтарға қарағанда шамамен үш есе артық болатын тұрақтылық көрсеткішін қамтамасыз етуі тиіс (косфакторлы аутентификация). Егер криптографиялық хэштеудің орнына шифрлеу қолданылса, онда шифрлеу кілтінің ұзындығы мен биометрия табандылығы арасындағы қатынас шамамен алғанда осындай болып қала беруі тиіс.

7.2. Нейрожелілік контейнердің мәліметтерін қарапайым шифрлау арқылы криптографиялық қорғау

Ең қарапайым және түсінікті қорғау тәсілдерінің бірі – алғашқы (ашық) нейрондарының шығысымен кілттің алынуы және онда өзге нейрондардың (қорғалған) мәліметтері шоғырлануы [92-94]. Бұл жағдай 7.1-суретінде көрсетілген.



7.1-сурет. Нейрожелілік контейнердің мәліметтерін саны өте көп болатын айқастырылған байланыстарды шифрлеу арқылы қорғау

7.1-суретінен алғашқы m нейрондардың мәліметтері ашық сақталатыны, ал келесі нейрондардың мәліметтері қорғалған контейнерді даярлау кезінде m ұзындықты кілтте шифрленгені көрініп тұр. Қорғалған контейнерді қолданған кезде пайдаланушы өзінің биометриясын көрсетеді, ол ұзындығы m биокодқа түрленеді және ары қарай осы кодта келесі нейрондық мәліметтерін бұрын қорғалған шифрлау жүргізледі.

Бұл жерде m шифрлау кілті кодының ұзындығы қандай болуы тиіс деген жанды сұрақ туындайды. Шифрлау кілтінің ұзындығы криптографиялық және биометрикалық шектеулер қатарынан шығуы тиіс. Ең қарапайым нұсқасы – кілт ұзындығын таңдау, таңдау шабуылының табандылығының үш еселік көрсеткішіне пропорционалды болып табылады. (Биометрия тұрақтылығы 2^{40} болғанда шифрлеу 2^{120} құрауы

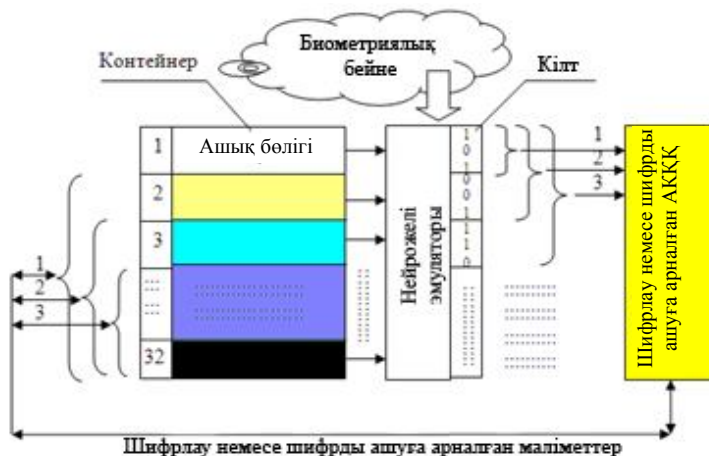
тиіс). Басқаша айтқанда 120 бит шифрлеу кілтiнiң ұзындығы кезінде 120 нейрон мәліметтері ашық сақталады (120 нейронға үшін таразылар мен байланыстар кестесі жалпы қолжетімді).

0.2 бит био-параметрінің орташа ақпараттылығы кезінде әр нейронның 5 кірісі бойынша орташа алғанда 600 био-параметрлер үшін 600 кіріс шығады. Егер нейрондар желісіне кіріс саны тек 480 болса, онда қалған 220 кіріс нейрондардың ашық бөліктерінде қайталанатын болады. Әр нейрон өз көршілерімен шамамен 2 кіріс арқылы байланысатын болады. Әр нейронның көршілерімен жабылатын екі кірісі Маршалко шабуылының табысты түрде ұйымдастырылуы үшін барынша жеткілікті болады.

Сондай-ақ үйретілген нейрондардың ашық мәліметтерінің ұзын серияларына разрядтардың тұрақтылығына шабуылдар қолданылуы мүмкін, энтропия бақылауы арқылы «Өзім» кілтiнiң кодын алуға шабуыл жасалуы мүмкін. Бұл шабуылдар код ұзындығын 80% -дан 90%-ға дейін қысқартуға алып келеді, б.а. 120 бит иллюзиялықтың (алдамшының) орнына біз 12 немесе 24 нақты битке шифрлеуді аламыз. Осындай шифрлеудің табандығы биометрикалық қорғаудың айтылған табандылығынан көп есе төмен болып шығады (2^{40} -тан 2^{12} -:- 2^{24} анағұрлым кіші).

7.3. Криптографиялық кілттің өсетін ұзындығымен блоктық шифрлау арқылы нейрондарды қорғау

Бір ұзын кілтте шифрлаудың барлығына түсінікті нұсқасын жүзеге асыру биометрияға жасалатын шабуылдардың тиімділігінен мүмкін болмайды екен. Бұл шабуылдардың барлығы ашық нейрондардың үлкен санына жасалатын барлық интегралды шабуылдардан тиімді қорғау үшін қорғалмаған нейрондардың көп мөлшердегі шығысының болуын бақылауға қарай құрылады. Биометрияға жасалатын интегралдық шабуылдың тиімділігін төмендету үшін бір ұзын кілтті жасаудан бас тартып, арттырылатын ұзындықты кілттердің жиынтығын қолдану керек. Осындай блоктық шифрлау үлгісінің мысалы 7.2-суретте келтірілген.



7.2-сурет. Мәліметтерді ұзындығы 3, 6, 12, 15..., 256, бит болып өсетін кілтті блоктық шифрлау арқылы қорғау

Барлық шағын кілттер бір-бірімен біріктіріледі және қорғалған нейрожелілік контейнерді дайындау процесінде барлық соңғы үйретілген нейрондардың мәліметтерін көп еселеп шифрлайды. Қорғалған нейрожелілік контейнерді пайдалану кезінде кері процесс жүреді, ашық нейрондарда алынған кілт барлық соңғы нейрондардың мәліметтерін ашады. Қайта қалпына келтірілетін кілттің тағы бір бөлігі ашық болады, олар біріншімен бірігеді де, келесі мәліметтерді ашады. Бұл 7.2-суретінде бояулардың қоюлатылуымен көрсетілген. Нейрондардың ашық бөлігі боялмаған.

Бір ұзын кілтті ашық биометрияға бірнеше интегралдық шабуылдың болуына байланысты қолдана алмайды екенбіз. Баяу артып отыратын кілт ұзындығы мен шифрленген мәтіннің кемитін ұзындығымен блоктық шифрлау кілтінің өсу дискретінің ұзындығын таңдау маңызды болады.

Шифрлау кілтінің өсу дискретінің ұзындығы 1-ден 16 битке дейінгі интервалында мүмкін болады. Бұл интервал үздіксіз мәліметтермен жұмыс істеудің есептеу қиындығының баяу өсуіне сәйкес келеді.

Түрлендіргіш жағдайының көп өлшемді энтропиясының $n=16$ нүктесінде биометрия-коды өзінің қасиеттерін өзгертеді және алдыңғы тарауда сипатталған интегралдық шабуылдар

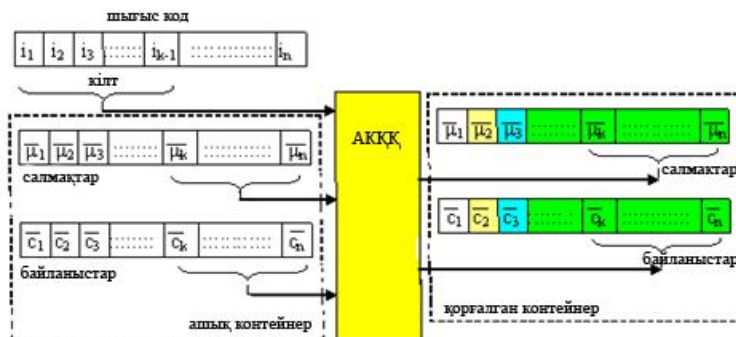
жұмыс істей бастайды. Интегралдық шабуылдар статистикалық зерттеулерге арналған қолжетімді биометрия-код ұзын болған сайын соғұрлым тиімдірек болады.

7.4. Нейрожелілік контейнердің мәліметтерін 1 биттен 256 битке дейін ұзындығы өсетін криптографиялық кілттерді қолдана отырып қорғау

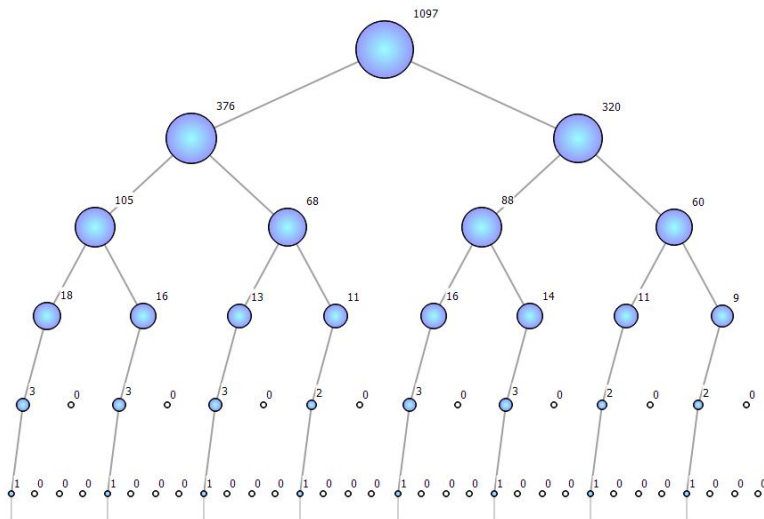
Кілтті 1 бит ұзындықты үйретілген нейрожелінің қорғалатын мәліметтерін көпеселік блоктың шифрлауының шектеулі жағдайын қарастырайық. Бұл желіде ашық болып бір ғана (алғашқы) нейрон қалады, қалған нейрондардың мәліметтерінің бәрі қорғалған болып шығады. 16 биттік кілтте өзінің тиімділік қорғанысы бойынша 16 сызықтық өсетін кілттердегі қорғаныс бірдей деген ой пайда болады. Бұл шынымен де осылай, егер тек 16 еселік ағаштың және бинарлық іріктеу күйін қарастырсақ.

