

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Развој система аутентификације на основу биометрије гласа

- Дипломски рад -

Ментор:

доц. др Александар Јевремовић

Студент: Милош Денић

Бр. индекса: 2009/200097

Београд, 2014.



УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Београд, Зорана Ђинђића 44

Кандидат: Милош Денић

Број индекса: 2009/200097

Смер: информатика и рачунарство

Тема: Развој система аутентификације на основу биометрије гласа

Задатак: Комбинацијом биометриских података на основу биометрије гласа унапредити систем аутентификације.

Датум одобрења рада:

Београд, ___.___._____.

МЕНТОР

_____

Проф. др Александар Јевремовић

ДЕКАН

_____

проф. др Драган Цветковић

Развој система аутентификације на основу биометрије гласа

Сажетак: Биометријски подаци представљају јединствене бихевиоралне особине појединаца на основу којих је могуће развити напредне системе аутентификације. До сада искоришћени биометријски подаци су: отисак прста, лице, ирис, глас и др.

У овом раду стављен је фокус на биометрију гласа која генерише податак. Тај податак је уствари производ низа звукова, вибрација гласних жица и њиховог положаја, облика и величина језика, усана и зуба. Карактеристике издвојене из говора су јединствене за сваког појединца. Управо на основу тих карактеристика могуће је развити један систем за аутентификацију појединаца. Обзиром да тренутни резултати показују да постојећи слични системи не постижу висок ниво безбедности, због недовољне количине информација које поседује овакав биометриски извор, у циљу превазилажења ових проблема, препоручујемо развој добро оптимизованог система који би се могао комбиновати са другим биометријским подацима у исте сврхе.

У овом раду ћемо подићи експериментално окружење на основу кога ће бити урађена евалуација комплетног предложеног система за потребе савремених сервиса аутентификације.

Кључне речи: (препознавање гласа, биометрија, аутентификација)

САДРЖАЈ

1. Увод ..... - 3 -

1.1 Предмет истраживања ..... - 3 -

1.2 Доприноси рада ..... - 4 -

1.3 Структура рада ..... - 4 -

2 Преглед у области истраживања ..... - 5 -

2.1 Аутентификација на основу биометрије гласа базирана на Теоплитзовим матрицама ..... - 5 -

2.2 Скривени Марковљеви Модели ..... - 7 -

2.2.1 Опис Марковљевог модела ..... - 7 -

2.3 Гаусова Мешавина модела ..... - 8 -

3 Теоријске основе истраживања ..... - 9 -

3.1 Биометријске методе ..... - 9 -

3.1.1 Отисак прста ..... - 9 -

3.1.2 Геометрија лица ..... - 10 -

3.1.3 Термограм лица ..... - 10 -

3.1.4 Геометрија руке и распоред вена ..... - 11 -

3.1.5 Скенирање ока ..... - 11 -

3.1.6 Препознавање гласа ..... - 12 -

3.1.7 Ход ..... - 12 -

3.1.8 Динамика потписа ..... - 13 -

3.1.9 Облик уха ..... - 13 -

3.1.10 Мирис тела ..... - 14 -

3.1.11 ДНК ..... - 15 -

3.1.12 Динамика куцања ..... - 15 -

3.1.13 УПОРЕЂИВАЊЕ БИОМЕТРИЈСКИХ МЕТОДА ..... - 16 -

3.2 Методи за прикупљање биометријских података ..... - 17 -

3.3 Аутентификација на основу биометријских података ..... - 18 -

3.4 Грешке у фази аутентификације ..... - 18 -

3.5 Унимодални и бимодални системи за аутентификацију ..... - 20 -

3.6 Развој система аутентификације на основу биометрије гласа ..... - 21 -

3.7 Настанак говорног сигнала ..... - 23 -

3.8 Механизам производње говора ..... - 24 -

3.9 Предности и недостаци биометријских решења ..... - 25 -

4 Преглед предложеног решења ..... - 27 -

4.1 Генеричка шема предложеног решења ..... - 27 -

4.2 Поставка и објашњење експерименталног окружења ..... - 28 -

4.3 Спроведене анализе и експерименти који су претходили пројектовању целокупног решења ..... - 28 -

4.4 Процес снимања гласовних секвенци за потребе аутентификације - 29 -

4.5 Процес упоређивања гласовних секвенци за потребе аутентификације.- 29 -

4.6 Крос корелација „*Cross-Correlation*“ ..... - 29 -

4.7 Евалуација предложеног окружења са приказом експерименталних резултата - 32 -

4.8 Област примене предложеног решења ..... - 42 -

5 ЗАКЉУЧАК ..... - 42 -

5.1 Сумарни циљеви рада ..... - 42 -

5.2 Остварени резултати ..... - 42 -

5.3 Предлог за будући рад ..... - 42 -

Матлаб команде које су коришћене: ..... - 43 -

Литература ..... - 44 -

1. Увод

У науци је добро познато да су неке особине људског тела као што су: отисак прста, геометрија руке, лица и ува, начин писања, начин ходања, распоред вена, скенирање ока, препознавање гласа и др карактеристичне са сваку особу. Управо нам ове особине говоре да је за потребе аутентификације потребно искористити предности које нам пружа биометрија. Добро је познато да сваки систем, па чак и биометријски има своје мане и своје предности. У овом раду ће бити детаљно објашњено како је могуће остварити везу између биометрије гласа и традиционалних лозинки или четвороцифреног пина и на тај начин ће бити побољшан систем аутентификације на основу биометрије гласа.

Аутентификација се може извршити на три начина, а то су: на основу онога што имамо, на основу онога што знамо и на основу онога што јесмо. Комбинацијом онога што јесмо (биометрија) и онога што знамо (лозинка или пин) долазимо до двофакторског система који ћемо користити у процесу аутентификације. Овакавим системом се добија много виши ниво безбедности.

