O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI URGANCH FILIALI

MADAMINOV XUSHNUD MADAMINOVICH

OZOVNI TANISH ALGORITMLARI

mavzusida

REFERAT

Urganch – 2017 y.

1. **Kirish**
2. Autentifikatsiya tizimlari ishonchligini ta’minlovchi vositalarni o’rganish.
3. 2.Ozovni tanish algoritmlari asosida dasturiy ta`minot ishlab chiqish.

Kirish.

Respublikamiz o’z mustaqilligiga erishganidan so’ng jamiyatimizda bir qator qonunlar va umummilliy dasturlarlarning qabul qilinishi, huquqiy demokratik jamiyatni barpo etishda va buyuk kelajak sari olg’a qadam qo’yishimizda mustaqil poydevor bo’lib xizmat qilmoqda. Respublikamizda barcha soha singari ta’lim tizimida axborot texnologiyalaridan samarali foydalanishga katta e’tibor qaratilmoqda. Shu sababli Respublikamizda axborot texnologiyalarini rivojlantirishga doir bir nechta davlat qonunlari, farmonlari va Prezident qarorlari qabul qilindi. Jumladan: O’zbekiston Respublikasi Prezidentining “Zamonaviy axborot-kommunikatsiya texnologiyalarini yanada joriy etish va rivojlantirish chora-tadbirlari to’g’risida”gi qarori (21 mart 2012 y.) va boshqalar.

Ta’lim tizimidagi islohotlarni amalda joriy qilishda o’qitishning ilg’or pedagogik texnologiyalarini qo’llash asosida talabalarga jahon andozalardagi bilim, ko’nikma, malakalarni shakllantirish o’quv jarayonini moddiy – texnika va axborot bazasi bilan ta’minlash yuqori darajali malakali kadrlarni tayyorlash sifatli o’quv – uslubiy, ilmiy hamda didaktik materiallar yaratish, ta’lim tizimi fan va ishlab chiqarish o’rtasida o’zaro samarali aloqadorlik o’rnatish, ta’limning dolzarb masalalardan hisoblanadi.

Hozirgi kunda vujudga kelgan iqtisodiy sharoit yangicha tafakkurga ega bo’lgan , dunyoga yangicha ko’z bilan qaraydigan , yangicha fikrlaydigan yangi avlodning ishtirokini taqazo etmoqda. Bu ish qanchalik tez amalga oshirilsa mamlakatimiz iqtisodiy salohiyati shunchalik tez yuksaladi. Bu o’rinda yoshlarning matematik tayyorgarligiga qo’yiladigan talablar ham juda muhim masala hisoblanadi.

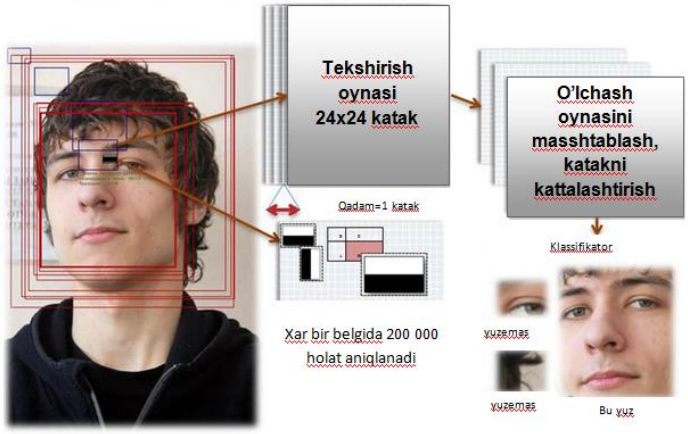
1. Autentifikatsiya tizimlari ishonchligini ta’minlovchi vositalari.