Биометрия үшін бұл жалған нәтиже, өйткені егер шабуыл кезінде параллельді түрде үлкен біркелкі толтырылған «Бөтен» базасын жасау керек екендігін ескерсек, онда «бір биттік» шифрлаудың артықшылықтары анықталады (7.3-сурет).

Көрсетілген тұжырымдарды дәлелдеу үшін қорғалған контейнердің шығыс кодының мүмкін жағдайы бойынша бинарлық ағаштың қалыптастырылуы және осы ағаштың мүмкін жағдайы бойынша «Бөтен» базасын сұрыптауды қарастырамыз. Осындай бинарлық ағаштың мысалы 7.4-суретінде келтірілген.



7.3-сурет. Ашық контейнерлердің 1,2,3,..., 256 бит кілттерінде шифрленіп қорғалған болып түрленуі



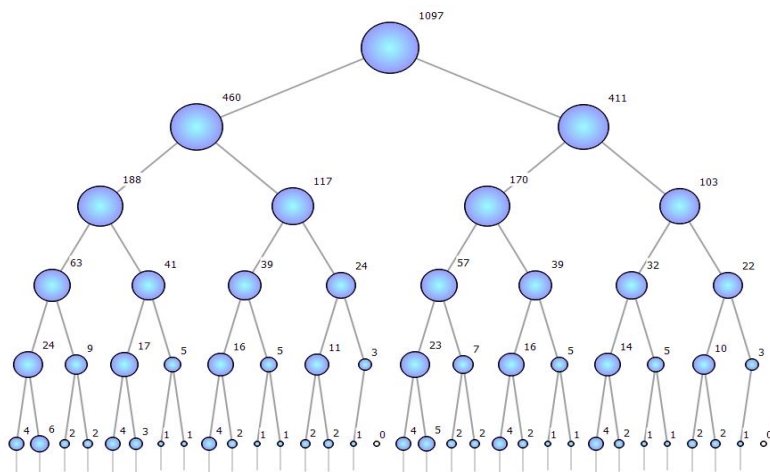
7.4-сурет. «Слон» қолжазба құпиясөзінің қорғалған контейнерді қолданатын 0,7 тұрақтылық деңгейі бойынша «Бөтен» бейнесі базасын сұрыптаудың бинарлық ағашы

7.4-суретінде көрініп тұрғандай «Бөтен» базасында 1097 бейнеден шыға отырып бастапқы базасының тұрақты бейнелері (тұрақтылық деңгейі 0,7 және одан да жоғары) ғана «Бөтен» үшінші деңгейдің өзінде нөлдік биіктікке ие болады. Ары қарай базаны сұрыптаса оны жеткілікті түрде толтырылған деп санауға мүмкін болмайды. Бесінші деңгейдің өзінде-ақ аталықтардың бейнелерінен оларды синтездей отырып «Бөтен» бейнелерінің жоқ үлгілерін толтыру қажет болады.

Егер бір тұрақсыз биометриялық бейнелерді шығарып тастасақ (тұрақтылық шегі 0,3 деп орнықтырайық), онда бинарлық ағаш айтарлықтай барынша толтырылады, бұл 7.5-суретінде көрсетілген.

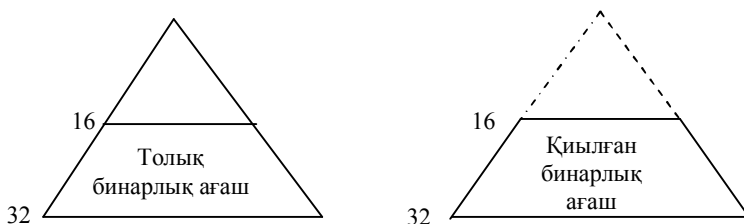
7.5-суретінде көрініп тұрғандай, тұрақсыз бинарлық бейнелерді сұрыптау барынша қалың бинарлық ағаш береді. Соның өзінде ұрпақ бейнелерінің қажетті санын синтездеу арқылы қосымша ақпаратты тартуға мұқтаж болады. Жоғарыда келтірілген бинарлық ағаштың маңызды қасиеттері олар кейбір

деңгейге дейін жеткілікті түрде біркелкі толтырылған болып шығады. Мәліметтерді «Өзім» биокоды бұтағына тарту эффектісі жоқ. Көрші бұтақтар (0-ден 7-ге дейін қашықтықта «Өзім» бұтағының кодына жуық) өздерінің статистикалары бойынша бинарлық ағаштың еркін бұтағынан ерекшеленбейді.



7.5-сурет. «Піл» қолжазба құпиясөзімен қорғалған контейнерді қолдана отырып 0,3 тұрақтылық деңгейі бойынша «Бөтен» бейнесінің базасын сұрыптаудың бинарлық ағашы

Бір биттік шифрлау кезінде қорғаудың барынша жоғары деңгейінің дәлелдемесі биометрикалық бейнелерінің үлкен базасын сұрыптауда болжамдап алатын ағаштарды қарапайым түрде салыстыруға алып келеді. Егер нейрожелілік контейнердің табандылығы 2^{32} -ні құрайтын және шабуылдаушының 2^{32} биометрикалық бейнесінің базасы болса, онда шабуылдаушы шифрлеудің бір битті қорғанысы кезінде базаны сұрыптай отырып 15 мәрте артық өтеді. «Бөтен» базасын жай оқуға кетегін қосымша шығындар «бір битті шифрлау» кезінде шамамен алғанда екі есе жоғары болып шығады. Бұл жағдаят 7.6-суретінде келтірілген.



7.6-сурет. Келесі қорғалған 15 нейронның параметрлерін білмейтін шабуылдаушыны тойтаруға мәжбүр болатын толық бинарлық ағаш (суреттің сол жағы)

7.6-суретінен көрініп тұрғандай қорғалған нейрожелілік контейнерге қатысты реттей отырып (Бөтен» базасын сұрыптай отырып), шабуылдаушы үйретілген нейрондардың параметрлерінің мүмкін болатын мәнісін қалпына келтіре отырып, базаны қосымша 15 мәрте сұрыптауға мәжбүр болады. Егер, үлкен базадағы мәліметтер жазбасын оқу барынша ұзақ операция десек, онда (1 биттен 32 битке дейінгі баяу өсетін мәліметтерді «бір биттік 32 еселік шифрлау 16 биттік кілтте бір еселік қорғаныс шифрлауына қарағанда екі есе көп уақытты қажет етеді. Дегенмен, бұл тапсырманы күрделендірудің ең аз мәнді сызықтың бөлігі ғана.

Қорғану деңгейіндегі ең айтарлықтай жеңу мүмкіндігі болатын жағдайда бинарлық ағаштың 32 деңгейлік толық жазу 2^{32+1} тексеру, сұрыптау операцияларын талап етеді, және жетіспейтін мәліметтердің көбеюін талап етеді. Егер біз 2^{16} жағдайдағы деңгей бойынша ағаштың бас жағын, яғни жоғары жағын кесіп алатын болсақ, онда шабуылдаушы бинарлық ағаштың төмен жағында жатқан 16 сөзді жазу қажеттілігін айналып өтуге тырысуы мүмкін. Ол белгісіз 16 биттік кілт кодын 2^{16} операциясын жұмсай отырып тауып алуы мүмкін, мұнда қысқа тексеру қолданылуы мүмкін. Мысалы, нейрондардың айқас байланыстарының болуы. Нәтижесінде сызық бойынша ұзындығы өсетін кілтті нейрондардың мәліметтерін 32 еселік криптографиялық қорғанысы «Бөтен» бейнесі базасын сұрыптаудың қиылған бинарлық ағашының 16 деңгейі 16 биттік кілтте бір еселік шифрлаудан 2^{16+1} есе

пайдалы. Бұл бетбұрыстық жағдаят болып табылады, өйткені бір еселік шифрлау кілтінің ары қарай өсуі, яғни 17, 18, 19, ..., 32 және одан да көп битке өсуі жоғары өлшемді интегралдық эффектiлердiң пайда болуына және осылайша үйретiлген нейрожелiнiң мәлiметтерiн қорғауды одан да әлсiретедi.

Алынған 1,2,3... 25 биттік кілттердің 256 еселік шифрлануымен алынған биометрикалық қорғанысты шабуылдаушы үшін 16, 32, 48,....., 256 биттік кілттердегі 32 еселік шифрлаумен алынған қорғанысқа қарағанда айтарлықтай күрделі. Шабуыл күрделілігінің өсуі экспонентті түсуі тиіс, өйткені биометрияның табандылығы 2^{40} –тан жоғары емес, б.а. ұзындығы 40 биттен бастай отырып, бір еселік шифрлау кілтінің ұзындығынан бастай отырып бір битке кілттің сызық бойымен өсетін ұзындығын көпеселік шифрлауды қолдануда айтарлықтай ұтатынын арттырады.

7.5. Бірін-бірі жабатын байланысы бар нейрондарды итерациялық үйретуге жекелей қайтып отыру есебінен шифрлау тұрақтылығын күшейтудің қазақша нұсқасы

Нейрожелілік контейнерге ең тиімді жасалатын шабуылдардың бірі – Маршалко шабуылы. Шабуыл үлкен жасанды нейрон желілерін үйретуші жылдам алгоритмдері – $\mu(E(v_i), \sigma(v_i), \sigma(\xi_i))$ нейрондар салмақтық коэффициенттерінің детерминделген есептелуіне құрылған дерлік. Дәл осы себеп бойынша үйренген алгоритмдері жылдам және осы себеппен Маршалко шабуылы орын алуы мүмкін.