Да бисмо направили овакав систем подићи ћемо експериментално окружење у програмском језику Матлаб где ћемо на основу математичких функција корелације упоређивати говорне сигнале. У тренуцима када заједничка информација два говорна сигнала није на одговарајућем нивоу, увешћемо још један фактор аутентификовања, а то је лозинка или пин.

1.1 Предмет истраживања

Биометрија је техника која се све више користи, она представља аутоматизован метод утврђивања идентитета особе на основу његових физичких карактеристика, као што су: отисак прста, геометрија руке, лица и уха, начин писања, начин ходања, распоред вена, скенирање ока, препознавање гласа и др. У данашње време, с обзиром да потреба за вишим нивоима сигурности све више расте, биометријски системи су мањи, бржи, прецизнији, а самим тим и поузданији. Они налазе све већу примену у разним делатностима где је неопходно недвосмислено утврдити или потврдити идентитет неке особе.

Људски фактор и даље представља “рупу” у сигурности бројних данашњих система за аутентификацију. То су немаштовите лозинке у виду датума рођења, имена партнера или чланова породице, лозинке написане на папиру које су залепљене на неком видном месту, пин кодови који се чувају у новчанику итд. Све већа потреба за памћењем лозинки и бројева тера нас на сталну употребу истих шифара. Ту ускаче биометрија зато што она елиминише потребу за памћењем лозинки, јер смо лозинка уствари ми сами. Некада смо само у научнофантастичним филмовима могли да видимо системе засноване на биометрији, а данас их виђамо све чешће у предворјима зграда великих компанија, у државним институцијама, на аеродромима итд.

1.2 Доприноси рада

- Аутентификација рачунањем корелације говорног сигнала
- Коришћење лозинке или пина као додатни фактор заштите
- Извршена информационо теоријска анализа

1.3 Структура рада

Рад је урађен по стандардној структури за израду дипломских радова. У уводном делу је описано који је предмет истраживања рада, као и доприноси које ће произаћи из овог рада. Након тога је описано стање у области истраживања где је дат осврт на један рад који се бави сличним проблемом и описане су технике које се користе за аутентификацију на основу биометрије гласа. Такође у истом поглављу су описане предности и недостаци биометријских система у процесу аутентификације. Трећа област представља теоријску анализу процеса који је коришћен у практичном решењу. У четвртом делу се налази детаљно описан предложени систем са перформансама и приказаним резултатима. На крају овог дела су описане и области примене предложеног решења. Закључак нам доноси информације о сумираним циљевима рада, као и предлог за унапређење предложеног решења у неком будућем раду.

2 Преглед у области истраживања

Током истраживања тренутног стања у области аутентификације на основу биометрије гласа и двофакторске аутентификације дошли смо до неколико радова који се баве овим и сличним темама. У даљем тексту детаљно ћемо описати радове и достигнућа која су у њима постигнута.

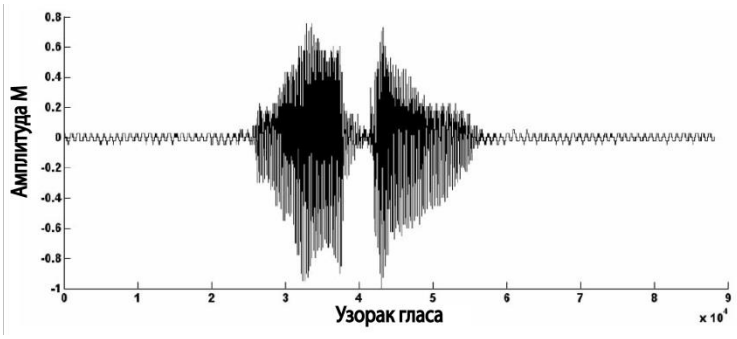
2.1 Аутентификација на основу биометрије гласа базирана на Теоплитзовим матрицама

Значај верификације и аутентификације на основу звукова и гласова има доказану своју практичну примену и значајну улогу у многим областима нашег живота и природе око нас. Главни алат који се користи у овом раду тј. математичка функција, базирана је на Теоплитзовим матрицама. Снимљени гласовни сигнали се филтрирају, обрађују и процењују у фреквентном спектру. Функција вектор се затим изводи из фреквентног спектра и Теоплитзове форме. Овакав вектор пружа јединствену биометријску информацију која разликује једну особу од друге. Главна идеја ове студије лежи у примени Теоплитзове матрице. Овај графички приступ обраде сигнала гласа за идентификацију људи доводи до новог биометријског приступа који може да пронађе своје место међу данашњим неконвенционалним методама за проверу људског гласа. [1]