Axborot texnologiyalarni rivojlanishi har bir mamlakat uchun ish unumdorligini oshishi, sifati va eng asosiysi ish samaradorligi yuqori darajada bo’lishini ta’minlab beradi. O'zbekiston Respublikasi mustaqillik yillari axborotlashtirish sohasida inqilobiy o'zgarishlar davrini boshdan kechirmoqda. Zamonaviy axborot-kommunikatsiya texnologiyalari qulayliklar yaratish bilan bir qatorda yangi muammolarni ham o'rtaga qo'ymoqda. Bundan kelib chiqib ushbu maqolada kompyuter tizimlari rivojlanayotgan bir vaqtda tarmoqdan foydalanishda xar bir foydalanuvchini shaxsini aniqlash va unga ma’lum huquqlar berish masalalariga bag’ishlangan.Videokuzatuv vositlari orqali tasvirlarni tanib olishning onlayn va oflayn usullaridan foydalanib foydalanuvchilarni legalligini aniqlash eng samarali usul hisoblanadi. Ushbu dastur tasvirlar (yuz, ko’z, burun va lab) o’lchamlarini ma’lumotlar omborida saqlab keyingisi bilan taqqoslaydi va mos kelsa ushbu shaxs legal hisoblanadi. Bu dastur boshqa shu turdagi dasturlardan ishonchliligi bilan ajralib turadi va yuqorida ko’rsatilgan muammolarni yechishga yordam beradi.

Yuzni kalit nuqtalarini tanib olish quyidagi algoritm asosida amalga oshiriladi:

- Qo’llaniladigan rasm uchun tekshiruv oynasi tanlanadi va tegishli belgilar olinadi;
- Shuningdek, tekshiruv oynasi rasm bo’ylab bir katakka siljish bilan ketma-ket boshlanadi (bizda oynada 24x24 katak bor). Tekshiriluvchi rasmda belgilarni 200 000variantda ifodalash mumkin;
- Xar xil o’lchamlarni tekshirish ketma-ket qo’llaniladi;
- O’lchamini soddalashtirish rasm uchun emas, u faqat oyna uchun(katak o’lchami o’zgaradi);
- Xamma topilgan belgilar klassifikartorga beriladi.

Xamma belgilarni topish va aniqlash uchun oddiy kompyuter shart emas. Shuningdek, sinflashtirish qurilmasi faqat aniqlangan belgilarnigina o’zini aniqlaydi.



1-rasm.Katakdagi piksellarni ifodalash.

Ushbu yuqorida berilgan algoritm ikki va uch o’lchamli tasvirlash uchun juda qulay hisoblanadi. Chunki tasvir vaziyati o’zgargan taqdirda xam piksel(nuta) o’lchami o’zgarmaydi.

Ushbu tezisda elektron raqamli imzoning jamiyat hayotida olib keladigan qulayliklari, u yechishi mumkin bo’lgan masalalar va tatbiq qilsh jarayonlari keltirilgan. Shu bilan birgalikda, raqamli imzoni shakllantirish va tekshirish jarayonlarida xesh funksiyaga qo’yiladigan talablar va xesh funksiyadan foydalanishda kelib chiqadigan yengilliklar sanab o’tilgan.

Bugun zamonaviy axborot-kommunikatsiya texnologiyalarini qo‘llagan holda axborot almashishning elektron uslubiga o‘tish jarayoni jadallashmoqda. Elektron hujjat almashish xizmatlariga davlat boshqaruvi, tijorat faoliyati, moliyaviy operatsiyalarni amalga oshirish va boshqa turli sohalarda talab ortib bormoqda.

2003-2004-yillarda Prezidentimiz Islom Karimov tashabbusi bilan mamlakatimizda axborot-kommunikatsiya texnologiyalarini rivojlantirishga qaratilgan qator qonun hujjatlari qabul qilindi. “Elektron raqamli imzo

to’g‘risida”gi qonun shulardan biridir. Ushbu hujjatga binoan elektron raqamli imzo o’z qo’li bilan qo’yilgan imzoga tenglashtirilgan va u bilan bir xil yuridik kuchga ega. “Elektron hujjat aylanishi to’g‘risida”gi qonun esa elektron raqamli imzo (ERI) majburiy rekvizitlaridan biri hisoblangan elektron hujjatning yuridik kuchini, “Elektron tijorat to’g‘risida”gi qonun elektron tijoratni huquqiy tartibga solish jihatlarini belgilaydi. Hozirgi kunda ERIni qo‘llagan holda, elektron hujjat aylanishini keng joriy etish va qo‘llash jarayonlarini faollashtirish, eng dolzarb muammolarni aniqlash, ko‘rib chiqish va hal qilish uchun keng ko’lamdagi chora tadbirlar olib borish muhim ahamiyat kasb etadi.

