1 ЖЕКЕ ТҰЛҒАНЫҢ БИОМЕТРИЯЛЫҚ ИДЕНТИФИКАЦИЯСЫ МЕН АУТЕНФИКАЦИЯСЫ ТЕХНОЛОГИЯСЫНЫҢ НЕГІЗГІ ТҮСІНІГІ ЖӘНЕ АНЫҚТАМАСЫ

Аутентификация (немесе түпнұсқаны растау) – субъект және оның кім екендігін көрсететін қайталанбас ақпараттың көмегімен сәйкестендіруді тексеру процедурасы [39].

Барлығына белгілі, аутентификация субъектінің түпнұсқасын тексеруді тұспалдайды. Субъекті ретінде тек адам ғана емес, сонымен қатар бағдарламалық процесс те қарастырылады. Жалпы алғанда, жеке тұлғаның аутентификациясы әртүрлі формада сақталынған ақпараттың берілуінде ғана жүзеге асырылады. Аутентификация жалпы қолданыстағы ақпаратқа қол жеткізу құқығын негіздеп және ақиқаттап шектеуге мүмкіндік береді. Бірақ, бір жағынан осы ақпараттың бүтіндігі мен ақиқаттығын қамтамасыз ету мәселесі туындайды. Қолданушы ақпаратқа сенімді дереккөзден қол жеткізгендігіне және осы ақпарат сәйкес санкцияларсыз өзгертілмегендігіне сенімді болуы керек.

Қазіргі уақытта жеке тұлғаның аутентификациясының үш дәстүрлі әдісі қолданылады [40]:

– меншіктігі бойынша – физикалық заттар, кілт, төлқұжат және смарт карта сияқтылар;

– білімі бойынша – белгілі бір адам ғана білетін және құпия түрде сақталған ақпарат, мысалы құпиясөз;

– Биометриялық параметрлері бойынша – жеке тұлғаның физиологиялық немесе мінез-құлықтық сипаттамасы.

Бүгінгі күні жеке тұлғаның аутентификациясының негізгі әдісі ретінде ақпараттық жүйеге қол жеткізуде құпиясөздік қорғау болып қалады. Оның негізгі проблемаларының бірі көптеген қолданушыларды өз кездейсоқ символдардан құралған ұзын құпиясөздерін есте сақтай алмауы. Сол себепті, негізінен, 5-8 символдардан құралған құпиясөздер қолданылады. Құпиясөз символдарының кездейсоқтығын ескергенде құпиясөзді теру шабуылдарынан қорғау тұрақтылығы 10^{10}–10^{16} теріп алу әрекетін құрайды.

3ГГЦ жиілікті Пентиум 4 стандартты компьютері 1 секундтың ішінде құпиясөздің 10^7 нұсқасын теріп алу мүмкіндігіне ие. Бұл, аутентификация жүйесі хэш-функциясынан шығарылған құпиясөзді хакер 5 символдан тұратын құпиясөздің 10^{10} нұсқасын тексере отырып қажет құпиясөзді шамамен 12 минут ішінде, ал бір тәулікте 5 символдан тұратын құпиясөздің 10^{12}, үш айда 7 символдан тұратын құпиясөздің 10^{14}, 21 жылда 8 символдан тұратын құпиясөздің 10^{16} нұсқасын тексере отыра теріп алатындығын білдіреді.

Кездейсоқ символдардан тұратын құпиясөздерді есте сақтаудың қиындығына байланысты, қолданушылар әдетте өз құпиясөзі ретінде ана тілін қолданады. Бұл құпиясөз қорғанысының тұрақтылығын күрт төмендетуге алып келеді. 8 символдық сөздің тұрақтылығы тек қана 10^5 мүмкіндікті құрайды.

Мұндай құпиясөзді теру заманауи компьютердің машиналық уақытының бірнеше минутын құрайды.

Құпиясөз қорғанысының проблемасы құпиясөзді енгізу кезіндегі оның тұлғасыздандырылуы. Бұл проблеманы шешудің бірден-бір жолы қолданушының өзінің биометриялық параметрлерін құпиясөз ретінде қолдану болып табылады.

Идентификация (тұлғаның сәйкестендірілуі) – белгілер жиынтығы бойынша салыстырмалы зерттеу жолымен адамның жеке басын растау [39].

Тұлғаның цифрлық идентификациясы тұлғалардың идентификациясы, биометрия, электрондық цифрлық қолтаңба, электрондық регистр, төлқұжат сияқты түсініктермен тығыз байланысты.

Биометрия – физиологиялық немесе мінез-құлықтық сипаттарына негізделген жеке тұлғалардың идентификациясының автоматтандырылған әдістері мен құралдары.

Биометриялық идентификация (немес бейнетану) – бұл файлдағы барлық белгілі биометриялық эталондық шаблондары бар үлгіден алынған биометриялық үлгі немесе кодты салыстыру процесі. Егер алынған үлгі сақталынған шаблонға рұқсат етілген қателік аймағына сәйкес болса, онда тізімге енгізілген адамның жеке басы алдын сақталған эталонмен де салыстырылады. Тұлға туралы сақталынған ақпарат негізінде биометрияны тасымалдаушының физикалық түпнұсқасына сәйкестілігі анықталмауы, бірақ қызметпен қолдануды немесе қол жеткізу рұқсатын алуға мүмкіндік беруі қажет.

Осылайша, идентификация – «бірдің көпке» іздеуі, әдетте мұндай алгоритмді жүзеге асыру тек қана қиын емес, сонымен қатар қымбат.

Верификация (немесе тексеру) – бұл тексеруді қажет ететін тізімдегі бір тұлғаның бірден-бір биометриялық эталонымен берілген биометриялық үлгіні салыстыру. Эталондық шаблонның үлкен деректер қорында орналасуы міндетті емес, оны смарт-картада немесе қорғаныс құрылғысында өзімен бірге алып жүруіне болады. Егер тексеру процесі жақсы баптalса, онда биометриялық ақпарат жүйеге енгізілмейді, тек шешімі ғана беріледі: сәкестігі немесе сейкес еместігі мақұлданады. Осылайша, верификация – «бірдің бірге» (бір атрибуты бойынша) сәйкестігін іздеу, жоғары жылдамдығымен ерекшеленеді де компьютердің есептеу қуаттылығына ең төменгі талап қойылады.

Барлық биометриялық идентификация немесе аутентификация технологиялары келесі 4 амалға негізделеді [17]:

– сурет – физикалық немесе мінез-құлықтық үлгі жүйе көмегімен тізімге ену кезінде, сонымен қатар идентификация және тексеру процесі кезінде түсіріледі;

– шығару (извлечение) – бірден-бір мәлімет үлгіден шығарылады да шаблон құрылады;

– салыстыру – шаблон жаңа үлгімен салыстырылады;

– сәйкестендіру/сәйкессіздену – жүйе жаңа үлгіден алынған сипаттамалар сәйкес келуі не келмеуін шешеді.

Биометриялық идентификацияның ең басты мақсаты өте сирек жағдайда ғана заңды қолданушыларды жүйеге кіргізбей қалуы мүмкін және компьютердегі ақпаратты сақтайтын орынға рұқсатсыз енуді толығымен болдырмайтын тіркеу жүйесін құру.

Биометриялық технологияларды екі үлкен – физиологиялық және психологиялық(мінез-құлықтық) категорияларға бөліп қарастыруға болады.

Физиологиялық категорияның ең басты идеясы адам идентификациясында оның статикалық биометриялық деректерін қолдану. Олардың ерекшелігі мұндай деректер адамға туылғанынан беріліп, өз қалауымен өзгермейтіндігінде. Идентификацияның мұндай деректеріне: көздің шатырша қабығы, саусақ бастары терісінің суреті (папиллярлық сызықтар өнері бойынша), қолдың бас жағының екі және үш өлшемді параметрлері, адам бет пішінінің екі және үш өлшемді геометриясы, көз түбінің, көз алмасының, қол басының сыртқы жағының қан тамырларының суреті, құлақ қалқаны геометриясы, жүрек электрокардиограммасы, дене иісі, ДНҚ анализі, тер іздерінің иондық спектрі бойынша идентификациялау жатады [18-25].

Тұлғаның мінез-құлықтық биометриялық бейнесі анағұрлым мықтырақ болып табылады. Олар бір жағынан адамның ағымдық психофизикалық күйіне сезімтал, ал екінші жағынан адамның қалауы бойынша өзгертілуі мүмкін. Бұл тұлғаның қолтаңба, пернетақталық жазу, дауыс сияқты динамикалық биометриялық сипаттамалары. Таза күйінде олар теру шабуылдарына төмен тұрақтылықтылыққа ие болғандықтан шектеулі қолданысқа ие, бірақ қолданушыны қашықтықтан идентификациялауға өте лайықты [26-30].

Мінез-құлықтық сипаттамалар уақыттың өтуімен өзгеруіне байланысты, тіркелген биометриялық үлгі әрбір қолданылғанында жаңартылып отыруы қажет. Мінез құлықтық сипаттамаларға негізделген биометрия арзандау және қолданушыларға өте аз мөлшердегі қауіп төндіреді; бірақ физиологиялық сипат бойынша тұлға идентификациясы анағұрлым нақты және қауіпсіз. Қандай болғанда да, екі әдіс те құпиясөздер мен карталарға қарағанда жоғары деңгейлі идентификацияны қамтамасыз етеді.

1.1 Тұлғалардың биометриялық идентификациясы мен аутентификациясының негізгі әдістері

1.1.1 Биометриялық идентификацияның статикалық әдістері

Тұлғалардың биометриялық аутентификациясының статикалық әдістері адамның туылғаннан бастап пайда болған ажырамас физиологиялық сипаттамаларына негізделген. Статикалық биометрияның негізгі артықшылығы қолданушының психофизиологиялық күйінен тәуелсіздігі, қолданушының биометриялық сипаттамаларын тіркеуге аз уақыт жұмсауы, биометриялық үлгіні теру тұрақтылығының біршама жоғары болуы (10^2 до 10^{13} мүмкіндік) [17].

Саусақ таңбасы бойынша тұлғаның аутентификациясы. Бұл әдістің негізгінде әр адамның саусақтарының папиллярлық өрнектерінің суреті бірегей

болуында. Бұл технология барлық биометриялық әдістердің ішінде ең көп тарағаны болып табылады.

Адам терісі екі қабаттан, төменгі қабат тер бездерінің шығу жолдарынан тұратын төбелері бар көптеген дөңестерден – бүртіктерден (латын тілінен алғанда бүртік – papillae) тұрады. Терінің негізгі бөлігіндегі бүртіктер бағдарсыз орналады және оларды көру қиындық тудырады. Адам денесінің кейбір бөліктеріндегі тері паппилярлары қатаң бір сызықтың бойында орналасып, бірден-бір папиллярлық өрнектерді құрайды. Яғни бұл өрнектер басқа адамда қайталанбайды.

Қол саусақтарының папиллярлық суреті негізінде тұлғаны идентификациялау Г.Фулдс пен В.Гершел авторларымен 1980 жылы ағылшынның «Nature» танымал журналындағы мақалада ұсынылған. Бұл әдіс криминалистикада кеңінен тараған. Осы себепті көптеген адамдар оған үрейлене қарайды. Ал АҚШ-та дактилоскопияны халықтан алуға үйреншікті қарайды.

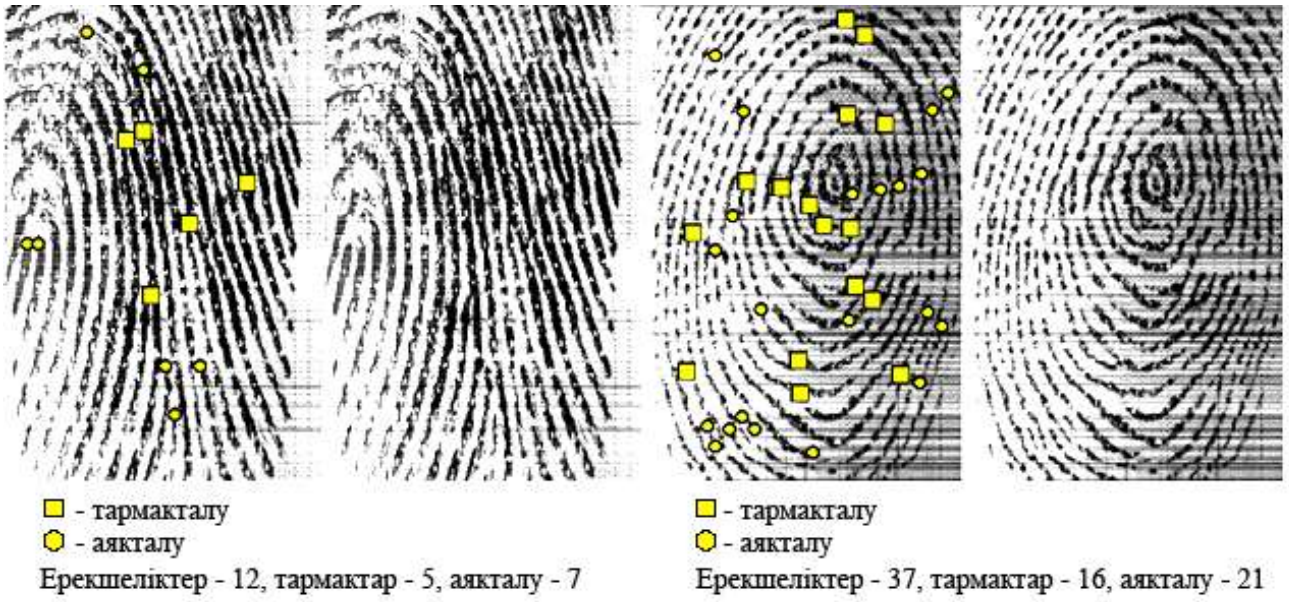
Тұлғаның дактилоскопиялық идентификациясы жүйелері қол жеткізу құқығын алуға өтініш берген адамның бір саусағынан арнайы сканер көмегімен папиллярлық өрнекті алып, оны эталондық суретпен салыстырады. Бүгінгі күні өндірісте саусақ таңбаларының суретін алатын, сканерлеудің әртүрлі физикалық принциптеріне негізделген бірнеше типтегі сканерлер шығарылады. Оптикалық, сыйымдылықты және радио толқынды сканерлер қолданылады [40, с. 30-32].

Оптикалық сканерлер папиллярлық сызықтарды жарықтандырады және сызғыш немесе сезімтал элементтер матрицасы бар жарық сезгіш микросхема арқылы саусақ таңбасы суретінің кескінін алады. Егер микросхемада сезімтал элементтер матрицасы бар болса, онда папиллярлық сызықтар суретін сканерлеу кезінде тексеріліп жатқан адамның саусағы тексеру уақытында қозғалыссыз болуы қажет. Егер микросхемада сезімтал элементтер сызғышы болса, онда қолданушы саусағын осы сызғыштан өткізуі қажет. Ал ары қарай, бағдарламалық құрал саусақ қозғалысының бірқалыпсыз жылдамдығын сканерлеу және кескінді қалпына келтіру кезінде түзетуі қажет.

Саусақтар таңбаларының талданып жатқан суреттерінің әрқайсысының ақпараттылығы ондағы ерекшеліктердің санына пропорционалды болып келеді [41]. Саусақ таңбаларының суретінде табылған ерекшеліктердің саны қанша жоғары болса, қорғаныс сонша жоғары болады. Ал ерекшеліктер саны аз болса, биометриялық қорғау әлсіз болады. Әртүрлі ерекшеліктер саны бар саусақ таңбалары суреттерінің мысалдары келесі 1.1 суретінде көрсетілген.

Папиллярлық суреттерді талдайтын жүйелер үшін тәуелсіз тестілеу нәтижесі бойынша бірінші текті қателіктер папилляр суреті анық емес адамдарды тестілеуде және құрғақ тері сияқты қолайсыз жағдайларды ескергенде 10% бен 20% аралығын құрайды. Папиллярлық биометриялық идентификация жүйелерін өндірушілер өз өнімдерін жарнамалауда бірінші текті қателікті 2% деңгейінде, ал екінші текті қателіктерді 0,0001% деңгейінде бағалайды. Соңғы цифр, мүмкін муляжды қолданбайтын, тәжірибесіз жүйені

бұзудағы жағдайға жататын шығар. Соңғы кезде көптеген жұмыстарда муляжды дайындау әдістері көрсетіліп келеді. Муляж көмегімен биометриялық қорғанысқа шабуыл жасау сарапшылар тарапынан өте қауіпті шабуыл деп саналады.



Сурет 1.1 – Ақпараттылығы әртүрлі екі саусақ таңбасы: сол жақтағы аз ерекшелікке, ал оң жақтағы көп ерекшелік санына ие

Папиллярлық суреттерді талдайтын жүйелер үшін тәуелсіз тестілеу нәтижесі бойынша бірінші текті қателіктер папилляр суреті анық емес адамдарды тестілеуде және құрғақ тері сияқты қолайсыз жағдайларды ескергенде 10% бен 20% аралығын құрайды. Папиллярлық биометриялық идентификация жүйелерін өндірушілер өз өнімдерін жарнамалауда бірінші текті қателікті 2% деңгейінде, ал екінші текті қателіктерді 0,0001% деңгейінде бағалайды. Соңғы цифр, мүмкін муляжды қолданбайтын, тәжірибесіз жүйені бұзудағы жағдайға жататын шығар. Соңғы кезде көптеген жұмыстарда муляжды дайындау әдістері көрсетіліп келеді. Муляж көмегімен биометриялық қорғанысқа шабуыл жасау сарапшылар тарапынан өте қауіпті шабуыл деп саналады.

Әрине, саусақ таңбасы суретінің муляжы сканер қолданатын технология бойынша жасалуы қажет. Мысалы оптикалық сканерге арналған муляж т.с.с.

Саусақ таңбалары суретінен алынатын биометриялық деректерді өңдеу процедурасы келесі стандарттарда сипатталған:

– МЕСТ Р ИСО/МЭК 19794-3-2009 «Автоматты идентификация. Биометриялық идентификация. Биометриялық деректермен алмасу форматы. Бөлім 3. Саусақ таңбасы кескінінің спектралды мәліметтері»;

– ISO/IEC 1.37.19795 «Биометриядағы тестілеуді және есеп беруді жүргізу процедуралары»;

– МЕСТ Р ИСО\МЭК 19794-4 «Автоматты идентификация. Биометриялық идентификация. Биометриялық деректердің алмасу форматы. Бөлім 4. Саусақ таңбасы кескінінің мәліметтері»;

– ISO/IEC 19794-8: 2006 «Ақпараттық технологиялар. Биометриялық деректердің алмасу форматтары. Бөлім 8. Саусақтар таңбаларының қаңқалық мәліметтері».

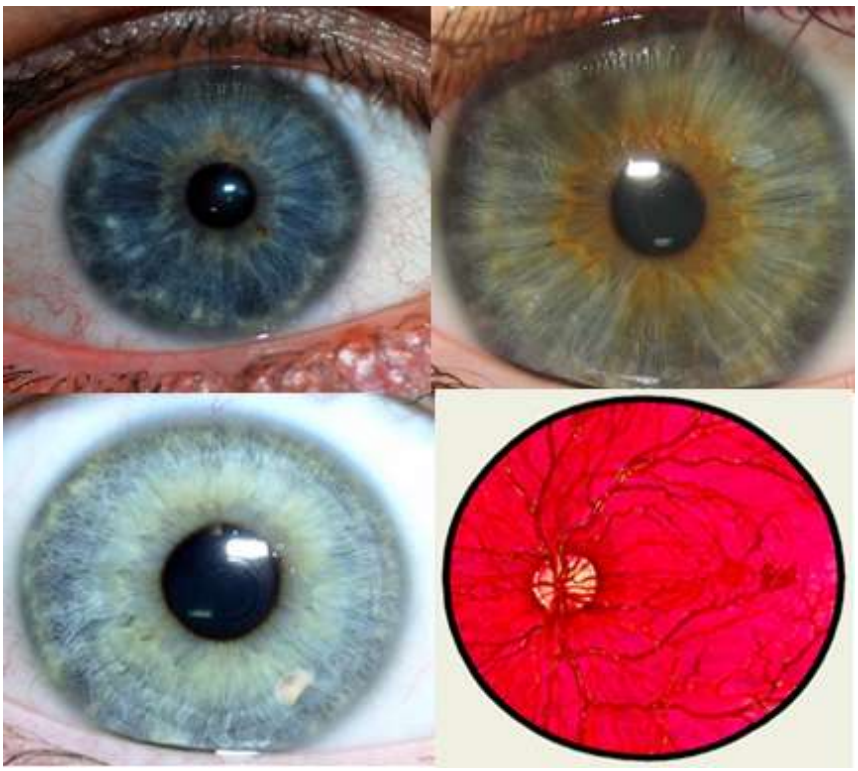
Айта кететін жайт, өз саусақ таңбаларымызды біз әр жерде қалдырамыз. Мәліметтерді электрондық теру тиімді шабуылын ұйымдастыру үшін саусақ таңбаларының барлық 10 суреттерін құпия түрде алу жеткілікті. Осы себепті саусақ таңбаларының суреттері жақын қаскүнемдер (адамның денесіне немесе оны қоршаған заттарға қол жеткізе алатын қаскүнемдер) шабуылдарынан бағдарламалық қосымшаларды биометриялық тиімді қорғай алмайды.

Саусақ таңбалары суреттерінің биометриясы Интернетте қолдану үшін олар туралы ақпаратты қорғалған нейрожелілік контейнерлерде және биометрия доноры анонимдігін (тұлғасыздандыру) қамтамасыз ету қажет [18, с. 189]. Егер сыртқы бақылаушы адамның не атын, не оның мекен жайын немесе оның басқа да жеке ақпаратын білмесе, онда саусақ таңбалары суретін жеке ақпаратты қорғауға қолдануға болады.

Көздің шатырша қабығы мен көз түбінің қан тамырлары бойынша тұлғаның идентификациясы. Көздің шатырша қабығы адамның басқа адамда қайталанбайтын сипаттамасы болып табылады. Шатырша суреті құрсақ ішінде сегізінші айдан бастап қалыптасып, шамамен екі жаста толығымен тұрақталады және өмір бойы өзгермейді. Тек қана ауыр жарақат немесе күрт паталогия салдарынан өзгеруі мүмкін. Бұл әдіс биометриялық технологиялар арасындағы ең нақтыларының бірі болып табылады.

Әрбір адамның денесінің геометриялық параметрлері, сонымен қатар көз параметрлері де қайталанбайтын болып келеді. Қазіргі кезде көз параметрлерін өлшеу негізіндегі биометриялық жүйелердің екі типі кездеседі. Бірінші типіне көздің шатырша қабығының суретін талдау негізінде құрылған жүйені жатқызуға болады. Даугмен бойынша [17; 23, p. 1928-1929] көздің шатырша қабығының суреті адам генетикасына тәуелсіз және бір жұмыртқалы егіздерде де бір бірінен ерекшеленеді. Екінші типке, көз түбі (көздің торлы қабығы) қантамырлары суретінің талдануы негізіндегі жүйелер жатады. Бірінші типтегі жүйе көзді сырттан көрсе, екінші типтегі жүйе көздің түбін көреді. Әрине, бірінші және екінші жүйенің оптикасы әртүрлі болады. Әртүрлі адамның көзінің торлы қабатының үш және көз түбі қантамырларының бір суретіне мысал келесі 1.2-суретте көрсетілген.

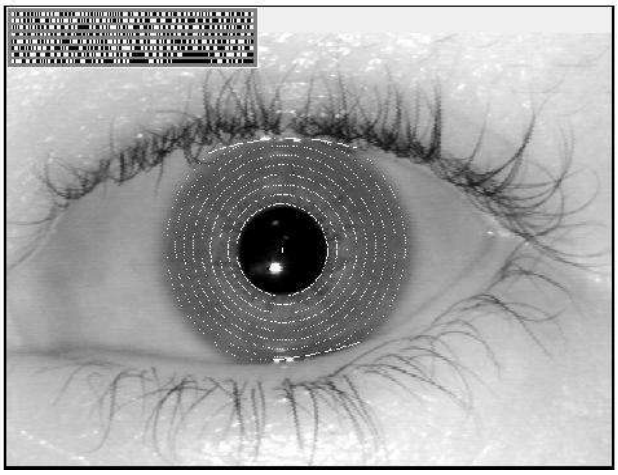
Қантамырлар бұтағын талдау қол сүйегінің немесе басқа да дене мүшелері қантамырларының бұтағын талдау сияқты принциптерге негізделеді. Шаблонды қалыптастыруда түбірі, діңгектері, бұтақтары табылады және ары қарай, олардың ұзындығы, өзара орналасуы, диаметрі бойынша жіктеледі. 1.2-суретінің төменгі оң жағында барлық қан тамырларының анық көрсетілген жалпы түбірі нақты көрініп тұр. Бұл түбір биометриялық геометрия жүргізілетін салыстырмалы орталық сияқты қарастырылуы қажет.



Сурет 1.2 – Әртүрлі адам көзінің торлы қабатының және бір адамның көз түбі қантамырларының суретіне мысал

Көздің шатырша қабығы суретінің талдануында оны көз қарашығы айналасында орналасқан параллелді концентриялық шеңбер бойынша сканерлеу жүзеге асырылады. 1.2-суретінде адамның көз қарашығы қарастырылатын заттың жарықтығына бейімделе өз өлшемін ауыстыра алатындығы анық көрсетілген. Осы себепті көздің шатырша қабығының және адамның суреті бойынша идентификациясын биометриялық шаблонының қалыптасуын бірдей жарық түсуі арқылы орындау орынды. Бұл жағдайда көз қарашығының диаметрі мен көздің шатырша қабығының сыртқы диаметрі тұрақты болып, қайта есептеуді қажет етпейді.

Көздің шатырша қабығын сканерлеуде алдын-ала берілген концентрациялық шеңбер айналасындағы кескіннің жарықтық деңгейінің орташа мәнін бағалайды. Әрі қарай, концентрациялық шеңбер берілген секторлардың санына бөлінеді, мәселен, 128 сектор болса, онда әрбір сектордың орташа жарықтығы есептелінеді. Жоғарғы жарықтық және әлсіз жарық орташа жарықтықпен салыстырғанда сканерлеуде «1» және «0» күйіндегі кодты береді. Егер сканерлеудің 8 концентрациялық шеңберін қолдансақ, онда сәйкесінше сканерлеудің ақырғы кодының ұзындығы 128x8= 1024 битке тең болады. Осындай кодтың мысалы келесі 1.3-суретінде көрсетілген [23, p. 1929-1931; 24].



Сурет 1.3 – Көздің шатырша қабығы жарықтығының айырмашылығын сканерлеуде 8 концентрациялық шеңберді қолдану

Айта кететін жайт, көздің шатырша қабық жарықтығы айырмашылығының қорытынды кодтық комбинациясы көршілес есептеулердің жоғарғы корреляциясына (жоғарғы тәуелділікке) ие. Көптеген биометриялық параметрлер үшін елеулі корреляция тән және өлшенетін мәліметтерді мүмкіндігінше тәуелсіз етуге рұқсат ететін арнайы декорреляциялық түрлендірулер қажет.

Әрине, офтольмалогиялық биометриялық жүйелер тек қана көздің шатырша қабығының суреті анализі негізінде ғана емес, сонымен қатар көз түбінің қантамырлары суретінің анализі негізінлде де құрылуы мүмкін. Жақсы оптика қолданылғанда фотосуреттегі көздің алмасын қанмен қамтамасыз ететін қантамырлары айтарлықтай дәрежеде анық көрінеді. Олардың суреті қайталанбайды және адам идентификациясы мен аутентификациясы үшін қолдануға болады. Бірақ бүгінгі күннің нарығында мұндай жүйелер қазірше жоқ.

Көздің шатырша қабығы және көз түбінің қантамырларының талдануы бойынша тұлға идентификациясы және аутентификациясы әдістері қазіргі уақытта ең сенімді болып табылады. Бірақ мұндай жүйелер биометрия нарығында қазірше өте сирек кездеседі. Сандия ұлттық зертханасының мәлімдеуінше бірінші текті қателік 0,4% құрайды, ал екінші текті қателік көрсетілмеген.

Әдістің кемшіліктеріне тіркеу процедурасын бірінші реттен тек 80-90% қолданушылар ғана өте алатындығын кіргізуге болады.

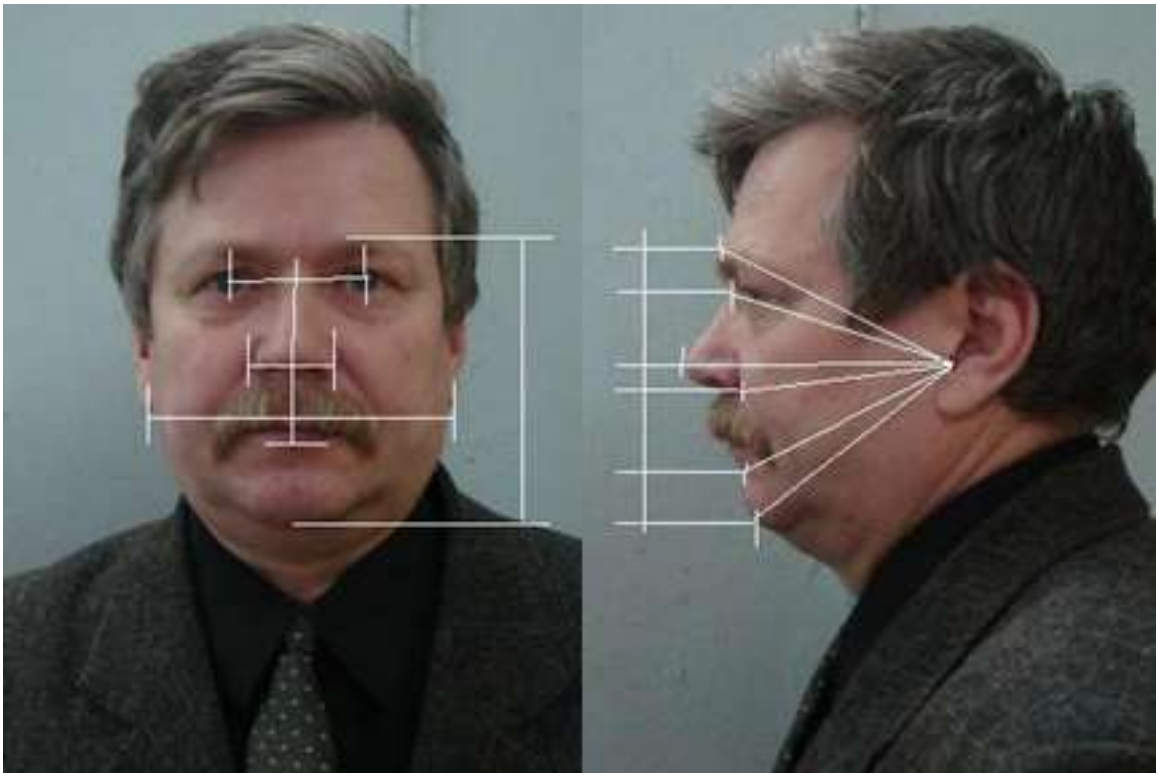
Көздің торлы қабығы бойынша бейне тану құрылғылары ең қымбат шамамен 4000 АҚШ доллары көлемінде болып табылады. Сонымен қатар, тіркеу процедурасы өте қиын [17; 42]. Мұндай жүйелерді IridianTechnologies, Inc (АҚШ), VisionicsFaceIt (АҚШ), Panasonic (CIS) OY (Жапония) компаниялары өндірумен айналысады.

Бет-әлпет геометриясы бойынша жеке тұлғаның идентификациясы. Әдетте адамдар бір-бірін бет-әлпетінің ерекшеліктері бойынша таниды. Жеке

куәлік, жүргізуші куәлігі, төлқұжат иесінің фотосуреті орналастырылады. Бет-әлпет ерекшеліктері бойынша [27, с. 21-22; 24; 25; 43] бейнетану процедурасын автоматтандыру әрекеті биометриялық идентификация құралының екі класының пайда болуына алып келді.