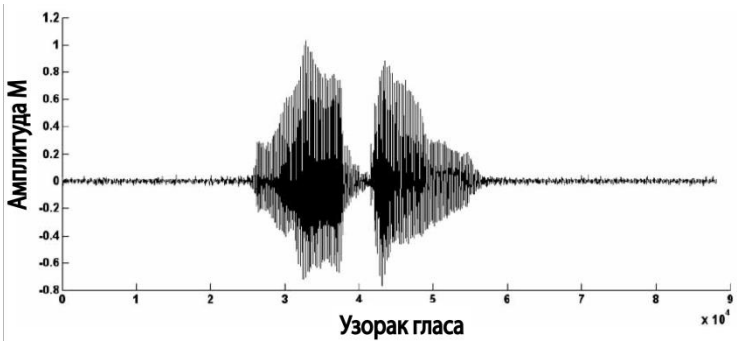


Сл. 1 – Теоплитзов дијаграм

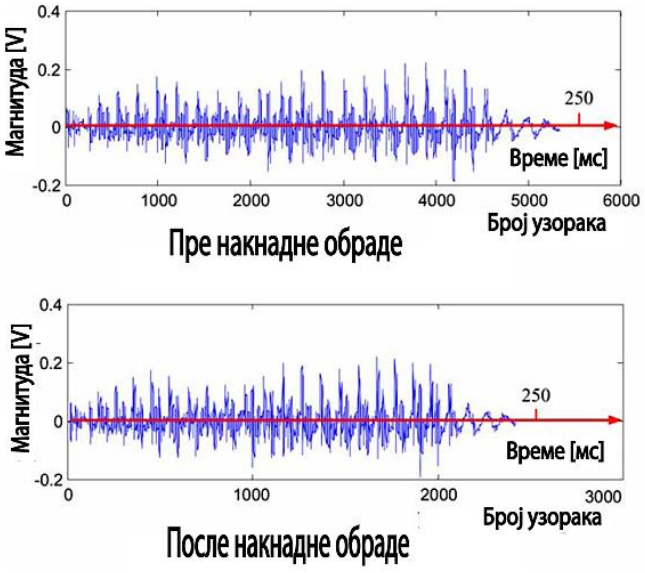
Улазни сигнал тј. глас се прво обрађује за класификацију и идентификацију. Обрада сигнала се на основу алгоритма извршава у програмском језику Матлаб. Забележени Сигнал се прво пропусти кроз филтер са фреквенцијом од 60 *Hz* (Сл. 2). Све фреквенције изнад 5 *KHz* се затим филтрирају са *HP* филтерима и добијени сигнал је семплован са 10 *KHz* (Сл. 3). Као резултат процеса накнадне обраде сигнала, број узорака је значајно смањен на мање од половине њиховог укупног броја информација без губљења корисне информације. Ово значајно смањује време за обраду (Сл. 4 показује смањење узорака од 6000 до 3000 за исто време обраде).



Сл. 2 – Оригинални гласовни сигнал



Сл. 3 – Гласовни сигнал после филтрирања



Сл. 4 – Гласовни сигнал пре и после обраде

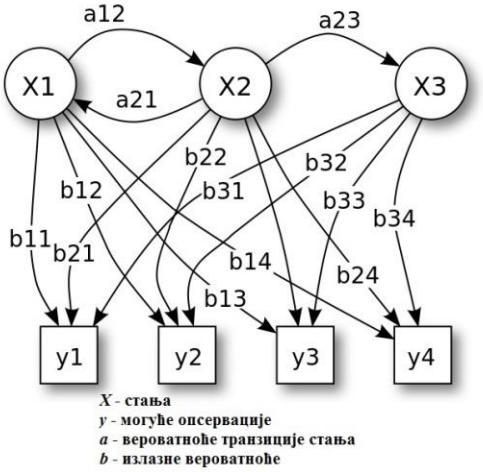
2.2 Скривени Марковљеви Модели

Код биометријских система препознавања гласа који су ограничени текстом (енг. *text dependent*) да би се податак унео у систем, корисник мора да изговори реч, или фразу која се углавном снима помоћу микрофона, а може и мобилним телефоном. Затим се узорак гласа конвертује из аналогног формата у дигитални формат. Када се то уради из сигнала се извлаче карактеристике појединца и креира се модел. Већина биометријских система препознавања гласа користи концепт скривеног Марковљевог модела (енг. *HMMs*) и он представља основне варијације и привремене промене у неком временском периоду, које се налазе у стањима које користи говор као што су квалитет, трајање, интензитет, висина тона и карактеристике тона. Скривени Марковљеви модели обезбеђују статистичко представљање звукова произведених од стране појединца.

2.2.1 Опис Марковљевог модела

У његовој дискретној форми, скривени Марковљев модел се може најјасније приказати као генерализација проблема урни: Дух се налази у једној соби која није видљива за посматрача. У тој скривеној соби постоје урне *X1*, *X2*, *X3*,... Свака од тих урни у себи садржи познату комбинацију кугли, а свака кугла је обележена са *y1*, *y2*, *y3*,… Дух бира урну и насумично извлачи кугле из ње. Дух затим кугле ставља на покретну траку на којој посматрач може да види изабрану секвенцу кугли, али не и секвенцу урни из које су изабране. Дух има неку своју процедуру којом бира урне. Избор урне за *n*-ту куглу зависи само од насумичног броја и извора урне за (*n-1*)-ту куглу. Избор урне није директно зависан од урни изабраних пре једне предходно изабране урне, стога се ово назива Марковљевим процесом.

Сам Марковљев процес се не може видети, једино је секвенца кугли видна зато се он и назива скривеним Марковљевим моделом. То је илустровано у доњем доле слике где се може видети да кугле *y1*, *y2*, *y3*, *y4* могу да буду извучене у сваком стању. Чак и ако посматрач зна садржај урни и треба да посматра само секвенцу од три кугле *y1*, *y2* и *y3* на покретној траци, посматрач још увек не може да буде сигуран из које урне је дух изабрао трећу куглу. Међутим посматрач може да одреди друге детаље, као што је идентитет урне из које је дух највероватније изабрао трећу куглу. [2]