Elektron raqamli imzo hujjatlardagi qo’yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab bo’lib, shaxsiy imzolarning mualliflarini hozirgi zamonaviy ilg’or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin. Ammo ERI xususiyatlari bundan farqli bo’lib, ikkilik sanoq sistemasi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog’liq.

ERI axborot kommunikatsiya tarmog’ida elektron hujjat almashinuvi jarayonida quyidagi uchta masalani yechish imkonini beradi:

– Elektron hujjat manbaining haqiqiyligini aniqlash;

– elektron hujjat yaxlitligini (o’zgarmaganligini) tekshirish;

– elektron hujjatga raqamli imzo qo’ygan sub’ektni mualliflikdan bosh tortmasligini ta’minlaydi.

ERIning umumiy tan olingan sxemasi (modeli) uchta jarayonni o’z ichiga oladi:

– ERI kalitlarini generatsiyalash;

– ERIni shakllantirish ;

– ERIni tekshirish (haqiqiyligini tasdiqlash).

Ma’lumot almashinishidan oldin ERI kalitlari generatsiya qilingan va o’z

egalarida mavjud bo’lishi kerak. Imzo qo’yish muallif tomonidan, faqat unga ma’lum bo’lgan maxfiy kalit asosida amalga oshiriladi. Imzoning haqiqiyligini tekshirish esa istalgan shaxs tomonidan, imzo muallifining ochiq kaliti bilan amalga oshirilishi mumkin.

Raqamli imzo bitlar ketma-ketligida ifodalangan biror sondan iborat. Shuning uchun uni boshqa elektron hujjatlarga ko’chirish yoki o’zgartirish kiritish katta qiyinchilik tug’dirmaydi. Shuning uchun elektron hujjat almashinuvi tizimida ERIni qalbakilashtirishning oldini olish chora-tadbirlari – ERI algoritmining elektron hujjatlarni qalbakilashtirishga bardoshlilik masalasini yechish talab etiladi. Zamonaviy ERI algoritmlari standartlarining bardoshliligi diskret logarifmlash, parametrli algebradan foydalanish va elliptik egri chiziq ratsional nuqtalari ustida amallar bajarish kabi masalalarga asoslangan. Shu bilan birgalikda ERIni shakllantirish va uni tekshirish jarayonining bardoshli bo’lishi va tezkorligini ta’minlashda xesh funksiyalar quyidagi xususiyatlarga ega bo’lishi kerak:

– kolliziyaga bardoshlilik, bu ERIni qalbakilashtirishdan himoyalaydi;

– chiqish bitlarining qisqaligi, bu xususiyat ERIni tezkorligini ta’minlaydi;

– uzatiladigan ma’lumotdagi kichik o’zgarish xesh qiymatni keskin o’zgarishiga olib kelishi, bu xususiyat ma’lumot o’zgarishidan himoyalaydi.

ERI algoritmida xesh funksiya algoritmning bir qismi hisoblanmaydi, shuning uchun ixtiyoriy ishonchli xesh funksiyalardan foydalanish mumkin. ERIda xesh funksiyalardan foydalanish quyidagi qulayliklarni keltirib chiqaradi:

– Hisoblashlardagi osonlik. Odatda xesh funksiya ma’lumotning kirish hajmini bir necha barobar qisqargan ko’rinishga olib keladi va xesh funksiyani hisoblash ancha tezkordir. Shuning uchun ma’lumotni xeshlash

va uni imzolash jarayoni faqat ma’lumotning o’zini imzolash jarayonidan oson va tez hisoblanadi;

– Leksik bir xillik. Imzolanishi kerak bo’lgan ma’lumot qanaqa turda yoki alifboda bo’lishidan qat’i nazar xesh funksiyadan chiqadigan format imzolovchi vosita formati bilan mos keladi;

– Butunlik. Xesh funksiyani ishlatmasdan imzolangan elektron ma’lumot katta hajmdan iborat bo’lganda bir necha qismlardan iborat bo’lishi mumkin va uni tekshirish jarayonida qismlar ketma-ketligi o’zgarib qoladi. Xesh qiymat imzolanganda imzo hajmi qisqa va butun saqlanadi.