Осындай құралдардың бірінші класы адам бет-әлпетінің жазық кескінін (2 өлшемді портреттерін) талдайды. Бұл құралдардың жұмысы 1.4-суретінде көрсетілген.

Жазық кескінінің екі өлшемді анализаторы адам портретінен анфасқа тән нүктелер мен екі көз ортасы, көз сызығы мен мұрын ұшы, мұрынның ең үлкен ені, қастардың доғалары мен бұғақтың төменгі нүктесі, құлақ сырғалығының төменгі нүктелері, мұрын ұшы мен еріннің төменгі нүктесінің арақашықтығын табады (сурет 1.4, сол жағы).



Сурет 1.4 – Адамның жазық фотосуретінен ерекше нүтелерді ерекшелеу және әрі қарай олардың арақашықтығын есептеу

Адамның портретін профильде екі өлшемді кескінін талдауда анық ерекшеленетін ұқсас точкалар қолданылады, сонымен бірге бет-әлпеттің кескінінде анық ерекшеленетін ұқсас точкалар, адамның құлақ қалқанында анық ерекшеленетін ұқсас точкаларға дейін арақашықтықтарымен толықтырылады

Әрине, бет-әлпет кескінінің өзара екі өлшемді орналасу анализаторы өте тапшы биометриялық ақпарат алуға рұқсат етеді. Күрделі үшөлшемді бет-әлпет геометриясының анализіне өту қабылданып жатқан биометриялық ақпараттың көлемін белгілі бір мөлшерде үлкейтуге мүмкіндік береді.

Үшөлшемді бейнені алу үшін, екі фото камера немесе бір арнайы жарықтығы бар фотокамераны қолдануға болады [44-47].

Идентификацияның ең төмен беріктігі әдЗстің кемшілігіне кіреді, себебі муляж-фотосуретін дайындау өте қиын техникалық мәселе болып табылмайды.

Үш өлшемді бейнені адамның мәселені көріп танып білуіне жақын жасау. Жүйе адамның жасы, мұрты, сақалы, көзілдірігі сияқты деректерге байланысты өзін-өзі үйрете алады.

Әдістің жетістігі бұл-бейнеконференция өткізуге арналған бейнекамералардың бағаларның өте төмен болуында. Олар 20-дан 200 АҚШ долларына дейін тұрады. Бет-әлпет бойынша қолданушылар идентификациясы үшін арналған бағдарламалық қамтамалар бағасы 40 пен 200 доллар арасында өзгеріп тұрады. Мұндай жүйелерді өндіретін арнайы FaceKeyTMCorporation (USA), IritechInc. (USA), IdentixInc. (USA), AcSysBiometrics (USA), A4Vision (Швейцария), CognitecSystemsGmbH (Германия), VicarVision (Голландия) компаниялары бар.

Құлақ қалқандары пішіні геометриялық ерекшеліктерінің көмегімен жеке тұлғаның идентификациясы. Альфонс Бертильон адам биометриялық идентификациясының алғашқы жүйесін жасағанда жадамның құлақ қалқанының пішіні мен типін анықтауға көп мән бөлген [47, с. 23-24]. Мұның себебі, адамдардың құлақ қалқаны көлемі мен орналасуының өзгерісі басқа дене бөліктерінің көлемінің өзгерісіне қарағанда анағұрлым жоғары. Сонымен қатар, құлақ қалқаны әр адамда әртүрлі пішінде келеді. 1.4-суретінде әртүрлі ер адамның құлақ қалқанының фотосуреттері нақты көлеміне сәйкес берілген.

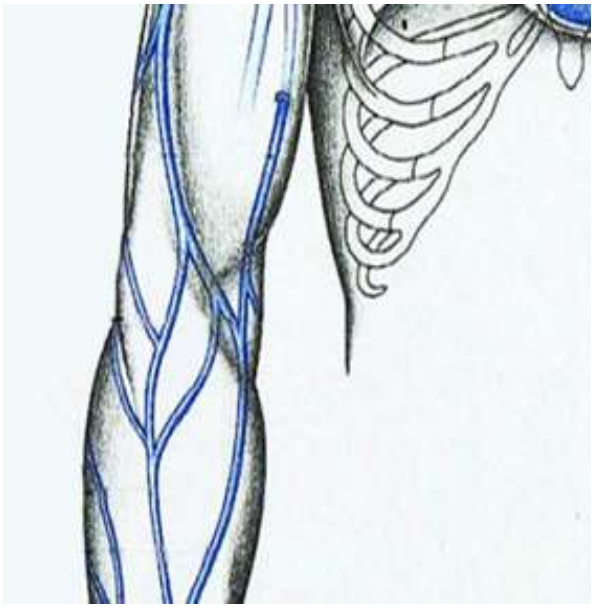
Сурет 1.5 – Кездейсоқ таңдап алынған ер адамдардың бір көлемде әртүрлі құлақ қалқандарының пішінінің берілуі

Құлақ қалқанының пішіні мен көлемінің анағұрлым өзгеруіне қарамастан, құлақ қалқаны геометриясын қолданушы тиімді биометриялық жүйелер қазірше жоқ. Бұл үшөлшемді техникалық көру мәселесімен байланысты. Екі өлшемді жасанды көру құралы тұрғанда олар құлақ қалқанының күрделі үшөлшемді пішінін жасай, әрі жаттай алмайды. Құлақ қалқанының екі өлшемді бейнесінен үлкен көлемді биометриялық ақпаратты алу мүмкін емес. Құлақ қалқанынң кескінін жиектеуді қолдану мүмкіндігі қабылданады, бірақ жиектеу

программалырының барлығы шеткі жарықтыққа сезімтал және тек қана жылжымайтын объектілерде жақсы жұмыс істейді.

Айта кететін жайт құлақ қалқаны геометриясының параметрлерін шаш арасында жасыруға болады, бұл оның тиімділігін асырады. Жеке ақпаратты қорғауда құлақ қалқаны геометриясын жасау шындығында да нейрожелілік контейнерде және аутентификация процедурасын орындау кезде биометрия иесін жасыру (тұлғасыздандыру) ды қосымша қамтамасыз еткенде ғана тиімді болады.

Қолдың көктамырлары бойынша жеке тұлға идентификациясы. Биометриялық нарықта қолдың көктамырларының жеке орналасуының анализі бойынша құрастырылған құрылғылар бар [27, с. 23]. Қол жұдырығының сыртқы жағында орналасқан көктамыр суреті назарға алынады (сурет 1.6). Көктамыр суретін бақылау телевизиондық камераның инфрақызыл жарықтығының көмегімен жүзеге асырады. Кескінді енгізу кезінде көктамырды ерекшелейтін бинарлау жүргізіледі. Мұндай құрылғыны жалғыз Vinchek ағылшын фирамасы шығарады.



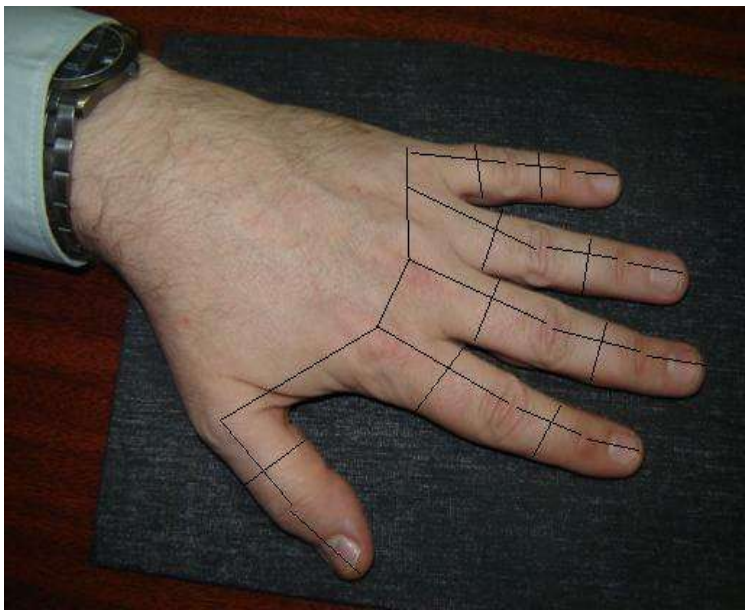
Сурет 1.6 – Қолдың көктамыр жүйесі

Қолдың көктамыр кескіні бойынша бейнетану жаңа технология болып табылады, және әлемдік нарқта олар 3%-ды ғана құрайды. Осыған қарамастан бұл әдіске көп қызығушылық танытады. Себебі, бұл әдіс өзі мүмкіндігі бойынша нақты бола тұрып, бет әлпет геометриясы немесе көздің шатырша қабығы бойынша бейне тану әдістері сияқты қымбат құрылғыны талап етпейді.

Қолдың көктамырларының суреті бойынша қауіпсіздік және биометриялық идентификация жүйелерінде де әзірлеу жаңа болып табылады. Мұндай алғашқы жүйе 2004 жылы ұсынылды. Оны өндірушілер бұл жүйенің қателік деңгейі өте төмен деп тұжырымдайды, нақтырақ айтсақ

идентификациялаудың жалған іске қосылу ықтималдылығы 0,00008%-ды және бейнені мүлдем танымау ықтималдылығы 0,01% .

Қолдың білезікке дейінгі параметрлерінің геометриялық қатынасы бойынша жеке тұлғаның идентификациясы. Тағы бір адамның биометриялық параметрлер жүйесін қолдың білезікке дейінгі параметлерінің геометриясын өлшей отырып алуға болады [47, с. 25-26]. Әрбір адамдамның өзіне тән бармақ ені мен ұзындығы, сонымен қатар, қол терісінде анық сипатталған әжімдері бар. 1.7-суретінде қолдың сыртқы жағының фотосуреті берілген, оның көмегімен геомертиялық параметрлеріне баға беруге болады.



Сурет 1.7 – Қолдың білезікке дейінгі аралығының сыртқы жағының фотосуреті

Бүгінгі күні қолдың білезікке дейінгі геометриясының анализі бойынша құрылған биометриялық жүйелердің екі типі бар: біріші тип қарапайым жарықтықта алынған қолдың алақаны немесе білезікке дейінгі аралық кескінінің анализі бойынша құрылған, екінші тип қолдың білезікке дейінгі сыртқы жағының қан тамырлары бұтағының тармақталуының орналасуын белгілеу негізінде құрылған жүйелер. Қолдың білезікке дейінгі аралығында құйылатын қан әдетте қолдың өзіндегіге қарағанда жылылау және қан тамырларының суретін белгілеу үшін спектрдің инфрақызыл бөлігіне сезімтал болып келетін оптикалық элементтерді қолдану қажет. Қол алақанындағы тері әжімдерін («Өмір сызығы» деп аталатын) белгілеу арқылы алынған параметрлер ақпараттылығы өте жоғары. Бұл әдістер биометриялық бақылау техникалық құралында қазіргі кезде көп қолданылмайды.

Бет-әлпет термограммасы бойынша тұлға идентификациясы. Әдістің мәні – дене бөліктерінің бейнесін қысқа толқынды (0,9-1,7 мкм), орта (3-50 мкм) және ұзын (80-120 мкм) толқынды инфрақызыл спектірі диапазонында тіркеу [17].

Қарапайым суреттерден термограмманың айтарлықтай артықшылығы жарықтықтан тәуелсіздігі болып табылады. Сондай-ақ термограммаға келбеттің сыртқы өзгерісі әсер етпейды [17].

Әдістің кемшіліктеріне сенсор-камерасы бағасының өте қымбат (50 мың АҚШ доллары көлемінде) болуында.

1.1.2 Биометриялық аутентификацияның динамикалық әдістері

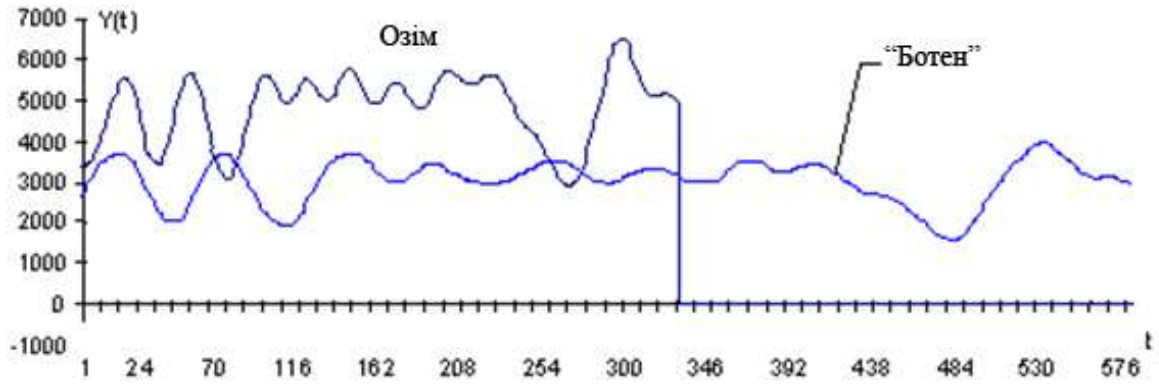
Адам өз қалауымен саусақ таңбасының суретін немесе өз денесі бөлігінің геометриялық параметрлерін өзгерте алмайды. Егер адамның саусақ таңбасының кескіні бір рет ашылып қалса, онда оны тиімді биометриялық ақпараттық қорғау деп қабылдау мүмкін емес. Бұл тараптан статикалық биометрия әрқашанда әлсіз болып қала береді.

Статикалық биометрияға қарағанда тұлғаның мінез-құлықтық биометриялық бейнесі жақсырақ. Себебі, олар адамның психофизикалық күйіне тәуелді және адам қалауы бойынша өзгереді [26; 27, с. 24-25]. Мұндай динамикалық биометриялық сипаттарға қолтаңба, клавиатуралық жазу, дауыс кіреді. Таза күйінде олар теру шабуылдарына төмен тұрақтылықтылыққа ие болғандықтан шектеулі қолданысқа ие, бірақ қолданушыны қашықтықтан идентификациялауға өте лайықты.

Қолжазба жазылуы динамикасының ерекшеліктері бойынша тұлғаның аутентификациясы. қолжазба динамикасын талдау арқылы алынған адамның биометриялық бейнесі қиын мәселелердің бірі болып табылады. Қаскүнем сөз-құпиясөз қолжазбасының жаңғырту динамикасын ашса да апаттық жағдай деп есептелмейді. Себебі оны басқа сөз-құпия сөбен лезде ауыстыра аламыз. Саусақ таңбасы кескінінің 10 нұсқасына қарағанда бір адамның жазуымен жазылған қолжазба құпиясөзінікі көп болып келеді [32, с. 165-168; 48; 49, 33-34б].

Әр адамның қолжазба динамикасының әртүрлілігі адам қолының күрделілігінде. Қолдағы бес саусақ 3 буыннан, әр буын шар тәріздес топса болып, яғни қолдың саусақтарының бірінші жуықтық жақындатуынан алатын бостандық дәрежесі 5×3×3=45. Бұл үш өлшемді кеңістігіміз үшін 42 қосымшаға артық айнымалыны басқару. Егер тетіктің бостандық дәрежесі тапсырманың өлшемімен сәйкес келсе, онда ешқандай артықтық кедергі келтірмейді. Бұл жағдайда жазбаның қайталанбау ерекшелігі бола алмайды, әрбір жазу орындау тетігінің геометриясы мен оны қолданудың тиімділік шарты бойынша анықталады.

Егер адам өз қолтаңбасын немесе қолжазба құпиясөзін ойланбай жазса, мұндай әрекетке аз уақыт кетеді. Бұл оқиға келесі 1.8-суретте көрсетілген. Мұнда «Өзім» қолтаңбасының жазылу динамикасы және бұл қолтаңбаны «Бөтенмен» айналып өту динамикасы көрсетілген [32, с. 165].



Сурет 1.8 – Автор және осы қолтаңбаны айналып өтетін қаскүнем қаламұшының Y(t) тербелісі

Амалдарды орындау уақыты адам өз көзі мен жоғары дәрежелі ой өрісін қосқанда күрт төмендеп кетеді. Көру бейнесін өңдеу – өте қиын, әрі ұзақ амал. Біз бір нәрсені көргенге қарағанда көбірек қозғала аламыз. Бірақ біз өз түйсігімізді қоссақ қана қозғалысымызға қарағанда жылдам көре аламыз. Тек көзіміз ғана іс-әрекетіміздің жылдамдығының төмендетпейді, сонымен қатар зердені қосу да жылдамдықтың күрт түсуіне алып келеді. Егер ойламаған жерден «қырықаяқ» қай аяқтан бастап жүру керек екенін ойланып қалса, арадағы үзіліс мейлінше сезіледі. Бұл оқиға келесі 1.9-суретінде көрсетілген [32, с. 166].

Сурет 1.9 – Басқарудың түйсіктік бағдарламасын зерде үзуі. «Қырықаяқ» әсері

Қолтаңба жазылуының динамикасына қарай, біз, баяулатылған әмбебап сананың жұмыс уақытында қаламұштың тоқтауын байқаймыз. Сананы қоспай «Өзім» қолданушысының сөз-құпиясөзі қолжазбасының жазылуы жылдам және тұрақты жұмыс жасайжы. Сол себепті барлық тұлғалардың қолжазбалық жазуының динамикасы бойынша аутентификациясы құралдарында осы режим қолданылады. Есептеу, қолжазбалық жазу биометриялық параметрлерін

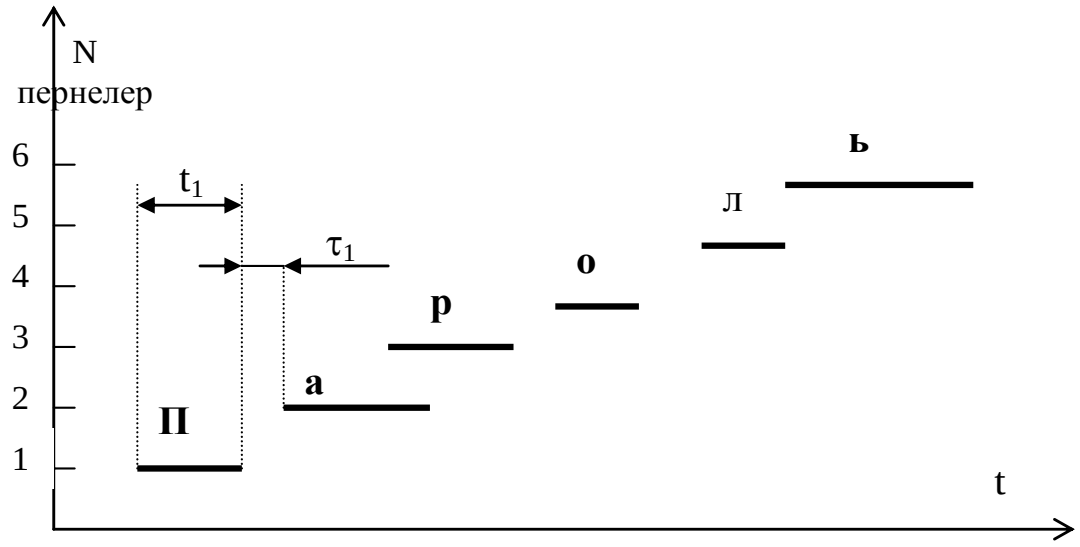
бақылау және олар бойынша шешім қабылдау процедураларын құрудың бірнеше жолы бар [8, P. 107-131; 9; 26; 27, с. 166-167]. Осындай жолдардың бірі Фурье коэффициенттерін есептеу және кіріс саны көп бір нейронды итерациялық үйретудің көмегімен құру. Фурье қатарына қаламұш тербелісі динамикасын жіктеудің орнына кез-келген басқа ортогоналды базистік функция (Уолш, Хаар, вейвлет жіктеу [50-52]) жүйесі бойынша жіктеуді қолдануға болатындығы анық. Сонымен қатар, шешуші ережелер де әртүрлі– шындыққа ұқсас Байес шарты бойынша классикалық шешімдер қабылдаудан бір және бірнеше нейрондар көмегімен нейрожелілік шешімдерге дейін болуы мүмкін [53].

Қолжазбалық жазу бойынша биометриялық аутентификация құралдарының барлығының ең маңызды өзгешелігі тек қана биометриялық қолжазба бейнесінің құпиясының қолданылуында. Егер биометриялық қолжазбалық құпиясөзі құпия сақталынатын шарты орындалса, онда оны жоғары сенімділікті биометриялық аутентификация құралына кіргізуге болады [27, с. 167].

Пернетақталық жазу динамикасы бойынша идентификация. Компьютер пернетақтасынан мәтінді жылдам енгізу көптеген адамдардың әр күн сайын туындайтын қиын тапсырмасының бірі болып табылады. Әдетте ақпаратты пернетақтадан жылдам енгізу екі қолдың он саусағын қолдану арқылы жүзеге асады. Соның салдарынан әрбір адамның өзіне тән пернетақталық жазуы қалыптасады.

Дәстүрлі түрде ақпаратқа қол жеткізуге шектеу құпиясөз көмегімен шектеледі. Бірақ, егер құпиясөзді ұлғайтып, оны оңай есте сақталатын етсек [54], онда қолданушының пернетақталық жазуына тән құпиясөз енгізуін бақылау мүмкіндігіне ие боламыз. Мәселен, құпиясөз ретінде келесі сөз тізбектерін қолданылады: «Құпиясөз – бұл ақпаратты қорғау әдісі». Осы секілді құпиясөз тізбегін енгізуде биометриялық жүйе әрбір перненің басылу уақытын және келесі перне басылуының арасындағы уақытты және алдынғы пернені жібергендегі уақытты белгілейді. Келесі 1.10-суретінде «Пароль» сөзінің уақыттық қатынасының графигі берілген.

1.10-суретінде көрсетілгендей, t_1, t_2, t_3, ..., t_N пернелерін басу уақыты әртүрлі, сәйкесінше бұл параметрлердің мәндері қолданушының жеке пернетақталық жазуының ерекшелігі ретінде қолданылады. Сонымен қатар, бақылау параметрлері ретінде көршілес перненің басылуы арасындағы уақыт τ_1, τ_2, τ_3, ..., τ_{N-1} қолданылады. $t_к$ және $\tau_к$ басқару параметрлері мәтінді теру кезінде қолданушының неше саусақты қолданғандығынан, қолдың әр саусағының қозғалысынан және қол қозғалысынан тәуелді. Атап айтқанда, егер адам бір қолдың бір саусағымен жұмыс істетуге мәжбүрлесе, онда пернетақталық жазу өзінің даралығын жоғалтады. Бұл жағдайда әр түрлі адам үшін пернетақтаны басу уақты олардың даралығын көрсетуді тоқтатады.



Сурет 1.10 – «Пароль» сөзін енгізудің уақыттық диаграммасы

Бұл биометриялық идентификация технологиясы сипатының маңыздылығы құпиясөз тізбегінің ұзындығында, практика құпиясөз тізбегінің жеңіл есте сақталатын болуын және 21-ден 42-ге дейін пернені басу керектігін көрсетеді. Құпиясөз тізбегін синтездеуде қандайда бір мағынасы бар мәтіннен мағыналы сөздерді қолдану орынды. Себебі қарапайым адам мағынасыз таңбалар жиынтығын дұрыс естей алмайды, осы себепті мағыналы құпия сөз тізбегі мейлінше ұзын болуы мүмкін, мұндай құпиясөз тұрақтылығы әр қашанда Хэмминг код кеңістігінде бағалануы мүмкін. Классикалық құпиясөздерге қарағанда ұзын құпиясөз теруде бір немесе екі символда қателік жіберуге болады. Бұл статикалық теруіге құпиясөз тізбегінің тұрақтылығын төмендетеді, бірақ бірінші текті қателік ықтималын едәуір төмендетеді. Құпиясөз тізбегіндегі қателіктердің елемес санын түзету әдетте қателіктерді табу және түзету кодтары немесе нейрожелілік түзеткіш көмегімен жүзеге асырылады [42; 55].

Құпиясөз тізбегін енгізудің биометриялық эталоны математикалық күтіліммен бақылау параметрлелімен дисперсиясын есептеуден алынады. Есептеулерде жалпы нормадан ауытқығанын үйрету іріктемелерінен алып тастау аса маңызды болып табылады [56]. Бастапқы деректердің анық еместігін азайту үшін айқын емес жиындар аппаратын қолдану жақсы нәтиже береді [57].

Бұл биометриялық идентификация технологиясындағы қиындық қолданушының жеке пернетақталық жазуының бар болуы мәселесі болып табылады. Бұл сұраққа жауап беруге көмектесетін және тұрақталығын өлшеуге, нақты бір тұлғаның пернетақталық жазуының даралығын арнайы есептеу процедуралары [58] әдебиетінде көрсетілген.

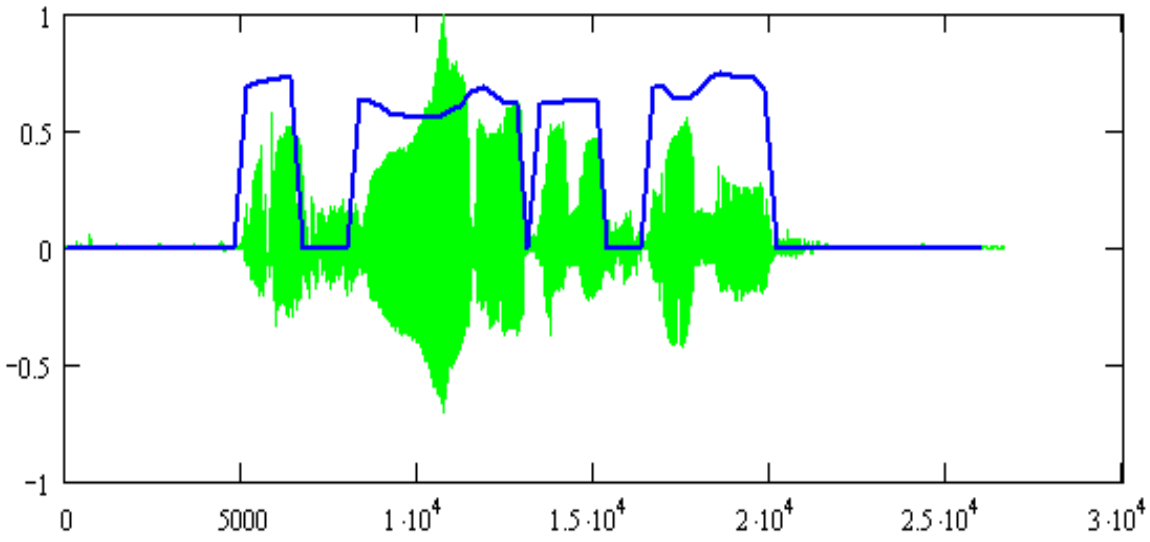
Дауыс ерекшелігі бойынша тұлғаның биометриялық аутентификациясы.

Аса дамыған жануарлардан адамның негізгі ерекшеліктерінің бірі – оның бір адамнан екінші адамға көлемді ақпаратты тілі арқылы беруі. Дыбысты есту

және оны айтуды адам туылғанынан бастайды, бірақ екі немесе үш жасында ғана айналадағыларға түсінікті тілде сөйлейді. Яғни біздің көмейімізді басқаруды үйренуімізге әр қайсысымызға екі немесе үш жыл уақыт кетті. Біздің әр қайсысымыздың дыбыстық аппаратымыз өте күрделі, оған бір рет ие болып өмір бойына дараланған сөйлеу ерекшеліктерін сақтап қаламыз [59].

Адам сөзі дыбыстардан тұрады ал олардың қалыптасуы әріптерге байланысты, сәйкесінше адамның ауызекі сөзі қолжазба немесе баспа мәтін түрінде көрсетілуі мүмкін. Адам сөзін текст түрінде ұсыну биометриялық ауызша сөзінің жоғалуына алып келеді. Ауызша сөзді қағазға жазған соң сойлеуші дауысының ерекшелігін қалпына келтіру мүмкін болмайды.

Барлық үндестік дыбыстар ашық көрінген кезеңдік жиынтықтан және оларды әрбір кезеңінің тербелісі көрші кезеңіне ұқсас, ал ызың дыбыстар керісінше кездейсоқ және қайталанатын фрагменттерге ие емес. Кезеңдік дыбыстар үшін олардың кезеңін есептеуге болады. Сөйлеу уақытында дыбыстың негізгі үн кезеңі бір ызың дыбыстан басқасына өтуде ауысады. Нәтижеде құпиясөздік тізім үшін негізгі үн кезеңінің өзгеру графигін құра аламыз. Мұның мысалы 1.11-суретінде көрсетілген.



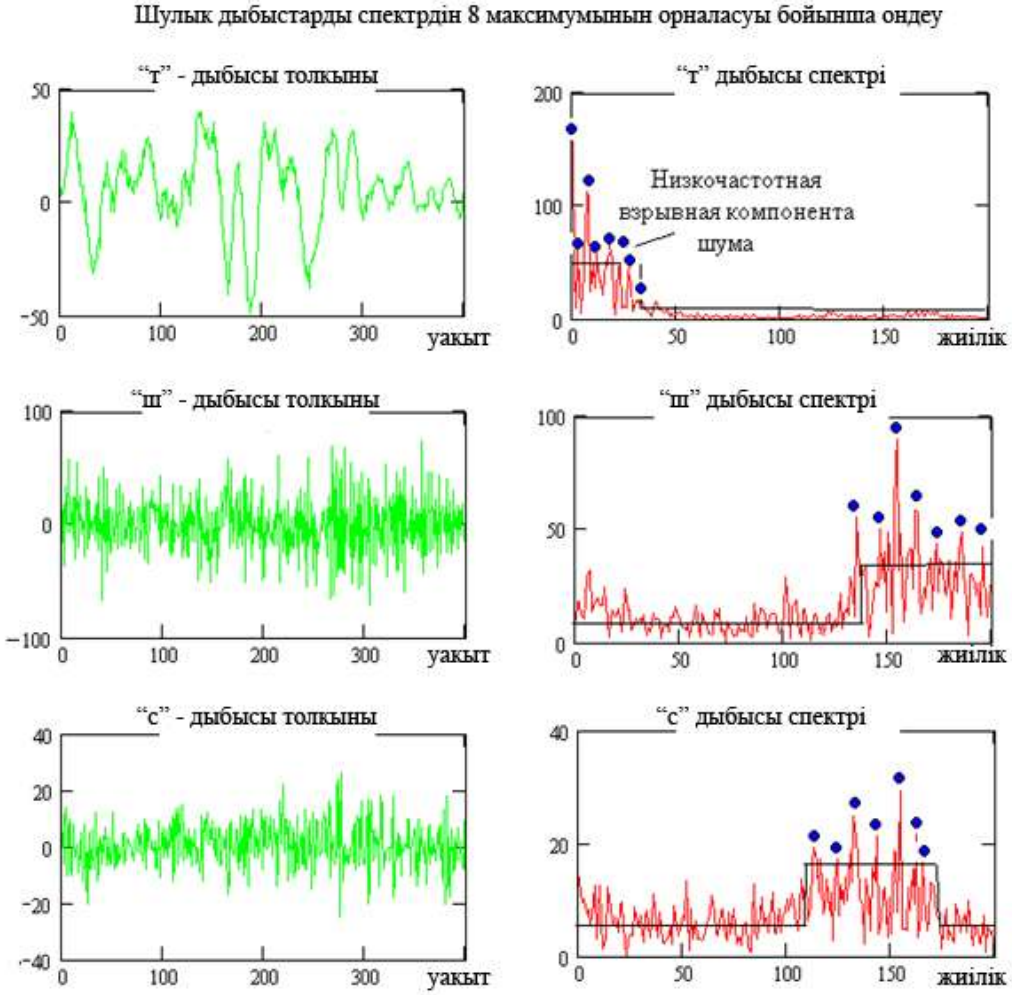
Сурет 1.11 – Диктордың дауыстық құпиясөзіне негізгі үн кезеңінің өзгеру графигі

Әрбір адам үшін негізгі үн кезеңінің өзгеру графигі бірден-бір және тұлғаның биометриялық аутентификациясы қолданылуы мүмкін.