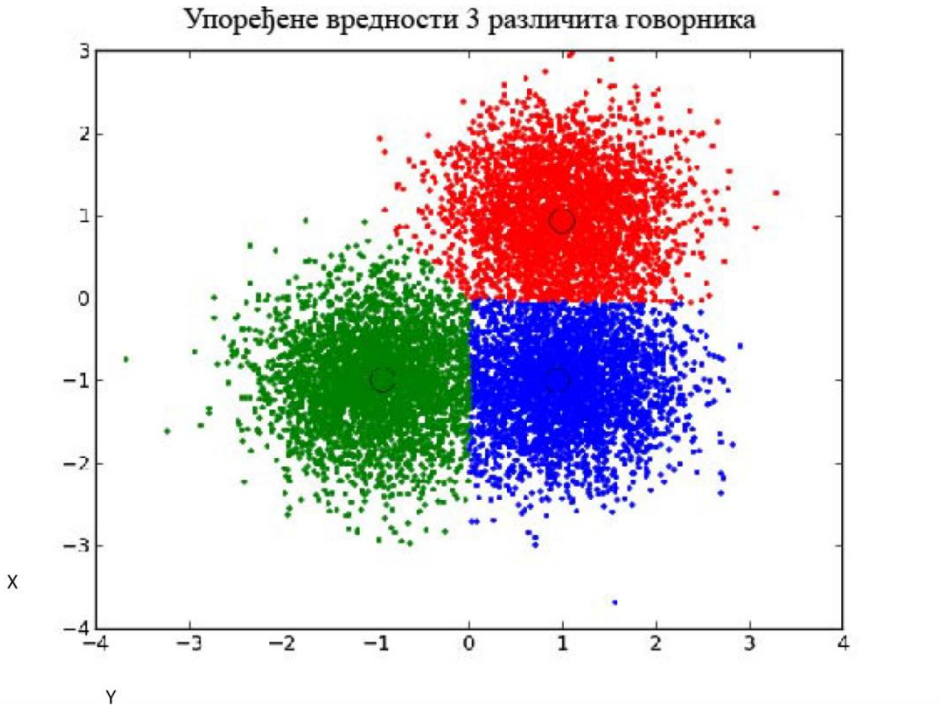


Слика 20 – Марковљев модел

2.3 Гаусова Мешавина модела

Други метод најчешће коришћен за преопознавање на основу биометрије гласа је Гаусова Мешавина модела (енг. *Gaussian Mixture Model)*. Овај метод је јако сличан скривеном Марковљевом моделу, али се он више користи код неограничених система који не зависе од текста (енг. *text independent*). Он функционише тако што користи глас од којег прави векторска стања која заступају разне звучне форме које су карактеристичне за понашање различитих појединаца. Оваквим начином рада, ове методе упоређују сличности и разлике улазног гласа са оним који се чувају у бази података и одлучују о томе да ли та особа јесте она за коју се представља.

Након уписа у базу података, током фазе препознавања, квалитет, трајање и јачина звука се издвајају из узорка, па се потом шаљу на упоређивање са већ снимљеним подацима свих говорника. Када се заврши фаза препознавања, добија се однос вероватноћа о томе ко је од упоређених говорника највише вероватан на основу претходно изведених карактеристика. [3]



Слика 5 - Гаусова метода

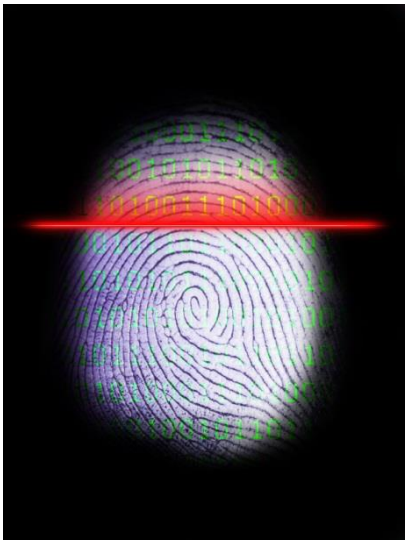
3 Теоријске основе истраживања

3.1 Биометријске методе

У науци постоји прегршт биометријских метода за утврђивање идентитета појединаца. У наставку текста поменућемо и описати неке од најпознатијих и најкоришћенијих у пракси.

3.1.1 Отисак прста

Када се помене биометрија прво на шта се помисли је отисак прста. Метода идентификације на основу отиска прста се користи још од најраније историје и употребљавали су је: Асирци, Вавилонци, Кинези и Јапанци. Овај начин утврђивања идентитета је распрострањен свуда у свету. Од 1897. године користи се за идентификацију криминалаца, што значи да данас постоји огромна база отисака прстију. Свака особа има јединствен отисак прста који се састоји од удубљења и испупчења. Постоје два начина узимања отиска прста. Први анализира само укрштања и завршетке завијутака отиска и заузима 250 бајта, док други прати целокупан правац сваке линије и заузима 100 килобајта. [9]



Слика 6 - Отисак прста

3.1.2 Геометрија лица

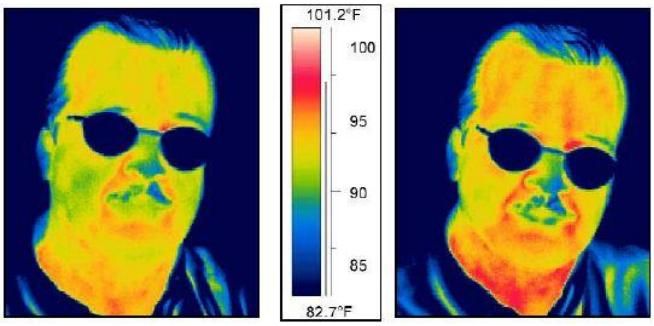
Лице представља основни начин на који разликујемо и памтимо особе, али ми људско лице доживљавамо као целину, док софтвер то ради на другачији начин. Приликом софтверског препознавања, лице се разлаже на 80 карактеристика, као што су: растојање између очију, ширина и дужина носа, јагодице, брада, облик вилице итд. Све те карактеристике се претварају у нумерички облик, а тај низ цифара се назива отисак лица. За успешно препознавање потребно је поклопити између 15 и 20 карактеристика, тако да се појединац може идентификовати чак и после пластичне операције. Технологија препознавања лица је изузетно популарна, јер слично отисцима прстију постоје велике базе фотографија. [9]