Yuqoridagi xususiyatlarni o’z ichiga olgan xesh funksiya milliy standartimiz - O’zDSt 1106:2009 asosida Elektron raqamli imzoning standarti – O’zDSt 1092:2009 ishlab chiqilgan bo’lib, ularning bardoshliligi parametrli algebraga asoslangan. Mazkur muammolar yangi matematik murakkabliklar hisoblanib ularni hal etish usuli hali taklif etilmagan.

Xulosa o’rnida shuni ta’kidlash kerakki, ERIning xesh funksiyadan foydalanilgan va foydalanilmagan algoritmlarida butunlik va tezkorlik kabi xususiyatlarida katta farq mavjud. Xesh funksiya algoritmining qanchalik to’g’ri tanlanishi, ERIning bardoshliligini oshirishga va axborot xavfsizligini oshirishga xizmat qiladi.

Ma’lumot himoyasini ta’minlashda, quyida ko’rsatilgan ma’lumot obyektlari va birliklarining qaysi birini himoyalash lozimligi aniqlanadi: berilgan qiymatlar maydoni yozuvlar, fayllar, dasturlar, disklar va hokazo, ofydalanuvchining ishlashiga ruhsat berish jarayoni va vakolatlari aniqlanadi.

Himoya tizimlarini loyihalashda himoya buzilishining turlarini turkumlash kata ahamiyatga ega, ya’ni kiritilgan qiymatlarni o’qib olish, o’zgartirish, ma’lumotlari buzish.

Ma’lumotlarni kiritiladigan qiymatlari, maullifning roziligini olgan

foydalanuvchi orqali, shuningdek eshitib olish, ekrandan ko’rib olish, ish jarayonini yopmagan foydalanuvchi ketidan EHMdan foydalanish va axborotlarni aloqa tarmoqlari orqali tutip olish usuli bilan ochiladi va oshkor etiladi. Disklar paketi, lentalardigi nusxalarini va ko’chma vinchesterlar ham o’grilanishi mumkin.

Ma’lumot qiymartlarini buzishning eng sodda usuli- ma’lumot manbasini jismoniy buzish. Ma’lumotlar omborini noto’g’ri toldirish va yangilashda ham ma’lumot qiymatlari yo’qolishi mumkin. Ma’lumotlar omborini boshqaruv tizimini buzib ham yakson qilish mimkin. Tizimga viruslar va boshqa buzuvchi dasturlar kirishi ayniqsa havflidir. Ma’lumotlar omboridan foydalanish imkoniyatining yo’qolishi- uning buzilishiga tenglashtiriladi.

Ma’lumotlarni himoyalashning asosiy omillari quyidagilardan iboratdir:

-tizimga yaratish jarayonida himoya vositalarini kiritish;

-himoyalashning ko’p pog’onali kompleks va egiluvchan tizimlari;

-iqtisodiy zarurligi ma’lumotni ochilishi yoki buzilishidan ko’rilgan zaralarni himoya chora-tadbirlarining qiymat bilan solishtirish;

-himoya vositalari va usullarini standartlashtirish va uyg’unlashtirish.

Ma’lumotlarning omboridan foydalanishni boshqarishda, birinchi navbatda foydalanuvchining shaxsini aniqlash, vakolatini tekshirish katta ahamiyatga egadir. Shaxsini aniqlashda odatda paroldan foydalaniladi. Parolning hususiy ko’rinishi- algoritmik: ya’ni foydalanuvhci mashina taklif etgan tasodifiy son bilan mahfiylashtirilgan amal bajariladi, natijasi esa mashina xotirasidagi bilan solishtiriladi.