Тұлғаның дауысы бойынша биометриялық аутентификациясының заманауи теориясы сөздің үндік дыбыстарын адамның жеке ақпаратын тасымалдайтын негізгі көз деп санайды. Шу сияқты дыбыстар іс жүзінде даралыққа ие емес және олардың көмегімен адамды идентификациялау мүмкін емес деп саналады [29; 30].

Ызың дыбыс толқынының мысалы 1.12-суретінде көрсетілген. Бұл суреттен әрбір ызың дыбыс спектрдің жоғары жиілігінің кейбір бөлігінде

энергияның өршуі көрініп тұр. Дәл осы дыбыстық тербеліс энергетикасының өршуі дыбыстық вокодерді жаңғыртады.



Сурет 1.12 – Шулы дыбыстарды спектрлік құрамы модулінің 8 максимумының орналасуы бойынша классификациялау

Нақтысы, бар вокодерлер адам сөзі тығыздығын байланыс каналдары параметрлерінің санын өзгерту арқылы өзгерту мүмкін. Адам сөзінің жіберілетін параметрлерінің үлкен көлемін қолдануда 64 килобит/секундтан 4.8 килобит/секундтқа дейінгі ағында цифрланады және дауыс биометриясын жаңғыртудың жоғарғы сапасын қамтамасыз етеді. Егер каналдар байланысы бойынша берілетін параметрлер санын төмендетсек, онда адам сөзі түсінікті болып қала береді, бірақ өзінің биометриялық қасиеттерін жоғалтады яғни робот дауысы сияқты болады.

Тұлғаның жүрісі бойынша идентификациясы. Адамның тұрақты мінез-құлықтық сипатының бірі оның жүріс болып табылады. Егер адам күніне бір рет бір бағыт бойынша жүрсе, онда осы бағыт бойымен орналастырылған сейсмодатчиктерден өңделген мәліметтер көмегімен оның идентификациясы жүзеге асырылуы мүмкін. Мұндай тұлғаның идентификациясын жасауға арналған жүйелерді толық күзет сейсможүйелерінде жүзеге асыру орынды. Жүріс бойынша тұлға идентификациясының жүйесі британдық Ұлттық

физикалық зертхананың зерттеушілерімен жасалды. Бұл жүйе бақылау камерасы көмегімен қандайда бір жабық ғимараттар мен объектілерде адамдарды бақылау үшін қолданылуы мүмкін.

Инженерлер бақыланатын кеңістіктің виртуалды моделін құру үшін автоматтандырылған жобалау бағдарламалық қамтамасын CAD-ты қолданған. Мұндай моделді қолдану нақты уақыт режимінде бақылау камералары көмегімен алынған видеодан ғимаратта қозғалып жүрген адамдардың анық сұлбасын алуға мүмкіндік берді. Осыдан соң, бағдарламалық қамтама көмегімен адам жүрісінің қадам ұзындығы, жүріс кезіндегі адам басының тербелісі сияқты негізгі сипаттары есептелінді. Осы есептеулер салдарынан негізгі сипаттар әр адамның өзіне ғана тән болып келетін сандар қатарын берді.

Ғалымдар, осы сияқты жүйелерді қолдану арқылы қоршаған ортаны бақылауға, әуежай, вокзал және тағы да басқа қоғамдық орындарда қауіпсіздік деңгейін көтеруге болады деп санайды [60].

Бірақ мұндай жүйені әзірлеушілердің ең басты проблемаларының бірі ауа-райының әртүрлілігіне қарай грунт қасиеттерінің тұрақсыздығы. Яғни адам идентификациясының сейсможүйесін ауа-райының әртүрлігіне сай үйрету қажет.

1.1.3 Тұлғаның мультибиометриялық аутентификациясы

Бірнеше биометриялық технологияларды біріктіру, яғни мультибиометриялық бірігу қолма-қол ақшаны алу немесе жеке есебін қашықтықтан басқару жүйесіне енуде тұлғаның биометриялық авторизациясы процедураларының қауіпсіздік деңгейін жоғарылатудың бір жолы болып табылады. Мультибиометриялық бірігуді қолдану арқылы келісі жетістіктерге жетуге болады:

– теру шабуылдарына биометриялық жүйе тұрақтылығын асыру. Әртүрлі биометриялық технологиялар арасындағы тұрақтылық айырмашылығы әсіресе статикалық және динамикалық биометрияны салыстырғанда жақсы көрінеді. Кейбір биометриялық бейнелер қажетті сапа мен биометриялық параметрлер санын әрқашанда қамтамасыз ете алмайды. Саусақ таңбасын қолдану да сол сияқты. Кейбір кезде, папилляр кескінінің суреті сапасыз және сурет күрделі болуы мүмкін. Қазіргі кезде екінші текті қателік ықтималдылығы саусақ таңбасы үшін 10^{-4}-10^{-6} құрайды. Бұл биометриялық бейне бойынша жүйеге кіруді кепілді шектеу мүмкіндігін бере алмайды. Осы сияқты бірнеше әлсіз биометрияларды біріктіру қажетті екінші текті қателік ықтималдығын қамтамасыз етеді;

– Биометрияны әшкерелейтін қауіпті төмендету. Биометриялық бейне бір әшкереленсе, ол қолдануға болатын тізімнен алып тасталынады. Бұл проблема статикалық биометрияның барлық түріне көкейкесті болып келеді. Бұл мәселенің шешімі мультибиометриялық бірігу құрамына статикалық және динамикалық биометрияны қосу болып табылады;

– аутентификацияның бірнеше нұсқасын қолдауы. Биометрияны енгізу мүмкіндігі болмағанда (мысалы, саусақ тілінгенде, тамақ ауырғанда дауысты

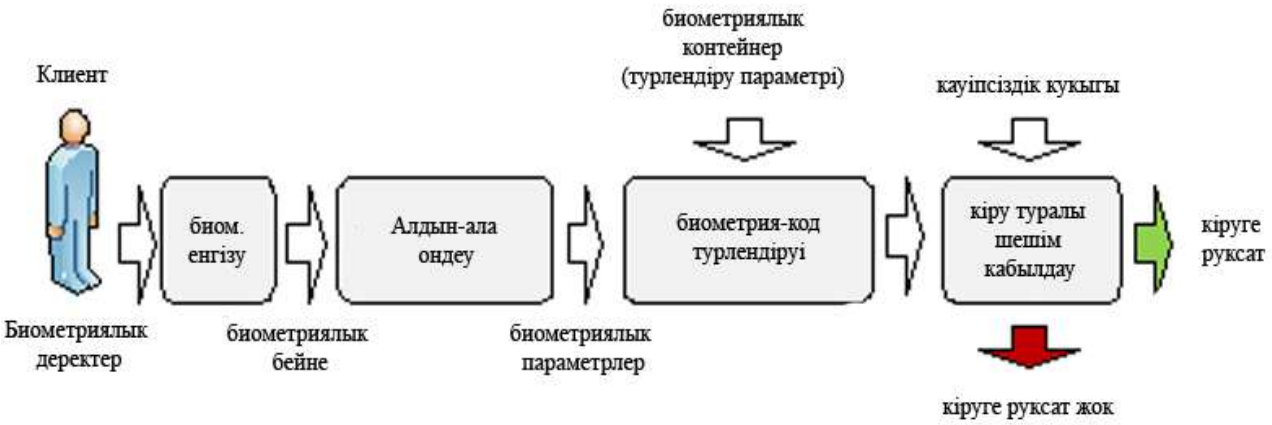
жоғалтуда) авторизация жәбірленуінен аутентификацияның бірнеше баламалы биометриялық технологияларын қолдану арқылы құтылуға болады;

– бірнеше қатысушыны қолдауы. Аутентификацияның бірсыпыра хаттамалары бір-бірінен жеке сақталынған бірнеше кілтті қолдануды талап етеді. Кілттің құрама бөліктерінің жеке биометриялық бейнелермен байланысы үшінші тараптан немесе ұйым тарапынан жүйеге қол жеткізуді бақылау және әртүрлі бірігу сұлбаларын қолдануға көмек береді;

– құпияны бөлу сұлбасын қолдауы. Қажет болса биометрия көмегімен биометриялық аутентификация процесінің бірнеше қатысушысы арасында үлестірілген құпия бөліктерімен байланыстыруды орындауға болады;

– нәтижелік код және биометриялық дерек құпиясын сақтау бойынша мультибиометриялық түрлендіргішке қойылатын қауіпсіздік талаптарын, үйрету аяқталған соң оның жойылуы бойынша талаптарын сақтауы.

Жоғары сенімділікті биометриялық аутентификация үдерісі жалпы алғанда бірнеше сатыдан тұрады: биометрияны енгізу, оны алдын-ала өңдеу, биометрия-код түрлендіруін орындау және шешім қабылдау (сурет 1.13)



Сурет 1.13 – жоғары сенімділікті биометриялық аутентификация үдерісінің оңтайланған сұлбасы

Қолданушы өз биометриясын енгізу кезінде өзінің биометриялық деректерін сандық форматқа ауыстыратын биометриялық сипаттарды түсіріп алу физикалық құрылғысына ұсынады.

Алдын-ала өңдеу кезінде қалыптастырылған биометриялық бейне маңызды биометриялық параметрлердің анализі мен оларды табу процедурасына ұшырайды.

Биометрия-код түрлендіруі кезінде жалпы жағдайда тұрақсыз биометриялық параметрлер қандайда бір банк жүйесіне қол жеткізу шығыс кодына түрлендіріледі.

Шешімдер қабылдау кезеңінде эталондық мәнмен қол жеткізу коды салыстырылады, сонымен қатар аутентификация нәтижесі туралы шешім қабылданып, жүйеге кіруге рұқсат беріледі немесе берілмейтіндігі анықталады.

Жоғары сенімділікті биометриялық аутентификация қай сатыда бірігуіне байланысты МЕСТ Р52633.7 келесі мультибиометрияның түрлерін бөліп көрсетеді:

– мультимодалды биометриялық аутентификация. Енгізу құрылғыларының әртүрлілігіне байланысты бірнеше биометриялық технологияларды қолдану арқылы орындалады. Мысал ретінде графикалық планшет пен саусақ таңбасының сканері арқылы орындалатын қолжазба бейнесі мен саусақ таңбасы бойынша биометриялық аутентификацияны келтіруге болады;

– мультибейнелік биометриялық аутентификация. Бір биометриялық технологияның бірнеше биометриялық бейнелерін қолдану арқылы орындалады. Мысал ретінде бір сканерге оң және сол қолдың саусақтарын қою немесе бірнеше қолжазбалық сөз-құпиясөзді бірінен соң бірін енгізу көмегімен орындалатын биометриялық аутентификацияны келтіруге болады;

– мультисенсорлық биометриялық аутентификация. Биометриялық бейнені енгізуге арналған бірнеше құрылғының көмегімен орындалады. Мысал ретінде аутентификациядан өтушінің кеңістікте орналасуын қадағалайтын бірнеше микрофонды қолданып, дыбыс тізбегін енгізуді қарастыруға болады. Екінші бір мысал – екі бақылау камерасын қолданып, бет-әлпеттің көлемді кескіні бойынша аутентификация;

– мультиүлгілік биометриялық аутентификация. Бір биометриялық бейненің бірнеше үлгісін қолдану арқылы орындалады. Алынып жатқан биометриялық бейненің сапасы төмен және оның сапасын көтеру қажет болған жағдайда ғана қолданылады;

– мультиалгоритмдік биометриялық аутентификация. Онымен бір биометриялық бейнеден мүмкіндігінше көп ақпарат алу мақсатында әртүрлі алгоритмдер көмегімен өңделеді;

– көп қолданушылық биометриялық аутентификация. Бірнеше биометриялық бейне донорларының қатысуымен орындалады. Құпияны бөлу немесе ұсақтаудың бірнеше сұлбаларын қолдануда жүргізіледі;

– көпнұсқалық биометриялық аутентификация. «немесе» логикалық амалының көмегімен мультибиометриялық аутентификацияның бірнеше түрін бірітіреді.

Жоғарыда көрсетілген мультибиометриялық аутентификацияның түрлері бір-бірімен бірлесе қолданылуы мүмкін.

1.2 Биометриялық технологиялардың салыстырмалы тиімділігі

Қашықтықтан аутентификациялауда тексеруші тексерілетін адамның шындығында да өз жеке кілтін сенімді сақтағандығына сенуі мүмкін, бірақ тексерілушінің үйретілген нейрожелісі басқа біреудің қолына түспегендігіне ешқандай кепілдік жоқ. Сәйкесінше қаскүнем белгісіз жеке кілтті нейрожелі кірісіндегі эмуляторға кездейсоқ мәліметтерді теріп көру арқылы қалпына келтіруге тырысуы мүмкін. Кездейсоқ теру шабуылына, яғни қаскүнемнің биометриялық бейнені теруіне қажет уақытты бағалау қажет.

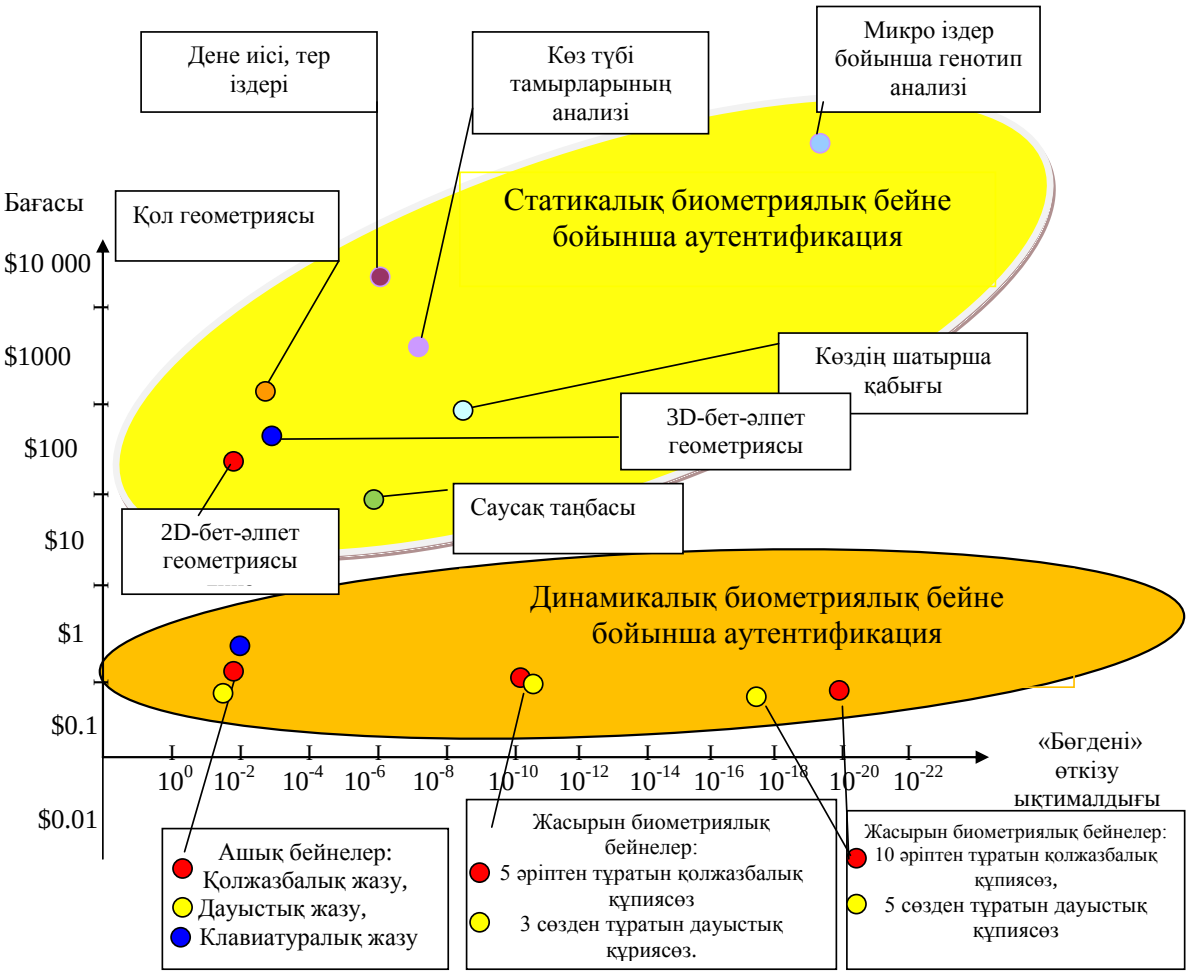
Анықтылық үшін, болжамдалған саусақ таңбасы суретінің анализі бойынша құрылған қандайда бір биометриялық қорғаныс жүйесін қарастырайық. Қос қабатты нейрожеліні шығару қарапайым ДЭЕМ көмегімен 10^{-3} с уақытта жүзеге асатындығынан бастайық. Сонымен қатар, қаскүнем шындыққа жанасатын биометриялық деректерді синтездейтін бағдарламасы бар деп есептейік. Мұндай деректердің синтезіне де 10^{-3} с уақыт кетеді. Бұл жағдайда ол секундына 1000 кездейсоқ бейнелерді нейрожелі кірісіне қойып шыға алады. Өндірушінің жариялаған екінші текті қателігін 10^{-8} («Бөтеннің» саусақ таңбасын қателесіп «Өзім» сияқты қабылдауы) жоғары ықтималдықпен сәтті теру үшін 10^{8} бейнені тексеріп шығу қажет. Секундына 10^{3} бейнені тексеруде теруге 10^{5} с жұмсалады. Бұл машинаның шамамен тәуліктік жұмысы болады. Егер қаскүнем есептеуді жылдамдатқышты қолданса, жүйені бұзуға бір сағат немесе бірнеше минут жұмсайды.

Егер қаскүнем заңды қолданушының саусақ таңбаларына тән ерекшеліктерін тани алса, онда ол комбинация іріктеулерін нөлге дейін түсіреді. Қолданушының ашық биометриялық бейнесі әшкерелеуге қарсы өте төмен тұрақтылыққа ие. Саусақ таңбаларын біз ыдыс-аяқта, үстелде, қағазда қалдыруымыз мүмкін. Сәйкесінше, қаскүнемнің сол адамның жанында жүруі мүмкін. Бұл биометриялық ашық бейнелердің теру шабуылына қарсы қорғаусыз қалатындығын білдіреді. Бұл жүйелер өз тиімділігін жояды. Олар сондай шабуылдарға төзбеуіне қарамастан қандайда бір бағаға ие.

Қорғау құралдарының тиімділігі олардың бағасының тұрақтылыққа қатынасы арқылы анықталады [32, с. 90-91]. 1.14-суретінде биометриялық параметрлер бойынша аутентификациялаудың әртүрлілігі мен олардың бағасының салыстырмалы графигі көрсетілген. Бұл тұрғыдан адамның физикалық денесінің ерекшеліктерінің анализі негізінде құрылған статикалық биометрияның биометриялық жүйелерінің тиімділігі аз болып келеді. Олар біріншіден қымбат, екіншіден «Бөтенді» жіберу ықтималдығы бойынша тұрақтылығы төмен. Керісінше, адамның жасырын биометриялық бейнесі (қолжазбалық және дауыстық құпиясөздері) мейлінше тиімді. Олар ешкімге белгісіз, әрі олардың тұрақтылығы оның ұзындығына байланысты. 5 әріптен тұратын қолжазбалық құпиясөздің биометриялық нейрожелілік қорғанысының тұрақтылығы орташа статистикалық қолданушы шабуылы үшін 10^{9} мүмкіндігі дейгейінде. Егер қолжазбалық құпиясөз тізбегінің әрқайсысы 5 әріптен тұратын 2 сөзден құралса, онда мұндай қорғаныстың теру шабулына тұрақтылығы 10^{18} мүмкіндігіне дейін өседі. Бұл жеке ақпараттың қауіпсіздігіне сезілетіндей кепілдік береді. 10^{18} күйіндегі деңгейдегі комбинация санымен белгісіз биометрияны теруге қарапайым машинаның бірнеше жүз жыл үзіліссіз жұмысы қажет.

Жасырын дауыс және қолжазба бейнесінің биометриялық қорғанысын қолданудың тиімділігінің жоғары болуы дыбыстық және қолжазбалық ақпараттарды енгізу аппараттық құралдарының қалта компьютерлері мен смартфондарында болуымен сипатталады. Яғни саусақ таңбасын, көздің шатырша қабығын, қолдың геометриясын тағы басқаларды енгізу құралдары

сияқты қымбат аппараттарды сатып алудың қажеті жоқ, ал бағдарламалық құралдар бағасы аса қымбат емес.



Сурет 1.14 – Тұлғаның биометриялық аутентификациясы технологияларының әртүрлілігі

2 АДАМНЫҢ ЖЕКЕ БИОМЕТРИЯСЫН НЕЙРОЖЕЛІЛІК ҚОРҒАУ

2002 жылдан бастап қазіргі күнге дейін жүріп жатқан зерттеулер жасанды нейрон жүйелерін қолдану есебінен биометриялық технологиялар айтарлықтай күшеюі мүмкін екенін көрсетті [27; 31-34; 47; 61-64].

2.1 Нейрондар моделдері мен нейрондық желілердің негізгі түсініктері, анықтамалары

Адамдардың миын құрайтын нейрондар желісі ақпаратты өңдеудің өте тиімді кешендік, әрі маңызды паралельдік жүйесін көрсетеді. Ол өз нейрондарын жоғары дәрежеде ұйымдастыра алады, мысалы, бейнені қабылдауды жүзеге асыру үшін, бұл тапсырмалардың шешімін ең заманауи компьютерлерден іздеуге қарағанда, оның танып білу қабілеті бірнеше есе жылдам. Мұндай жылдамдық тек қана адамның миында таныс бет-әлпетті танып білуі 100-120 мс болады, ал компьтерге бірнеше минут немесе сағаттар қажет болады.

Бүгінгі күні, әрине 40 жыл бұрын сияқты, адамдардың ойлап тапқан кез-келген есептеуіш машиналарына қарағанда, адам миы жоғары дәрежеде, айтарлықтай өзге принциптермен жұмыс істейді. Дәл осы дерек қаншама жылдар бойы нейрондық желілердің (НЖ) зерттелуі мен қайта жаңғыруы бойынша ғаламдардың жұмысына бағыт беріп отырады [65].

«Нейрондық желі» термині нақ биологиялық термин болып табылады, сондықтан нейрондық желілер негізінен жасанды қейронды желілер (ЖНС) деп аталуы тиіс. Бірақ бұған көңіл бөліп, терминдерден шатыспау үшін, жалпыға бірдей түсінікті Нейрондық Желі терминін қолдана берейік.

Нақты нейрондық желі – бұл нейрондардың жиынтығы – біздің миымызды құрайтын кішкентай ұяшықтар. Желі әр түрлі әдістермен өзара әрекет етуші әрі байланысушы бірнеше миллиард нейрондардан құралуы мүмкін. НЖ көмегімен осы биологиялық құрылымның үлгісін қайта өңдеу талпынысы архитектурада да, өзара әрекет етуде де жасалады. Бірақ бұл жерде кішкене проблема туындайды: біз нақты НЖ-нің анық қалай жұмыс істейтінін білмейміз. Нақты НЖ архитектурасы түбегейлі бір типтен екінші типке өзгереді, бұл жерде жалғыз ғана нейрон желісінің қарапайым ұяшығы қалай орналасқанын білетінімізге сүйенуге болады. Оның құрылымы толық түрде төменде қарастырылады.

Бүгінгі күні іс жүзінде НЖ қолдану туралы көптеген "қарсы" және "қарсы емес" пікірлер кездеседі. НЖ-нің көзге көрініп тұрған жетістіктерінің біріне дәстүрлі әдіс жұмыс істемейтін аудандарда оларды қолдануға болатындығын кіргізуге болады. Мысалы, НЖ-ні әртүрлі үлкен көлемді түрлі қала мәліметтері ағынында жұмыс жасайтын жүйелердегі қолданысын көрсетуге болады. НЖ көптеген типтері биологиялық тұрғыдан дұрыс, яғни олардың көмегімен адам миында жүретін, ойлау процестерін үйренуге болады. НЖ аймағындағы заманауи зерттемелер жақын болашақта оларды сұрыптау және объектілерді өңдеуде жоғары жылдамдыққа алып келетініне сендіреді.

НЖ аймағындағы зерттеулер белсенділендірудің үш кезеңінен өтті. Біріншісі 40-жылдарда өтіп, МакКалок пен Питтстің алғашқы жұмысымен негізделеді [66; 67]. Онда жүйке клеткаларына ұқсас логикалық амалдар орындай алатын шектік элементтер негізінде автоматты құру идеясы мазмұндалды.

Алайда, шектік элементтер негізіндегі жүйені жобалау тапсырмасы өте қиын болып шықты. 20 жылдан соң табылған шешімінің қиын болғаны сонша, оның оннан жоғары нейроннан тұратын автоматтарының синтезі жоққа шығарылды. Осы себепті, алғашында осындай автоматтардың практикалық жүзеге асуын тірі организмнің жүйке жүйесіне ұқсастырып үйрету әдістерін іздестірумен байланыстырылды. Шектік элементтер негізінде үйретілетін жүйе жасанды нейрондық желі атына ие болды.

Жандандырудың екінші кезеңі 1959 жылы пайда болған Розенблат перцептронының жинақтық теориясының арқасында 60-жылдарда туындады [68]. 60-жылдардың аяғына қарай АҚШ-та нейрондық желінің (НЖ) бірнеше эксперименталды моделі болды.

Аналогты және сандық техника ("Адам-А" и "Адам-Д") негізіндегі алғашқы күрделі перцептрондар 1969-1971 жылдар аралығында Киевтің ғылыми-зерттеу институттарының бірінде құрылды [69].

Розенблаттың қарапайын перцептронының сұлбасы келесі 2.1-суретінде кескінделген. Ол шектік элементтердің үш қабатынан тұрады. Кіріс сигналдары (стимул) рецепторларға (S-элементтеріне) әсер етіп, оларды қозу күйіне ауыстырады. S-элементтер ассоциативті нейрондар (А-элементтер) жиынтығымен кездейсоқ байланысқан. А-элементінің шығысы 0-ден ерекшеленеді, егер онымен байланысқан рецепторлардың жеткілікті саны қосса. А-элементтерінің реакциясы байланыс арқылы эффектор кірісіне түседі. Олардың саламағы үйрену кезінде өзгереді. Эффекторлерде постсенаптикалық потенциялы – келіп түскен сигналдардың өлшенген суммасы есептелінеді. Әдетте есте сақталатын әр бір бейне үшін перцептронда бір эффектор бөлінеді және постсенаптикалық потенциял мәнінің максимумы бойынша шешім қабылданады.

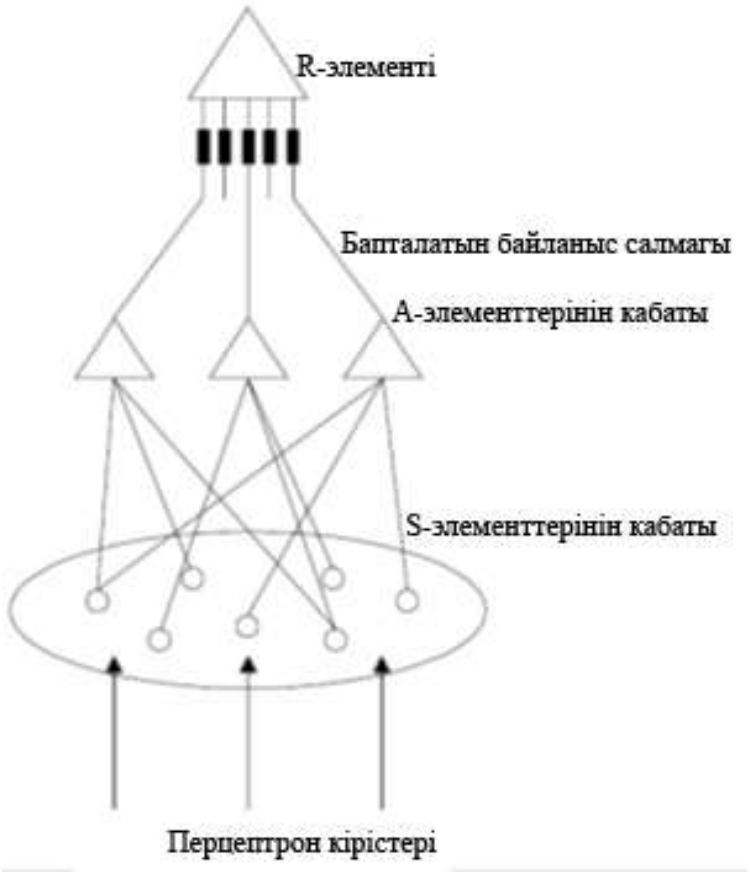
Розенблат перцептронына тән құрылымның біркелкі еместігі (SA және R Элементтерінің бөлінуі) НЖ соңғы модельдерінде жойылған. Минскии және Пейпер жұмыстары қарапайым перцептронның шектеулі мүмкіндіктерін көрсетті [70]. Олардың нәтижелері көптеген зерттеушілердің әсіресе есептеу ғылымы аймағында жұмыс істейтіндердің ынтасын өшірді. Нейрондық желі бойынша зерттеулер 20 жылдай тоқтап тұрды.

Нейрондық желіге қызығушылықтың қайта оянуына бірнеше себептер әсер етті:

– Жапониялық жоба шеңберінде жасалып жатқан ЭЕМ-нің бесінші ұрпағы жасанды зерде логикалық жүйелерін жүзеге асырудағы қиындықтар;

– нейрондық желіні үйрету және жадысын ұйымдастыруда жаңа идеялардың пайда болуы;

– ЭЕМ өнімділігінің өсу қарқынының қажет жоғары өнімді есептеулердің өсуіне қарағанда артта қалуы.



Сурет 2.1 – Қарапайым перцептрон сұлбасы

80-жылдардың басынан НЖ-ге зерттеушілердің қызығушылығы қайта оянды. Оған себеп Хопфилдтің энергетикалық жолы және Вербос алғаш рет ұсынған көп қабатты перцептронды (тікелей тарату көп қабатты желісі) үйретуге арналған кері тарату алгоритмі [71].

Румельхарттың көмегімен 1986-жылы алгоритм танымал болды [72]. 80-жылдардың ортасыныан бастап нейрондық желілерді модельдеуге қызығушылық үздіксіз өсіп келеді. Олардың ерекшелігі параллельді жұмыс болып табылады және осы себепті мұндай желілерді дәстүрлі архитектураға ие ЭЕМ-де модельдеу көп уақыт алады. Бұл процессті жылдамдату үшін әлемнің әр түрлі елдерінде арнайы құрылғылар пайда бола бастады. Олар нейрокомпьютерлер деп аталды.

Нейрокомпьютинг – бұл ғылыми бағыт болып, параллельді жұмыс істейтін қарапайым есептеу элементтерінің (нейрондарының) көптеген санынан тұратын нейрокомпьютерлердің алтыншы ұрпағы есептеу жүйелерін құрумен айналысады. Элементтер өзара нейрондық желі құрастыру арқылы байланысқан. Олар біркелкі есептеу әрекеттерін орындайды және сыртқы басқаруды талап етпейді. Параллельді жұмыс істейтін есептеу элементтерінің үлкен саны жылдамдықты қамтамасыз етеді.