Слика 7 - Геометрија лица

3.1.3 Термограм лица

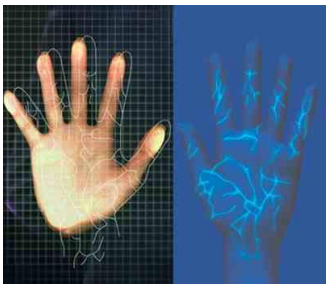
Термограм лица је најновија метода која има велику перспективу, али још увек није нашла своју комерцијалну примену. Лице сваког човека прожето је разгранатим мрежама крвних судова. Те мреже крвних судова су јединствене за сваког човека, па чак и за близанце. Из лица се шири топлина која се може очитати инфрацрвеном камером. Јединственост добијених биометријских узорака је велика и за разлику од методе препознавања лица, слике тј. узорци се могу прикупљати без обзира какво је позадинско светло. Јако је битно то да препознавање не зависи од израза лица, узраста и естетских операција. Због изузетно високе тачности и брзине препознавања овај метод је јако погодан за аутентификацију особа. Једини разлог због којег ова метода није нашла широку примену је скупа опрема. [7]



Слика 8 - Термограм лица

3.1.4 Геометрија руке и распоред вена

Геометрија руке није јединствена за сваког појединца као што је то отисак прста, стога се ова техника користи за верификацију идентитета, а не за саму идентификацију. Геометрија руке је процес у којем се врши анализа облика шаке и дужине прстију и у том процесу се узима око 90 параметара. Она се комбинује са анализом распореда вена на шаци и ова метода тражи места укрштања вена која праве карактеристичну шару. [7]



Слика 9 - Геометрија руке и распоред вена

3.1.5 Скенирање ока

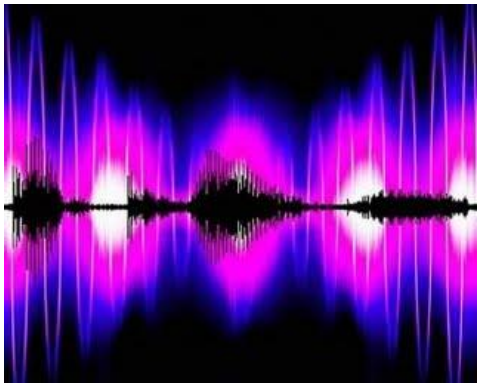
Ова јако популарна метода одређивања идентитета помоћу ока се ради на два начина: први је скенирање дужице ока (ириса), а други скенирање мрежњаче ока (ретине). Скенирање дужице се заснива на анализи појединости прстена у боји који окружује зеницу (ириса). На дужици постоји више од 200 тачака које се могу искористити за идентификацију као што су прстенови, бразде, пегице. Те шаре су јединствене за сваког појединца, чак се лево и десно око исте особе разликују. Скенирање мрежњаче користи индивидуалност крвних судова у дну ока. Овај вид идентификације је најпоузданији зато што не постоји начин да се мрежњача фалсификује, она се не мења током целог живота особе, а мрежњаче мртве особе толико брзо пропадну да није потребан начин утврђивања да ли је особа жива или не. [9]



Слика 9 - Скенирање ока

3.1.6 Препознавање гласа

Ова техника бележи ритам, фреквенцију, висину и тоналитет гласа. За снимање гласа могуће је користи обичан микрофон или мобилни телефон, мада се поузданост повећава употребом квалитетнијег микрофона. Ова метода има своје недостатке, те се највише користи у верификационе сврхе. Предност ове методе је у томе што је потребна опрема изузетно јефтина и сваки данашњи рачунар уз адекватан софтвер може се користити као платформа за препознавање гласа. Међутим, низак ниво поузданости препознавања гласа чини ову методу допунском уз неку другу поузданију биометријску методу. Такође се ова метода може унапредити тако што би се у њу уградио још један фактор аутентификације, нпр: пин код. [9]



Слика 10 – Препознавање гласа

3.1.7 Ход

Ход представља сложену просторно-временску биометрију понашања и није јединствен за сваког појединца, али је довољно карактеристичан да омогући проверу идентитета. Карактеристике хода се изводе из анализе видео материјала. Ова техника се све више развија, зато што се јавља све већа потреба за провером идентитета на великим раздаљинама, као и маскираних особа. [9]



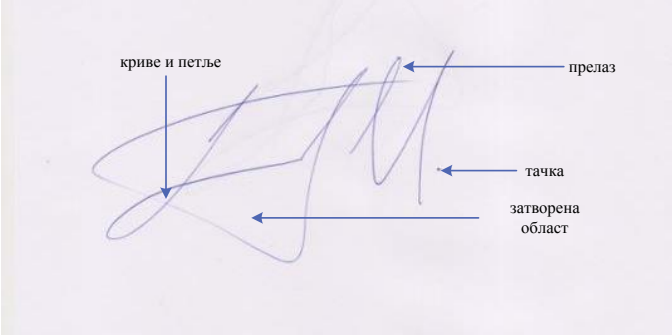
Слика 11 – Ход

3.1.8 Динамика потписа

Препознавање динамике потписа се заснива на начину на који настаје потпис и обично се не узима у обзир изглед самог потписа. Анализира се: смер, брзина, притисак, дужина, трајање и број потеза руке. Постоје два начина за утврђивање ових података:

- ✓ Плоча осетљива на додир (енг. *tablet*) региструје покрете и притисак оловке на површину.
- ✓ Паметна оловка која функционише као и свака друга. Ова оловка има у себи уложак који бележи покрете у све три димензије и притисак на површину.