Foydalanuvchining shaxsi odatda fismoniy kalit- magnit kartasi, kontaktli plastina, barmoq izi, kaft o’lchamlari va boshqalar bilan tekshiriladi.

Keltirilgan himoya usullari nihoyatda mas’uliyatli holatlarda

kriptografik himoya(kiritiladigan ma’lumot qiymatlarini avtomatik ravishda shifrlash) bilan birga ishlatiladi.

Ma’lumot saqlaydigan magnit manbalarini o’girlash va ma’suliyatini aloqa tarmoqlari orqali tutib olishdan saqlashning nisbatan ishonchli bo’lgan birda bir usuli shifrlashdir.

Ozovni tanish algoritmlari asosida dasturiy ta`minoti

Dastlabki olimlar tomonidan ovoz orqali boshqariladigan nogironlar aravachasi prototipi yaratilgan edi.Ushbu nogironlar aravachasi harakatlanish bilan bog’liq muammolari bor va ba’zi mexanik qurilmalardan foydalana ololmaydigan,masalan, joystick ular bilan muammolari bor jismoniy cheklangan odamlar uchun ishlab chiqilgan.Shu sababli olimlar nogironlar aravachasini boshqarishning boshqacha yo’lini ovoz orqali boshqarishni ishlab chiqishdi.

Loyihani ishga tushirish 2003-yil sentabrda boshlandi.Ishning qanchalik yirikligi haqida tassavurga ega bo’lish uchun,loyihaga Mexatronika va Kompyuter Ilmi yo’nalishidagi 11 ta talaba , 5 tasi birinchi qismida va 6 tasi ikkinchisiga biriktirilgan edi.Loyiha bir yilda muvaffaqiyatli yakunlandi.

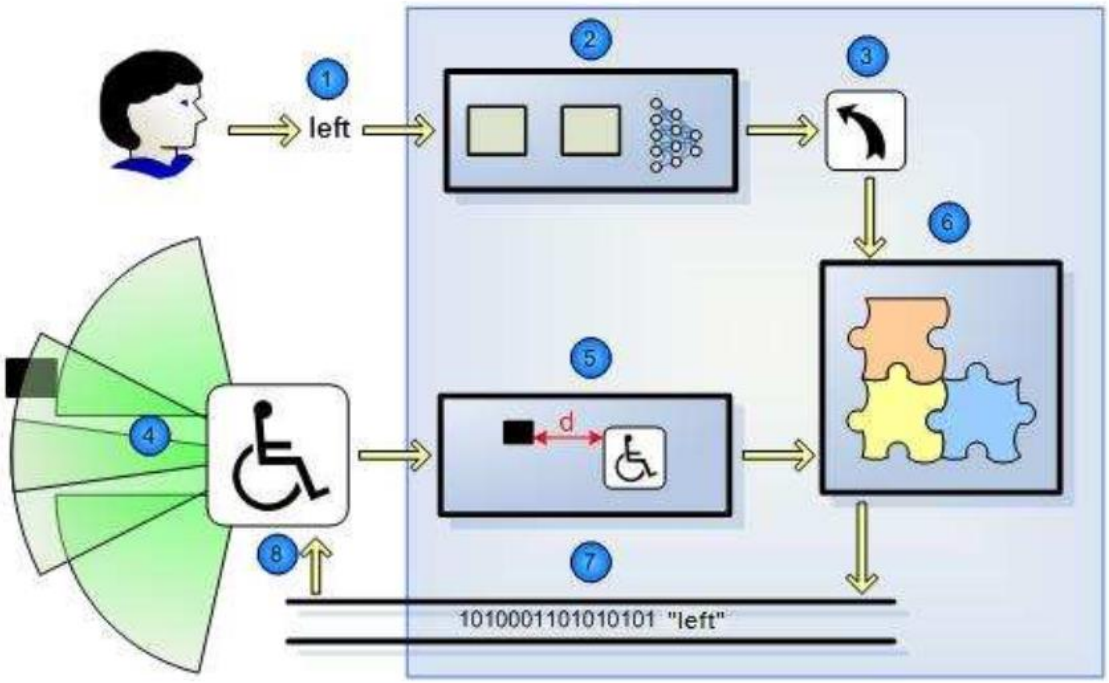
Birinchi qism aravachani boshqaradigan belgilangan nazorat moduli qurilmasi va atrofdagi ma’lumotni ,masalan, uzoq masofa, distansiyalardan ushlab qoladigan ultratovushli sensorlarning mos tizimilari birlashmasidan tashkil topgan.