НЖ анықтамасының саны өте көп, бірақ адоптивті машина ретінде НЖ-нің анықтамасын келесі түрде беру орынды [73]: жасанды нейрондық желі (neural network) бұл тәжрибелі білімді сақтауға және репрезентация қабілетіне ие айтарлықтай параллельді – таратылған процессор. Ол миға екі тұрғыдан ұқсас:

– білім желіні үйрету процессінде алынады;

– білімді сақтау үшін синаптикалық салмақ деп аталатын нейро желілер арасындағы байланыс күші қолданылады.

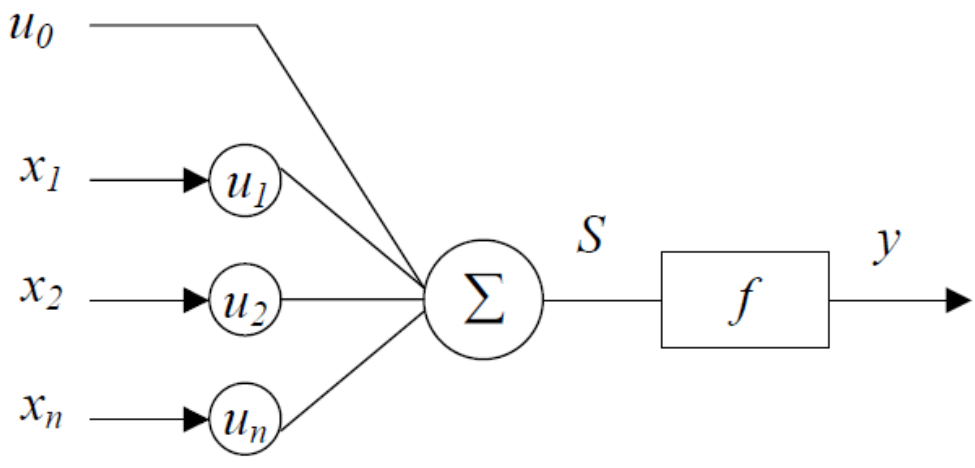
НЖ теориясындағы үш негізгі түсінік: нейрон, желі архитектурасы және үйрету түсінігі болып табылады. Бұл түсініктердің анықтамаларын қарастырайық.

Нейронның алғашқы моделі МакКаллок пен Питтс ұсынған [67]. Олар нейрон ретінде бинарлық шектік элементті қолданған. Бұл математикалық нейрон x_i, i = 1, 2... n, кіріс сигналдарының n салмақты суммасын есептейді және егер бұл сумма u анықталған шегінен асып кетсе, онда бір өлшеміндегі сигналды шығысына қалыптастырады ал кері жағдайда 0 ді қалыптастырады. u x_0=1 тұрақты кірісімен байланысты салмақтық кеэффиценті ретінде қарастыру қолайлы. Оң салмағы қоздыруші байланыстарға, ал терісі- тежегіш байланыстарға сәйкес. Берілген концепцияның математикалық өрнегі (2.1) формуласымен сипатталады:

$$S = \sum_{i=1}^{n} u_i x_i + u_0, \qquad (2.1)$$

мұндағы u_0 – жылжу мөлшері.

Нейронның моделі 2.2-суретінде ұсынылған.



Сурет 2.2 – Нейрон моделі

Дәстүрлі активациялық функция сатылық түрге ие, яғни y нейрон шығысында сигнал тек қана кіріс әсерінің суммасы қандайда бір сыни мәннен асқанда ғана пайда болады.Активациялық функцияның негізгі үш типін келтірейік:

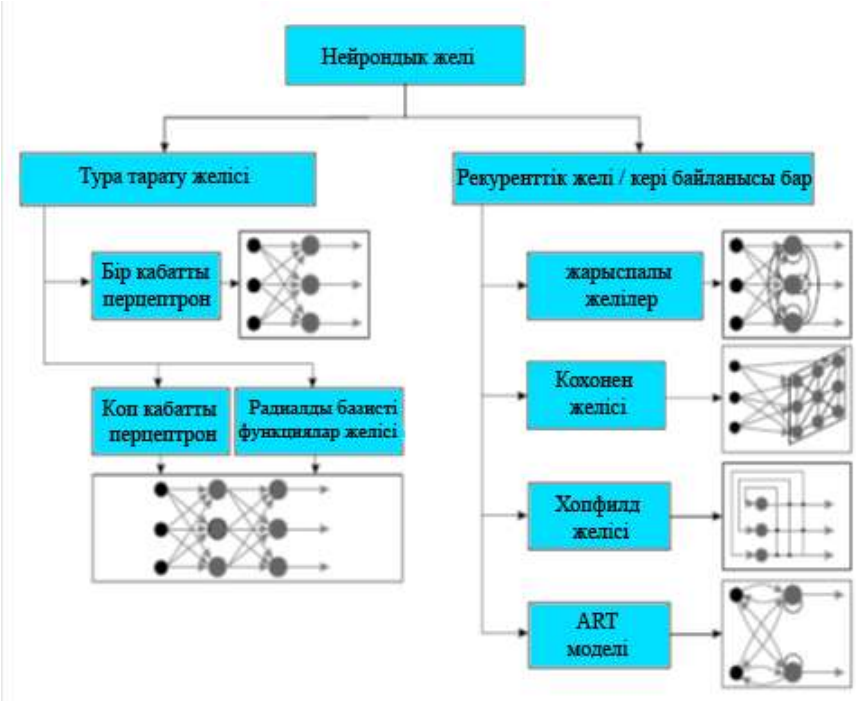
$$f(s) = \begin{cases} a, \text{егер } s > a \\ s, \text{егер } -a \le s \le a \\ -a, \text{егер } s < -a \end{cases}$$ – сызықтық,

$$f(s) = \frac{1}{1+e^{-s}}$$ – сигмоидтық,

$$f(s) = e^{\frac{s^2}{\sigma^2}}$$ –радиалды-симметриялық.

МакКаллок пен Питтс осы типтегі параллелді жұмыс жасайтын нейрондар жиынтығының сәйкес таңдалған салмағында әмбебап есептеулер жүргізуге болатындығын дәлелдеді.

НЖ архитектура көз қарасы тарапынан қалыптастырылған біркелкі байланыстарымен бағытталған граф ретінде қарастырыла алады. Онда жасанды нейрондар түйіндер болып табылады. Нейрондық жүйе байланыстарының архитектурасы бойынша екі класқа топтастырылуы мүмкін (сурет 2.3): тікелей тарату желісі және рекурентті желі немесе кері байланыс желісі. Көбірек тараған желілер тобының бірінші класында көп қабатты перцептрондар деп аталатын бірінші класындағы нейрондары қабаттармен орналасып, қабаттар арасында бір бағытты байланыстарға ие.



Сурет 2.3 – НЖ байланыстарының архитектурасы

2.3-суретте әрбір класстың типтік желісі көрсетілген. Тікелей тарату жүйесінің статикалық болуының себебі берілген кірісте олар желінің алдынғы күйіне тәуелсіз шығыс мәндерінің бір жиынын шығаруында. Рекуренттік желілер динамикалық болып есептелінеді, себебі кері байланысына қатысты

нейрондар кірісі модификацияға ұшрайды. Бұл желі күйінің өзгерісіне әкеліп соғады.

Үйретуге қабілеттілік мидың негізгі қасиеті болып табылады. НЖ аясында үйрету процессі келесі анықтамаға ие: НЖ үйрету – желі архитектурасын баптау және арнайы тапсырманы тиімді орындау үшін байланыс салмақтары. Желі жұмысы коэффициенттер салмақтарын итеративті баптау арқылы жақсартылады. Үлгі бойынша желінің үйрену қасиеті сарапшылар қалыптастырған жұмыс істеу ережелері бойынша істейтін жүйе мен салыстырғанда анғұрлым тиімді. Үйрету процессін құрастыру үшін нейрондық желі жұмыс істейтін сыртқы ортаның моделі қажет. Бұл модель үйрету парадигмасын анықтайды [74]. Екіншіден, желі параметрлерінің салмағын қалай модефикациялау қажет екенін яғни баптау процессін қандай үйрету ережесі басқаратындығын түсіну қажет. Үйрету алгоритмі салмақ баптау үшін қолданылатын үйрету ережелерінің процедурасын білдіреді.

Нейрондық желілер парадигмасын категориялау. Түсінуге оңай және мазмұндамасын жеңілдетуге және категориялау үшін олардың қысқаша классификациясы 2.1-кестеде көрсетілген.

Кесте 2.1 – Нейрондық желінің классификациясы

Нейропарадигма атауы	Авторлары	Әзірленген жыл	Қолдану аймағы
1	2	3	4
Бірқабатты перцептрон (Single layer perceptron)	R.Rosenblatt	1959	Бейнетану, классификациялау / категориялау
Қателіктерді кері тарату (BackPropagation)	R.Rosenblat, M.Minsky, S.Papert	1960	Бейнетану, классификациялау, болжау
Қарама-қарсы бейнетану (Counter Propogation)	R. Hecht-Nielsen	1986	Бейнетану, бейнені қалпына келтіру (ассоциативті жады), мәліметтерді сығу
Кіріс жұлдыз (Instar Network)	S.Grossberg	1974	Бейнетану
Шығыс жұлдыз (Outstar Network)	S.Grossberg	1974	Бейнетану
Жасанды резонанс- 1 (Art-1 Network)	S.Grossberg G.Carpenter	1986	Бейнетану, кластерлік талдау
Хопфилд желісі (Hopfield Network)	J.J.Hopfield	1982	Фрагменттері арқылы мәліметтерді іздеу және қалпына келтіру
Хэмминг желісі (Hamming Network)	R.W.Hamming	1987	Бейнетану, классификация, ассоциативті жады, бөгет жағдайында сигналдарды сенімді жіберу

2.1-кестенің жалғасы

1	2	3	4
Кохонен желісі (Kohonen Network)	T.Kohonen	1984	Кластерлік талдау, бейнетану, классификация
Максимумды іздеу желісі (MAXNET)	R.P.Lippman	1987	Хемминг желісімен бірге, бейне тану жүйесі НЖ құрамында
Тура байланыспен максимумды іздеу желісі (Feed-ForwardMAXNET)	R.P.Lippman	1987	Хемминг желісімен бірге, бейне тану жүйесі НЖ құрамында
Қосбағытталған авто ассоциативті жады (BAMNetwork)	B.Kosko	80-жылдардың II жартысы	Ассоциативті жады, бейнетану
Больцман үйретуі (Boltzman machine)	J.Hilton, T.Sejnovsky H.Szu	1985	Кескінді, радар сигналдарын, сонарды тану
Гаусс классификаторы (Neural Gaussian Classifier)	R.P.Lippman	1987	бейнетану, классификациялау
Генетикалық алгоритм (Genetic training algorithm)	J.Holland, D.Goldberg	1975 1988	НЖ үйрету, сонар сигналдарын тану

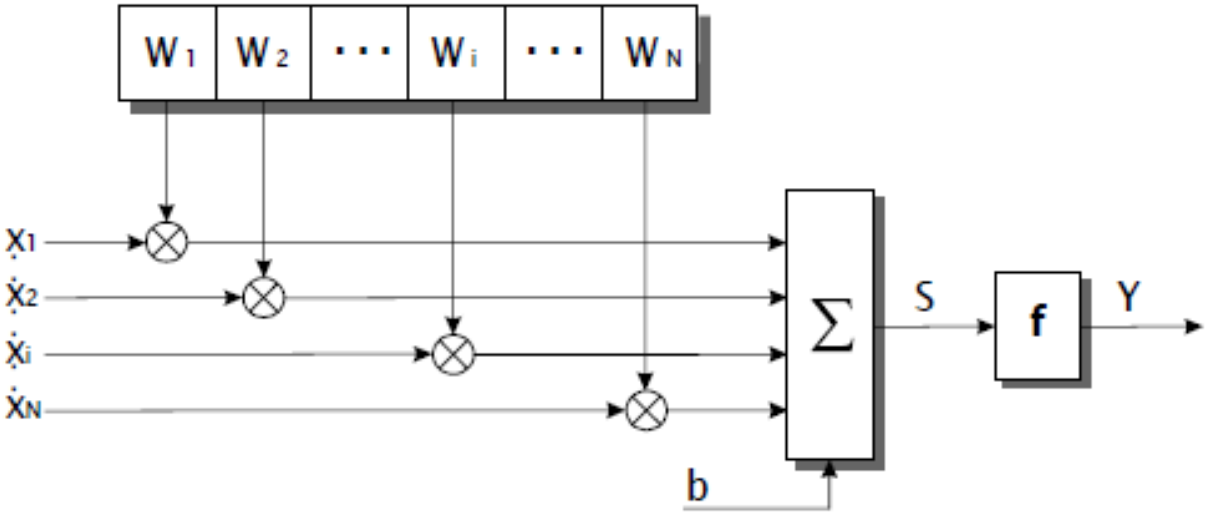
2.1.1 Бір қабатты перцептрон

Бір қабатты перцептрон НЖ теориясында негізгі түсінік болып табылады, бірақ бұл түсініктің қазірге дейін жеке анықтамасы жоқ. Бүгінгі күні перцептрондарға негізделген саналған алгоритмдер бар, бірақ бұл алгоритмдердің көбіне бір біріне ұқсайтын тұстары аз.

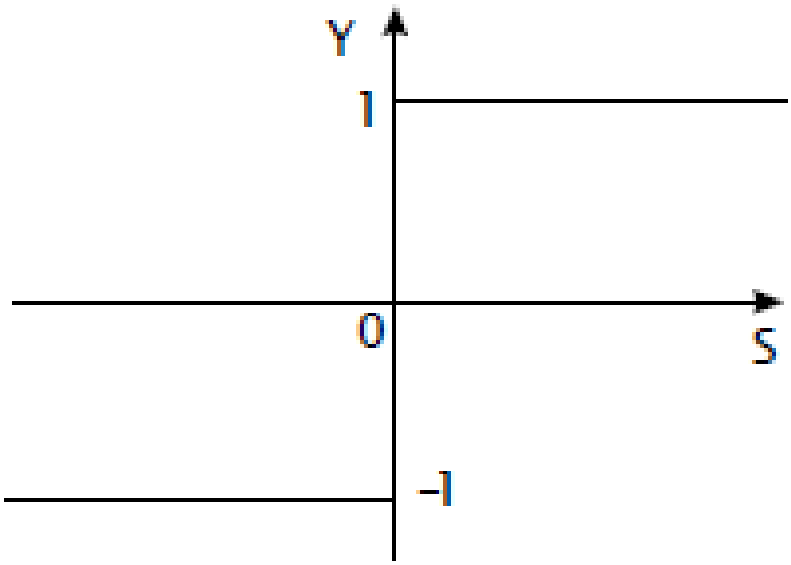
Бір қабатты перцептрондардың негізгі қолдану аймағы қарапайым бейнені тану.

Бір қабатты перцептрондардың құрылысы өте қарапайым. Қандайда бір $X_1 \ldots X_N$ анықталған кіріс саны бар. Олардың әр қайсысының салмағы $W_1 \ldots W_N$ салмақтық функциясымен анықталады. Сонымен қатар кіріс сигналдарының салмағын синаптикалық салмақтар деп атайды, себебі олар нақты НЖ-да синапстар функциясына сай қалыптасқан. Жеке перцептрон функциясы (2.4-суретте оның сұлбасы көрсетілген) кіріс сигнал элементтерінің қалыптастырылған суммасын есептеу болып табылады, және одан b жылжуының мәні алып тасталады, сонымен қатар нәтиже шығысы +1 немесе -1 ге тең шектік функциясынан өткізіледі.

Шығыс сигналының мәніне байланысты шешім қабылданады: “+1 ” – кіріс сигнал А класына тиісті, “-1 ” – кіріс сигнал В класына тиісті шектік элементті ауыстыру функциясының графигі 2.5-суретінде көрсетілген.



Сурет 2.4 – Қарапайым перцептрон жұмысының сұлбасы



Сурет 2.5 – Шектік элементтің өзгеру функциясының графигі

Бір қабатты перцептронды үйрету алгоритмі синаптикалық салмақтың берілу коэффициенттерінің өзгерісіне негізделген. Бір қабатты перцепртронды үйрету алгоритмін осы процесстің бағдарламалық жүзеге асу алгоритмін анықтау мақсатында толығырақ қарастырайық.

1-қадам. Синаптикалық салмақ және өзгерісті меншіктеу:

Синаптикалық салмақ мәні $W_i(0)$ және b нейрон жылжуы кейбір аз кездейсоқ сандарға тең алынады мұндағы $W_i(t)$ – t уақтындағы нейронға кіріс сигналының і-элементіне салмақтың байланысы ($0 \le i \le N$).

2-қадам. Желінің жаңа кіріс және қажетті шығыс сигналдарының ұсынылуы: $X=(X_0,X_1...X_{N-1})$ кіріс сигналын қажетті d шығыс сигналымен бірге нейронға ұсынылады.

3-қадам. Нейронның шығыс сигналын (2.2) формуласымен есептеу

$$y(t) = f\left(\sum_{i=0}^{N-1} W_i(t)X_i(t) - b\right). \quad (2.2)$$

4-қадам. Салмақ мәнін бейімдеу (баптау) (2.3) формуласымен есептеу

$$W_i(t+1) = W_i(t) + r[d(t) - y(t)]X_i(t), 0 \le i \le N-1 \quad (2.3)$$

$$d(t) = \begin{cases} +1, & \text{егер A} \\ -1, & \text{егер B} \end{cases}$$

мұндағы *r* –үйрету қадамы (1 ден кіші болуы қажет),

d(t)–қажетті шығыс сигналы

Егер желі дұрыс шешім қабылдаса синаптикалық салмақ модификацияға ұшрамаиды.

5-қадам. Екінші қадамға өту.

Бұл алгоритмнің бағдарламалық жүзеге асуында кірісі және шығысының өлшемі тек қана есептеу машинасының мүмкіндігіне қарай шектеледі; аппараттық жүзеге асуда технологиялық мүмкіндіктермен шектеледі.Кіріс сигналдарының типі бинарлы (дискретті) немесе аналогты (үздіксіз) болуы мүмкін.Бір қабатты перцептрон негізіндегі желі сиымдылыға нейрондар санымен сәйкес келеді.

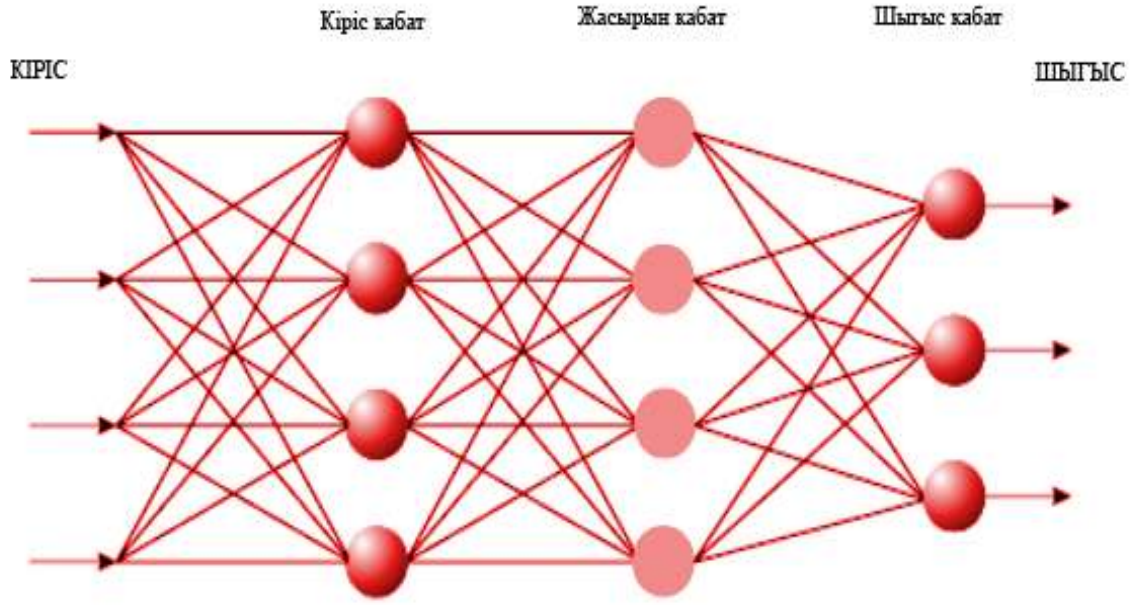
Кескінді тану жүйелеріндегі бір қабатты перцептрон негізінде НЖ-нің көрнекі артықшылығы бағдарламалық және аппараттық жүзеге асуының қарапайымдылығы, сонымен қатар алгоритмнің үйрету жылдамдығының жоғары болуы. Ал кемшілігіне 2.5-суретінде көрініп тұрғандай тек ең қарапайым бейне тану есебін шешуге арналған тегістікті бөліп тұрған түзу болып табылады. Көп қабатты перцептрондар тегістікті күрделі айырғыш құруға мүмкіндік береді және осы себепті оларды бейне тану есебін шешуде кеңнен қолданады.

2.1.2 Көп қабатты нейрондық желілер. Қатені кері тарату алгоритмі

Көп қабатты нейрондық желілер немесе көп қабатты перцептрон Розенблат, Минск, Пейпер және тағыда басқалар тарапынан зерттеліп, алғаш рет 60-жылдары ұсынылды [68; 70]. Бірақ зерттеулер ары қарай тоқтатылды, себебі оларды үйретететін тиімді алгоритм болмады. Тек 1980-жылдардың ортасында ғана бір-бірінен тәуелсіз бірнеше зерттеушілер көп өабатты перцептронды үйрету алгоритмін ұсынды. Олардың негізі қате функциясының градиентін есептеу болды. Алгоритм «қатені кері тарату» деп аталды. Айта кететіні, қазіргі кезде бұл алгоритм тізбектелген байланыстары бар нақты көп қабатты НЖ үшін қолданылады.

2.6-суретінде үш қабатты НЖ-нің үлкейтілген кестесі берілген, мұндағы нейрондар дөңгелекпен белгіленген, ал олардың арасындағы байланыс

бағдаршамен белгіленген. Көп қабатты тізбектелген байланысы бар НЖ-ге олардың желідегі нейрондарының жалпы кіріс сигналдары бар белгілі бір топ – қабаттарға бөлінуі, және де ағымдық қабаттың әрбір нейроны алдыңғы қабаттағы барлық шығыс сигналдарға берілуі тән құбылыс. Ағымдық қабат бірінші болған жағдайда құрамындағы әрбір нейронға сыртқы кіріс сигналының барлық элементтері беріледі.

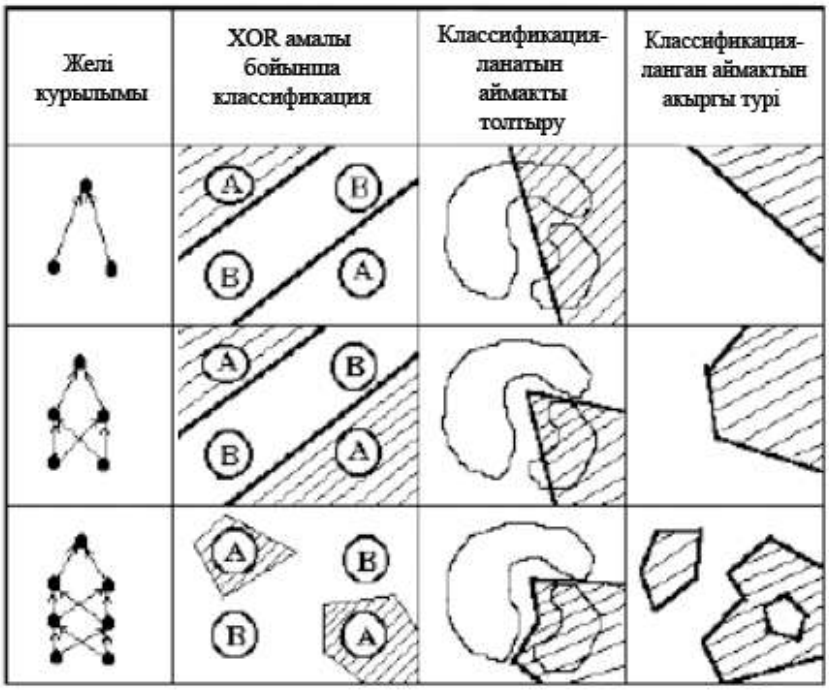


Сурет 2.6 – Нейрожелінің үш қабатты жүйесі

Нейрондар кіріс сигналдары элементтерінің салмақтанған қосындысын орындайды. Сәйкес синаптикалық салмаққа көбейтілген кіріс сигнал элементтерінің қосындысына нейронның орынауыстыруы қосылады. Қосындының нәтижесіне сызықты емес түрлендіруі – белсенділендіру функциясы орындалады. Нейронның шығысы белсенділендіру функциясының мәні болып табылады.

2.6-суретінде көрсетілгендей, көпқабатты перцептрондарды ұйымдастыру бір қабаттыға қарағанда анағұрлым күрделі. Осылайша, олардың осындай кемшіліктеріне қарамастан оны қолданудың тиімділігі туралы сұрақ туындайды. Көп қабатты перцептрондардың негізгі артықшылығы кіріс кескін кеңістігін бөлетін түзу пішінін күрделендіру есебінен бір қабатты перцептрондарға қарағанда күрделірек тапсырмаларды шешуінде болып табылады. Көп қабатты НЖ архитектурасы мен өзгеріссіз кіріс кескінді бөлетін түзу түрі 2.7-суретінде көрсетілген.

Кері тарату әдісінің кемшіліктері ретінде итерацияның әрбір қадамында желі параметрлерінің мәні өзгеруіне байланысты үйрету жылдамдығының төмендігін айтуға болады. Кері таратудың классикалық әдісі сызықтық ұқсастығы бар әдістерге кіреді.



Сурет 2.7 – Көп қабатты НЖ архитектурасына мысалдар

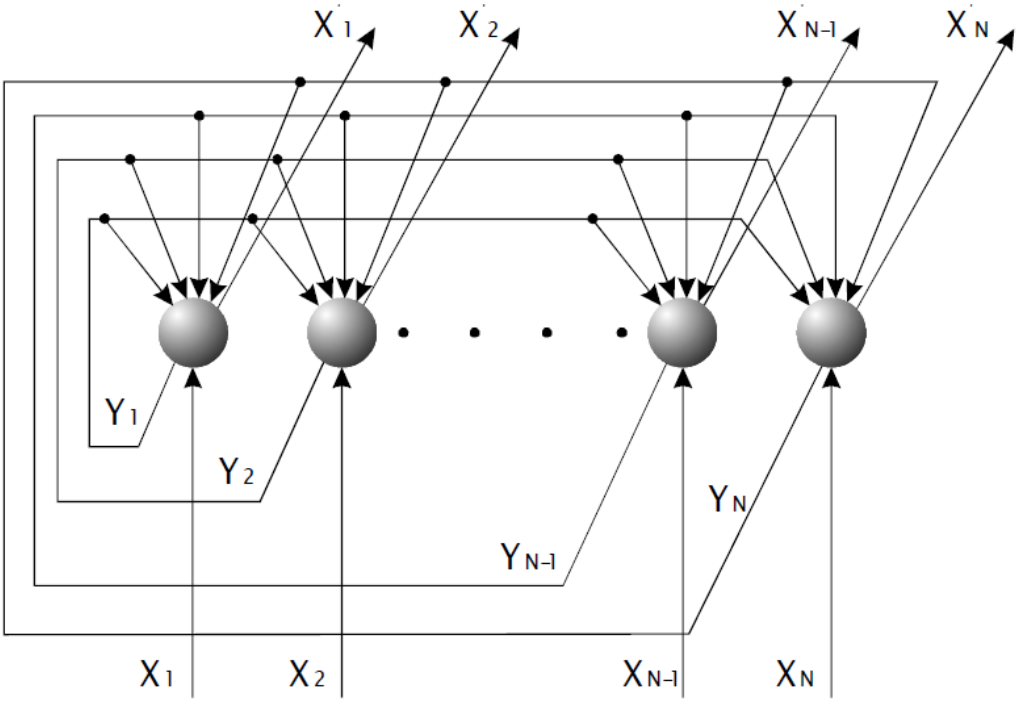
2.1.3 Хопфилдтың желісі

Биофизик Хопфилд 1974-жылдан бастап ассоциялық жадыны ұйымдастыру саласында жұмыс істеген [71; 75]. Ол қоршаған ортамен қарым-қатынасқа түскенде энергияның таралатын динамикалық жүйе сияқты НЖ-ні ұйымдастырудың энергетикалық тәсілінің авторы болып есептеледі. Хопфилд энергохимиялық желідегі нейрондардың арасындағы қарым-қатынаста пайда болған құбылыстарды қарастырады. Осы жүйедегі әрбір элемент дәрежесінің қосындысына тәуелді автогенерация адрестері бар – физикалық жүйе динамикалық жады түрінде берілетін энергетикалық деңгей.

Сонымен бірге физикалық жүйені жады түрінде қарастыруға болады, егер оның әрбір элементтердің энергетикалық деңгейі бұл жүйеде тұрақты қалпқа ие болған әрі басым болатын элементтердің деңгейіне (потенциялно) тәуелді. Хопфилд кіріс және шығыс типіне тәуелді дискреттік және үздіксіз нейрондарға жүгінетін екі желінің моделін қарастырды. Бірінші модель өте қарапайым себебі нейрон кірісінде бинарлық сигналды қабылдайды да бинарлық сигнал береді. Хопфилд екінші моделде кіріс және шығыс сигналының үздіксіз болған нейронның биологиялық қызметтегі (вероятное) моделін жасауға тырысты. Хопфилд жасаған модельдер тек жадыны ассоциативті түрде ұйымдастыру үшін ғана қолдануға болады, сонымен бірге классификация үшін, категоризация үшін, ықшамдаудың кей бір есептерін шешу үшін де қолданылады.

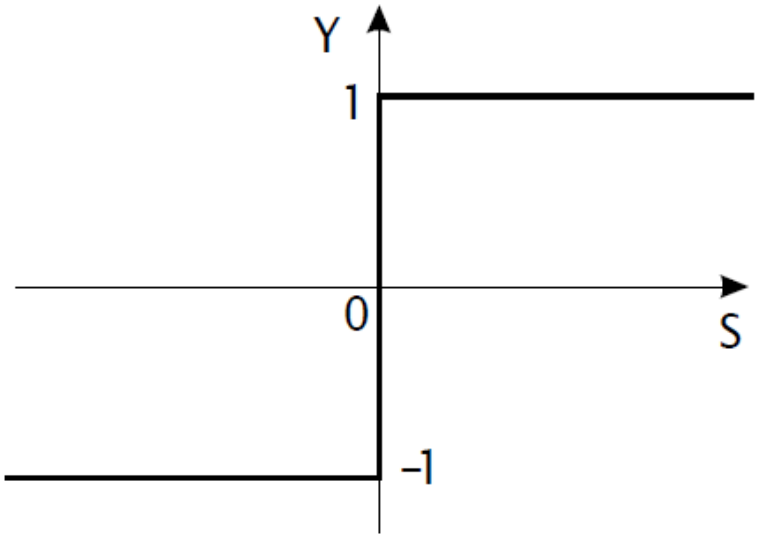
Хопфилдтың ұсынған ең бірінші желі модельдерінің бірі ассоциативті жады түрінде қолданылады. Желінің синаптикалық салмақтары мәндерін есептеуге арналған бастапқы мәндер векторлар – класс үлгілері болып

табылады. Желі циклдық түрде қызмет етеді. Нейрондардың әрбір шығысы басқа нейрондардың барлық шығысына беріледі (сурет 2.8).



Сурет 2.8 – Хопфилд желісінің моделі

Желі нейрондары қатаң шектік функцияларға ие. Желі итерациясы нейрондардың шығыс сигналдары өзгермейтін жағдайға жеткенде ғана тоқтайды. Хопфилд желісінің өзгеріс функциясы 2.9-суретінде көрсетілген.