Егер біз үлкен нейрожеліні және МЕСТ Р 52633.5-те жазылған есептеулерден кейін олардың үйрету тактикасын өзгертіп, итерациондық дәлелдеулерін қолдансақ, онда біз стандартты шешімдер қабылдағанда стандарттан жақсы және нашар болатын жуық шешімдердің жиынтығын табамыз. Мұнда шешімдердің шырғалану қаупі теріске шығару рөлін емес, оңтайлы рөл атқарады. «Өзім» мысалдарының шағын сандарының ішкі шуылдарынан барлық итерациондық үйрету

алгоритмдерін реттелетін параметрлердің әрқайсысы бойынша сапа көрсеткішін есептеу кезінде жіберілген өз қатесінің әсерін минималды ете отырып, кейде көп өлшемді беттер бойынша флюктуирлейді. Итерациялық үйрету және нейрондардың саны көп кіріс кезінде нейрондардың коэффициент салмақтары шуылдарының табиғи процесі пайда болады. Ол 4.4-суретінде көрсетілген.

Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университетінің зертханасында жүргізілген зерттеулер, үйретілген нейронның итерациялық алгоритмі арқылы табылған барлық шешімдері арасында бір-біріне өзара дәл келетін салмақ коэффициенттері жоқтығын көрсетті.

Оның үстіне осы шешімдердің 1%-дан 15%-ға дейінгі салмақ коэффициенттері түрлі таңбаларға ие болады. Бұл жағдайда Маршалко шабуылы қабілетсіз болады, б.а. итерациондық үйретуді бірнеше рет іске қосу және оны тағы да зерттеу арқылы шешім табуға болады, нейрондардың жалпы байланыстарының салмақ коэффициенттері таңбалары МЕСТ 52633.5-2011 бойынша үйрету алгоритмінің таңбаларына қайшы келетін жиі итерациондық үйрету алгоритмі немесе нейрожелі толық итерациондық үйрету алгоритмі үйрету процесін айтарлықтай баяулатады, бірақ мұнда нейрондардың артық санды байланыстарына жасалатын шабуылдарына тиімді қорғаныс пайда болады.

Зерттеулер нәтижесінде әзірленген тағы бір алгоритм – мәліметтерді мәжбүрлеп бұзудың жылдам алгоритмі. Бұл алгоритм үшін нейрондардың жалпы байланысының 50%-ы шағын (үлкен емес) болады және олардың таңбасы өзгереді. Ары қарай үйрету кезінде бүлінген байланыстар өзгермейді. Бұл нейронды алғаш үйретуден соң керек нәтижені алуды қамтамасыз етеді. Мұнда үйретудің итерациялық алгоритмі жұмыс істеу үшін нейрондардың басқа кірістерінің салмағы бейнесін кездейсоқ 15%-ға дейін өзгертеді (таңбасын өзгертпей) және осыдан кейін ғана үйретудің итерациялық алгоритмін қолдана отырып, шамамен алғанда 100-200 итерацияда үйретудің алдында жоғалтқан сапасын қайтарып алуға болады. Бұдан өзге жаңа шешімдердің шамамен алғанда 60%-ы МЕСТ

52633.5-2011 бойынша итерациялық түрде емес алынған шешімге қарағанда жақсы болып шығады.

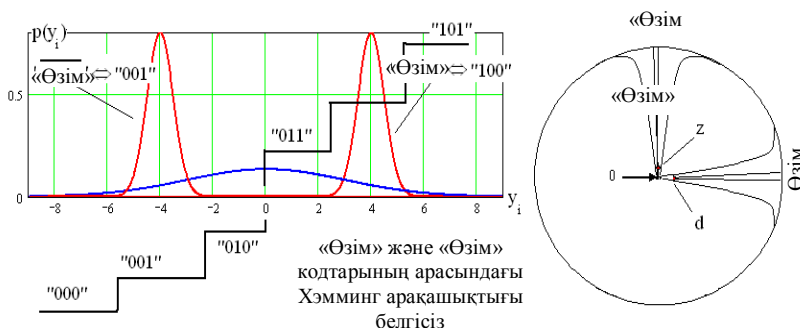
Жүргізілген зерттеу нәтижесінде болар-болмас бүлінетін биометриялық кодтың нейрожелілік түрлендіргішін итерациялық емес үйретудің гибридті нұсқасы және оларды ары қарай үйрету Маршалко шабуылына өте табанды, барынша сапалы шешім (тойтарыс) беретіні дәлелденді.

8. КӨП ШЕКТІ КВАНТТАУ ФУНКЦИЯЛАРЫ БАР НЕЙРОНДАР КӨМЕГІМЕН ЖЕКЕ БИОМЕТРИЯЛЫҚ МӘЛІМЕТТЕРДІ ҚОРҒАУ

8.1. Екі немесе одан да көп шекті кванттау арқылы нейрондарды қолдануға өту

Егер кедей биометриялық мәліметтер алдын ала нейрожелі арқылы байытылмай кванттау жүргізілген жағдайда, биометриялық мәліметтердің көпшілік бөлігі алып тасталынады, себебі, олар өте төмен сападағы шешімдерді береді (олар үшін қаскүнем кері тапсырманы оңай орындайды). Тек қана болар-болмас биометриялық мәліметтерді байытылмаған бөлігі бинарлық кванттаудан кейін ақпараттылықтың жоғарғы көрсеткішін береді.

Егер кванттауға дейін нейрожелілік байыту жүзеге асырсақ, онда жағдай өзгереді. Кіріс санын арттыра отырып, біз «өзім» бейнесінің мәліметтерді үлестіруді қысу арқылы шығыс мәліметтердің ақпараттылығын анағұрлым көтереміз. Мәселен, біз жұп функциялы «өзім» бейнесінің белгілену ақпараттылығының екі немесе үш биттен тұруына қол жеткізе аламыз. Бұл жағдай келесі 8.1-суретінде бейнеленген.

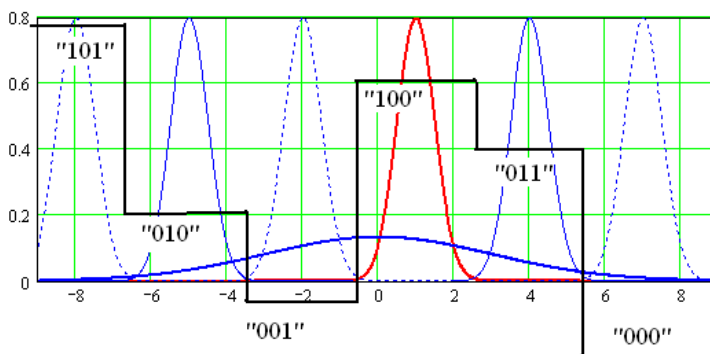


8.1-сурет. Алты шығысты 5-тік шекті дискреттік күйлер бойынша нейрон сумматорының шығыс сигналын кванттауды қолдану

«Өзім» бейнесі мәліметтерінің үлестіру диаметрі, «барлығы бөгде» бейнесі диаметрінен шамамен алты есеге кіші екенін

8.1-суреттен көруге болады. Яғни «барлығы бөгде» үлкен диаметрінде кіші диаметрлі 6 «өзім» үлестіруін орналастыруға болады. Сонымен қатар, сыртқы бақылаушы (үйрету мәліметтерін жойған соң) «бөгде» үлестіруінің қай бөлігінде «өзім» мәліметтерінің үлестірілуі орналасқанын білмейді [94-96].

5-шек бойынша (6 шығыс деңгейі бойынша) кванттау әртүрлі шектік функциялармен жүзеге асуы мүмкін. Атап айтқанда, 8.1-суретте қарапайым монотондық кванттау функциясы көрсетілген. 8.2-суретте көрсетілгендей, күрделірек монотонды емес кванттау функциясы қолданылуы да мүмкін.

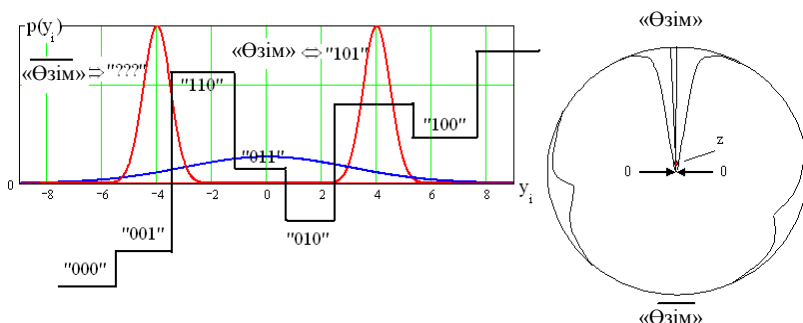


8.2-сурет. Үлкен диаметрдегі «Барлығы бөгде» үлестіруінің ішіндегі «өзім» бейнелері мәліметтерінің 6 үлестіруін орналастыру мүмкіндігі

Айта кететін жайт, қарапайым бинарлық кванттаушылардан t -нарлық кванттаушыларға ауысу ақпаратты қорғау бойынша өте тиімді болып табылады. Мұндай ауысу жоғары деңгейлі энтропияның қандайда бір инверсиялық кодтан өзгеше күйі «инверсиялық тесік» орын ауысуына әкеліп соғады. Бұл – бір нейронның күйі екіден жоғары болуынан жүреді. Егер бинарлық кванттаушы «өзім» бейнесі үшін «1» («өзім инверсиясы») бейнесі үшін ол «0» күйін береді) күйін берсе, онда 6-лық монотонды кванттаушыға «өзім бейнесі» «100» кілтінің үш битіне сәйкес келеді («өзім инверсиясы» бейнесі үшін ол «001» күйін береді). Бұл кодтар арасында инверсия байланысы жоқ. Бұл ақпаратты қорғау деңгейін жоғарылатады. Бинарлы

нейрондық желілер көмегімен құрылған шабуылдар (6 бөлімді қараңыз) күрделірек кванттау функциялары бар нейрондық желілердің мәліметтерін қорғауда тиімсіз болып табылады.

Егер «Өзім инверсиясы» бейнесі кванттау интервалының біреуінің дәл ортасына түспесе, жоғары мәнді энтропия сферасының екінші тесігі мүлдем жоғалып кетеді (8.3-сурет). Сонымен бірге бұл биометриялық мәліметтердің нейрожелілік қорғанысының дәрежесін күшейтеді.