Ikkinchi qism aravani boshqarish uchun ovoz kamandalarini aniqlash va tovushni tanib olish tizimini qurishni aniqlash maqsadida joylashtirilgan edi.

Loyihadan asosiy maqsad turli muhitlarda foydalanuvchi ovozini faxmlash va muntazam ravishda aravani boshqarish edi.Nutq orqali tanish

masalasi tabiiy va odamlar uchun oson hisoblanadi, ammo u haliham kompyuterlar uchun qiyin masala va hozirgacha mukammal yechimi topilmagan.

Umuman olib qaraganda, Nutq tovushlar yordamida boshqariladigan aravachaning va ultratovushli sensor net tizimi 1.1 Rasmda ko’rsatilgan va quyidagi chiqiqlarda tasvirlangan:



1.1 Rasm nogironlar aravachasining umumiy ishlash prinsipi

1. Nogiron odam buyruqni tovush orqali aytadi

2. Nutqni tanish tizimi tovush signalini amalga oshiradi,analiz qilib koeffitsientlar o’lchamini qisqartiradi va signal trayektoriyasini aniqlab oladi.Natija mos holdagi kodlashtirilgan va aniqlangan buyruq bo’ladi.

3. Buyruq o’zi barqarorligi saqlanishi va bajarilishi kerak bo’lgan tizimning qismiga jo’natiladi.

4. Dinamik to’siqlar qurshovidagi arava bajarilishi jarayonida ultratovush sensor net to’qisqacha masofani o’lchash orqali hamisha

kuzatilib turiladi.

5. Maxsus qurilgan komponenta to’siqacha bo’lgan masofani o’lchaydi.

6. Nazorat tizimi barcha kerakli axborotlarni to’playdi va ushlangan tovush komadasini bajarishga havfsiz ekanligini hal qiladi.

7. Aniqlangan tovush nogiron foydalanuvchiga va atrofidagi odamlarga hech qanday tahdid yo’qligini tasdiqlagan holatda , buyruq aravachaning amal bajarishiga yo’naltiriladi.

8. Nogironlik aravachasi buyruqni qabul qilib oladi va uni bajaradi.

Dastlabki ta’rifga binoan, barcha vazifalar nazorat tizimiga markazlashtiriladi va butun tizim asosan *Texas Instruments* tomonidan ishlab chiqariladigan DSP Card TMS320C6711DSK kartochkasida bajartiriladi. DSP protsessoriga dastur yozish uchun Code Composer Studio va shuningdek C dasturlash muhiti uchun Visual Studio .NET 2003 dasturi qo’llaniladi.

Shu vaqtgacha barchasi yaxshi ketayotgan edi ,ammo DSP Card buzilganida muammo paydo bo’ldi.Bunga nisbatan olimlar yangi turdagi DSP Card ga o’zgartirishni o’ylab qolishdi biroq ular u allaqchon urfdan chiqqan texnologiya ekanligini tushunib yetishdi.Shuning uchun qaror quyidagicha edi : DSP Card ni yangi turdagi bir xil vazifani bajaradigan maxsulot.U barcha kerakli interfeyslar ovoz signallarini ushlab olish uchun audio kiritivchi qurilma keyinchalik nutqni tanish vazifasini yaratish yoki ultratovush sensor tizimi uchun CAN shinasi hisoblandi.Qo’shimcha ravishda, bu qurilma turli turdagi tizimlarni nazorat qilishga qodir bo’lishi , qo’llashga qulay , aravaga ulashga oson ,iqtisod tejaydigan kichkina hajmga ega bo’lishi kerak edi.