Предност ове методе је у томе што се може утврдити фалсификовање потписа. Фалсификовање потписа може успети само ако неко детаљно анализира начин на који се корисник потписује. Величина добијених података из сваког потписа је 20 КВ, отисак добијен из 3 до 10 потписа заузима од 90 В до 1 кВ. Упркос величини отисака, једнаки удео у грешкама (енг. *equal error rate* - *EER*) је јако висок за ову методу и она није погодна за идентификацију. [7]

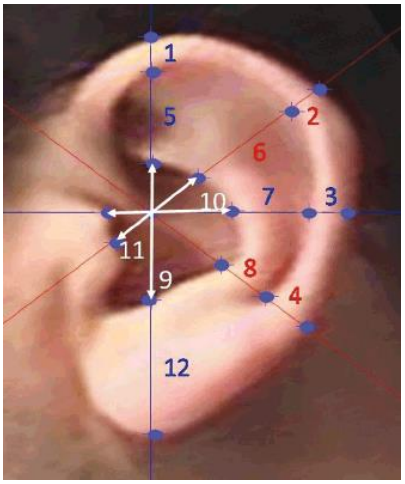


Слика 12 - Динамика потписа

3.1.9 Облик уха

Облик уха и структура хрскавог ткива на површини уха разликују се од особе до особе, али те карактеристике нису толико добре да би се на основу њих особа аутентификовала. Препознавање помоћу уха се заснива на поклапању вектора дужине испупчених тачака на површини уха до локације граничних тачака на уху. Иако ова метода даје фантастичне резултате потребно је још додатних истраживања како би се ова метода усавршила и одговорило на следећа питања:

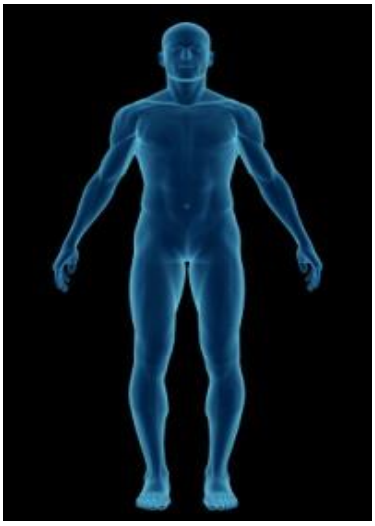
- ✓ Да ли се може извршити екстракција уха у разним условима са задовољавајућом поузданошћу?
- ✓ У случају када је ухо прекривено косом ова метода није применљива. Потребно је наћи одговор да ли је у овом случају могуће постићи делимичну аутентификацију и да ли би можда употреба термограма решила овај проблем? [7]



Слика 13 - Облик уха

3.1.10 Мирис тела

Познато је да сваки објекат лучи свој јединствени мирис који је карактеристичан за његов хемијски састав. Биометријски системи који су базирани на овој методи раде тако што сензори увуку ваздух који окружује особу, а сваки сензор је осетљив на одређену групу ароматских смеса. Поузданост оваквог мерења зависи од нормализације сваког сензора. Мирис тела има неколико функција међу којима су: комуникација, привлачење партнера, одбрана од напада и слично. Компонента мириса коју емитује људско или животињско тело се разликује за сваку јединку. Ова метода је још у фази истраживања зато што треба одговорити на питање да ли постоји утицај хемијских компоненти као што су: дезодоранс, сапун и слично на квалитетну детекцију мириса. [7]



Слика 14 - Мирис тела

3.1.11 ДНК

ДНК је једнодимензионална јединствена ознака за нечију индивидуалност, а највише се користи за аутентификацију у форензици. Већина људских ДНК идентична је за целу људску врсту, мада постоје и мале варијације код неких популација. С обзиром да се из ДНК могу добити и приватни подаци као што су разне врсте болести и слично, оваква идентификациона техника још увек није толико популарна код крајњих корисника.



Слика 15 – ДНК

3.1.12 Динамика куцања

Ова метода се развила још за време Другог светског рата код радиотелеграфа. Тада је уочено да се на основу брзине куцања могу лако разликовати пошиљаоци порука. Данас се говори о динамици куцања, али у контексту куцања на тастатури. Значај ове технике темељи се на временском размаку између притискања дугмади на тастатури. Одређени софтвери врло лако могу разликовати особе на основу ове методе.



Слика 16 - Динамика куцања

3.1.13 УПОРЕЂИВАЊЕ БИОМЕТРИЈСКИХ МЕТОДА

Методе	Лице	Отисак прста	Геометрија длана	Ирис	Мрежњача	Глас	Ход
Универзалност	**висока**	**средња**	**висока**	**висока**	**висока**	**средња**	**средња**
Јединственост	**ниска**	**висока**	**средња**	**висока**	**висока**	**ниска**	**ниска**
Трајност	**средња**	**висока**	**средња**	**висока**	**средња**	**ниска**	**ниска**
Прикупљивост	**висока**	**средња**	**висока**	**средња**	**ниска**	**средња**	**висока**
Изводљивост	**ниска**	**висока**	**средња**	**висока**	**висока**	**ниска**	**ниска**
Прихватљивост	**висока**	**средња**	**средња**	**ниска**	**ниска**	**висока**	**висока**
Варање	**ниска**	**висока**	**средња**	**висока**	**висока**	**ниска**	**средња**

Табела 1 – Упоређивање биометриских метода [8]

Универзалност – свака особа би требала да има овакву карактеристику.

Јединственост – описује колико добро биометријска метода разликује две особе.

Трајност – описује колико је биометријска метода отпорна на старење.

Прикупљивост – описује колико је тешко прикупити биометријске узорке.

Изводљивост – описује прецизност, брзину и робусност система.

Прихватљивост – описује прихватљивост методе у свакодневном животу.

Варање – описује колико је тешко преварити систем за препознавање.

3.2 Методи за прикупљање биометријских података

Сваки биометријски систем има своје предности у зависности од тога где се примењује и која се метода користи. За корисника први сусрет са системом представља прикупљање његових биометријских података и упис у базу података. Овај процес се може поделити у неколико фаза приказаних на слици.



Слика 17 - Прикупљање биометријских података

У првој фази се обавља прикупљање корисникових биометријских података на уређају за очитавање. Први узорак је кључан за даљу аутентификацију, зато се велика пажња мора посветити квалитету узетог узорка. Процес учитавања се по потреби може поновити више пута како би се добили задовољавајући резултати. Уколико се након поновљеног учитавања не добије довољно квалитетан резултат, корисник улази у скуп неуспелих регистрација. (енг. *fail to enroll - FTE*). У другој фази се затим анализирају добијени необрађени подаци на начин на који се из њих издвоје параметри који су карактеристични за корисника. Добијени подаци су биометријски отисци, (енг. *biometric template*) који често може да садржи у себи више узорака у зависности од тога која од биометријских метода се користи. Биометријски отисак се у трећој фази складишти у базу података са осталим подацима о кориснику.