8.3-сурет. Монотонды емес көп шекті функциялы нейрон сумматорының шығыс мәліметтерін кванттау мысалы

8.3-суретінен кванттаушы шектік функция монотонды емес болуы мүмкін екені көрініп тұр. Мұндай сызықты емес кванттаушы түрленудің монотонды еместігі монотонды функцияны қолдану мен кездейсоқ ауыстыру жекешеленген кестелер арқылы тәжірибеде оңай жүзеге асады (8.1-суретінде). Мұндай кестелерді қолдануды қабылдау қорғаныс деңгейін хэштеніп жатқан биометрия-код түрлендірушісінің қасиетінің өсу есебінен күшейтеді. Шындығында нейрондардың әрбір шығысында мәліметтерді қосымша кестелік хэштеу жүргізіледі. Мәліметтерді хэштеуді әртүрлі амалдармен орындауға болады, сонымен бірге кездейсоқ сандардың хэш-кестесін қолдануға болады.

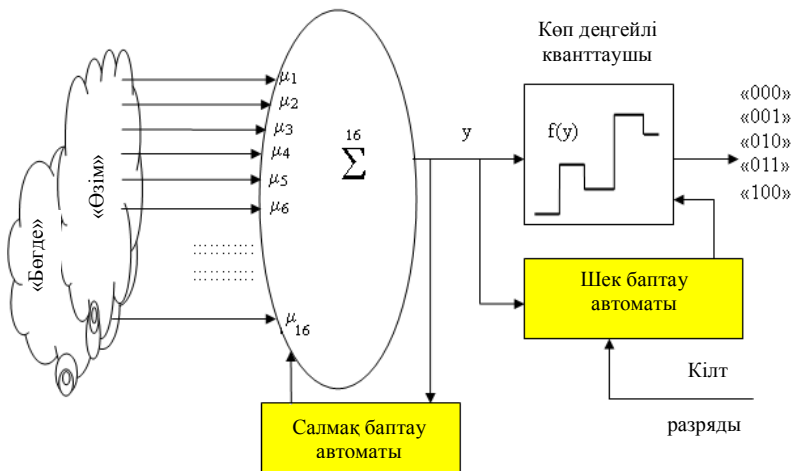
Хэштеуді кестелік орындаудың сапасы ауыстыру кестесінің қаншалықты жағдайға ие екендігіне және осы ауыстырулардың қаншалықты кездейсоқ екендігіне байланысты. Әдетте ең көп хэштенуші нәтиже жағдайдың аз санымен хэштеніп жатқан

кестелер үшін «Бөгде» бейнелердің мәліметтерінің корреляциялық байланысының бұзылуымен қарастырылады. Хэштеніп жатқан кестелер жағдайының санының өсуіне байланысты хэштеу тиімділігіне олардың жағдай санының әсері әлсірейді, себебі нейрон сумматорының шығысында орналасқан «Бөгде» бейне мәліметтерінің корреляциялық байланысы бұл кезде нөл болады.

8.2. Нейронды сумматордың шығыс сигналының көп деңгейлі квантталуымен үйретуге қойылатын талаптар

Бинарлық нейрондарды қолданудан, мәліметтерді көп деңгейлі кванттаған нейрондарға өту [94-98], жасанды нейрондық желілердің үйрету идеологиясын толық өзгертеді. Нейронның сызықты бөлімін үйрету ішкі тапсырмасының біреуінің орнына көп деңгейлі кванттау босағасын баптаудың қосымша тапсырмасы туындайды. Бұл жағдай 8.4-суретінде екі әр түрлі нейронның сызықты және сызықты емес бөлімдерін үйрету автоматтарының пайда болуы түрінде бейнеленген.

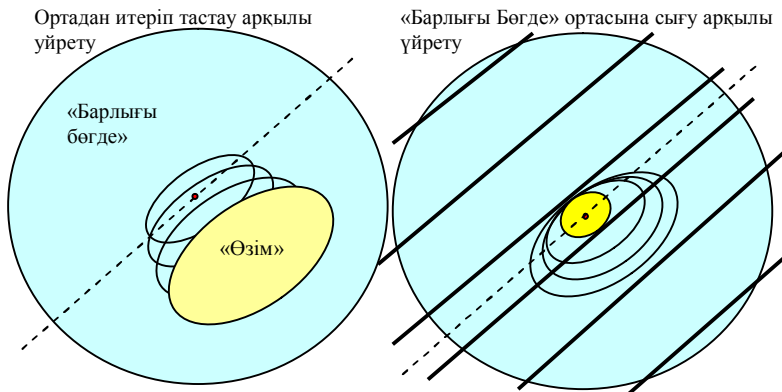
Үйрету тапсырмасы екі тәуелсіз тапсырмаларға ыдырайды. Алдын ала көп деңгейлі нейронның сызықты бөлімін кейбір жеткілікті дәрежеде тұрақты автоматтық үйрету алгоритмі бойынша үйрету қажет. Әрі қарай кванттау функциясының сызықты емес жарамсыздануына шекті орналастырудың немесе нейронның сызықты емес бөлімін үйретудің екінші тапсырмасына өту қажет. Бұл тапсырманың екеуі де тәуелсіз шешілуі керек, тек қана нейронды үйрету функциясы екі кіші функцияға бөлінген кезде екі жеткілікті дәрежеде тұрақты үйрету автоматтарын құруға болады.



8.4-сурет. Нейронның сызықты және сызықты емес бөлімдерін бөліп үйрету

8.3. «Өзім» таралу тұрақтылығын жоғарылату шарты бойынша көп шекті нейронның сызықтық бөлімін үйрету

Алдында белгіленгендей шек функциясы «Барлығы Бөгде» бейнелерінің көп өлшемді сферасын гипержазықтыққа сәйкес келетін «0» мен «1» екі аумағына бөледі. МЕСТ Р 52633.5 бойынша үйреткен кезде бөлуші гипержазықтық «Барлығы Бөгде» аумағының ортасы арқылы өтеді. Салмақ коэффициенттерін МЕСТ Р 52633.5-2011 бойынша баптау кезінде «Өзім» аумағының көлемін үлкейтудің әсері мен оны «Барлығы Бөгде» аумағының перифериясына итеру әсері болады. Бұл жағдай 8.5-суретінің сол жағында бейнеленген. Үйретудің мұндай тәсілі «Өзім» бейнесінің мәліметтерін тарату ертелі-кеш бөлуші гипержазықтықпен қиысуды тоқтатуға алып келеді де, нейрон «Өзім» бейнесінің үлгілерін сенімді танып бастайды.



8.5-сурет. Нейронның сызықты бөлігін үйрететін екі стратегия

Егер үйретудің сапа критериясын өзгертсек және критерия бойынша үйрету алгоритмінен «Өзім» мәліметтерінің таралуын мүмкін болғанша қатты сығуын талап етсек:

$$Q_c = \frac{\sigma(y_{\xi})}{\sigma(y_v)} \quad (8.1)$$

онда жағдай түбегейлі түрде өзгереді.

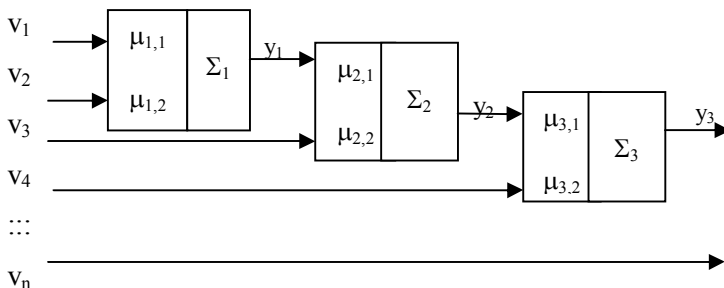
Тұрақтылық көрсеткіштерін (8.1) жоғарылататын барлық үйрету алгоритмдері «Өзім» мәліметтерінің таралу диаметрін сыға отырып, оның ортасын «Барлығы Бөгде» бейнелерінің көпшілік аймағының ортасына жылжытып жұмыс істейді. Бұл жағдай 8.1-суретінің оң жағында суреттелген. Сонымен бірге критерияның қалай максимумдалуы (8.1) ешбір мәнге ие емес.

Жеке туындыны есептеуде құрылған $\frac{\partial Q_c}{\partial \mu_i}$ максимумды іздеу

итерационды алгоритмдері түрінде, сонымен бірге өзге салмақ коэффициенттерін есептейтін итерационды емес алгоритмдер қолданылуы мүмкін.

Мысалы, нейрондардың сызықтық бөлімін жылдам үйретудің итерационды емес алгоритмдері күрделі көп өлшемді

бір тапсырманы бірнеше қарапайым екі өлшемді тапсырмамен ауыстыру арқылы биометриялық мәліметтер жұбын байланыстыру процедурасының қорында құрылуы мүмкін. Тапсырманы мұндай бөлшектеп байланыстыру 8.6-суретінде бейнеленген.



8.6-сурет. Көп өлшемді тапсырманы екі өлшемді тапсырманың реттелген шешіміне бөлшектеп байланыстыру

Басында сумматордың салмақ коэффициенттері екі кіріспен v_1 , v_2 және y_1 шығысы келесі есептеу жолымен орналасқан:

$$\begin{cases} \mu_{1,1} = \frac{1}{\sigma(v_1)}; \\ \mu_{1,2} = -\text{sign}\{r(v_1, v_2)\} \frac{1}{\sigma(v_2)}; \\ r(v_1, v_2) = \frac{1}{N} \sum_{i=1}^N \frac{(E(v_{1i}) - v_{1i}) \cdot (E(v_{2i}) - v_{2i})}{\sigma(v_1) \cdot \sigma(v_2)}; \end{cases} \quad (8.2)$$

Салмақ коэффициенттерінің бірінші олардың екі кірісті сумматорларын салмақ коэффициенттерінің екінші сумматоры есептейді:

$$\begin{cases} \mu_{2,1} = \frac{1}{\sigma(y_1)}; \\ \mu_{2,2} = -\text{sign}\{r(y_1, v_3)\} \frac{1}{\sigma(v_3)}; \\ r(y_1, v_3) = \frac{1}{N} \sum_{i=1}^N \frac{(E(y_{1i}) - y_{1i}) \cdot (E(v_{3i}) - v_{3i})}{\sigma(y_1) \cdot \sigma(v_3)}; \end{cases} \quad (8.3)$$