Loyihaning maqsadi va imkoniyatlari

Oldin eslatib o’tilganidek, loyihaning maqsadi buzilgan DSP Card larni to’liq tizimni nazorat qila oladigan va ba’zi kerakli xususiyatga ega masalan,

foydalanuvchining tovush signallarini amalga oshiruvchi audio interfeys(mikrofon), ultratovush sensorlar tarmoqni nazorat qiluvchi CAN shinasiga almashtirish edi: U yangi texnologiya qo'llashga qulay iqtisodiy taraflama arzon bo'lishi kerak edi.

Ko'plab chuqur izlanishlardan so'ng , ushbu xususiyatlarni o'z ichiga oluvchi Colibri XScale® PXA320 kompyuter modulini topdik.

Asosan, ushbu loyihaning imkoniyatlari yaqinda qo'llanilayotgan yangi texnologiyaga moslashtirilgan edi.

Shu vaqtgacha , shuni aytishimiz kerakki, bu unchalik ham oson topshiriq emasdi, asosan rivojlantrilgan kodga moslashtirish.Barcha C tilidagi yozilgan dastur DSP Cardga yo'naltriligani sababli, biz uni yangi qurilma va yangi texnologiya bilan moslashtirish uchun deyarli boshidan boshlashimizga to'g'ri keldi.Qo'shimchasiga, oldingi loyiha 11 ta talaba o'rtasida qilingan edi va hozirgi loyiha bitta odam tomonidan qilindi, biz maqsadimizni nutq orqali tanish tizimi bo'lagini yechishga qaratamiz va ko'proq Feature Extraction blokini aniqlashga qaraymiz.

Nutqni tanish masalasida hosil bo'ladigan chiquvchi ma'lumot tanish jarayonini osonlashtirish maqsadida FE bloki kelayotgan ma'lumotni,tovush signalini amalga oshirishi kerak.FE blokini ishlab chiqadigan ushbu loyihada qo'llanilgan yondashuv uni ikkita mos bloklar ostiga bo'ladi: birinchisi nutqni kodlashtirish texnikasiga asoslangan, va ikkinchisi kelajakdagi yaxshilashlar uchun SOM(ma'lumot o'lchamlilik qisqartmasi).

Qisqacha qilib aytganda, loyihaning asosiy hissasi quyidagicha:

Birinchisi bizning ehtiypjlarimizni qondiradigan yangi texnologiyani topish uchun bozor tadqiqotini olib boorish.Biz uni topdik va shuningdek uni adekvat rivojlantirish muhiti uchun tayyorladik.

Keyinchalik, biz to'liq audio yozgich va pleyr qurdik. Bu vazifa unchalikham kerakli emas edi, ammo undan ko'zlangan maqsad C++

dasturlash malakasini oshirish edi. Ushbu audio rekorder va pleyr bilan biz biror bir vaqt mobaynida ovozni yozib olishga qodirmiz, turli hil namunaviy tezliklar , turli o’lchamlar va nihoyat nutq kodlashtirishga o’xshagan kelasi jarayonlar uchun biz uni .wav faylida saqlay olamiz.Qo’shimchasiga biz yozib olingan signallarni ijro etishimiz va tinglashimiz mumkin bo’lamiz.

Nihoyat, biz ITU-Tning G.729 Tavisyasi ga asoslangan nutq tanish tizimi uchun FE blokini yaratdik.Bu tavsiya Chiziqli Bashorat Qiluvchi Kodlashtirishdan qo’llaniladigan nutq signallarning kodlashtirish uchun algoritmning tasnifini o’z ichiga oladi.Bu tavsiya shuningdek, qoniqtiradigan natijalarni oladigan o’zimizning dasturni qurish uchun namuna sifatida qo’llaniladigan C kodining electron nusxasini o’z ichiga oladi.