Сурет 2.9 – Хопфилд желісінің өзгеріс функциясы

Желі сиымдылығы нейрондар санымен шектелген, яғни N нейрондардан тұратын желі $M = 0{,}15 * N$ бейнеден артық сақтай алмайды. Сондай-ақ

сақталатын бейнелер толығымен корреляцияланған болмауы тиіс. Корреляция шамасы ретінде келесі (2.2) формула қарастырылады:

$$K = \sum_{j,k}^{M} \sum_{i=1}^{N} x_i^j x_i^k,\ j \neq k, \tag{2.2}$$

мұндағы N – кіріс сигналының өлшемі,

M – үлгі-векторлар саны,

x_i^j – j-ші баған-векторының i-ші элементі.

Желінің синаптикалық салмағын қалыптастыру келесі (2.3) формуламен жүзеге асырылады:

$$w_{i,j} = \begin{cases} \sum_{s=1}^{M} x_i^s\, x_j^s, i \neq j \\ 0, i = j \end{cases} \tag{2.3}$$

$$1 \leq i,j \leq N,$$

мұндағы $w_{i,j}$ – j-ші нейронның i-ші синаптикалық салмағы.

Желі қызметі келесі (2.4) формулаға сәйкес:

$$\begin{gathered} y_j(0) = x_j, 1 \leq j \leq N \\ y_j(t+1) = f(\sum_{i=1}^{N} w_{i,j} y_i(t)), 1 \leq j \leq N \end{gathered} \tag{2.4}$$

мұндағы y_j – j-ші нейрон шығысы.

Бұл формула үшін желі қызметі келесі (2.5) шарты орындалғанда тоқтатылады:

$$y_j(T) = y_j(T-1). \tag{2.5}$$

Осылайша, желінің жалпы шығыс сигналы (2.6) тең болады:

$$x_j = y_j(T). \tag{2.6}$$

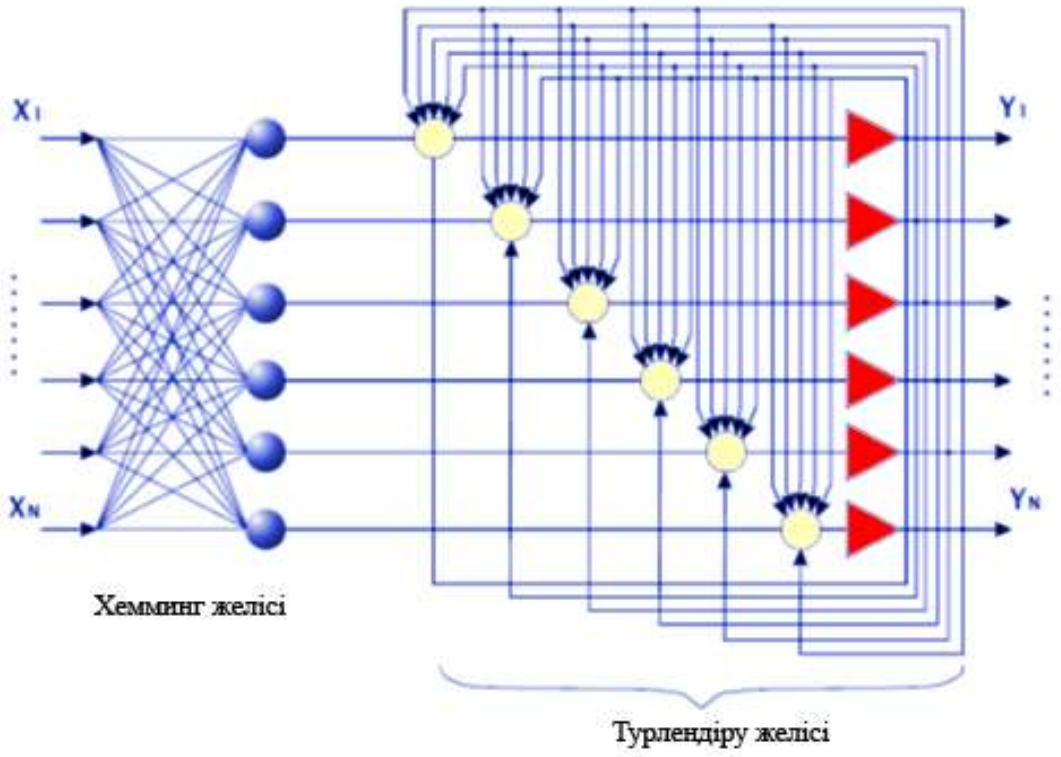
Берілген желідегі негізгі параметрлердің бірі желінің энергетикалық функциясының өзгерісі болып табылады. Қазіргі жағдайда оның төмендеуі:

$$E = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} w_{i,j}x_i x_j \qquad (2.7)$$

Желінің негізгі кемшіліктерінің бірі оның сиымдылығының төмендігі, желіде сақталған бейнелер мен қатар олардың келеңсіз бейнелерінің де сақталуынан оның пайдалы мәнінің де төмендеуі болып табылады. Бейнетану есептерінде де оның қолданысы шектелген мүмкіндікке ие, себебі оның кіріс сигналдары мен шығыс сигналдарының өлшемі сәйкес келуі қажет.

2.1.4 Хемминг желісі

Бірдей ұзындықтағы екі бірдей бинарлық вектордың Хемминг арақашықтығы – бұл осы векторларға сәйкес келмейтін биттер саны. Кіріс векторынан бірнеше үлгі-векторларға дейінгі Хеммингтің арақашықтығын параллельді түрде есептеуді жүзеге асырушы нейрондық желі Хемминг желісі атауына ие болды (сурет 2.12) [74; 76]. Бұл екі қабатты тура бағытталған желі желіні үйрету кезінде қосылған шуы бар кескіннен объектіні тану мүмкіндігіне ие.



Сурет 2.10 – Екі қабатты тура бағытталған желі

2.10-суретінде Хемминг желісі немесе ішкі желі деп аталатын бірінші қабат нейрондық желідегі синаптикалық салмақ мәнінің өзгерту жолымен жадыға енгізілген вектор мен кіріс вектор араларындағы Хемминг арақашықтығын есептейді. Ішкі желі немесе түрлендіру желісі басымрақ

амплитудаға ие шығыс сигналды яғни шығыс векторы мен вектор үлгісінің арасындағы Хеммингтің арақашықтығы ең кішісі болып табылатын нейронның бірінші қабатынан нейронды таңдау қызметін атқарады. Мұндай текті нейрон нейрон жеңімпаз деп те аталады.

Синаптикалық салмақтар мен қарастырылып отырған желі орын ауыстыруын баптау Хемминг арақашықтығын есептеу жолымен жүзеге асып, келесі (2.8) формуласының көмегімен анықталады.

$$w_{i,j} = -x_i^j, b_j = -N, 1 \le i \le N, 1 \le j \le M. \quad (2.8)$$

Бірақ әдебиеттерде орын ауыстыру мен синаптикалық салмақтарды (2.9) формуласымен есептеу әдісі кездеседі:

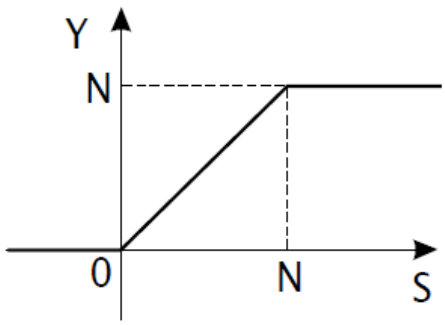
$$w_{i,j} = \frac{x_i^j}{2}, b_j = \frac{N}{2}, 1 \le i \le N, 1 \le j \le M, \quad (2.9)$$

мұндағы b – орын ауыстыру,

N – кіріс сигналының өлшемі,

M – желідегі нейрондар саны.

Хемминг желісінің өзгеріс функциясынының көрінісі келесі 2.11-суретінде көрсетілген. Суретте көрсетілгендей ол сызықтық функция түрінде берілген.



Сурет 2.11 – Хемминг желісі өзгерісі функциясының көрінісі

Хемминг желісі қызметін көрсететін функция (2.10) формуласында көрсетілген:

$$y_i = \left(\sum_{i=1}^{N} w_{i,j} x_i - b_j\right), 1 \le j \le M. \quad (2.10)$$

мұндағы y_j – желінің j-ші нейронының шығысы.

Хемминг желісі тек аздап шуланған кіріс сигналдарын ғана тану алады. Бұл кескінді тану есептерінде оның қолданысын шектеуі мүмкін.

Бірақ шуланған кескіндерді тануда бұл желіні қолдану және желінің кіріс және шығыс сигналдарының сәйкес келмеу мүмкіндігінің өзі оны кескінді тану

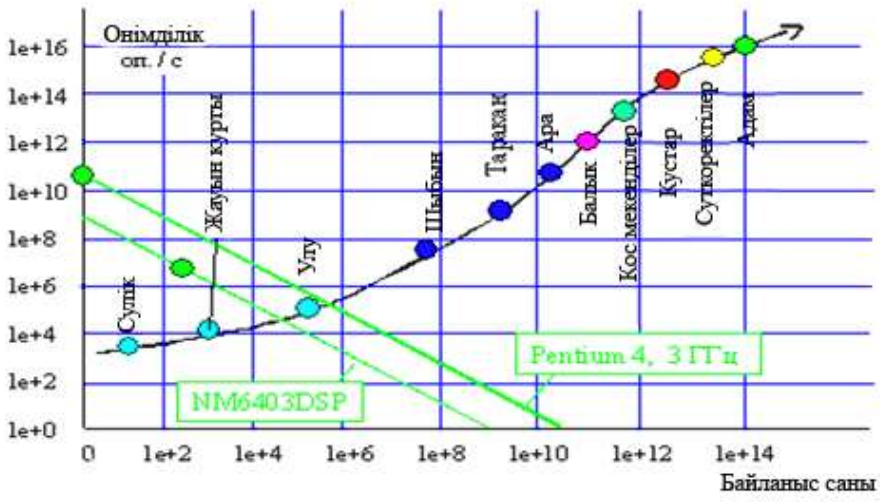
есептерінде Хопфилд желісіне қарағанда тиімдірек етеді. Сонымен қатар, шығыс сигнал нейрондардың бір қабаты ғана өтуінің нәтижесінен қалыптасатындығынан желі жылдамдығының жоғарылығын айта кетуге болады. Желіні үйрету Хемминг арақашықтығын есептеуге негізделген өте қарапайым алгоритм негізінде жүзеге асады. Бұл желіні үйрету жылдамдығының жоғары екендігін айқындайды. Хопфилд желісінен ерекшелігі Хемминг желісінің сиымдылығы кіріс сигналдарының өлшемінен тәуелсіз екендігінде, ол (M) нейрондар санына тең.

2.1.5 Үлкен және шамадан тыс үлкен нейрондық желілер

Нейрожелілік технологиялар тек нейрондық желі айтарлықтай үлкен және саннан сапаға өтуде ғана елеулі артықшылыққа ие болуы мүмкін. Басым көпшілік заманауи нейрожелілік қосымшалар олардың жасанды нейрондық желілерін ұйымдастырудың күрделілігінің жеткілікті дәрежеде жоғары еместігінен сенімсіз болып көрінеді [76].

Егер адамды эволюцияның шыңы деп қарастыратын болсақ, онда күрделі жүйе ретінде өзара 10^{14} дейін байланысты құрайтын 10^{11} нейрондардан тұратын адам миын қабылдау қажет. Әрбір табиғи нейрон өз көршілес нейрондарымен 1000 дейінгі байланысты құрайды. Бұл қазіргі кезде жасанды нейрондар үшін қол жеткізбейтін көрсеткіш. Релаксация уақыты есебінен нейрондардың нақты реакциясы 5мс-ті құрайды, ал біздің процессор жұмысының тактілік жиілігі 200 Гц-тен аспайды, бірақ оның жалпы өнімділігінің жоғары параллелдігінен біздің ми секундына $2 \cdot 10^{16}$ амалдан тұрады. Әрине, біздің мидың кремнийлік нұсқасы оған қарағанда анағұрлым төмен.

2.12-суретінде әртүрлі тірі организмдердің ұйымдастырылуының салыстырмалы күрделілігінің ауытқымасы және заманауи дербес компьютер мен ресей өндіретін нейрондық желілерді есептеуге арналған NM6403 сигналдық процессорының мүмкіндіктері көрсетілген [32, с. 21-22].



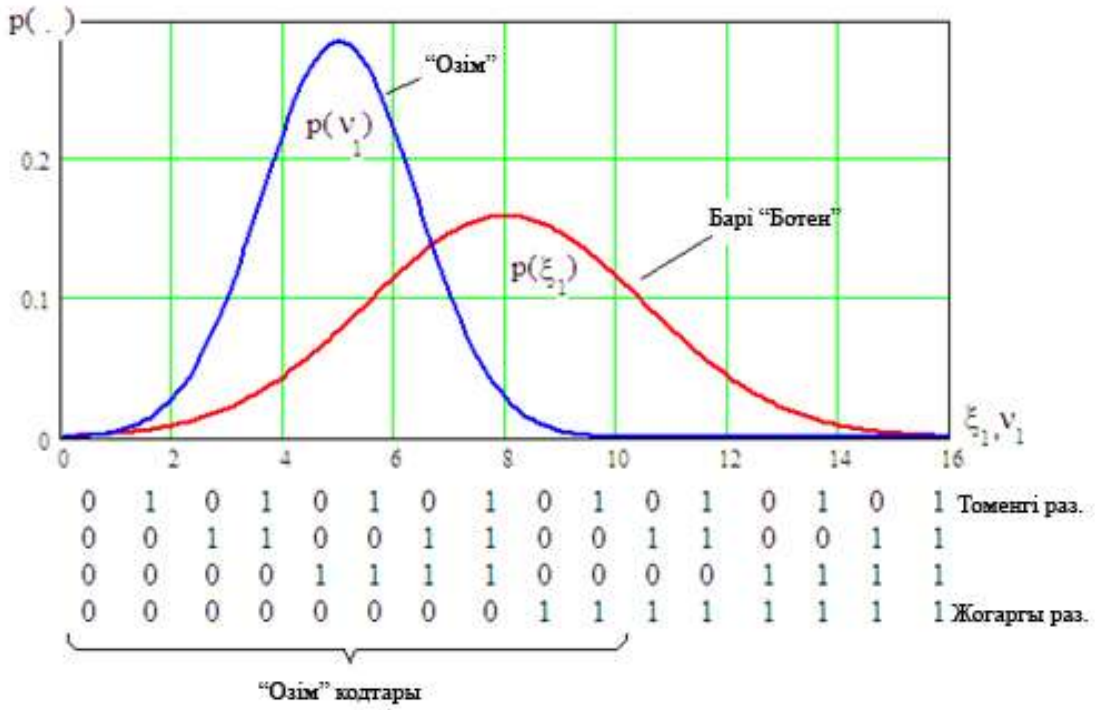
Сурет 2.12 – Табиғи және жасанды эволюция өкілдерінің зерде күрделілігі мен өнімділігінің ара қатынасы

Бұл процессорлардың мүмкіндігін түзу түрінде көрсетуге тура келеді, себебі есепті параллелдеу дәрежесі бағдарламадан – нейрожеліні жаңғыртатын эмулятордан тәуелді. Бұл түзу бойындағы қара дөңгелектермен осы процессордың бір тактілік есептеуге сәйкес келетін күйлері белгіленген. Қарапайым процессор такт аралығында ММХ бір амалын, ал NM6403 векторлық нейропроцессор 288 саннан тұратын вектормен немесе 288 ММХ жинақтайтын көбейту амалдарын орындауы мүмкін.

Суреттен өз механизмдерімізді нақты уақытта жобалай отырып, біз олардың мүмкіндігінің тірі шыбын немесе тарақаннан да төмен екендігін байқау қиын емес. Біздің нақты мүмкіндігіміз – бұл біз күрделі басқару нейрожелісін құруға тырысқанымызда, ұлу нейрожүйесінің мүмкіндігі мен шешім қабылдау жылдамдығына ие екенін түсінеміз.

2.2. Жеке биометриялық деректерді қол жеткізу кодына түрлендіру

Шығыс кодтарына үздіксіз биометриялық мәліметтерді (параметрлерді) түрлендіру үшін формальды түрде кәдімгі аналогты-сандық түрлендіргіштерді (АСҚ) қолдануға және солардың көмегімен көптеген үздіксіз биометриялық шамаларды сәйкес келетін дискреттік кодқа түрлендіруді іске асыруға болады. Осыған ұқсас мысал «Өзім» биометриялық бейнесінің ν_1 үздіксіз параметрін және бәрі «Бөтендер» ξ_1 биометриялық бейнелерінің аналогты параметрін 4-разрядты бинарлық кодқа түрлендіру 2.13-суретінде келтірілген.



Сурет 2.13 – «Өзім» биометриялық бейнесінің ν_1 үздіксіз параметрін және бәрі «Бөтен» биометриялық бейнесінің ξ_1 аналогты параметрін сандық кодқа түрлендіру

Әлбетте, АСҚ-ның динамикалық диапазоны бәрі «Бөтендер» бейнелерінің кіріс динамикалық диапазонымен сәйкес келуі үшін, аналогты-сандық түрлендірудің алдында барлық түрленген биометриялық параметрлерді ауқымдап және орталықтандыру қажет. Мұндай жағдайда АСҚ-ның әрбір кіріс коды кірістік үздіксіз биометриялық параметрдің кейбір жағдайына сәйкес келеді. Осыған орай кіріс кодтарының бөлігі «Өзім» биометриялық бейнесіне сәйкес келеді.

Алғашқы жақындатуда «Өзім» бейнесінің биометриялық параметрлерінің $p(\nu_i)$ кіріс мәліметтері мәнін бөлудегі тығыздықты дұрыс деп санауға болады. Сондай-ақ «Бөтен» биометриялық бейнесінің параметрлері $p(\xi_i)$ мағынасын бөлудегі тығыздықты да дұрыс деп санауға болады. «Өзім» бейнесінің биометриялық параметрлері тұрақты болып саналады, егер де олардың өзгерісіндегі динамикалық диапазон бәрі «Бөтен» бейнесіндегі динамикалық диапазоннан 30%-ға аз болса. Орташа тұрақтылықтағы биометриялық параметрлер мүмкін болатын бәрі «Бөтен» динамикалық диапазонынан 30%-дан 60%-ға дейін динамикалық диапазонды иеленеді. Тұрақты емес биометриялық параметрлер мүмкін болатын бәрі «Бөтен» бейнесінің динамикалық диапазонынан 60%-дан 90%-ға дейінгі аралықты құрайтын динамикалық диапазонға ие.

МЕСТ Р 52633.1-2009 [77] биометриялық параметрлердің тұрақтылық көрсеткішін бәрі «Бөтен» және «Өзім» бейнелері параметрлері мәнінің орташа квадраттық ауытқуына қатынасы ретінде анықтайды:

$$s_i = \frac{\sigma(\xi_i)}{\sigma(\nu_i)} \tag{2.11}$$

мұндағы $\sigma(\xi_i)$ – биометрия-код түрлендіргішінің і-ші кірісіндегі бәрі «Бөтен» бейнелерінің і-ші биометриялық параметрінің орташа квадраттық ауытқуы;

$\sigma(\nu_i)$ – биометрия-код түрлендіргішінің і-ші кірісіндегі «Өзім» бейнелерінің і-ші биометриялық параметрінің орташа квадраттық ауытқуы.

Бұдан басқа, қосымша МЕСТ Р 52633.1-2009 биометриялық параметрлердің қайталанбайтындығының көрсеткішін келесі формула арқылы анықтайды:

$$u_i = \frac{\left|E(\xi_i) - E(\nu_i)\right|}{\sigma(\xi_i)} \tag{2.12}$$

мұндағы $E(\xi_i)$ – биометрия-код түрлендіргішінің і-ші кірісіндегі бәрі «Бөтен» бейнелерінің і-ші биометриялық параметрінің математикалық болжамы;

$E(\nu_i)$ – биометрия-код түрлендіргішінің і-ші кірісіндегі «Өзім» бейнелерінің і-ші биометриялық параметрінің математикалық болжамы.

Сол немесе басқа биометриялық параметрдің бөлу орталығы $p(\nu_i)$ ортастатистикалық бөлу $p(\xi_i)$ деп аталатын орталықтан қаншалықты айырмашылықта екенін қайталанбайтын u_i көрсеткіші сандық түрде бағалауға мүмкіндік береді. Биометриялық бейнелерге арналған қайталанбайтын көрсеткіші әдетте 0-ден 4-ке дейінгі интервалда өзімгереді. Ережеге сай қайталанбайтын параметрлер аз, мәселен, «Өзім» бейнесінің орта статистикасы үшін 1-еуден артық қайталанбайтын көрсеткіштің параметрлері 25%-дан кем екен.

«Өзім» бейнесінің биометриялық параметрлерінің орташа тұрақтылығы $E(s_i)$ неғұрлым жоғары және орташа қайталанбауы $E(u_i)$ неғұрлым жоғары болса, «Өзім» биометриялық бейнесін бір мағыналы шығыс кодқа түрлендіру мәселесін шешу соғұрлым жеңіл болады.

Бұдан басқа, өткен ғасырда кең қолданыста болған белгілеу [45; 53; 78] мен барынша ақпараттық параметрлерді қолдану тәжірибесі жоғары сенімділікті биометрия үшін мынадай себептерге байланысты қолайсыз екенін есте сақтаған жөн. Біріншіден, тек қана барынша ақпаратты параметрлерді қолдану «Өзім» биометриялық бейнесін айтарлықтай қаралайды, өйткені әрбір қайталанбайтын биометриялық бейненің барынша ақпаратты параметрлері өздік қайталанбайтын орналасуларға ие. Екіншіден, тек қана барынша ақпаратты параметрлерді қолдану ақырғы шешімнің сапасын айтарлықтай төмендетеді.

Тәжірибе көрсеткендей, тек қана 16 ақпараттық параметрлерді қолдану «Пенза» қолжазба сөзін жаңғырту динамикасында сәйкестендіру кезінде 10^{-3} деңгейіндегі екінші тектес («Бөтен» қателігін жіберу мүмкіндігі) қателік мүмкіндігін береді. Егер де біз тек қана айтарлықтай ақпаратты параметрлердің тәжірибесін қолданудан бас тартсақ және есептелген параметрлерді 416-ға дейін ұлғайтсақ, онда екінші тектес қателіктер мүмкіндігі 10^{-12}-ге дейінгі көлемге төмендейді. Шешілетін мәселелердің көлемін 16 талданатын параметрлерден 416 биометриялық параметрлерге дейін ұлғайту кезінде қателік жіберу мүмкіндігі миллиард есеге дейін төмендеу байқалады.

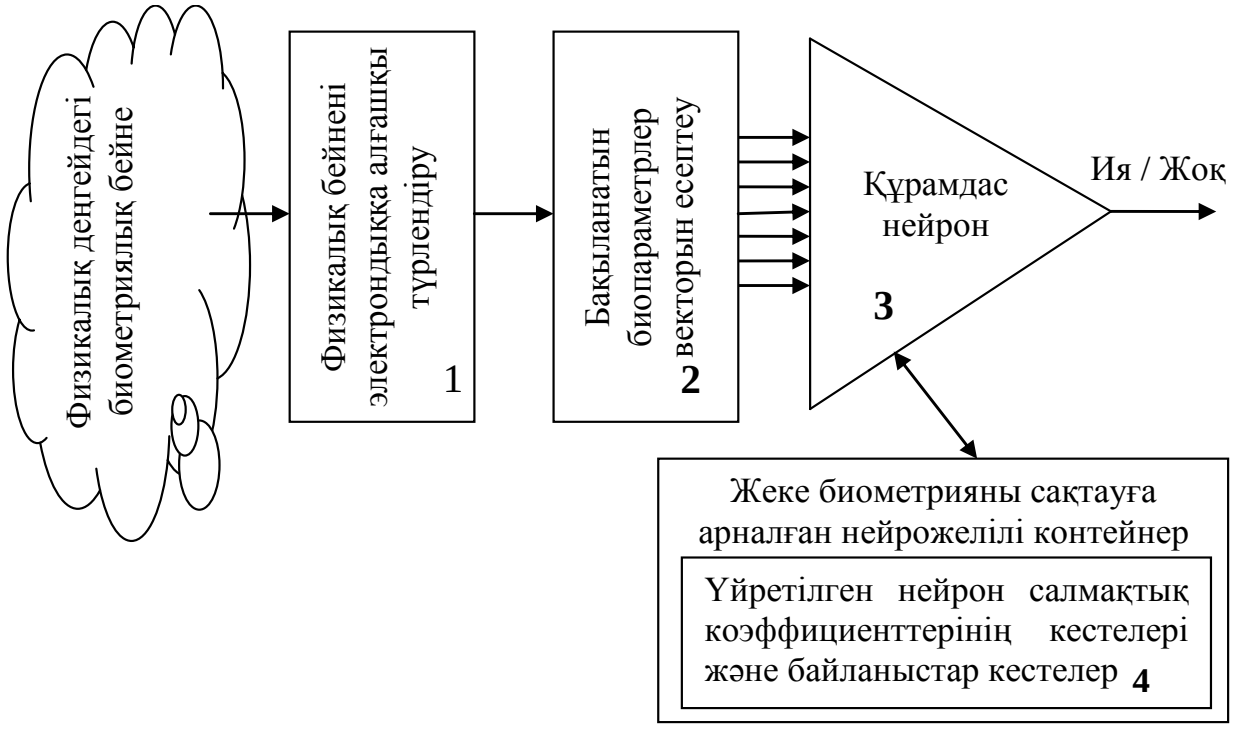
«Пенза» қолжазба сөзіндегі 16 ақпараттық параметрлердегі ақпарат шамамен 10 бит ($P_2 \approx 10^{-3} \approx 2^{-10}$). «Пенза» қолжазба сөзіндегі 416 ақпараттық параметрлердегі ақпарат шамамен 40 бит ($P_2 \approx 10^{-12} \approx 2^{-40}$). Яғни, 400 нашар ақпараттық қатынастағы параметрлерге 30 бит ақпарат сияды. Ақпараттың үлкен бөлігі (3/4) дәл осы аталған нашар мәліметтерде болады. Жақсы мәліметтерде биометриялық бейненің аз бөлікті (1/4) ақпараты сақталады.

Биометрия-кодтың тиімді түрлендіргіші биометриялық параметрлердің қарапайым сандауымен құрылуы, сондай-ақ биометриялық бейнелерді классикалық процедураларда танып білуде мүмкін емес [45; 53; 78-80]. Мәліметтерді қарапайым сандауда [33] «Өзім» бейнесінің шығыстық кодтары өте тұрақсыз болады және классикалық әдіспен қателерін табу мен оларды жөндеу мүмкін болмайды [81-84]. Мәліметтерді алдын-ала өңдеуге әрекет жасау кезінде жасанды зерделіктің классикалық процедураларында

айтарлықтай ақпаратты жоғалтулар болады және ақпараттың басым бөлігі шығарылып тасталынады.

2.3 Нейрондық желілердің негізінде биометрия-кодты түрлендірудің қағидалары

Дербес биометриялық ақпараттарды қорғау бағыттарының бірі – жасанды нейрондық желілерді қолдану болып табылады [14; 16, p. 135-138; 18, c. 188-190; 31-34; 41; 47; 61; 63-65]. Нейрондық желілердің ерекшеліктері шығыстық кодқа үздіксіз биометриялық мәліметтерді түрлендіруге қабілетті болып табылады. Жекелеп алғанда, бұл үшін «Өзім» немесе «Бөтен» шешім қабылдайтын бір ғана нейрон қолданылуы мүмкін. 2.14 суретінде бір шығар жолы бар биометрия-кодтың төмендік нейрожелілік түрлендіргіштің блок-сұлбасы ұсынылған [85].



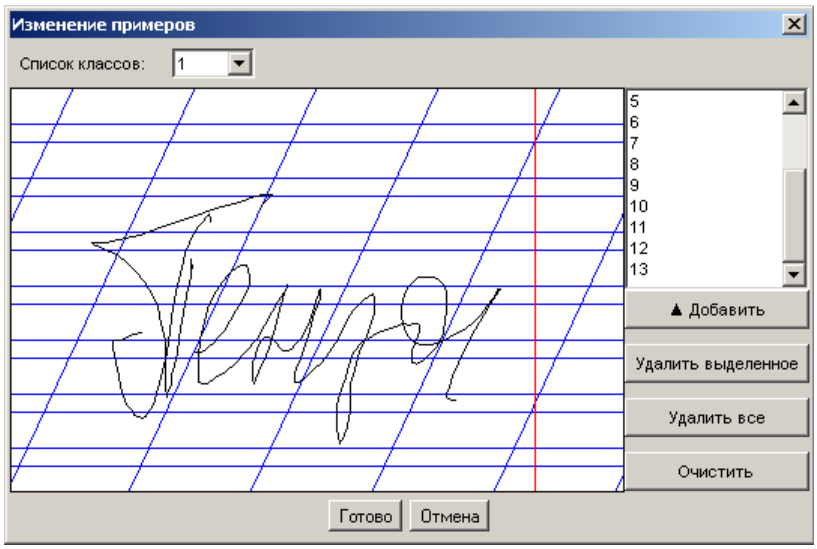
Сурет 2.14 – Биометрия-кодтың төмендік нейрожелілік түрлендіргіші бірегей құрамдас нейронмен бірге

Биометриялық автомат бірегей шығыс нейронмен табыс табу үшін оны үйрету қажет. Автоматтың бірегей нейронын оқыту үшін бүгінгі таңда үйретудің жүздеген белгілі түрлерінің бірі қолданылуы мүмкін [31; 32; 64; 77; 86-90]. Бір нейронды үйрету аса қиындық туғызбайды.

Егерде үйретудің шығыстық мәліметтері ретінде қолжазбалық динамикалардың биомтериялық параметрлерін қолданса, онда үйретілетін үзінділерді «Өзім» мысалдарынан және «Бөтен» мысалдарының бірнешеуінен құрастыруға болады. Үйретудің үдерісін мысалмен сипаттау үшін

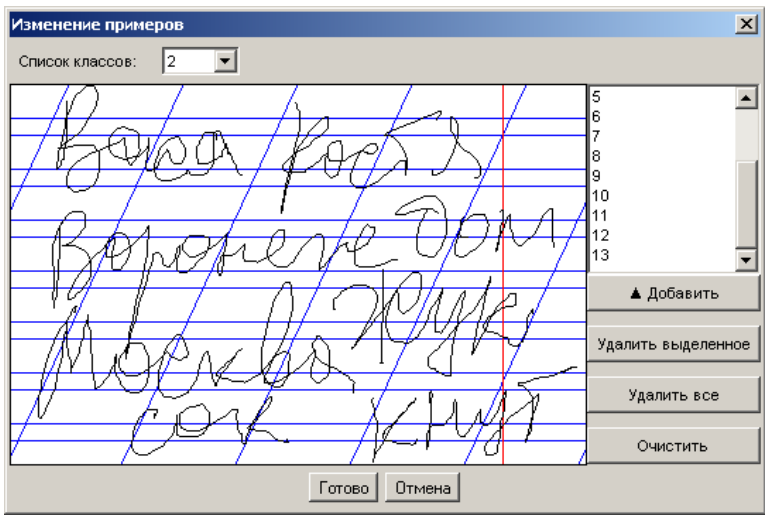
модельдеудің ақпараттық ортасы «НейроОқытушы» қолданылуы мүмкін [32, с. 208-210].

«Өзім» бейнесінің мысалы ретінде бір адаммен ғана жасалынған «Пенза» сөзінің 13 қолжазбалық бейнесін қолданамыз (сурет 2.15).