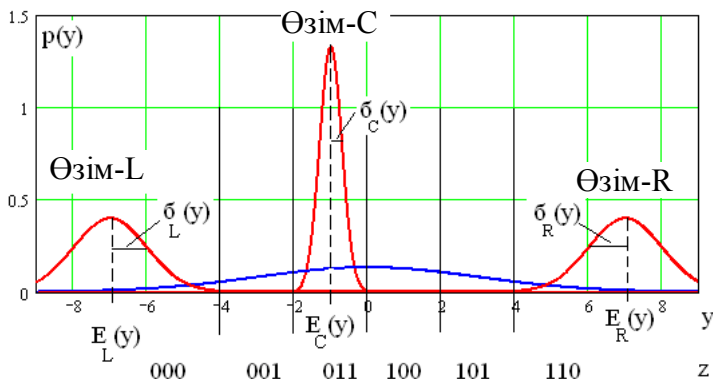
(8.2) және (8.1) формулаларын салыстыра отырып әрбір сумматордың салмақ коэффициенттерін есептеу кезінде оның биометриялық параметрлер кірісінің орташа квадраттық ауытқуын білу керек. Демек, есептеуді қалағанымызша осындай алгоритммен өте көп санды кірісті нейрондарды үйрете отырып, ұзақ жалғастыруымызға болады. Сонымен бірге есептеу тұрақтылығы жеткілікті дәрежеде жоғары, себебі жұп корреляция коэффициенттерінің үлкен мәнділігі кезінде салмақ коэффициенттерінің белгісін таңдаумен қате жіберу мүмкін емес. Жұп корреляцияның коэффициенттерінің аз мәнділігі кезінде белгіні анықтаудың қате ықтималдығы жоғары, бірақ мұндай жағдайда корреляцияның коэффициент белгісі сапа көрсеткішінің өсуіне ешқандай әсер етпейді. Егер биометриялық мәліметтер корреляцияланған болмаса, онда салмақ коэффициенттерінің белгілері еркінше таңдалуы мүмкін.

К кірістінің екі кірісті сумматорларының салмақ коэффициенттері есептелгенде барлық жеке сумматорлар жалпы бір k кірісті нейрон сумматорына оралуы мүмкін. Сонымен бірге жалпы кірісті салмақ коэффициенттері жеке салмақ коэффициенттерінің туындысы сияқты есептелінеді:

$$\left\{ \begin{array}{l} \mu_1 = \prod_{i=1}^k \mu_{i,1} \\ \mu_2 = \prod_{i=1}^{k-1} \mu_{i,2} \\ \dots\dots\dots \\ \mu_k = \mu_{k,k} \end{array} \right. \quad (8.4)$$

8.4. Нейронның сызықты бөлімін үйретудің екі әр түрлі алгоритмдерін құрастыру

Нейронның сызықты бөлімі үшін екі шешімді алғаннан кейін («Өзім» бейнесін сызып және итере отырып), оларды құрамдастыра отырып, осы шешімдердің көптеген сызықты амалдарын алуға болады. Бұл жағдай 8.7-суретінде бейнеленген.



8.7-сурет. Екі сызқты шешімнен үшінші сызқты шешімді алу

Бұл, «а» реттемелі параметрді 0-ден 1-ге дейін морфинг теңдемесінде өзгерте отырып,

$$\mu_i(a, C, R) = a \cdot \mu_i(R) + (1 - a) \cdot \mu_i(C) \quad (8.5)$$

«Өзім-С» таралуының математикалық болжалын «Өзім-Р» таралуының математикалық болжалы жағына бір қалыпты жылжытуға болады деген сөз. Сонымен бірге, $b_C(y)$ бір қалыпты $b_R(y)$ дейін артады.

Нейрожелілік $\mu_i(R)$ шешімді қарапайым инверсиялау жолымен $\mu_i(L)$ инверсиялық шешімін оңай алуға болатыны белгілі. Соңғысының мағынасы, нейрожелінің табылған үш $\mu_i(R)$, $\mu_i(L)$, $\mu_i(C)$ шешімінің салмақ коэффициенттерін қолдана отырып, «Барлығы Бөгде» таралуының кез келген нүктесіне «Өзім» таралуының ортасын орналастыруға болады. Әрі қарай осы таралудың шегін табу қажет және сәйкесінше нейронның сызқты емес элементінің шығыс мәліметтерін дискреттеушінің жағдай санын анықтау. «Өзім» үндеуінің математикалық болжалының таңдаған жағдайына байланысты сызқты емес жағдайының тұрақтылық саны $f(y)$ төменде көрсетілген қатынас сияқты жайғасады:

$$k \approx \frac{\sigma(y_\xi)}{\sigma(y_v)} \quad (8.6)$$

«Өзім» шекарасының шын мәніндегі жағдайын жасыру үшін қосымша жалған шекараның оң немесе сол жағына енгізген жеткілікті. 8.7-суретінде «Өзім-С» таралуының шын мәніндегі жағдайының оң немесе сол жағында қойылған жалған шекараның үлгісі берілген.

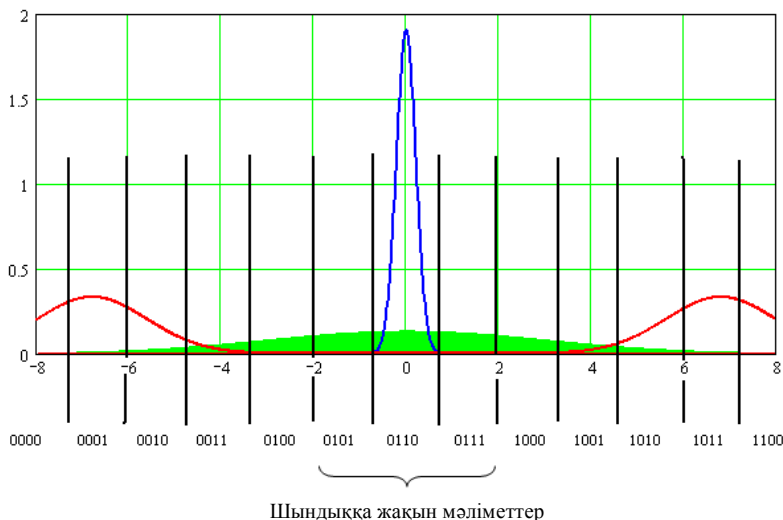
Жалған шекаралар шынайы болуы керек, демек, «Барлығы Бөгде» таралуының шетінен шықпауы, сонымен бірге олардың арасындағы интервал қимыл өлшемі бойынша «Барлығы Бөгде» таралуының периферия жағына кеңеюі керек. «Өзім» шекарасының шын мәніндегі жағдайының құпия кепілі жалған шекаралардың шынайы орналасуы болып табылады. Жалған шекаралардың шынайы орналасуы «Өзім-С», «Өзім-R», «Өзім-L» шын мәніндегі таралуларының параметрлерін сыртқы бақылаушы білмейтіндігінде. Сызықты емес элементті баптауы туралы аралық мәліметтер әрбір нейрон үйретілгеннен кейін жойылады.

8.5. Көп деңгейлі кванттау функциясының шегін баптау

Нейронды үйретудің екінші бөлімі кванттау функция шегінің санын таңдау мен кванттау шегінің орналасуын баптау болып табылады. Шек санын жоғарыдан бағалаудың ең қарапайым әдісі «Бөгде» және «Өзім» бейнелерінің орташа квадраттық ауытқуының қатынасын сыққаннан кейін есептеу болып табылады:

$$\max(n) \approx \frac{\sigma(y_{\xi})}{\sigma(y_c)} \quad (8.7)$$

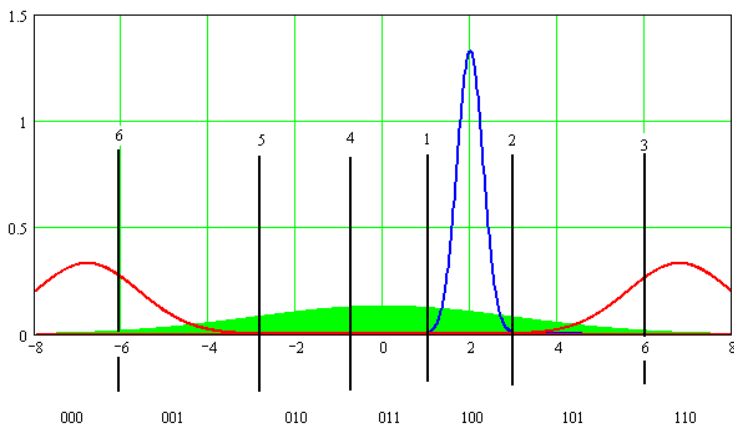
(8.7) формуласы бойынша бағаланған шек саны шығынды болып табылады, егер шектің соншалықты көп санын пайдалансақ, онда біз 8.8-суретіндегі жағдайды аламыз.



8.8-сурет. Кванттау функциясы шегінің мүмкін болған
максималды (шығын) саны

8.8-суретінен көрініп тұрғандай, шабуыл жасаушы шектің торын жиі бақылап отырып, тек «Барлығы Бөгде» таралуының ортасында орналасқан шектерді ғана шынайы сияқты қарастырады. Шабуыл жасаушыға «Өзім» таралу бейнесінің ортасында орналасқан көрші шектердің арасындағы енінің статистикасының байланысы белгілі болады. Демек, бірдей арақашықтағы шектердің тым көп санын енгізу «Барлығы Бөгде» таралуының ортасында «Өзім» бейне мәліметтерінің орналасуы туралы гипотезаға сөзсіз алып келеді.

Осыған байланысты тиімдірек тәсіл шектің орналасу жағдайын баптау кезінде бір жағынан «Өзім» бейне мәліметтерінің орналасу жағдайына байланысты жүргізілуі, ал екінші жағынан ол шектің кеңею тиімділігін олардың «Барлығы Бөгде» бейнелер мәліметтерінің перифериясына қозғалуы кезінде есепке алуы керектігі болып табылады. Сонымен бірге, «Барлығы Бөгде» бейнелерінің ортасына шектерді орналастыру автоматының қозғалысы кезінде шектердің арасындағы арақашықтық сығылуы қажет. 8.9-суретінде суреттелген осы жағдайда шектің орналасу жағдайы шынайы болады.