Постоје три класична приступа складиштења података:

- ✓ Локално складиштење на уређај је сигуран и брз начин аутентификације. Овај приступ неупотребљив је у ситуацијама када је потребна могућност аутентификације као што је случај код банкомата.
- ✓ Складиштење података на удаљену локацију при чему подаци морају да се размењују преко сигурне везе. Овај начин је добар зато што омогућава аутентификацију са различитих локација, али корисници који држе до своје приватности се не слажу са тиме да се њихови подаци чувају у централној бази података.
- ✓ Складиштење података на преносивим медијима као што су паметне картице, решава проблеме у претходно наведеним примерима. Подаци се не чувају у централној бази и не путују мрежом, већ их корисник сам носи на жељене локације. Једини мана је у томе што овакав систем за аутентификацију треба бити опремљен и читачем преносног медија.

3.3 Аутентификација на основу биометријских података

Процес верификације састоји се од провере поклапања свежих биометријских података са већ сачуваним биометријским подацима. Корисник прво мора приложити идентификациони податак помоћу којег ће систем пронаћи одговарајући биометријски отисак за тог корисника. Тај податак се може приложити на више начина: у виду корисничког имена или лозинке, у виду пина или паметне картице итд. Процес аутентификације на основу биометријских података приказан је на слици.



Слика 18 - Аутентификација на основу биометријских података

Идентификациони податак може да испоручити и сам систем помоћу процеса биометриске идентификације. У таквом случају унесени биометријски податак се упоређује са свим подацима из базе постојећих корисника. Очигледно је да овај процес може бити дуготрајан и непрецизан, а његова имплементација скупа и захтевна.

3.4 Грешке у фази аутентификације

Поузданост, уверљивост и брзина система аутентификације базираног на биометрији зависе од метода које се користе. Из тих разлога је јако битно да се при пројектовању темељно провере сва својства и перформансе тог система. Код анализирања метода често се проверавају врсте грешака. Постоје две врсте грешака које се јављају код биометријских система:

- ✓ Погрешно прихватање (енг. *false acceptance*). Ово је грешка првог типа и она значи да систем погрешно прихвата особу као легитимног корисника, јер је у бази података пронашао шаблон довољно сличан унесеном.
- ✓ Погрешно одбијање (енг. *false rejection*). Ово је грешка другог типа и она значи да систем одбија легитимног корисника, јер није пронашао довољно подударања очитаних података са шаблоном из базе. Погрешно одбијање представља неугодност за корисника, али се сматра прихватљивијим од грешке првог типа, јер корисник може поново покушати да се аутентификује.

Како би се грешке у оваквим системима боље описале уводе се два фактора:

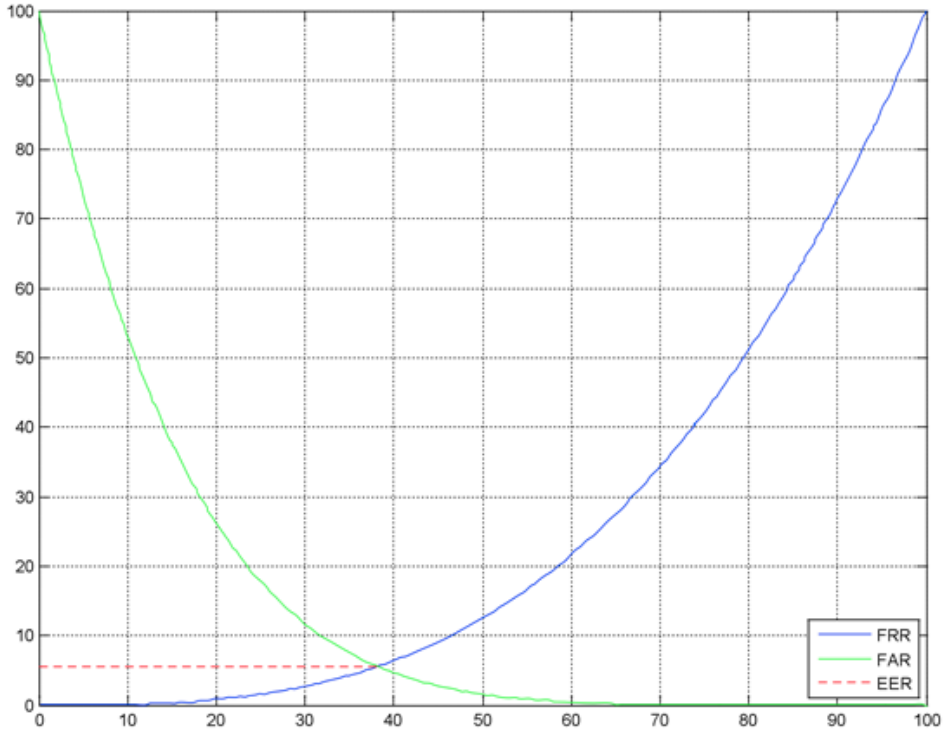
- ✓ Удео погрешних прихватања (енг. *False Acceptance Rate – FAR*).
- ✓ Удео погрешних одбијања (енг. *False Rejection Rate – FRR*).