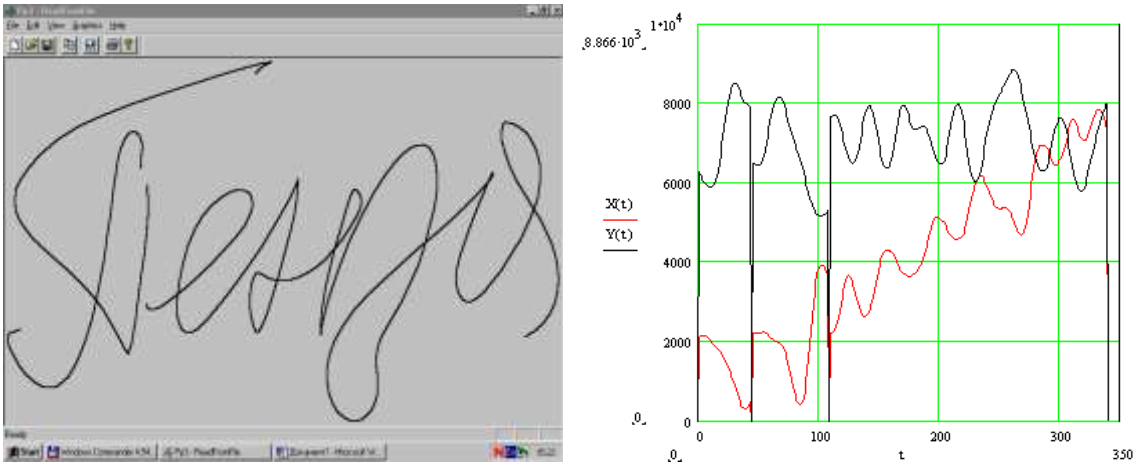
Сурет 2.15 – «Нейро Оқытушы» модельдеу ортасында «Өзім» қолжазбалық паролін енгізудің экрандық үлгісі

«Бөтендер» бейнесі ретінде әртүрлі адамдардың қолжазбасымен берілген «Вася», «Костя», «Воронеж» (сурет 2.16), сөздері қолданылды [47, с. 49-50]. Яғни, нейронды үйрету кезінде оның салмақтық коэффициенттерін «Бөтендердің» көптеген бейнелері мен «Өзім» бейнесінің көптеген мысалдарының барынша күшті болуына көңіл бөліп таңдау керек. Ережеге сай, нейрон ретінде сумматорды шығыс жолындағы кейбір сызықсыз элементпен қарастырады.



Сурет 2.16 - «Нейро Оқытушы» модельдеу ортасында «Бөтендер» қолжазбалық мысалдарын енгізудің экрандық үлгісі

Талданатын параметрлер ретінде «НейроОқытушы» модельдеу ортасы талданатын сөздердің қолжазбасынан алынатын Фурьенің коэффициенттерін қолданады. 2.17-суретте осыған ұқсас тербелістер келтірілген [47, с. 50].



Сурет 2.17 – «Пенза» және «Пароль» құпиясөздерінің қолжазбалық жаңғырту кезіндегі қаламның сәйкес ось бойынша *X(t)* және *Y(t)* бойынша тербелісі

Тәжірибе көрсеткендей, 4,5,6-дан тұратын қолжазба сөздер үшін Фурьенің (k=1,2,3,…., 24) 24 косинустық және синустық коэффициенттер қатарын есепке алса жетіп жатыр. Сонда екі координатты есепке алу, 96 биометриялық параметрлерден вектор алуға мүмкіндік береді (2.13-2.16):

$$\nu_k = \frac{1}{T}\int_0^T Y(t)\cdot\cos(k\frac{2\pi}{T}t)dt, \quad (2.13); \qquad \nu_{2k} = \frac{1}{T}\int_0^T Y(t)\cdot\sin(k\frac{2\pi}{T}t)dt \quad (2.14);$$

$$\nu_{3k} = \frac{1}{T}\int_0^T X(t)\cdot\cos(k\frac{2\pi}{T}t)dt, \quad (2.15); \qquad \nu_{4k} = \frac{1}{T}\int_0^T X(t)\cdot\sin(k\frac{2\pi}{T}t)dt \quad (2.16);$$

мұндағы T – қолын енгізудің толық уақыты (қолжазбалық құпия сөз).

Нәтижесінде бізге нейронды үйрету кезінде оның салмақтық коэффициенттерін - μ_i сумматордың барлық кірістерін итерациялық таңдаған жөн. Егер «Өзім» бейнесіне сумматордың шығыстық үні арқылы $z(\overline{\nu})$ белгілесек, онда біз мынадай жазба аламыз:

$$z(\overline{\nu}) = \mu_0 + \sum_{i=1}^{96}\mu_i\nu_i. \qquad (2.17)$$

Бізге ең қажеті, «Пенза» қолжазбалық сөзінің барлық мысалдары «1» нейронына шығуда үн қатса, онда бірегей сызықсыз элементті икемдеу төмендегідей ережемен іске асуы тиіс:

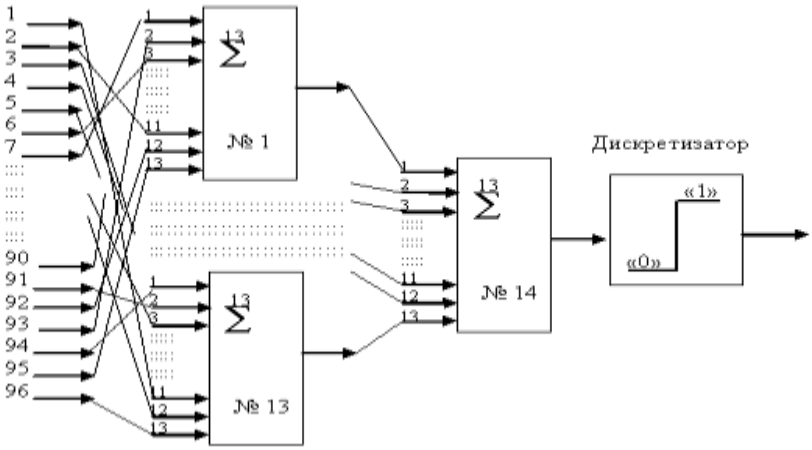
$$\begin{cases} y(\xi_i) = "0" \text{ егер } \xi_i < \min(z(\bar{v}_i)); \\ y(\xi_i) = "1" \text{ егер } \xi_i \geq \min(z(\bar{v}_i)). \end{cases} \quad (2.18)$$

Өкінішке орай, нейронның 97 салмақтық коэффициентін икемдеу «Өзім» және «Бөтен» бейнелерінің 13 мысалын қолданудағы үйрету іріктемесінде, автоматты түрде іске асыру үнемі бола бермейді. Егерде үйретілетін нейронда кіріс саны үйрету іріктемесіндегі мысалға жақын болса, қарапайым алгоритм үшін автоматты үйретуде мәселе туындамайды.

Біздің жағдайымызда мысалдар саны тұрақты үйрету үшін жеткіліксіз. Осыған байланысты нейронның сумматорын құрамдас етіп жасау қажет, бұл 2.18-суретінде көрсетілген [47, с. 52].

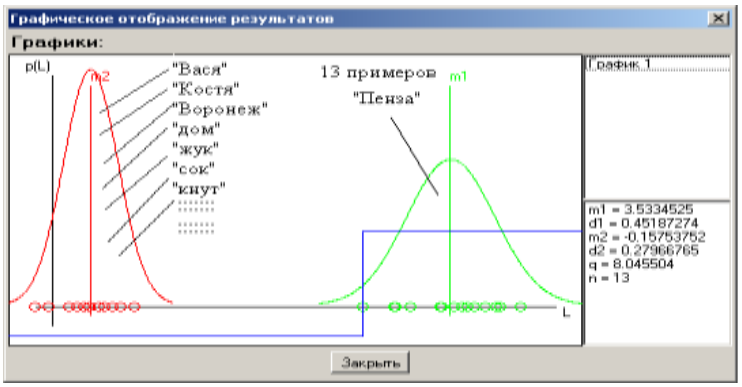
Әрбірін үйрету үшін құрамдас нейронның 14 сумматорынан оқушыға 13 мысалдан үзінділер жеткілікті болады, әрбір сумматор 13 кіріске ие (кіріс саны мысал санынан аспайды). Құрамдас сумматорды ұйымдастыруда бірінші қабаттың әрбір сумматорынан нейрон кірісіне кездейсоқ қосу ұсынылады. Әлбетте, барлық кірістерді қолдану дәйектерін қадағалау қажет.

Алғашқы қабаттың әрбір сумматорлары «Өзім» және «Бөтендер» бейнелерінің мысалдарында өзбетінше оқытылады. Алғашқы қабаттың сумматорлары үйретілгеннен кейін, олардың кірістеріндегі мысалдар мәліметтері сумматорлар шығысында таратылады және ары қарай екінші қабаттың бірегей сумматорын үйретуде қолданылады. Сызықсыз элементтер алғашқы қабат сумматорларының шығысында болмайды, сол себепті де барлық сумматорлар кірістің үлкен санымен бір сумматор ретінде қарастырылады. 14 барынша қарапайым мәселе астылықта үйретудің толық мәселесін декомпозициялау автоматты үйрету тәртібі үшін ғана қажет. Нейронды қолмен үйрету тәртібінде (мұндай тәртіп «Нейро Оқытушы» модельдеу ортасында) ойдағыдай нәтижеге қол жеткізуге болады.



Сурет 2.18 – Құрамдас сумматорлармен жасанды нейрон

«Нейро Оқытушы» ортасында құрамдас нейронның соңғы сумматорын автоматты түрде үйретудің нәтижелері 2.19 суретінде бейнеленген [47, с. 53].



Сурет 2.19 - «Нейро Оқытушы» модельдеу ортасында нейронды үйретудің нәтижелерін енгізудің экрандық формасы

Сол оң дәлелдің, үйретілген нейрон параметрлері жөніндегі ақпараттарды пайдалануда, биометриялық үлгідегі ақпаратқа қарағанда, анағұрлым қиынырақ екенін есте ұстаған жөн. Биометриялық үлгілерді қалыптастыру шарттары биометриялық параметрлердің бақыланатын ережелеріне тура көрсетеді.

Салмақтық коэффициентермен және нейронның үйретілген құрамдас байланыстарымен іс мүлде басқаша болады. «Өзім» биометриялық параметрлерінің пайда болуын күтуді олар арқылы нақты көрсетуге болмайды. Құрамдас нейрон байланысының кесте үлгісі мен үйретілген құрамдас нейронның салмақтық коэффициенттері 2.20-суретте келтірілген [47, с. 53].

Биометрияны қауіпсіз (ашық немесе жасырын немесе тұлғасыздандырылған) сақтау үшін арналған нейрожелілік контейнер	
Құрамдас нейрон сумматорларының кіріс және шығыс байланыстарының кестесі	Нейронның үйретілген сумматорлары салмақтық коэффициенттерінің кестесі
70 19 18 46 10 13 94 90 23 42 64 46 60 86 63 57 19 56 25 61 59 50 75 63 81 58 92 73 67 32 31 11 86 16 08 65 55 41 47 16 74 83 88 34 13 79 61 48 36 11 23 92 67 50 15 51 69 61 01 11 87 75 39 56 96 :::::::::::::::::::::::::::::::::::::: ::	+94-05-84-40+95-54+70-26-53-40+59-69+44 -01-61-58+23-31-09-86+82+70+54+15-73-14 +65-09-95-28+99-30-37-22+25-91+71+29+18 -78-22-01+12 +32+04-19+16+89-20 -65-91-93 -16+57+95-58-26-36-80-08+60+20 -65-61+45 :::::::::::::::::::::::::::::::::::::: ::

Сурет 2.20 – Үйретілген құрамдас нейронның биометриялық параметрлері орналастырылған нейрожелілік контейнердің үлгісі

Биометриялық контейнерде орналастырылған ақпарат, суретте көрсетілгендей шифрлі мәтінге өте ұқсас. Оны жай ғана биометриялық үлгінің ақпараты ретінде түсіндіруге болмайды. Бұл қатынаста жасанды нейрондық желілерді пайдалануды қолданушының дербес биометриялық ақпаратты жасыру әдістерінің бірі ретінде қарастырған жөн.

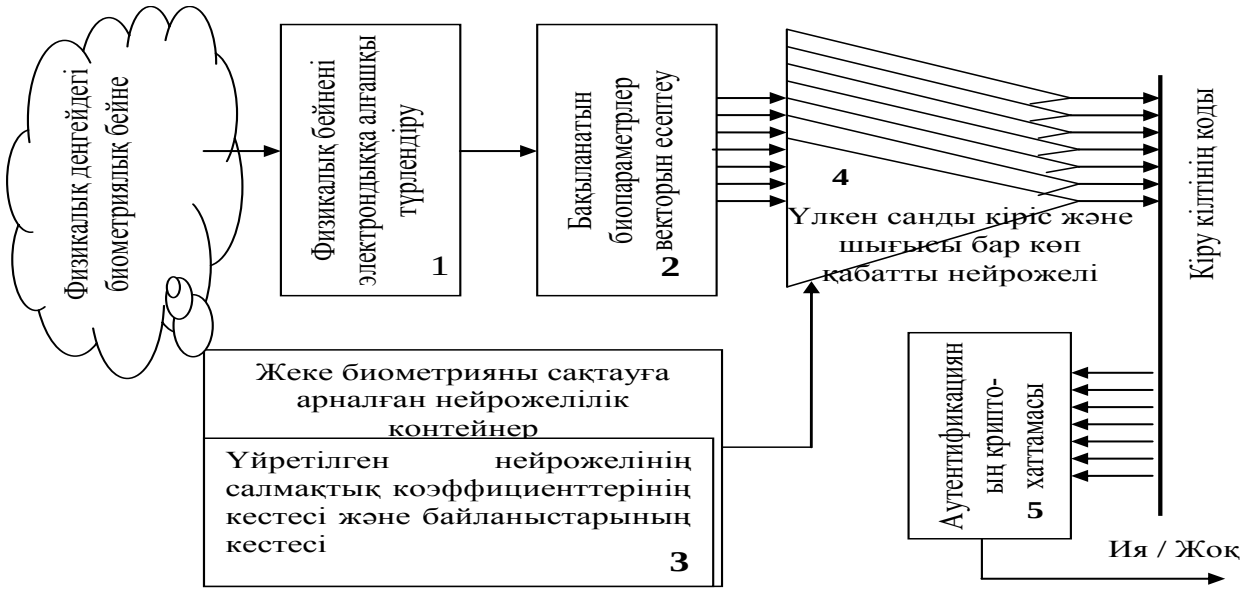
2.4 Үлкен нейрондық желілерді пайдаланатын биометриялық технологиялар

Қарапайым биометрияның негізгі проблемасы «Жыртқыштың баспалары» қаупі болып табылады [14, с. 183-184]. Өкінішке орай, Сіздің саусағыңыздың ізі немесе көзім жанарыңыздың қарашығының биометриялық үлгісі тек қана Сіздің биометриялық мәліметтеріңіздің картасына ғана түсіп қоймай, сәйкес келетін орталықтандырылған мәліметтер базасына түседі. Бұл корпоративтік биометриялық базалар мәліметі болуы мүмкін, онда сол корпорацияда жұмыс істейтін адамдар жөніндегі құпия биометриялық ақпараттар шамамен 1000 есе жиналуы мүмкін. Құпия биометриялық ақпараттардың үлкен көлемі мемлекеттік биометриялық мәліметтер қорында жинақталуы мүмкін. Адамдардан олардың биометрияларын жинап және оларды үлкен мәліметтер қорында орналастыру айтарлықтай қауіпті.

Биометриялық үлгілердің атына кір келтірушілік қаупін болдырмау үшін жаңа биометриялық технологиялар құру қажет, яғни ол бір жағынан, адамды оның биометриясымен сенімді сәйкестендіруге мүмкіндік береді, екінші жағынан, адамның биометриясын қадағалау мен түсіну үшін қол жетімсіз етеді. Жеке құпиялылық пен биометриялық мәліметтердің жасырынды болуын қамтамасыз етудің мәселелерін шешудің бір жолы үлкен және өте үлкен көлемдегі нейрондық желілерді қолдану болып табылады [32-34].

Нейрожелілі шешімнің оң сәті ертеректе анық түрде сақталынған биометриялық үлгінің жоғалып кетуі болып табылады. Оның орнына пайдаланушының биометриялық мәліметтерінің нейрожелілік контейнері пайда болады. Бұл кесте нейрожелілер нейрондарының байланысы (салмақтық коэффициенттері) мен синоптикалық байланыстар кестесі «Өзімнің» нейрондық желісін үйретілгенін айырып тану (сурет 2.21). 3 суреттің блок-сұлбасы бойынша орындалған тәсілдер жоғары сенімді болып табылады, себебі нейрожелілі түрлендіргіш биометрия-кодты қолдануға құрылған (блок-3 пен блок-4) [47, с. 55].

4 сурет блок-сұлбасын қолданудағы биометрияның құпиясы үйретілген нейрондық желілердің кестесі бойынша және салмақтық коэффициенттің кестесі бойынша донордың биометриясын (биометриялық бейне базасы бойынша адамды табу) табу техникалық тұрғыдан қиын екендігімен қамтамасыз етіледі. Нейрожелілі контейнерде орналастырылған биометрияның құпиялылығы таңбаланумен, құпиялылығымен салыстырылмалы деңгейінде қамтамасыз етіледі.



Сурет 2.21– Жоғары сенімділікті биометриялық сәйкестендіру тәсілдерін ұйымдастырудың типтік блок-сұлбасы

МЕСТ Р 52633.0 бойынша нейрожелілі түрлендіргіш биометрия-код қолданушының жеке кілтіне «Өзім» құпия биометриялық бейнесінің түрлендіруін алдын-ала үйретуі тиіс екендігі негізгі сәті болып табылады. «Бөтеннің» кез-келген басқа биометриялық бейнесі нейрожелілі түрлендіргіш биометрия-код кездейсоқ кілтке түрлендірілуі тиіс. Егер «Өзім» биометриялық бейнесі мен жеке кілт тараптағы қадағалаушыға белгісіз болса, онда қаскүнем 1 000 000 000 әрекеттен (шабуылға тұрақтылықты таңдау 10^9) кейін ғана таба алуы мүмкін. Қаскүнемнің кілтті іздеуіне 3×10^9 секунд немесе шамамен 300 жыл кетуі тиіс, егер қаскүнемге уақыттың үшсекундты интервалының кездейсоқ биометриялық бейнелерінің бірін ұсынуға рұқсат етілсе.

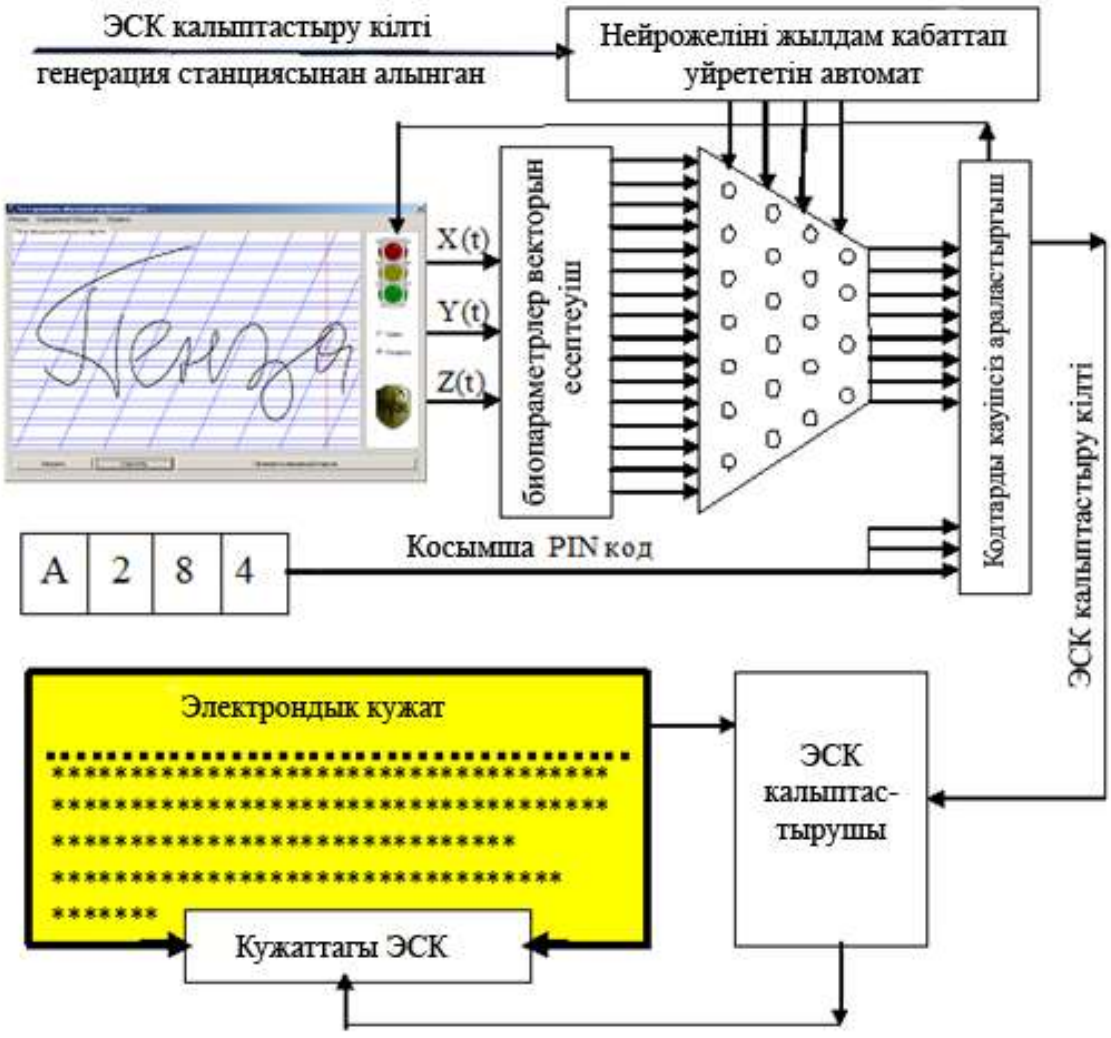
Егер адамның биометриялық бейнесінің беделі түссе, онда оның таңдауға шабуылдаудағы қалған төзімділігі әрекеттің 10^3 көлеміне дейін төмендейді (таңдау уақыты 1 сағатқа қысқарады). Биометрия құпиясын қамтамасыз ету биометрияға қарағанда айтарлықтай тиімді.

Кілттің ұзындығы 256 бит – бұл өте-мөте сенімді қорғау екенін есте ұстаған жөн, мәселен, ресейдің ұлттық стандарты бойынша және алгоритммен сәйкес келетін азаматтың электронды сандық қолдарын құру үшін [91]. Егерде ағылшындар ресейліктерден олардың саусақ іздерінің анық түрін емес, ресей саусақтары іздерінің нейрожелілі контейнерлерін жинаса, онда оларға ешқандай талап қойылмас еді. Мұндай контейнер болса, онды оның алдында иесінің өзімі отырғанына сенімді болуыға болады. Сонымен бірге саусақ іздері еш жерде сақталынбайды және еш жерде көрінбейді. Саусақ іздерінің суреттері нейрондық желілердің байланыс параметрлерінде «еріп кететін көрінеді». Адамды аяғынан шалу және оның саусақ іздерін ашық түрде қол жетімді етуді ешкім жасай алмайды, яғни адамның құқы шын мәнінде сақталынады.

ЭСҚ-ны пайдаланушы кілтті жоғары сенімділікті биометрика-нейрожелілі сақтауды қолдану флеш-тасушыларға және ЭСҚ қалыптастырушы ұлттық

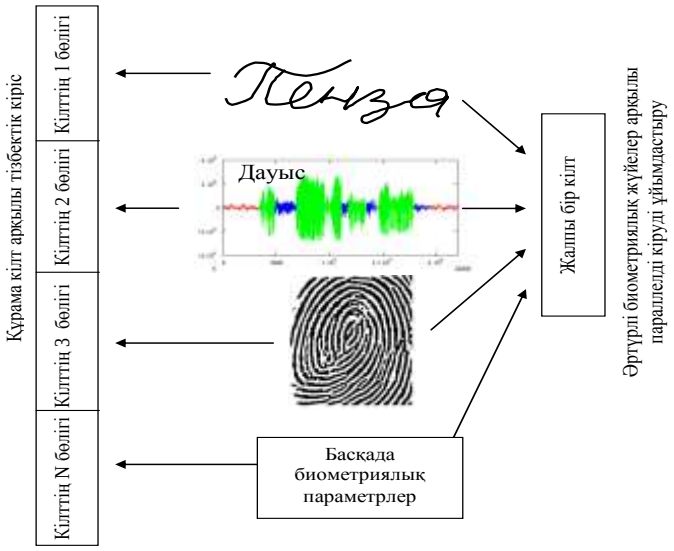
биометриялық куәләндыратын орталықтарда енгізу ұсынылады. Ұлттық БКО жеке тұлғалар мен заңды тұлғаларды ашық кілттерді сертификациялау бойынша дәстүрлі қызмет көрсетуді ғана ұсынып қоймай, сонымен қатар адамдардың локальды және қашықтық биометриялық сәйкестендіру жөніндегі басқа да қызметтерін атқарады.

Адамдарға тек бір рет қана куәландыру орталығына келіп өзінің биометриялық тіркеуін жасатса болғаны, ары қарай тұлға қауіпсіз делдалдың – жаңа ұрпақтың биометриялық куәландыру орталығы қызметін пайдалана отырып, өзінің биометриялық сәйкестігін электронды үкіметке, электронды бизнеске, басқа азаматтарға дәлелдей алады (сурет 2.22).



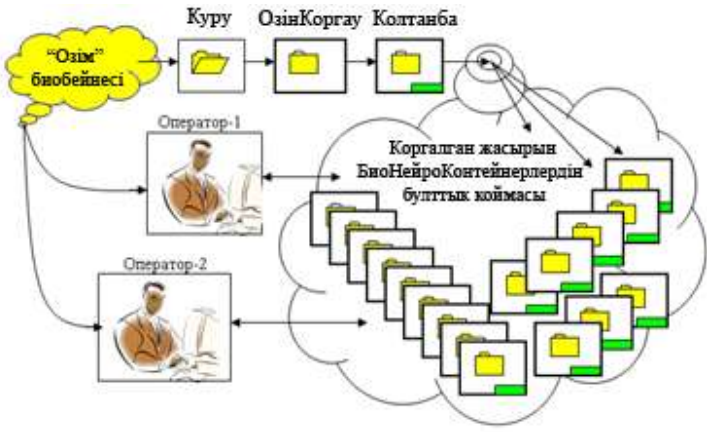
Сурет 2.22 – Жоғары сенімді биометриялық авторизациялаумен ЭСҚ-ны құрастырушының құрылымы

Биометриялық сәйкестендіру тәсілдерінің тұрақтылығын күшейту бірнеше биометриялық технологияларды қолданудың есебінен болуы мүмкін, сонымен бірге кілттің әрбір бөлігі әр биометриялық параметрден қалыптасқан жеке көріністерден құралады (сурет 2.23) [32, с. 246].



Сурет 2.23 – Кілт кодының мультибиометриялық қалыптасуының сызбасы

Осыған орай, Ғаламтор желісінде сақталатын және ашық ақпараттық кеңістіктерде пайдалану үшін арналған биометриялық электронды жеке куәліктер, өзімінің иесі тез аша алатындай және бөгде адамның аша алмайтынына кепіл болатын, жабық нейрожелілі контейнерлерде орналастырылған биометриялар болуы тиіс [92]. Ашық нейрожелілі контейнерлер МЕСТ Р 52633.4, МЕСТ Р 52633.0, МЕСТ Р 52633.5 [91; 93; 94] талаптарына сай құрылуы және ары қарай өзін-өзі Қорғауы (жабылуы) тиіс. Адамдардың басқа да дербес мәліметтері электронды биометриялық жеке куәлікке орналастырудың алдында куәлік иесінің кілтінде таңбалануы тиіс. Ары қарай электронды жеке куәлік оны берген органда ЭСҚ қол қойылуы тиіс. Осыдан кейін жасырын электронды куәліктер функционалдық ресурстары негізгі компоненттерінің арасында үлестірілетін таратылған компьютерлік жүйелерде сақталуына болады [95]. Бұл технологияның негізгі элементтері 2.24-суретте бейнеленген [47, с. 59].



Сурет 2.24 – Электронды куәліктерді бұлттық сақтаудың технологиясы

Бұл технология өзіңмен бірге ешбір құжат алмай жүруге мүмкіндік береді. Өз өкілеттілігіңді растау үшін өзіңіздің атыңыз бен биометриялық бейнеңізді ақпараттық қызмет көрсететін операторға айтсаңыз болғаны. Аты немесе биометриялық бейнесі бойынша ақпараттық қызмет көрсетуші оператор немесе қолданушының өзі де бұлттағы сақтаудан қажетті электронды жеке куәлікті таба алады. Өзінің биометриялық куәлігін қолданушы ғана оператордың қатысуымен немесе қашықтан пайдалана алады.

3 АҚПАРАТТАРДЫ НЕЙРОЖЕЛІЛІК БИОМЕТРИЯЛЫҚ ҚОРҒАУ ҚҰРАЛДАРЫНА ТӨНЕТІН ҚАУІП ПЕН ОЛАРҒА ҚАРСЫ ӘРЕКЕТ ЕТУДІҢ ӘДІСТЕРІ

3.1 Ақпараттарды нейрожелілік биометриялық қорғау құралдарына төнетін қауіптер және оны жүзеге асыратын шабуылдар

3.1.1 Биометриялық қорғау автоматының мүмкін болатын кіріс және шығыстық күйін теру қаупі

Ұзын шығыстық био-кодтарды (мәселен, ұзындығы 256 бит) пайдалану жағдайында кодтың мүмкін болатын жағдайының саны 2^{256} болады. Соншалықты үлкен санды таңдаудың еш мәні жоқ. Криптографиялық қиындыққа тап болатын хакерлер қорғанысқа мүлдем шабуыл жасамай-ақ, оны ашудың басқа жолын іздейді.

Биометриялық қорғанысқа шабуыл жасауға әрекет жасауға биометриялық ақпараттарды сканерлеудің алғашқы тетіктері тараптарынан аңғаруға болады. Мұны саусақ ізінің суретін сканерлеу мысалынан көрсетеміз, яғни жарықтың 256 градация есебінің мүмкіндігінен 320×480 (500 dpi) көрінеді. Мұндай тетіктердің мүмкін болатын комбинациялар саны $2^{1\,228\,800}$ құрайды. Мұндай аса үлкен санды іріктеп алудың еш мәні жоқ.

Ерекше нүктелерді бөлу алгоритмін орындау кезіндегі алдын-ала өңдеу сатысында саусақ іздерінің суретінде көлемі 153 600 болатын дискреттік мәндегі 1 және 0 вектор пайда болады.осы жағдайда биометриялық мәліметтер жағдайының жалпы саны $2^{153\,600}$ болады. Жағдай саны айтарлықтай төмендеді, әйтседе қарапайым асыра сілтеу үшін қол жетімсіз.

Келесідегі дискреттік мәліметтерді екі өлшемді түрлендіру бақыланған үздіксіз параметрлерде олардың өлшемдерін 256-ға дейін қысқартады. Жасанды нейрондық желілер кірісінде үздіксіз параметрдің көптеген жіберілетін мәндерін континуммен сипатталады және оның ұсынылуының туралығымен шектеледі. Егер бір үздіксіз биометриялық параметрді кодтауға 4 бит (ол 16 жағдаймен ұсынылуы мүмкін) қолданылса, онда биометриялық параметрлер комбинация мәнінің саны түрлендіргіштің кіре берісіндегі биометрия-коды 2^{1024} –ті құрайды. Бұл 10^8 немесе 2^{26} таңдаудың шабуылына өндірушілермен жарияланған биометрияның бір қалыптылығына қарағанда айтарлықтай көбірек. Яғни, кіре беріске «Бөтен» биометриялық бейнесінің 10^8 немесе 2^{26} биометрия-кодын қойып, биометрияға шабуылдау айтарлықтай тиімді. Бұл әдіс басқаларына қарағанда айтарлықтай тиімді.