8.9-сурет. Шектердің орналасу процедурасының шынайылығы

Ең бірінші «Өзім» бейнесінен бөлініп шыққан таралудың айналасына шектер қойылуы қажет (8.9-суретіндегі бұл шектер 1 және 2 нөмірлерімен). «Өзім» бейнесінен бөлініп шыққан шын мәніндегі шектерді біле отырып, бапталатын i -ші нейрон үшін екінші текті қате ықтималдығын табуға болады:

$$P_{2,i} = \frac{1}{\sigma(y_{\xi})\sqrt{2\pi}} \int_{\min(y_{vi})}^{\max(y_{vi})} \exp\left\{-\frac{(E(y_{\xi}) - y_{\xi})^2}{2\sigma^2(y_{\xi})}\right\} dy_{\xi} \quad (8.8)$$

Идеалды түрде шектерді шындыққа сай орналастыру кезінде барлық шек интервалдары үшін бірдей екінші текті қате ықтималдығы болуы қажет (8.8). Осыған сүйене отырып, 8.9-суретінде көрсетілгендей, 3,4,5,6 шектерін орналастыру қиын емес. «Өзім» бейне мәліметтерінің таралуының ортасын шектердің ортасына жылжыта отырып, шектердің шындыққа сай келуіне көз жеткізу өте оңай.

Егер енді 8.8-суретіндегі және 8.9-суреттеріндегі шек сандарын салыстырсақ, онда шектің шындыққа сай сандары олардың максималды бағасынан әрқашан екі есеге үлкен болады.

БИБЛИОГРАФИЯЛЫҚ ТІЗІМ

1. *Feng Hao, Ross Anderson, and John Daugman.* Crypto with Biometrics Effectively, IEEE TRANSACTIONS ON COMPUTERS. – VOL. 55. – № 9. – SEPTEMBER 2006.
2. *Y. Dodis, L. Reyzin, A. Smith.* Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, pages 523–540, 2004.
3. *Arakala A., Jeffers J., Horadam K. J.* Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. // *Advances in Biometrics (LNCS 4642)*, Springer. – Pp. 760–769, 2007.
4. *Чморра А. Л.* Маскировка ключа с помощью биометрии «Проблемы передачи информации». – 2011. – № 2(47). – С. 128-143.
5. *Чморра А. Л., Уривский А. В.* Биометрическая система аутентификации / Патент № RU2316120. – Оpubл. 27.01.2008. – Бюл. № 3. – Приоритет от 12.05.2004.
6. ГОСТ Р 52633.0–2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». – М.: Стандартинформ, 2006.
7. *Язов Ю. К. и др.* Нейросетевая защита персональных биометрических данных / *Ю. К. Язов (редактор и автор) / В. И. Волчихин, А. И. Иванов и др.* – М.: Радиотехника, 2012. – 157 с.
8. ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа». – М.: Стандартинформ, 2012.
9. *Волчихин В. И., Иванов А. И., Фунтиков В. А.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации // *Монография.* – Пенза: Изд-во Пензенского государственного университета, 2005. – 273 с.
10. *Ахметов Б. С., Иванов А. И. и др.* О связи высокоразмерной энтропии и высокоразмерной корреляции с математическим ожиданием модулей коэффициентов парной корреляции. – Усть-Каменогорск: ВКГТУ, 2013. – С. 240–244.
11. *Ахметов Б. С., Иванов А. И. и др.* Оценка вероятностей появления ошибок нейросетевых преобразователей биометрия-

код на основе малых выборок. Высокие технологии – залог устойчивого развития // Мат. II Межд. науч. конф. – Т.1. – Алматы, 2013. – С. 234–237.

12. *Ахметов Б. С., Иванов А.И. и др.* Синхронизация процедур нейросетевого обучения особенностям рукописного почерка по точкам смены направления движения пера. – Алматы: КазНТУ // Сб. тр. II Межд. науч.-прак. конф. «Информационно-инновационные технологии: интеграция науки, образования и бизнеса». – 2011. – Т. 2. – С.118–123.

13. ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора». – М.: Стандартинформ, 2012.

14. *Ахметов Б. С., Волчихин В. И. и др.* Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации // Монография. – Алматы: LEM. – 2013. – 152 с.

15. *Ахметов Б. С., Захаров О. С. и др.* Метод оценки вероятностей появления ошибок нейросетевых преобразователей биометрия-код, использующий очень малые тестовые выборки // Вестн. КазНТУ. – 2013. – № 3.

16. *Ахметов Б. С., Иванов А. И. и др.* Энтропийно-корреляционный подход к расчету вероятности совместного появления большого числа зависимых событий // Вестн. КБТУ. – 2013. № 2(25) – С. 55–59.

17. *Ахметов Б. С., Иванов А. И. и др.* Биометрическая аутентификация граждан в открытых информационных пространствах // Тр. I Межд. науч.-прак. конф. «Интеллектуальные информационные и коммуникационные технологии – средство осуществления третьей индустриальной революции в свете стратегии "Казахстан-2050"». – Астана: ЕНУ им. Л. Н. Гумилева, 2013. – С. 458–459.

18. *Малыгин А. Ю., Ахметов Б. С. и др.* Учет влияния корреляционных связей на результаты тестирования преобразователей биометрия-код // Информационные и телекоммуникационные технологии: образование, наука, практика: Сб. тр. Межд. науч.-практ. конф. – Алматы: КазНТУ, 2012. – С. 34–37.

19. Болл Руд и др. Руководство по биометрии / Болл Руд, Коннел Джонатан Х. и др. – М.: Техносфера, 2007. – 368 с.

20. Ларин П. З., Реввер Е. И. Обведем вокруг пальца? Обман биометрических систем доступа, использующих дактилоскопическую идентификацию личности // Информационная безопасность – Information Security». – Groteck. – 2004. – № 3.

21. Arakala A., Jeffers J., Horadam K. J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication // Advances in Biometrics (LNCS 4642). Springer. – 2007. – Pp. 760–769.

22. Ratha N. K., Chikkerur S. – Generating cancelable fingerprint templates // IEEE Trans. PAMI, 29(4). – 2007. – P. 561–572.

23. ISO/IEC 19784–1:2006 "BioAPI – Biometric Application Programming Interface – Part 1: BioAPI Specification", <http://www.bioapi.org/>

24. ГОСТ Р ИСО/МЭК 19784–1–2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс». – Ч. 1. Спецификация биометрического программного интерфейса. – М.: Стандартинформ, 2007.

25. ГОСТ Р ИСО/МЭК 19784–2–2010 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс». – Ч. 2. Интерфейс поставщика биометрической функции архива. – М.: Стандартинформ, 2011.

26. ГОСТ Р ИСО/МЭК 19794–2–2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными». – Ч. 2. Данные изображения отпечатка пальца – контрольные точки. – М.: Стандартинформ, 2007.

27. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152–ФЗ «О персональных данных». Режим доступа: <http://www.rg.ru/>

28. ГОСТ Р ИСО/МЭК 19794–10–2010 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Данные геометрии контура кисти руки». – М.: Стандартинформ, 2011.

29. John Daugman «Probing the Uniqueness and Randomness of Iris Codes: Results From 200 Billion Iris Pair Comparisons» Proceedings of the IEEE | Vol.

30. Язов Ю. К. и др. Нейросетевая защита персональных

биометрических данных. – М.: Радиотехника. – 2012. – 160 с.

31. Белоцерковский О. М., Глазунов А. С., Щенников В. В. Компьютерное распознавание человеческих лиц // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – 1997. – № 8. – С. 3–14.

32. Глазунов А. Компьютерное распознавание человеческих лиц // Открытые системы. – 2000. – № 3, www.osp.ru/os/2000/03/043.htm.

33. Пентланд А., Чаудхари Т. Распознавание лиц для интеллектуальных сред // Открытые системы. – 2000. – № 3, www.osp.ru/os/2000/03/028.htm.

34. Шапиро Л., Стокман Дж. Компьютерное зрение. – М.: Бином, 2009. – 752 с.

35. Дуда Р., Харп П. Распознавание образов и анализ сцен. – М.: Мир. 1976.

36. А.с. № RU 112 992 «Устройство бесконтактного измерения геометрических параметров лица человека» / Захаров С. М., Митрохин М. А. Оpubл. 27.01.12.

37. ОКР «Разработка и подготовка производства телекоммуникационного оборудования, разработка программного сетевого, прикладного и специального обеспечения для создания цифровых сетей связи с персонализированным доступом». – Пенза: ОАО «НПП «Рубин», ФГБОУ ВПО «ПГУ», 2012.

38. А. с. RU 2451409 С2. Способ однозначного хэширования неоднозначных биометрических данных / А. И. Иванов, С. М. Иванов. Заявлено 26.01.2010; Оpubл. 20.05.2012, Бюл. № 14.

39. Uludag U., Pankanti S., Prabhakar S., Jain A. K. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE. – 2004. – Vol. 92. – № 6. – P. 948–960.

40. Juels A., Sudan M. A. Fuzzy Vault Scheme // Proceedings of IEEE International Symposium on Information Theory. Lausanne, Switzerland, 2002. – P. 408.

41. Dodis Y., Reyzin L., Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // Advances in Cryptology – EUROCRYPT 2004. Christian Cachin

and Jan Camenisch, ed. – Vol. 3027 of Lecture Notes in Computer Science. Springer – Verlag, 2004. – P. 79–100.

42. *Sahai A., Waters B.* Fuzzy identity-based encryption // Proceedings of EUROCRYPT 2005, LNCS 3494. Springer – Verlag, 2005. – P. 457–473.

43. *Baek J., Susilo W., Zhou J.* New construction of fuzzy identity-based encryption // Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. ACM New York. NY, USA, 2007. – P. 368–370.

44. *Fang L. M., Wang J. D., Ren Y. J., Xia J. Y., Bian S. Z.* Chosen – Ciphertext Secure Fuzzy Identity – Based Key Encapsulation without ROM. Cryptology ePrint Archive: Report 2008/139, 2008. URL: <http://eprint.iacr.org/2008/139>.

45. *Fang L., Xia J.* Full Security: Fuzzy Identity Based Encryption. Cryptology ePrint Archive: Report 2008/307. URL: <http://eprint.iacr.org/2008/307>.