Дәл осындай жағдай басқа да биометриялық технологияларды қолдануда туындайды. Мысалы, дауыстық биометриялық қорғаудың типтік тәсілі ұзындығы 4 секунд болатын құпия фразаны («Невероятно сильный мороз») қолданады. Оларды сандау кезінде 8 кГц жиілігімен 8-дәрежелі АЦП-да 32 000-нан 8-биттік мәліметтер ағыны пайда болады. Шығыстық мәліметтер мәнінің мүмкін болатын комбинациялар саны $2^{256\,000}$-ды құрайды. Фурьенің бір өлшемді түрлендіруінің 512 коэффициентін табуда және оларды 4-дәрежеге дейін

дөңгелектегенде мүмкін болатын комбинациялар саны 2^{2048}-ге дейін қысқарады. Жағдайдың бұл саны 10^6 немесе 2^{20} таңдаудағы шабуылына бір қалыптылық өндірушінің көрсеткенінен айтарлықтай көп. Мұндай жағдайда кіре беріске дауыстық фразаларды қойып шабуылдаған тиімдірек.

3.1.2 Биометриялық бейнені ұстап қалу қаупі, нақбейнені пайдаланып шабуылдау

Биометриялық бейнені ұстап қалу, келешекте оның нақбейнесін дайындау шабуылдардың ең тиімдісі болып табылады. Мұндай шабуылға тек қана ұйымдастсрылған-техникалық іс-шаралар қарсы тұра алады. Өзімінің дербес мәліметтерін қорғау мақсатында пайдаланушы қол ізінің суретімен сканердің әйнегінде терлі-майлы ізін қалдырады. Егер бұл ізді сүртіп тастамаса, келесі пайдаланушы оның мәліметтерін ала алады. Қажетті саусақ іздерінің суреті салынған нақбейнені дайындау күрделі техникалық мәселе болып табылады.

Мұндай ұқсас ұстап қалуларға қарсы тұру тек пайдаланушыны өзімінен кейін сканерді сүртіп кетуді талап ету немесе автоматты түрде сканерден іздің өзімінің өшіп қалу мүмкіндігі бар техниканы алу.

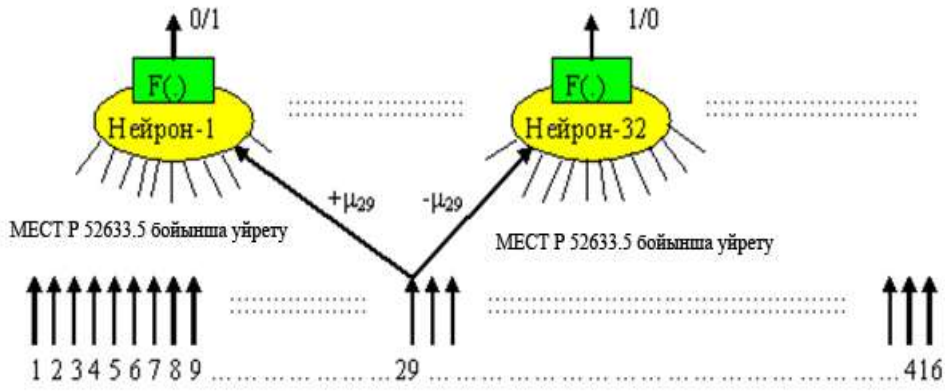
Ұйымдастырушылық техникалық шараның тағы бірі қорғалатын ақпаратты дараландыру. Саусақ іздері айтарлықтай биометриялық қорғаныс болады, егер шабуылдаушы адамның атын және қандай биометриялық технологияны қолданатынын білмесе. Бұл айтарлықтай жүзеге асырылады, мәселен, электронды дараландыру төлемдері кезінде провайдер төлеушінің IP адресін жасырып қалады және транзакциялауды өзімінің IP адресінен іске асырады.

Мұндай жағдайда шабуылдаушыға IP адресті білуі қажет болады және жеке заттарынан қол ізін алу үшін пәтеріне ұрлыққа түсуге тура келеді. Егер шабуыл іске аспай қалса, шабуылшы дауыстық парольді білу үшін тыңдайтын құрылғы немесе бейне камера орнатуына тура келеді.

3.1.3 Нейрожелілердің артық байланыстары болуынан био-кодтың ішінара әшкерелену қаупі, Маршалко шабуылы

Жасанды нейрондық желілердің «анық емес экстракторлардан» айырмашылығы алғашқы кедей биометриялық мәліметтерді байытуға қабілетті және байыта отырып, оларды кванттауды іске асырады. 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) био-кодтың беделін түсіру үшін қолданылуы мүмкін. Шабуылдың бұл түрін алғаш рет Г.Б. Маршалко [96] жазды. Маршалко шабуылының мәні 3.1-суретінде бейнеленген.



Сурет 3.1 – Жасанды нейрондық желілердің артықшылығына бағытталған Маршалконың шабуылы

3.1-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 салмақты коэффициенттердің белгілерін салыстыра отырып, био-код 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 био-кодтың қалған тұрақтылығы небары 56 күшті корреляцияланған битті құрайды. Мұндай тиімді шабуылға үш тәсілмен қарсы тұруға болады:

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);

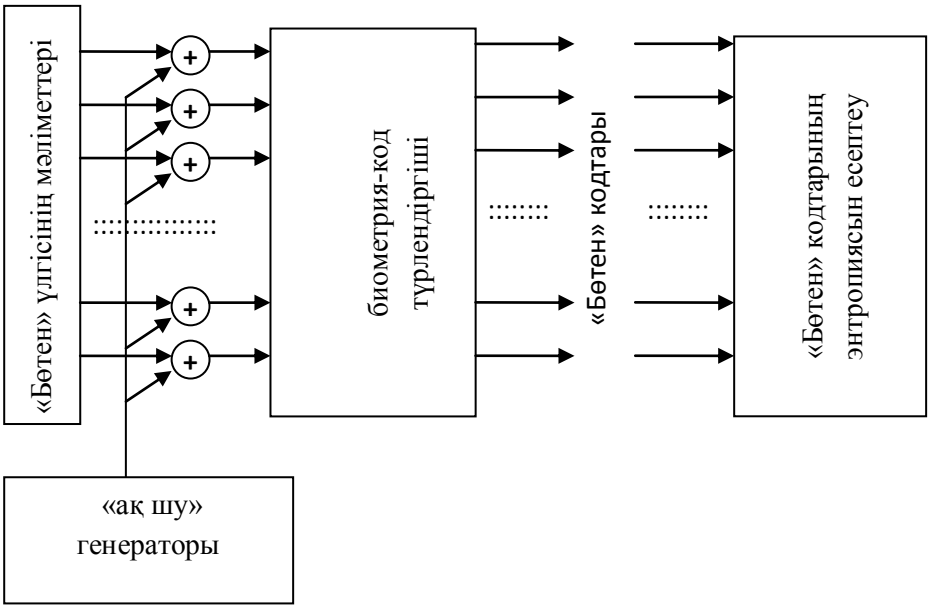
3-тәсіл. Жалпы байланыстары бар нейрондарды үйретудің итерациялық алгоритміне жиі оралу және анықталған 50% нейрондардың жалпы кірістік байланыстары үшін МЕСТ Р 52633.5 кері алгоритмінің салмақтық коэффициенттерінің белгісін беретін басқа да сапалы нейрожелілік шешімдерді табу.

3.1.4 «Бөтен» бейнесінің үлгілеріне код жауабының энтропияларын қадағалауды қолдану арқылы ашық нейрожелілік контейнерге шабуылдау

Біз биометрия түрлендіргішінің жоғары өлшемді шығыс кодтарының энтропиясын тиімді бағалай аламыз, қаскүнем осыны пайдаланып, ашық нейрожелілік контейнерге шабуыл жасауы мүмкін. «Бөтен» бейнесінің «Өзім»

бейнесіне жақын бейнелері әріректегі «Бөтен» бейнесімен салыстырғанда аз энтропияны меңгерген. «Өзім» бейнесінде энтропия мүлдем жоқ. Бұл қасиет «Өзім» коды үшін анық көрінген, бірақ ол да ерікті таңдалған код үшін де бірдей.

Осы немесе басқа биометриялық бейненің энтропиясын бағалау осы биометриялық бейнені есептеу орталығы арқылы ыңғайлы. Мұндай бағалауды жүзеге асырудың блок-сызбасы 3.2-суретте келтірілген [47, с. 122].



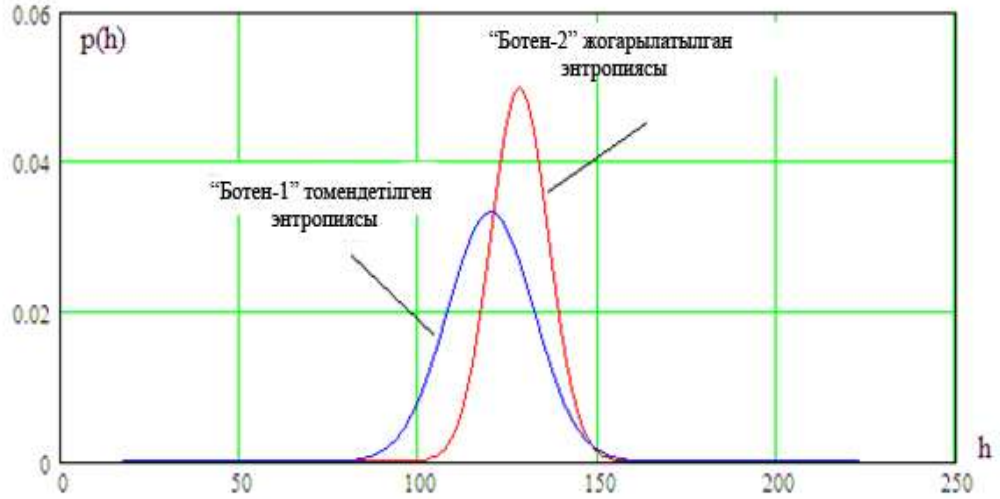
Сурет 3.2 – «Бөтен» кодтарының энтропиясын бағалаудың блок-сұлбасы

Әдетте «Бөтен» бейнелерінің параметрлер дисперсийлерін математикалық күту «Өзім» бейнелерінің аналогты параметрлерінен үш есеге жоғары:

$$E(\sigma(\bar{\xi}_i)) \approx 3 \cdot E(\sigma(\bar{\nu}_i)). \qquad (3.1)$$

Өзім кезегінде, «Өзім» бейнесін кездейсоқ генерациялауда, оның ортасының орташа квадраттық ауытқуында 1/3 от $\sigma(\nu_i)$ шыға берісте жақсы оқытылған нейрожелілі қайта құрушы биометрия-код $H(\bar{c}) \approx 0.0$ нөлдік энтропия иеленетін әркезде де «Өзімнің» бірдей кодтары пайда болады. «Ақ шу» генераторының орташа квадраттық ауытқуының ұлғаюы $\sigma(\nu_i)$ -тен 1/3 артығырақ екені кодтың пайда болу мүмкіндігіне әкеледі (сурет 3.2).

Жоғарыда келтірілгеннен шығатыны «ақ шу» генераторының орташа квадраттық ауытқуы 3.2-суретінің блок-сұлбасынан $E(\sigma(\xi_i))$ -дан 1/9-ға тең таңдау қажет. Мұндай жағдайда «Бөтен» бейнесінің әрекетіне үн қату кодтарының энтропиясын айтарлықтай сенімді бағалау жеткілікті. 3.3 суретте Хэммингтің арақашықтықты бөлуі келтірілген [47, с. 122].



Сурет 3.3 – Энтропиясы әртүрлі мәнді «Бөтен-1» және «Бөтен-2» бейнелері мысалында Хэмминг кодын үлестіру

3.3-суретінен $E(h_1) < E(h_2)$ және $\sigma(h_1)>\sigma(h_2)$ екендігі көрініп тұр. Бұл екі шартты орындау «Бөтен-1» бейнесіне қатынайтын кодтармен «Бөтен-2» бейнесіне қатынайтын кодтарды салыстырған кезде энтропияның айтарлықтай төмен мәнді екенін дәлелдейді. Барынша күрделірек жоғарыда келтірілген теңсіздіктердің бірі орындалмаған жағдайында, салыстырылатын энтропияларды күрделірек (3.1) өрнектеріне сәйкес есептеуді жүзеге асыру керек болады. Ашық нейрожелілік контейнердің (қорғалмаған биометрия-кодты түрлендіргіш) энтропия шығыс кодтарында жақсы бақыланатын бір қалыпсыздық бар екендігін аламыз.

Бұл минималды энтропиялы биометрикалық бейнелерді таңдау арқылы биометрикалық бейненің генетикалық таңдау шабуылын ұйымдастыру үшін және энтропияның айтарлықтай төменірек көрсеткіштері бар бейнелі-ұрпақтардың жаңа буынын айқастыру және синтездеу үшін ары қарай қолданылуы әбден мүмкін.

Мұнда «Өзім» кодын білу міндетті емес, өйткені «Өзімнің» бейнесіне қатынайтын кодтар энтропиясы әрқашан нөлдік болады.

3.2 Жеке мәліметтерді биометриялық қорғау құралдарына төнетін қауіп және шабуылдарға қарсы тұру әдісі

3.2.1 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 қол жазбаның бірқалыпты және бірден-бірлігіне болуына байланысты. Биометриялық құпиясөзді жасарын 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.

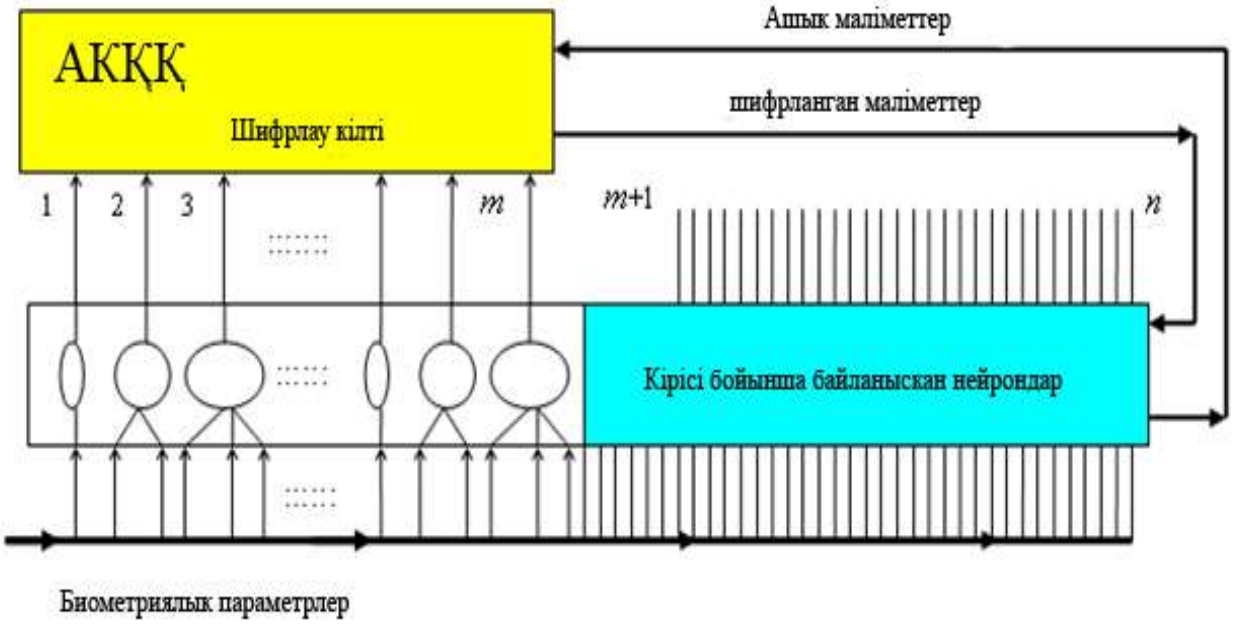
Арнайы құрастырылған криптографиялық хэш-функцияларды пайдаланғанда құпиясөздердің хэш-функциясы мен қолжеткізу био-кодтарын сақтау қауіпсіз болып саналады. Нақты криптографиялық хэш-функцияларды қайтымсыз етіп қарастыруға болады. Басқаша айтқанда, олардың тікелей есептелуіне уақыт аз кетеді, ал бастапқы 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 био-кодтар 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 био-кодтарға қарағанда шамамен үш есе артық болатын тұрақтылық көрсеткішін қамтамасыз етуі тиіс (қосфакторлы аутентификация). Егер криптографиялық хэштеудің орнына шифрлеу қолданылса, онда шифрлеу кілтінің ұзындығы мен биометрия

табандылығы арасындағы қатынас шамамен алғанда осындай болып қала беруі тиіс.

3.2.2 Нейрожелілік контейнердің мәліметтерін қарапайым шифрлеу арқылы криптографиялық қорғау

Ең қарапайым және түсінікті қорғау тәсілдерінің бірі – алғашқы (ашық) нейрондарының шығысымен кілттің алынуы және онда өзге нейрондардың (қорғалған) мәліметтері шоғырлануы [47; 97; 98]. Бұл жағдай 3.4-суретінде көрсетілген.



Сурет 3.4 – Нейрожелілік контейнердің мәліметтерін саны өте көп болатын айқастырылған байланыстарды шифрлеу арқылы қорғау

3.4-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 био-кодқа түрленеді және ары қарай осы кодта келесі нейрондық мәліметтерін бұрын қорғалған шифлау жүргізіледі.

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 кілтінің ұзындығы кезінде 120 нейрон мәліметтері ашық сақталады (120 нейронға үшін таразылар мен байланыстар кестесі жалпы қол жетімді).

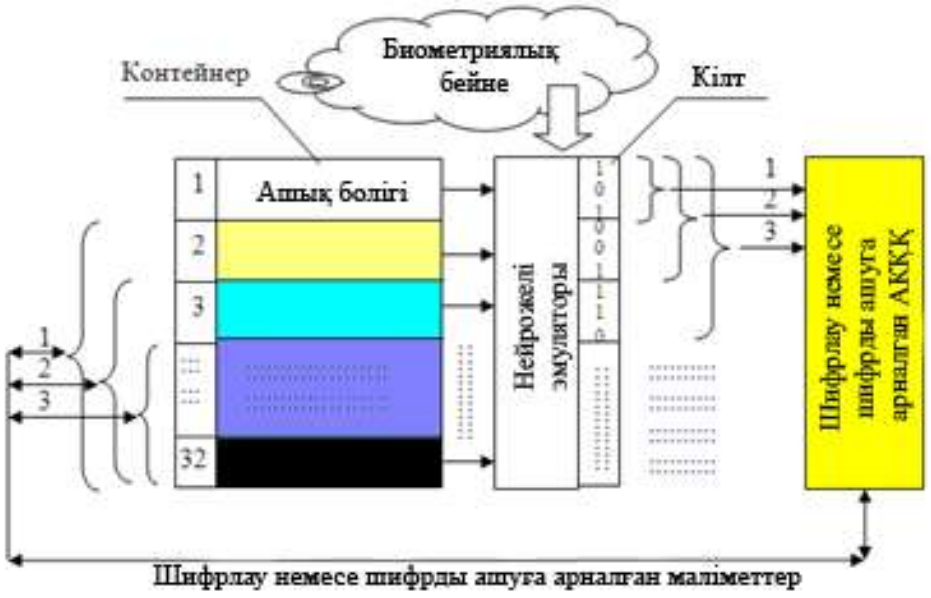
0.2 бит био-параметрінің орташа ақпараттылығы кезінде әр нейронның 5 кірісі бойынша орташа алғанда 600 био-параметрлер үшін 600 кіріс шығады.

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» кілтінің 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).

3.2.3 Криптографиялық кілттің өсетін ұзындығымен блогтық 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 3.5-суретте келтірілген [47, с. 57].



Сурет 3.5 – 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 3.5-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.

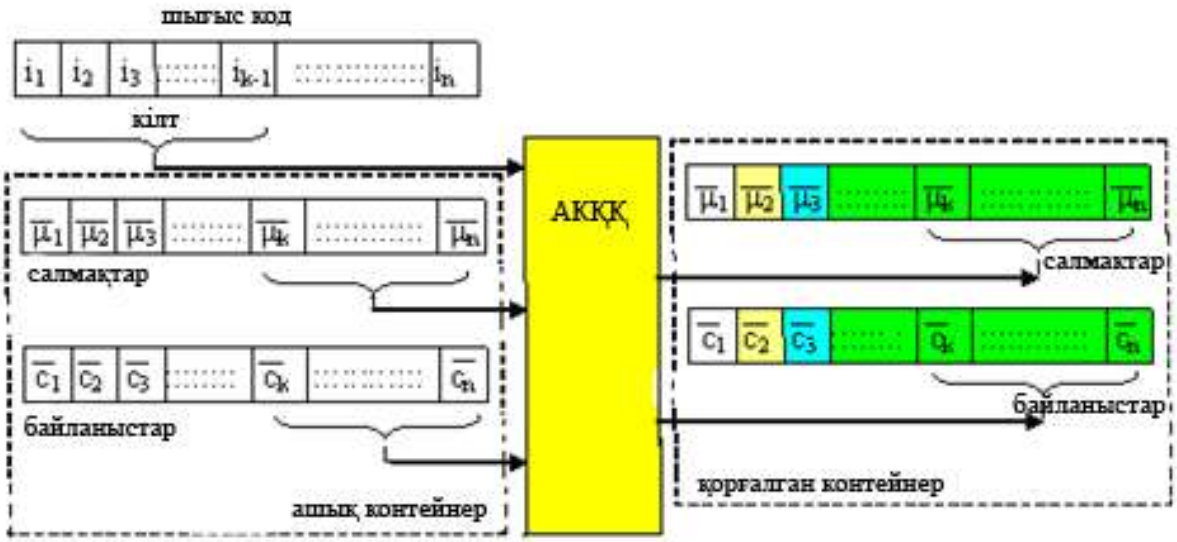
Түрлендіргіш жағдайының көп өлшемді энтропиясының n =16 нүктесінде биометрия-коды өзінің қасиеттерін өзгертеді және алдыңғы тарауда сипатталған интегралдық шабуылдар жұмыс істей бастайды. Интегралдық шабуылдар статистикалық зерттеулерге арналған қолжетімді биометрия-код ұзын болған сайын соғұрлым тиімдірек болады.

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

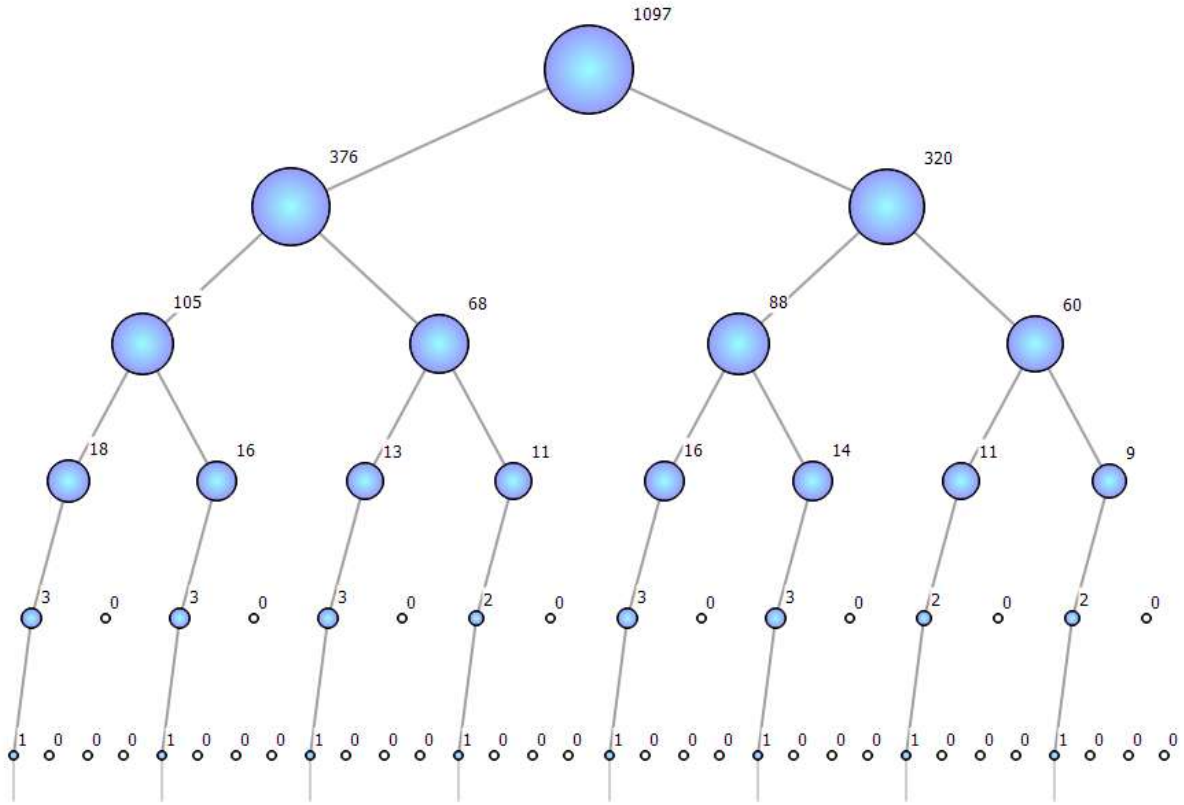
Кілті 1 бит ұзындықты үйретілген нейрожелінің қорғалатын мәліметтерін көпеселік блоктың шифрлауының шектеулі жағдайын қарастырайық. Бұл желіде ашық болып бір ғана (алғашқы) нейрон қалады, қалған нейрондардың мәліметтерінің бәрі қорғалған болып шығады. 16 биттік кілтте өзінің тиімділік қорғанысы бойынша 16 сызықтық өсетін кілттердегі қорғаныс бірдей деген ой пайда болады. Бұл шыныменде 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 (сурет 3.6).

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 3.7 суретінде келтірілген.



Сурет 3.6 – Ашық контейнерлердің 1,2,3,…, 256 бит кілттерінде шифрленіп қорғалған болып түрленуі

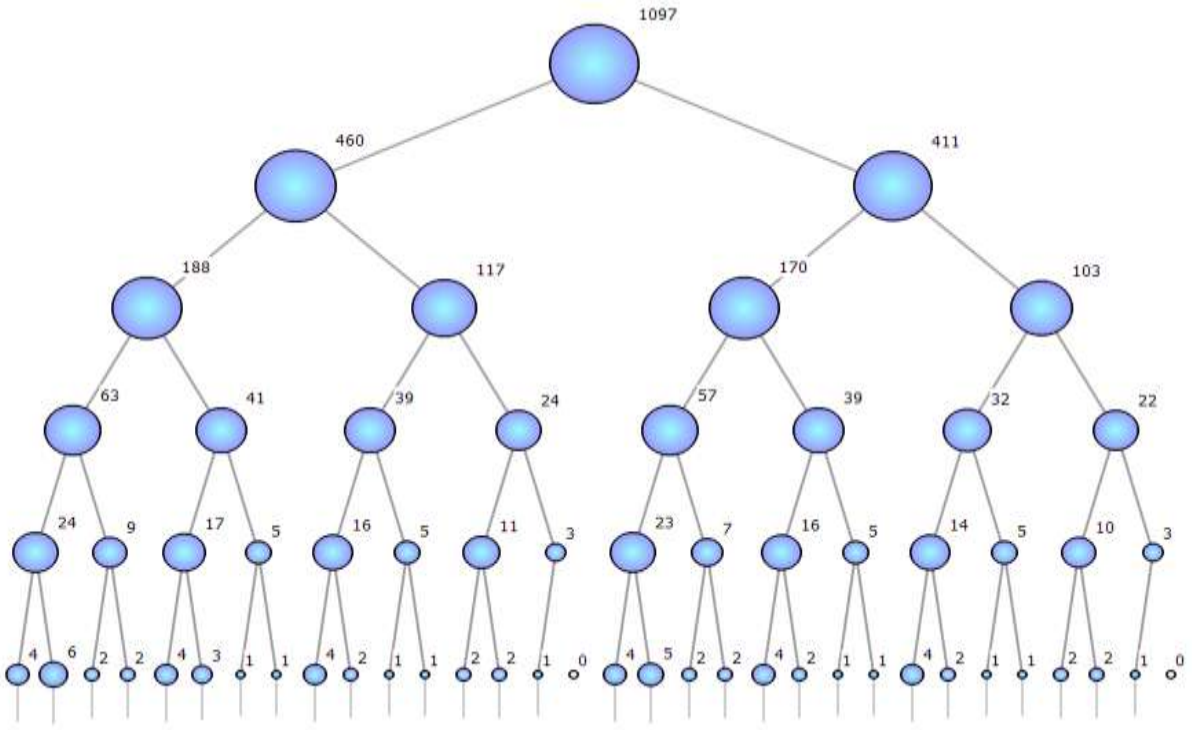


Сурет 3.7 – «Піл» қолжазба құпиясөзінің қорғалған контейнерді қолданатын 0,7 тұрақтылық деңгейі бойынша «Бөтен» бейнесі базасын сұрыптаудың бинарлық ағашы

3.7-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 ата-аналардың 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 3.8-суретінде көрсетілген.

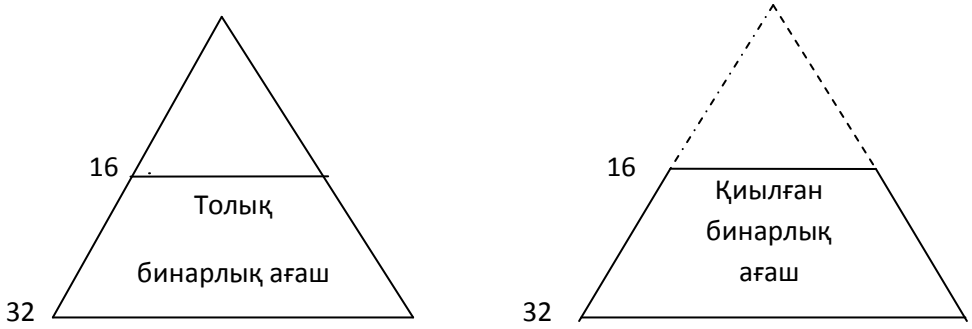


Сурет 3.8 – «Піл» қолжазба құпиясөзімен қорғалған контейнерді қолдана отырып 0,3 тұрақтылық деңгейі бойынша «Бөтен» бейнесінің базасын сұрыптаудың бинарлық ағашы

3.8-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» био-коды бұтағына тарту эффектісі жоқ. Көрші бұтақтар (0 ден 7-ге дейін қашықтықта «Өзім» бұтағының кодына жуық) өздерінің статистикалары бойынша бинарлық ағаштың еркін бұтағынан ерекшеленбейді.

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 кететін қосымша шығындар «бір битті шифрлау» кезінде шамамен алғанда екі есе жоғары болып шығады. Бұл жағдаят 3.9-суретінде келтірілген.



Сурет 3.9 – Келесі қорғалған 15 нейронның параметрлерін білмейтін шабуылдаушыны тойтаруға мәжбүр болатын толық бинарлық ағаш (суреттің сол жағы)

3.9-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 есі 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 эффектілердің пайда болуына және осылайша үйретілген нейрожелінің мәліметтерін қорғауды одан да әлсіретеді.

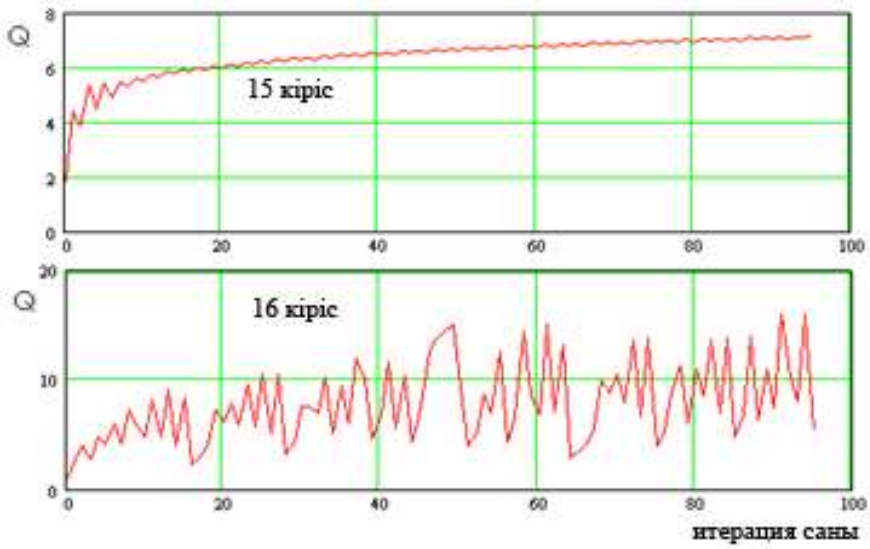
Алынған 1,2,3... 25 биттік кілттердің 256 еселік шифрлануымен алынған биометрикалық қорғанысты шабуылдаушы үшін 16, 32, 48,….., 256 биттік

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.

3.2.5 Жабылатын байланысты нейрондарды итерационды үйретуге жекелей айналып келуі есебінен шифрлау табандылығын күшейту

Нейрожелілік контейнерге ең тиімді жасалатын шабулыдардың бірі – Маршалко шабуылы. Шабуыл үлкен жасанды нейрон желілерін үйретуші жылдам алгоритмдері – $\mu(E(v_i), \sigma(v_i), \sigma(\xi_i))$ нейрондар салмақтық коэффиценттерінің 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, кейді көп өлшемді беттер бойынша флюктуирлейді. Итерациялық үйрету және нейрондардың саны көп кіріс кезінде нейрондардың коэффицент салмақтары шуылдарының табиғи процесі пайда болады. Ол 3.10-суретінде көрсетілген [47, с.66].



Сурет 3.10 – Бір нейронды итерациялық үйрету процедурасының тұрақтылығын жоғалтуы

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 немес нейрожелі толық итерациондық үйрету алгоритмі үйрету процесін айтарлықтай баяулатады, бірақ мұнда нейрондардың артық санды байланыстарына жасалатын шабуылдарына тиімді қорғаныс пайда болады.

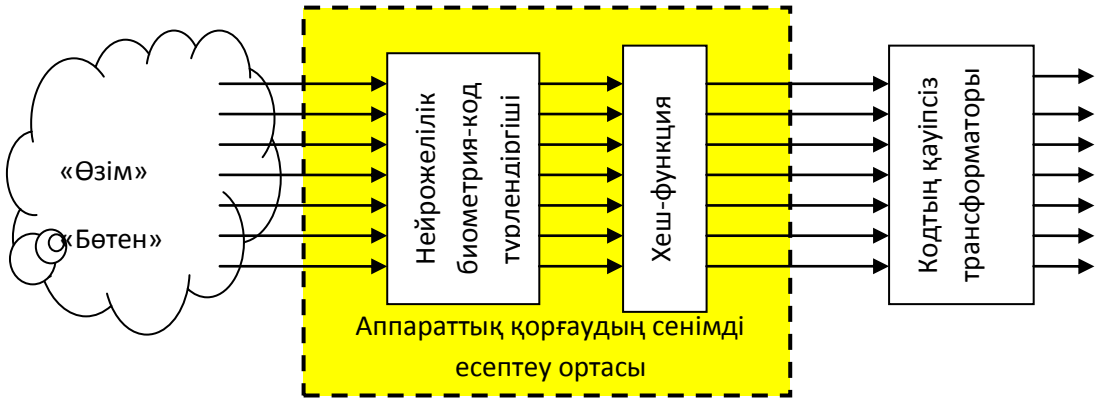
Диссертациялық жұмыста тағы да бір әзірленген алгоритм - мәліметтерді мәжбүрлеп бұзудың жылдам алгоритмі. Бұл алгоритм үшін нейрондардың жалпы байланысының 50% -ы шағын (үлкен емес) болады және олардың таңбасы өзгереді. Ары қарай үйрету кезінде бүлінген байланыстар өзгермейді. Бұл нейронды алғаш үйретуден 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 оқытудың 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 зерттеулер 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.

3.2.6 Энтропияның әркелкілігін сырттай қадағалаудың әрекетінен нейрожелілік контейнерді қорғаудың әдістері

Кемінде 16 разрядтан тұратын топты есепке алатын, төменгі өлшемдегі кодтардың энтропиясын қадағалауды қолдану кезінде «Бөтен-1», «Бөтен-2», ..., «Бөтен-к» кодтар энтропиясының әркелкілігін дұрыс қадағалау болмай қалады. Егер біз энтропияны есептеудің классикалық әдісін Шеннон бойынша қолдансақ, онда биометриялық бейнелерді генетикалық таңдауға бағытталған шабуылды ұйымдастыру мүмкін болмас еді. Тек қана жай кодтардың кеңістігінен Хемминг кодтарының кеңістігіне өту «Бөтен-1», «Бөтен-2», ..., «Бөтен-к» биометриялық бейнелеріне үн қату-кодтары топтарының энтропия әркелкілігін қадағалау әрекетінен нейрожелілі контейнерлерді қорғаудың қажеттілігін күн тәртібіне қояды.

Қорғау жолдарының бірі оның программалық бөлігіне кіре алатын физикалық қорғанысы бар, кейбір аппараттық құралдар түрінде атқарылған сенімді есептеу ортасын қолдану болып табылады. Мұндай қорғаудың блок сұлбасын жүзеге асыру 3.11-суретте бейнеленген.

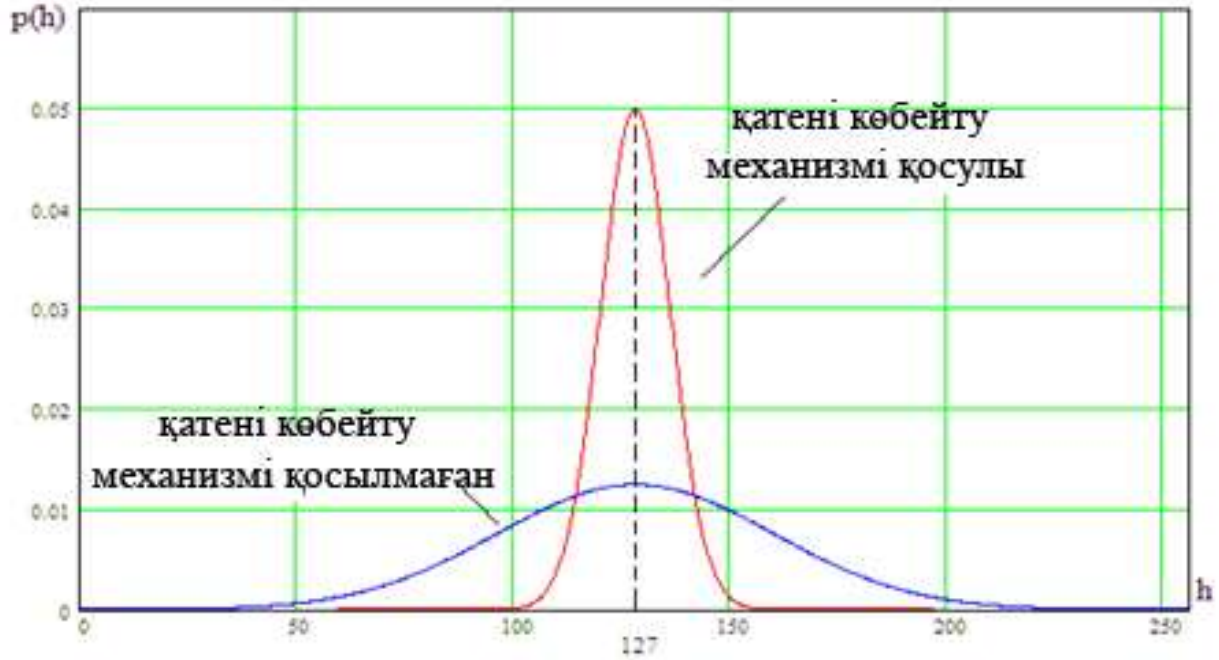


Сурет 3.11 – Энтропияның әркелкілігін қадағалау әрекетінен физикалық қорғауды ұйымдастырудың блок-сұлбасы

Физикалық (аппараттық) қорғаныстың болуы қаскүнемге биометрия-код нейрожелілі түрлендіргіштің ішкі байланыстарын қадағалауына жол бермейді. Бұдан басқа, биометрия-код нейрожелілі түрлендіргіштің шығар жолдары оларды хеширлеу арқылы қайта жасалуы тиіс. Шығыс кодтарды энтропияның әркелкілігін қадағалаудан қорғау үшін криптографиялық хеширлеудің белгілі функциялары қолданылуы мүмкін [99-101]. Аппараттық ортада жүзеге асырылған криптографиялық хеширлеудің функциясы пайда болысымен, сыртқы қадағалаушы «Бөтен» биометриялық бейнесінің мысалдар энтропиясын көруге қабілетсіз, демек, «Өзім» бейнесін генетикалық таңдауға бағытталған шабуылды ұйымдастыруға қабілетсіз.

Аппараттық ортаға енгізілген хеширлеу функциясы бір жағынан шығыс кодтар энтропиясының әркелкілігін қадағалауға кедергі келтіретіндіктен дұрыс болып табылады. Әйтседе, екінші жағынан, хеширлеудің пайда болуы кіруші кілтке биометрия-код түрлендіргішті үйретуді мәнсіз етеді. Нейрожелілі түрлендіргіш биометрия-кодты үйрету кезінде кейбір аралық кездейсоқ код пайдаланған жөн. Нейрожелілердің шығу жолдарындағы аралық кездейсоқ кодты біле тұрып, біз оның хеш-функциясын жеңіл түрде есептей аламыз және ары қарай сыртқы қауіпсіз трансформатор хеш-функциясының алғашқы аралық кодын кіруші кілтке салу. Ережеге сай, кодтың қауіпсіз транформаторы әрбір хеширлеудегі 2 «тұздар» модулін қосумен сенімді есептеу ортаның үн қату кодын бірнеше рекурсивті хеширлеуде құрылады. «Тұздар» рөлін ойнайтын мәліметтер әдетте трансформатор кодында сақталынады. Сыртқы қадағалаушы ішкі физикалық тұрғыдан қорғалған сенімді есептеу ортасының сыртқы хеширлеудің функциясын жүзеге асыру фактісіне сенуіне болады. Негізінде хеширлеу функциясы қателіктерді көбейту механизмінің рөлін атқарады. Егер хеширлеу функциясы сөндірілсе, онда қателіктердің көбею механизміде

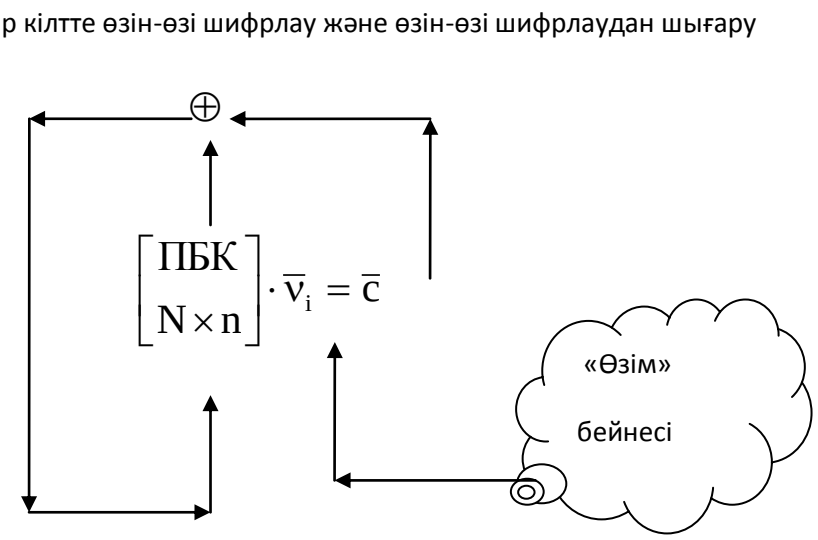
тоқтатылады. 3.12-суретте қателіктердің қосулы және сөндірулі кездердегі көбеюімен биометрия-код қос түрлендіргішке арналған Хэммингтің кодтарды бөлу функциясын сипаттайтын мысалдар келтірілген [47].



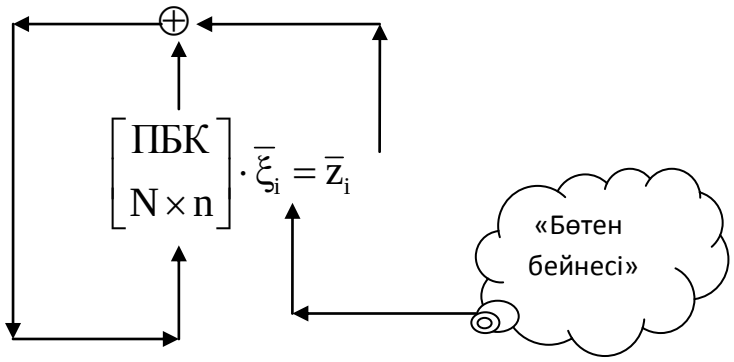
Сурет 3.12 – 256 Шығыспен және бәрі «Бөтендер» бейнелері арқылы тестілеумен түрлендіргіш биометрия-кодқа арналған қателіктер көбеюінің қосылуға дейінгі және кейінгі механизмінің Хэмминг кодтарының мәндерін бөлудегі қос сипаттаушылық функциялары

Нейрожелілік түрлендіргіш биометрия-кодты аппаратты қорғаушы іске асыруға болмайтын жағдайда, өзін-өзі қорғау үшін нейрожелілі контейнердің өзін-өзі шифрлеу технологиясын қолдану қажет. Бұл жағдайда «Өзім» кодында нейрожелілі контейнердің өзін-өзі шифрлау мен өзі шифрды ашу мазмұны сәйкестендіру процедурасына әсер етпейді. Бұл жағдай 3.13-суретінде бейнеленген.

Алайда, егер «Бөтен» сәйкестенгісі келсе, онда $\bar{c}$ кілтіндегі өзін-өзі шифрлау контейнері кездейсоқ $\bar{\xi}$ кілтте өзі шифрды ашуға тырысады. Сонымен бірге өзі шифрды ашу болмайды ды, мәліметтерді хештеу (кездейсоқ араласулар) туындайды. Бұл жағдай 3.14-суретінде бейнеленген. Стандартты хеш-функцияларды пайдалану кезіндегі туындайтын мәліметтерді хеширлеудің сапасы мен өзі шифрды ашудағы белгісіз кілтті кездейсоқ алмастырып қою кезіндегі мәліметтерді хеширлеудің сапасы шамамен бірдей болады екен. Осы екі жағдайда да сыртқы қадағалаушы «Бөтен» бейнесіне код-үн қатулардың энтропия әркелкілігін көруге қабілетсіз болады.



Сурет 3.13 – Шығыс кодпен 2 модуль бойынша түрлендіргіш мәліметтерін қосу арқылы нейрожелілік түрлендіргіш биометрия-кодтың өзін-өзі шифрлау механизмін түсіндіру



Сурет 3.14 – $\bar{c}$ кілтінде шифрланған кездейсоқ $\bar{z}$ кілтте оны өзін-өзі ашуға әрекет етудегі нейрожелілі түрлендіргіш биометрия-кодпен іске асырылатын хештеу механизмін түсіндіру

3.3 Өте аз тестілік таңдауды қолданатын, нейрожелілік биометрия-код түрлендіргішінің пайда болатын қателіктерінің ықтималдығын бағалау әдісі

Үлкен көлемдегі мәліметтерді тез өңдеу айтарлықтай мүмкін болады, егерде жаңа есептеу процедуралары мен үлкен көлемді нейрожелілік өңдеулерге көшсе [102; 103]. Ертеректе бұл мүмкін болды, себебі нейрондық желілерді оқыту қажет болмайтын. Бұл мәселе шешімін тапқан, Ресейде үлкен және аса үлкен жасанды нейронды желілерді автоматты үйретудің тез абсолютті тұрақты алгоритмдері құрылған болатын [47]. Бұл алгоритмдер МЕСТ Р 52633.5-2011 ұлттық биометриялық стандарттың негізіне жатты [94].

Үлкен жасанды нейронды желілерді жылдам автоматты үйретудің мәселесі шешілгеннен кейін оларды әртүрлі қосымшаларда қолдануға болады. Сонымен қатар мәліметтер базасын сол немесе басқа бейнеге жақындығы бойынша реттеу мүмкіндігі бар (мәселен, Ғаламтор кеңістігі). Іздеу мен сұрыптау технологиясы нейрожелілі биометрия технологиясына өте ұқсас [47]. Осыған байланысты кодтарды үйретілген нейрондық желілер шығысында туындайтын, корреляцияланған разрядтарды есепке алу қажеттілігінің ғылыми проблемасы туындады.

Адамдардың биометриялық мәліметтерін ең қарапайым түрлендіргіш ұзындығы *n* бит кодында қарастырамыз. Анық болуы үшін «Өзім» кодының қайта құрастырушысы белгісіз және «1» жағдайынан тұратынын болжаймыз. «0» жағдайының біреуінің пайда болуының өзі «Өзім» биометриялық бейнесінің донорына қол жеткізе алмайтынын білдіреді. Түрлендіргіш биометрия-код жұмысының сапасын бағалау үшін, көптеген тәуелді жағдайлардың ұзын тізбегінің бірлесе пайда болу мүмкіндігін есептеуге әкелетін, бірінші және екінші тектес қателіктердің мүмкіндігін есептей білу қажет. Жекелеп алғанда, 256 биометриялық параметрлерді ұзындығы 256 бит кодқа түрлендіру үшін салыстырудың 256 ережесін есепке алу қажет. Проблеманың күрделенуі сол, биометриялық параметрлер қатты тәуелді, биометриялық параметрлерді корреляциялау коэффициентінің орташа модулі *r = 0.3- ді* құрайды.

Егер жағдайлар тәуелсіз (корреляцияланбаған) болса, олардың бірлесе пайда болуын биномиалды заңды пайдаланып есептеуге болады [104; 105]:

$$P(n, m, p) = \frac{n!}{m!(n-m)!} \cdot p^m \cdot (1-p)^{n-m}, \qquad (3.2)$$

мұндағы *n* – биометриялық параметрлерді есепке алатын сан;

m – биометриялық параметрлерді табу саны;

p – барлық *n* параметрлер бойынша жағдайды табудың орташа мүмкіндігі.

Параметр *p* мазмұнын білдіруде барлық мағына бойынша классикалық биномикалық заңнан ерекшеленетінін атап өткен жөн. Биномиалды заңның классикалық нұсқасында параметрді *p* бөлу – бұл параметрлердің әрқайсы бойынша сәйкес келудің бірдей мүмкіндігі. Заңды бөлудің классикалық нұсқасы Бернуллидің сынағы кестесінен алынған. Классикалық жағдайда параметр *p* – тиынның «0» жағдайына түсу мүмкіндігі. Тиынның «0» және «1» жағдайына тең мүмкіндікпен түсуінде параметр *p* 0,5-ке тең болады.

Бернулли сынағының кестесін өзгертіп, *n* тиынды тастаймыз, әрқайсысы өз параметрін p_i иеленеді. Үлгіге айналған Бернулли сынағының кестесі параметрді p_i барлық тиын бойынша орталандыруды талап етеді:

$$p = \frac{1}{\mathrm{n}} \sum_{i=1}^{n} p_i \qquad (3.3)$$

Үлгіге айналған Бернулли сынағының тағы бір маңызды факторы тасталынған тиындардың ақырғы жағдайлары арасында тәуелділіктің пайда болуы болып табылады. Бұл тәуелділікті биометриялық мәліметтерді корреляциясының коэффициенттері модулінің орташалау мәні арқылы бағалауға болады:

$$r = \frac{1}{n^2} (\sum_{i=1}^{n} \sum_{i=1}^{n} \left| r_{i,j} \right|) - \frac{1}{n} \qquad (3.4)$$

Корреляцияланған байланыстардың орташалау мәнінің модулін төрт реттік функция $P(n, m, p, r)$ түрінде есепке алу биометриялық тәсілдерді тестілеу кезіндегі мүмкін болатын шынайы бағалар жасауға мүмкіндік береді.

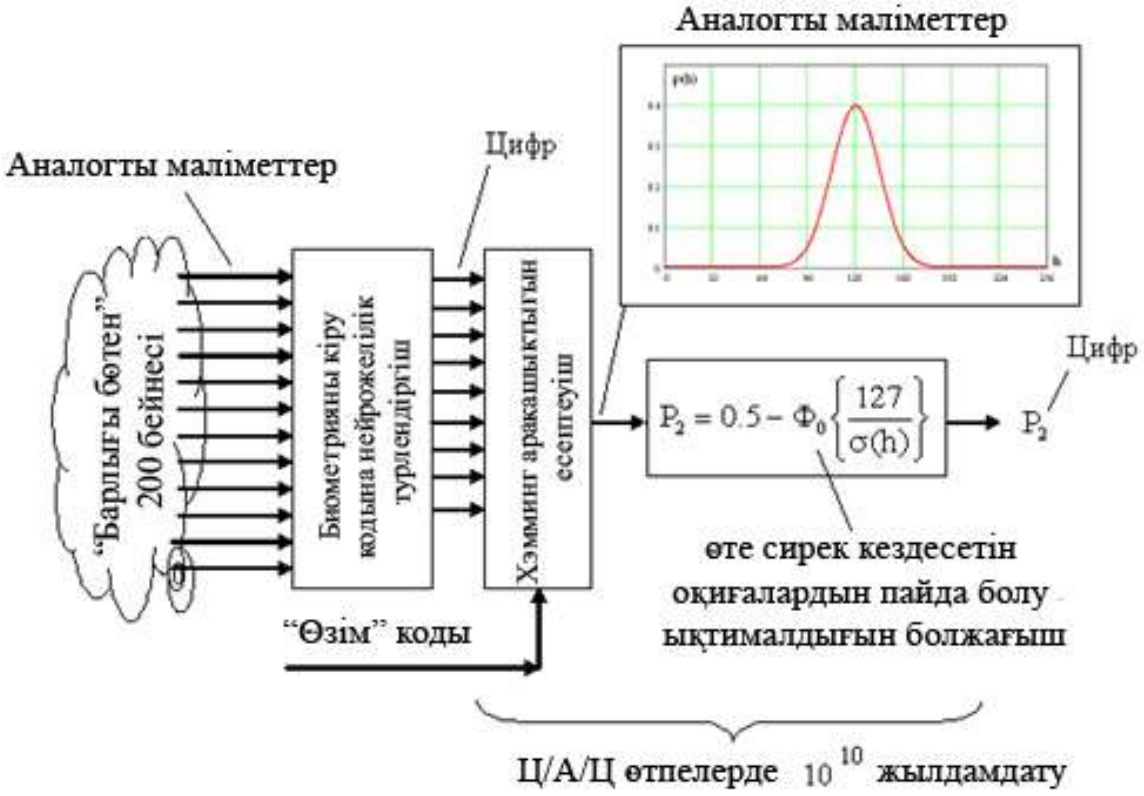
Ұзындығы 256 бит болатын биометриялық кодтар қаскүнемнің таңдаған шабуылына қарсы тұра алуды қамтамасыз ете алады, яғни «Өз» образы 10^{12} және таңдаудың жоғары әрекетін білмейді. Бұл қарапайым статистикалық әдіспен екінші тектес қателіктің пайда болу мүмкіндігін дұрыс бағалау үшін, олардың миллиардтаған «Бөтен» бейнелерінен тұратын тестілеу базасы талап етілетінін білдіреді. Мұндай базаларды талап ету қымбат, бұдан басқа, оларды қолдану олардың бір тектестігінің дұрыс нәтижесіне кепіл болмайды.

Ресейде бұл мәселе ұлттық МЕСТ Р 52633.3-2011 стандартымен шешіледі [106]. Осы стандартқа сәйкес әдеттегі кодтарды талдаудан Хэммингтің «Өзім» коды мен «Бөтен» кодының арасындағы қашықтықты статистикалық өңдеуіне өту қажет.

$$h = n - m \qquad (3.5)$$

Ресейдің ұлттық стандартымен ұсынылған тестілеу сұлбасы 3.15 суретінде келтірілген.

Әдеттегі кодтардың статистикасын зерттеуден Хэмминг кодтарының статистикасын зерттеуге көшуде ұтымдылық басым. Ол Хэмминг қашықтығын бөлудің үлкен мәні үшін дұрыс заңмен жақсы сипатталуымен шартты болады. Бұл «Өзім» және «Бөтен» кодтары коллизиінің сирек дискреттік жағдайының пайда болуын күтуден бас тартуына мүмкіндік береді. Хэмминг *E(h)* қашықтығының математикалық күтуін есептеу мен олардың «Бөтен» бейнелерінің небары 200 мысалынан стандартты ауытқуды $\sigma(h)$ есептеу жеткілікті. Миллиардтаған бейнелерді математикалық күту мен стандартты ауытқуда есептеу үшін дұрыс заңның қажеті шамалы. Дәл осы себепке байланысты түрлендіргіш биометрия-кодты тестілеу кезіндегі ұзындығы 256 бит коды үшін ұтымдылық 10^{10} –ды құрайды.



Сурет 3.15 – Екінші тектес қателіктер мүмкіндігін жылдам тестілеудің сұлбасы

«Өзім» шығыстық кодының ұзындығы кез-келген болуы мүмкін, код ұзындығының ұлғаю шамасы бойынша тестілеу уақытын қысқартудан ұтымдылық артатынын есте ұстаған жөн. Осы сәттегі аса бір шынайы ұтыс 10^{80}-ді құрайды. Барлық бұл жылдамдықтарды биномиалды заң $p = 0.5$ и $r \leq 0.37$ [61; 104] көрсеткіштері үшін дұрыс болатынына сүйене отырып алуға болады.

Түрлендіргіш биометрия-кодты тестілеу кезіндегі тағы бір маңызды сипаттама бірінші тектегі қателіктер мүмкіндігі болып табылады. «Өзім» бейнесінің биометриялық коды үшін бір корреляция мен нөлдік энтропияға сәйкес келетін мүлдем басқаша соңғы жағдай тән:

$$\begin{cases} |r| \approx 1 \\ H(n) \approx 0 \end{cases} \tag{3.6}$$

Бұл соңғы жағдайда мәліметтер тәуелсіздігінің гипотезасы мүлдем жұмыс жасамайды, шығыстық кодтың барлық разрядтары өте қатты корреляцияланған. Шарттарды орындау барысында қандай соңғы бөлуге ұмтылу қажет екенін білу дұрыс (3.6).

Жүргізілген зерттеулер биномиалды заңның ақырғы бөлуі бостандық дәрежесінің нөлдік санымен χ^2 бөлу болып табылатынын көрсетеді:

$$P(n,h,p\approx 0.5,r\to 1)\to \chi^2(\omega\approx 0)\,, \tag{3.7}$$

мұндағы ω – Хэммингтің нормаланған арақашықтықты сипаттайтын, «Өзінің» тәжірибесінде алғашқы бас тартуында табылған, алғашқы жақындаудағы бостандық дәрежесінің саны:

$$\omega=\frac{h}{k} \tag{3.8}$$

Егерде k тәжірибесін жүргізуде Хэмминг арақашықтығының нөлсіз мәнімен бірнеше қате табылса, онда χ^2 бостандық дәрежесінің санын бөлу Хэммингтің орташа арақашықтығы ретінде есептеледі:

$$\omega=E(h)\approx\frac{1}{k}\sum_{i=1}^{k}h_i \tag{3.9}$$

k тәжірибесінен тұратын сынақ сериясын жүргізгенде қол жеткізуге қарсылық фактісі табылмады, бостандық дәрежесінің санын есептеу гипотезадан бастау алуымен іске асырылады, келесідегі (k+1) сынағында бір битке тең минималды қате табылады:

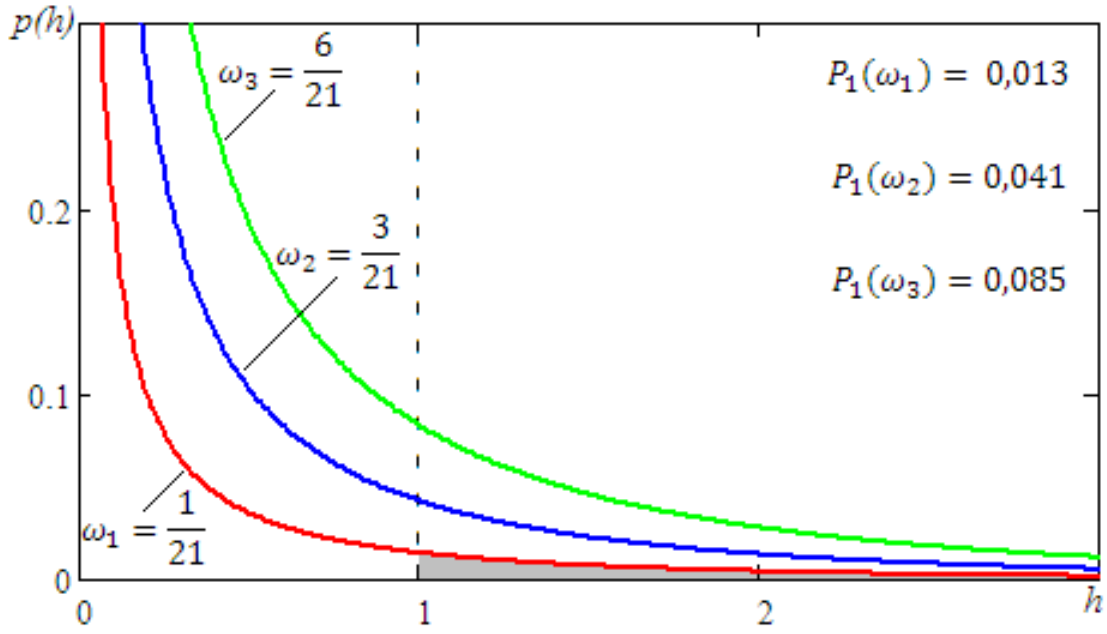
$$\omega=\frac{1}{k+1} \tag{3.10}$$

Тестілеу уақытын үштен 10 есеге дейін қысқартса, бірінші тектес қателік мүмкіндігін бағалауды мынадай формуламен орындаған жөн:

$$P_1\approx\int_1^{\infty}\frac{1}{2^{\frac{\omega}{2}}\cdot\Gamma\left(\frac{\omega}{2}\right)}\cdot x^{\frac{\omega}{2}-1}\cdot e^{-\frac{x}{2}}\cdot dx\,, \tag{3.11}$$

мұндағы $\Gamma(.)$ – функция гаммасы.

(3.11) формуласы бойынша бірінші текті қателіктің мүмкіндігін бағалау мысалдары 3.16-суретінде келтірілген.



Сурет 3.16 – Бостандық дәрежесі санының аз көрсеткіштерімен хи-квадратбөлу бойынша бірінші тектес қателіктер мүмкіндігін бағалаудың мысалдары

Корреляцияның орташа көрсеткіштерін есептеу «Өзім» коды разрядтарының арасында келесідегідей формула бойынша жүргізіледі:

$$r \approx (1 - \frac{2 \cdot E(h)}{\mathrm{n}}) \qquad (3.12)$$

Биометриялық кодтың ұзындығы n биометриялық мәліметтер арасында корреляция коэффициенттерінің орташа модулін бағалау кезінде маңызды рөл атқара бастайды. (3.12) формуласы дөрекі жақындау болып табылады және корреляция модульдері коэффициенттерінің өте үлкен мәндері үшін ғана жұмыс істейді. Нақты тура есептеу үшін Хэммингтің орташаквадрат ауытқуының арақашықтығын қосымша есепке алған жөн [47].