46. *Yang P., Cao Z., Dong X. I.* Fuzzy Identity Based Signature. Cryptology ePrint Archive: Report 2008/002. URL: <http://eprint.iacr.org/2008/002>.

47. *Burnett A., Duffy A., Dowling T. A.* Biometric Identity Based Signature Scheme. Cryptology ePrint Archive: Report 2004/176. URL: <http://eprint.iacr.org/2004/176>.

48. *Dodis Y., Katz J., Reyzin L., Smith A.* Robust fuzzy extractors and authenticated key agreement from close secrets // Advances in Cryptology – CRYPTO 2006. Cynthia Dwork, ed. Vol. 4117 of Lecture Notes in Computer Science. Springer – Verlag. – 20–24 August 2006. – P. 232–250.

49. *Kanukurthi B., Reyzin L.* Key Agreement from Close Secrets over Unsecured Channels. Cryptology ePrint Archive: Report 2008/494. URL: <http://eprint.iacr.org/2008/494>.

50. *Boyen X.* Reusable cryptographic fuzzy extractors // Eleventh ACM Conference on Computer and Communication Security. ACM. – October 25–29 2004. – P. 82–91.

51. *Boyen X., Dodis Y., Katz J., Ostrovsky R., Smith A.* Secure remote authentication using biometric data // Advances in Cryptology – EUROCRYPT 2005. R. Cramer, ed. Springer – Verlag, 2005. – Vol. 3494 of LNCS. – P. 147–163.

52. *John Daugman*. Probing the Uniqueness and Randomness of Iris Codes: Results From 200 Billion Iris Pair Comparisons» Proceedings of the IEEE. – Vol. 94. – № 11. – November 2006. – Pp. 1928–1935.

53. *Daugman John G*. Biometric personal identification system based on iris analysis, US Patent Number: 5,291,560 Data of Patent: Mar.1, 1994.

54. *Ушмаев О. С., Кузнецов В. В.* Получение устойчивого криптографического ключа из биометрической характеристики изображения отпечатков пальцев. – The 22nd International Conference on Computer Graphics and Vision, Russia, Moscow, October 01–05, 2012. – Pp. 125–127.

55. *Смит Ричард Э.* Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2002. – 424 с.

56. А. с. RU 2316120 С2 Биометрическая система аутентификации / *Чморра А. Л., Уривский А. В.* Заявлено 05.10.2014; Опубл. 27.01.2008, Бюл. № 3.

57. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. – М.: Техносфера, 2007. – 320 с.

58. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки // Монография / Под ред. Добрушиной Р. Л., Самойленко С. И. – М.: МИР, 1976. – 364 с.

59. *Самойленко С. И.* Помехоустойчивое кодирование. – М.: Радио и связь, 1968. – 240 с.

60. *Безяев А. В.* Нейросетевой преобразователь биометрии в самокорректирующийся код, совершенно не обладающий избыточностью // Нейрокомпьютеры: разработка и применение. – 2012. – № 3. – С. 52–55.

61. *Безяев А. В., Фунтикова Ю. В.* Оптимизация параметров хэш-кодов, осуществляющих обнаружение и корректирование ошибок в биометрических преобразователях // Тр. науч.-техн. конф. кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. – Т 8. – Пенза, 2012. – С. 76–78 (<http://пниэи.рф/activity/science/BIT/T8-p76.pdf>).

62. *Круглов В. В., Дли М. И., Голунов Р. Ю.* Нечёткая логика и искусственные нейронные сети. – М.: Физматлит, 2001. – 221 с.

63. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / Пер. с польского И. Д. Рудинского. – М.: Горячая линия – Телеком, 2004.
64. Саймон Хайкин. Нейронные сети: Полный курс. – М.: Вильямс, 2006. – С. 1104.
65. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика. – М.: Мир, 1992. – 240 с.
66. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений // Монография. – Пенза: Изд-во ПГУ, 2000.
67. Волчихин В. И., Иванов А. И., Фунтиков В. А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации // Монография. – Пенза: Изд-во ПГУ, 2005. – 273 с.
68. Иванов А. И. Нейросетевые алгоритмы биометрической идентификации личности. Сер. «Нейрокомпьютеры и их применение». – М.: Радиотехника, 2004. – Вып. 15. – 144 с.
69. Иванов А. И., Кисляев С. Е., Гелашивили П. А. Искусственные нейронные сети в биометрии, медицине, здравоохранении. – Самара: ООО «Офорт», 2004. – 236 с.
70. Минский М., Пейперт С. Перцептроны. – М.: Мир, 1971. – 261 с.
71. Розенблатт Ф. Принципы нейродинамики: Перцептроны и теория механизмов мозга. – М.: Мир, 1965. – 480 с.
72. Куликов С. В., Секретов М. В. и др. Учет «тяжелых» хвостов ненормального закона распределения биометрических параметров все «Чужие» при настройке нелинейного элемента нейрона с несколькими дискретными состояниями // Нейрокомпьютеры: разработка, применение. – 2012. – № 3. – С. 56–59.
73. ГОСТ Р 52633.4–2012 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код». – М.: Стандартинформ, 2012.

74. ГОСТ Р 52633.7–2013 «Защита информации. Техника защиты информации. Высоконадежная мультибиометрическая аутентификация». – М.: Стандартинформ, 2013.

75. *Минский М., Пейперт С.* Персептроны. – М.: Мир, 1971.

76. ГОСТ Р 52633.3–2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора». – М.: Стандартинформ, 2011.

77. *Язов Ю. К., Волчихин В. И. и др.* Нейросетевая защита персональных биометрических данных // Монография. – М.: Радиотехника, 2012. – 160 с.

78. *Надеев Д. Н.* Синтез таблиц вероятности ошибок первого и второго рода для неидеальных биометрико-нейросетевых преобразователей с 256 выходами // Нейрокомпьютеры: разработка, применение. – 2007. – № 12. – С. 30–31.

79. *Иванов А. И., Майоров А. В., Язов Ю. К.* Энтропийно-корреляционная оценка хэширующих свойств нейросетевого преобразователя биометрия-код доступа // Нейрокомпьютеры: разработка, применение. – М.: Радиотехника. – 2012. – № 3. – С. 35–40.

80. *Ахметов Б. С., Волчихин В. И. и др.* Моделирование длинных биометрических кодов, воспроизводящих корреляционные связи выходных данных нейросетевого преобразователя // Нейрокомпьютеры: разработка, применение. – М.: Радиотехника. – 2012. – № 3. – С. 40–43.

81. *Ахметов Б. С., Волчихин В. И. и др.* Учет влияния корреляционных связей на результаты тестирования преобразователей биометрия-код // Сб. тр. Межд. науч.-прак. конф. «Информационные и телекоммуникационные технологии: образование, наука, практика». – Алматы: КазНТУ, 2012. – С. 34 – 37.

82. ГОСТ Р 52633.5–2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа». – М.: Стандартинформ, 2011.

83. *Ахметов Б. С., Безяев В. С.* Сравнительная оценка уровня безопасности средств биометрической аутентификации // Сб. тр. II Межд. науч.-прак. конф. «Информационно-инновационные технологии: интеграция науки, образования и бизнеса». – Алматы: КазНТУ, 2011. – Т. 1. – С. 382–386.

84. *B. Akhmetov, A. Ivanov, V. Funtikov, I. Urnev* Evaluation of Multidimensional Entropy on Short Strings of Biometric Codes with Dependent Bits. «Progress in Electromagnetics Research Symposium» PIERS Proceedings, August 19–23, Moscow, RUSSIA, 2012. – P. 66–69.

85. ГОСТ Р 52633.2–2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации». – М.: Стандартинформ, 2011. 24 с.

86. *B. Akhmetov, A. Ivanov, A. Malygin, I. Urnev, V. Funtikov.* Statistical description of output states of the neural network “biometrics-code” transformers «Progress in Electromagnetics Research Symposium» PIERS Proceedings. – August 19–23. – Moscow, RUSSIA, 2012. – P. 61–65.

87. *Иванов А. И., Фунтиков В. А.* Моделирование кодовых последовательностей с энтропией естественных и искусственных биометрических языков «Инфокоммуникационные технологии». – 2010. – Т. 8. – № 4. – С. 75–79.

88. *Маршалко Г. Б.* Вопросы оценки стойкости нейросетевой системы биометрической аутентификации // Мат. конф. «РусКрипто–2013»

http://www.ruscrypto.ru/netcat_files/File/ruscrypto.2013.051.zip

89. *Ахметов Б. С., Иванов А. И., Кармбаев Т. С.* Нейрожелілердің артық байланыстары болуынан биометриялық-кодтың ішінара әшкерелену қаупі мен оларға қарсы тұру әдісі // ҚазҰТУ хабаршысы. – 2014. – № 2 (102). – Б. 147–151.

90. *Андреев Д. Ю.* Оценка эффективности применения обычной и взвешенной метрики Хэмминга при упорядочивании баз естественных биометрических образов // Нейрокомпьютеры: разработка, применение. – 2012. – № 3. – С. 31–34.

91. *Андреев Д. Ю.* Сокращение затрат на нечеткую адресацию биометрических образов через использование взвешенной меры Хэмминга. Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих Безопасность информационных технологий. – 2012. – Т. 8. – Пенза. – С. 32–36 (<http://www.pniei.penza.ru/RV-conf/T8/C32.pdf>)

92. А. с. RU 2346397 С1. Способ защиты персональных данных биометрической идентификации и аутентификации / *Иванов А. И., Фунтиков В. А., Ефимов О. В.* Заявлено 26.06.2007; Опубл. 10.02.2009, Бюл № 4.

93. *Фунтиков В. А., Назаров И. Г., Бурушкин А. А.* Национальные стандарты России: конфиденциальность персональных биометрических данных // Стандарты и качество. – 2010. – № 7. – С. 28–33.

94. *Язов Ю. К. и др.* Нейросетевая защита персональных биометрических данных / *Ю. К. Язов* (редактор и автор), соавторы *В.И. Волчихин, А.И. Иванов, В.А. Фунтиков, И.Г. Назаров.* – М.: Радиотехника, 2012. – 157 с.

95. *Иванов А. И.* Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Изд-во ПГУ, 2000. – 188 с.

96. *Волчихин В. И., Иванов А. И., Фунтиков В. А.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации // Монография. – Пенза: ПГУ, 2005. – 273 с.

97. *Куликов С. В., Секретов М. В. и др.* Учет «тяжелых» хвостов ненормального закона распределения биометрических параметров все «Чужие» при настройке нелинейного элемента нейрона с несколькими дискретными состояниями // Нейрокомпьютеры: разработка, применение. – 2012. – № 3. – С. 56–59.

98. А. с. RU 2451409 С2. Способ однозначного хэширования неоднозначных биометрических данных / *А. И. Иванов, С. М. Иванов.* Заявлено 26.01.2010; Опубл. 20.05.2012, Бюл. № 14.

МАЗМҰНЫ

	КІРІСПЕ.....	3
1.	БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫҢ ПАЙДА БОЛУ ЖӘНЕ ДАМУ ТАРИХЫ.....	5
1.1.	Негізгі түсініктер және анықтамалар.....	8
1.1.1.	Бірінші және екінші текті қателіктер ықтималдығы.....	8
1.1.2.	Жүйеге кіру кілтінің кодына биометриялық бейнелерді түрлендіру.....	9
1.1.3.	Биометриялық бейнелер көп өлшемді континуумын аз дискреттік үлгілер санымен ұсыну.....	11
1.1.4.	Хэмминг арақашықтығы кеңістігіне өту.....	14
1.1.5.	Биометриялық параметрлердің ақпараттылығы.....	16
1.1.6.	Биометрия-код түрлендіргішінің энтропиясын бағалау.....	18
1.1.7.	Шешіліп жатқан биометриялық тапсырманың өлшемін бағалау.....	20
2.	ЗАМАНАУИ БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАР ТАЛДАУЫ.....	22
2.1.	Саусақ таңбасы суретін талдау технологиясы.....	22
2.2.	Саусақ және алақан қантамырлары ағашын талдау технологиясы.....	24
2.3.	Алақан геометриясын талдау технологиясы.....	26
2.4.	Көздің шатырша қабығы мен көз түбінің тамырларын талдау технологиясы.....	27
2.5.	Адам беті геометриясы талдауының екі және үш өлшемді технологиялары.....	30
2.6.	Құлақ қалқаны геометриясын талдаудың үш өлшемді технологиясы.....	35
2.7.	Дауыс ерекшелігі талдауының бір және екі өлшемді технологиясы.....	37
2.8.	Қолжазбалық жазу динамикасы талдауының технологиясы.....	38
2.9.	Мультибиометриялық қосымшаларды қолданудың болашағы.....	42

3.	БИОМЕТРИЯЛЫҚ ПАРАМЕТРЛЕРДІҢ АЙҚЫН ЕМЕС ЭКСТРАКТОРЛАРЫ.....	48
3.1.	Биометриялық мәліметтерді кванттаудың қарапайым нұсқасы.....	48
3.2.	Гамманы салу арқылы ақпаратты жасырып ұстайтын «айқын емес экстрактор».....	50
3.3.	Гамманы салу және биокодты хэштеу мен «айқын емес экстракторлар».....	52
3.4.	«Айқын емес экстракторлардағы» қолданылатын өзін-өзі түзететін кодтарды таңдау.....	53
4.	БИОМЕТРИЯ-КОДТЫ НЕЙРОЖЕЛІЛІК ТҮРЛЕНДІРГІШ.....	57
4.1.	Дара нейронның (персептрон) итерационды Үйрету алгоритмі.....	57
4.2.	Нейронды үйретудің абсолют тұрақты итерациялық емес алгоритмі.....	62
4.3.	Нейрондар желілерін үйрету мен қалыптастыру. Нейрожелілік контейнерлер.....	66
4.4.	Жасанды нейрондардың екі қабатты желісінің әмбебаптығы.....	69
4.5.	Нейрожелілік түрлендіргіштердің биокод ұзындығын ұтымды таңдауы.....	74
4.6.	Нейронның екінші қабатымен биокодты нейрожелілік түзету.....	76
4.7.	Екінші қабат нейрондары орындайтын «Бөгде» мәліметтерін хэштеу.....	78
5.	БИОМЕТРИЯЛЫҚ МӘЛІМЕТТЕР ҚОРЫН ҚАЛЫПТАСТЫРУ МЕН НЕЙРОН ЖЕЛІЛЕРІН ҮЙРЕТУ САПАСЫН СЫНАУ.....	80
5.1.	Шағын сынақ сұрыптамасында бірінші текті катенің пайда болу ықтималдылығының бағасы.....	80
5.2.	Екінші текті кате ықтималдығын бағалау проблемалары, биометриялық бейнелердің үлкен қорларын қалыптастыру қажеттілігі.....	83
5.3.	Биометриялық бейне үлгілерінің тоғысуы арқылы көбеюі.....	87

5.4.	«Барлығы бөгде» көп өлшемді кеңістігін біркелкі толықтыратын биометриялық бейнелер қорының синтезі.....	91
5.5.	Жұп корреляциялық байланыстардың орташаланған модулі бойынша іріктеу шабуылына тұрақтылықты жылдам бағалау.....	94
6.	БИО-МӘЛІМЕТТЕРДІҢ КРИПТОГРАФИЯЛЫҚ ҚОРҒАНЫСҚА ИЕ ЕМЕС АҚПАРАТЫНА ҚОЛ ЖЕТУДЕН БИОМЕТРИЯЛЫҚ ҚОРҒАЙТЫН ҚҰРАЛДАРҒА ТӨНЕТІН ҚАУІПТЕР ЖӘНЕ ОСЫ ҚАУІПТЕРДІ ЖҮЗЕГЕ АСЫРУШЫ ШАБУЫЛДАР.....	99
6.1.	«Соңғы» битке шабуыл арқылы ақпаратты қорғау программасының модификациясына төнетін қауіп..	99
6.2.	«Бөгде» бейнелерінің үлкен қорын іріктеу шабуылы арқылы биометриялық егіздерді іздеу қауіпі.....	100
6.3.	Биометриялық қорғаныс автоматының мүмкін болған кіріс және шығыс жағдайын іріктеу қауіпі...	102
6.4.	Нақ бейнені дайындау шабуылы, биометриялық бейнені қағып әкету қауіпі.....	103
6.5.	Нейрожелідегі артық байланыстарының бар болғандығынан биокодтың біртіндеп әшкерелену қауіпі, Маршалко шабуылы.....	104
6.6.	Кілттің шығыс кодын білу кезіндегі нейрожелі функционалдар матрицасының қатынау шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі.....	106
6.7.	Биокод дәрежелерінің тұрақтылық параметрлері бойынша генетикалық іріктеу жолымен нейрожелілік функционалдар матрицасының қатынауы шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі.....	109
6.8.	Шығыс био-кодтың және минимум энтропияға ие оның инверсиясын біртіндеп әшкерелеу қауіпі....	113

6.9.	Хэммингтің өлшенген метрикасының минимизацияланған іріктеу жолымен нейрожелілік функционалдар матрицасының катынау шабуылымен «Өзім» бейнесінің біртіндеп әшкерелену қауіпі.....	115
7.	НЕЙРОЖЕЛІЛІК КОНТЕЙНЕРЛЕР ҚҰРАМЫН КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ.....	117
7.1.	Құпиясөздерді және жүйеге қолжеткізу биометриялық кодтарын хэштеу арқылы жеке мәліметтерді классикалық қорғау.....	117
7.2.	Нейрожелілік контейнердің мәліметтерін қарапайым шифрлау арқылы криптографиялық қорғау.....	119
7.3.	Криптографиялық кілттің өсетін ұзындығымен блоктық шифрлау арқылы нейрондарды қорғау.....	120
7.4.	Нейрожелілік контейнердің мәліметтерін 1 биттен 256 битке дейін ұзындығы өсетін криптографиялық кілттерді қолдана отырып қорғау.....	122
7.5.	Бірін-бірі жабатын байланысы бар нейрондарды итерациялық үйретуге жекелей қайтып отыру есебінен шифрлау тұрақтылығын күшейтудің қазақша нұсқасы.....	126
8.	КӨП ШЕКТІ КВАНТТАУ ФУНКЦИЯЛАРЫ БАР НЕЙРОНДАР КӨМЕГІМЕН ЖЕКЕ БИОМЕТРИЯЛЫҚ МӘЛІМЕТТЕРДІ ҚОРҒАУ.....	129
8.1.	Екі немесе одан да көп шекті кванттау арқылы нейрондарды қолдануға өту.....	129
8.2.	Нейронды сумматордың шығыс сигналының көп деңгейлі квантталуымен үйретуге қойылатын талаптар.....	132
8.3.	«Өзім» таралу тұрақтылығын жоғарылату шарты бойынша көп шекті нейронның сызықтық бөлімін үйрету	133
8.4.	Нейронның сызықтық бөлімін үйретудің екі әр түрлі алгоритмдерін құрастыру.....	136
8.5.	Көп деңгейлі кванттау функциясының шегін баптау.... БИБЛИОГРАФИЯЛЫҚ ТІЗІМ.....	138 141

Оқулық басылым

Бахытжан Сражатдинұлы Ахметов
Александр Иванович Иванов
Тимур Саатдинұлы Картбаев
Александр Юрьевич Малыгин
Вячеслав Александрович Фунтиков

ТҰЛҒАЛАРДЫҢ БИОМЕТРИЯЛЫҚ
АУТЕНТИФИКАЦИЯСЫ НЕГІЗДЕРІ

Оқу құралы

РБ бастығы	<i>З.А. Ғұбайдулина</i>
Редакторы	<i>А.И. Бейсебаева</i>
Компьютерде беттеген	<i>Л.П. Өмірбекова</i>

Басуға қол қойылды 13.11.2014 ж.
Пішімі 60x84 1/16. №1 баспаханалық қағаз.
Көлемі 9,7 есепті баспа табақ. Шартты баспа табағы 9,0.
Таралымы 300 дана. Тапсырыс №27 .
Бағасы келісімді.

Қ.И. Сәтбаев атындағы
Қазақ ұлттық техникалық университетінің басылымы,
Оқу-баспа орталығы.
Алматы қ., Сәтбаев көшесі, 22

ISBN 978-601-228-698-4



9

7 8 6 0 1 2 2 8 6 9 8 4