Ова два фактора се израчунавају према следећим формулама:

$$FAR = \frac{\text{број погрешних прихватања}}{\text{број неовлашћених приступа}}$$

$$FRR = \frac{\text{број погрешних одбијања}}{\text{број овлашћених приступа}}$$

FAR и *FRR* зависе од прага сигурности (енг. *Security Threshold*). Тај праг може бити параметар алгоритма за упоређивање или вредност са којом се упоређује резултат добијен алгоритмом. Виши праг сигурности значи да ће биометријски систем пажљивије обављати упоређивање тренутно унесених података са подацима који се налазе у бази. У том случају ће се смањити број погрешних прихватања и вредност *FAR- a*, али ће се повећати број погрешних одбијања и пропорционално ће порасти вредност *FRR-a*. Обрнуто свему овоме у случају смањивања прага сигурности вредност *FRR-a* ће се смањити, а вредност *FAR- a* ће се повећати. Закључујемо да су *FAR* и *FRR* функције прага сигурности. На слици су илустроване вредности *FAR-a* и *FRR-a* за неки систем. Одлука о висини сигурносног прага зависи о сврси биометријског система и представља компромис између употребљивости и сигурности.



Слика 19 - ФАР и ФРР

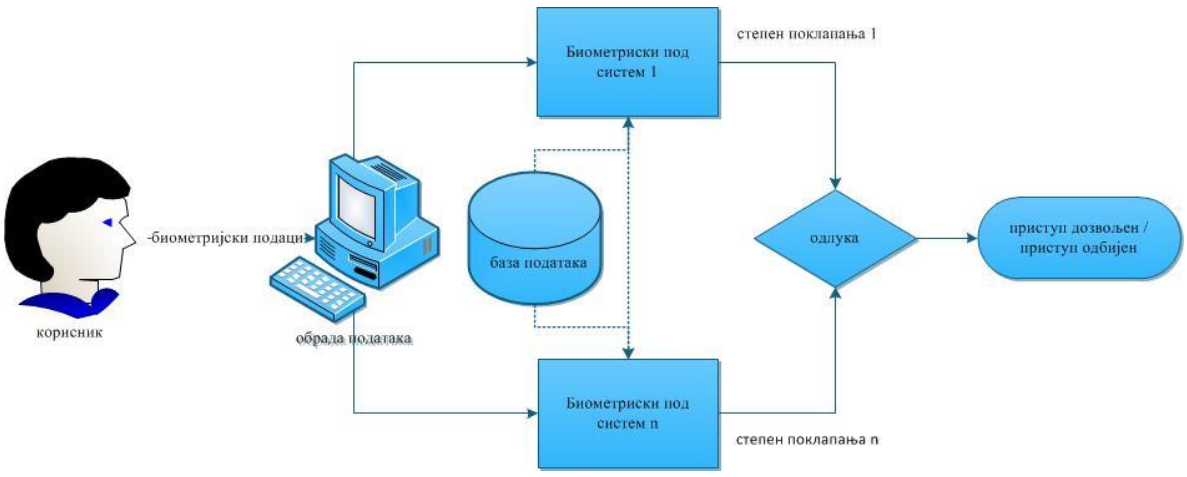
Вредност *FAR-a* и *FRR-a* на месту у коме се секу криве зове се једнаки удео у грешкама (енг. *equal error rate - EER*). *EER* у пракси не може послужити за упоређивање уређаја различитих произвођача, нарочито ако се вредности много разликују. Ово се догађа зато што произвођачи система базираних на биометрији не желе да објаве услове под којим обављају своја мерења, а на производима објављују најбоље резултате мерења који су обављени у идеалним условима који се тешко могу поновити у пракси.

3.5 Унимодални и бимодални системи за аутентификацију

Унимодални системи за аутентификацију користе само један биометријски извор. Овакви системи су повољнији и једноставнији за употребу али су подложнији броју погрешних одбијања, због неповољних услова учитавања, као што су нпр. лоше осветљење или нечистоћа код оптичких скенера. У великим популацијама неке од биометријских карактеристика нису довољно јединствене за све особе нпр. две особе могу имати јако слично лице.

Бимодални системи за аутентификацију користе две или више биометријска извора.

Свака метода својим алгоритмом израчунава степен поклапања. Када се добију сви степени поклапања онда се ускладе и доноси се коначна одлука. Што више биометријских извора употребимо омогућиће да имамо већу тачност, а самим тим и веће трошкове. Не постоји једноставан начин одабира биометријских метода које ћемо употребљавати у бимодалним системима. Углавном изабране биометријске методе зависе од примене бимодалног система, међутим у већини случајева најбоље резултате дају комбинације биометријских метода велике и средње тачности. Методе које се највише користе су: отисак прста, препознавање лица и скенирање ока.



Слика 20 - Унимодални и бимодални системи за аутентификацију

3.6 Развој система аутентификације на основу биометрије гласа

Препознавање говорника (енг. *speaker recognition*) тј. биометрија гласа има своју историју стару пет деценија и користи акустичне карактеристике говора за које је утврђено да се разликују од особе до особе. Ови звучни обрасци рефлектују анатомију вокалног тракта и био-информације појединца. Препознавање говорника је другачија технологија од препознавања говора (енг. *speech recognition*). Препознавање говора је препознавање изговорених речи, а то није препознавање на основу биометрије гласа.

Биометрија гласа је еволуирала од технологије препознавања изговорених речи зато што имају јако сличне карактеристике и међусобно су повезане. Године 1960. "Гунар Фант" шведски професор објавио је модел који описује физиолошке компоненте акустичности говора. Овај рад базиран је на анализи појединаца, коришћењем икс зрака и он показује да свака особа има свој специфичан фонетски звук. Године 1970. "др Џозеф Паркер" користи исту технику кретања икс зрака, али у истраживање додаје језик и вилицу како би проширио "Гунар Фант"-ов модел. Године 1976. компанија "*Texas Instruments*" прави прототип овог система које су тестирале "*United States Air Force"* и "*The MITRE Corporation*". Средином 1980-их Национални Институт за Стандарде и Технологије (*NIST*) "Говор Група" који служи за проучавање и промовисање употребе система аутентификације на основу биометрије гласа. Од 1996. године у оквиру средстава које покрива Национална Безбедносна Агенција, *NIST*-ов "Говор Група" је домаћин годишњих семинара, са циљем да подстакне континуирано унапређење и развој оваквих система.

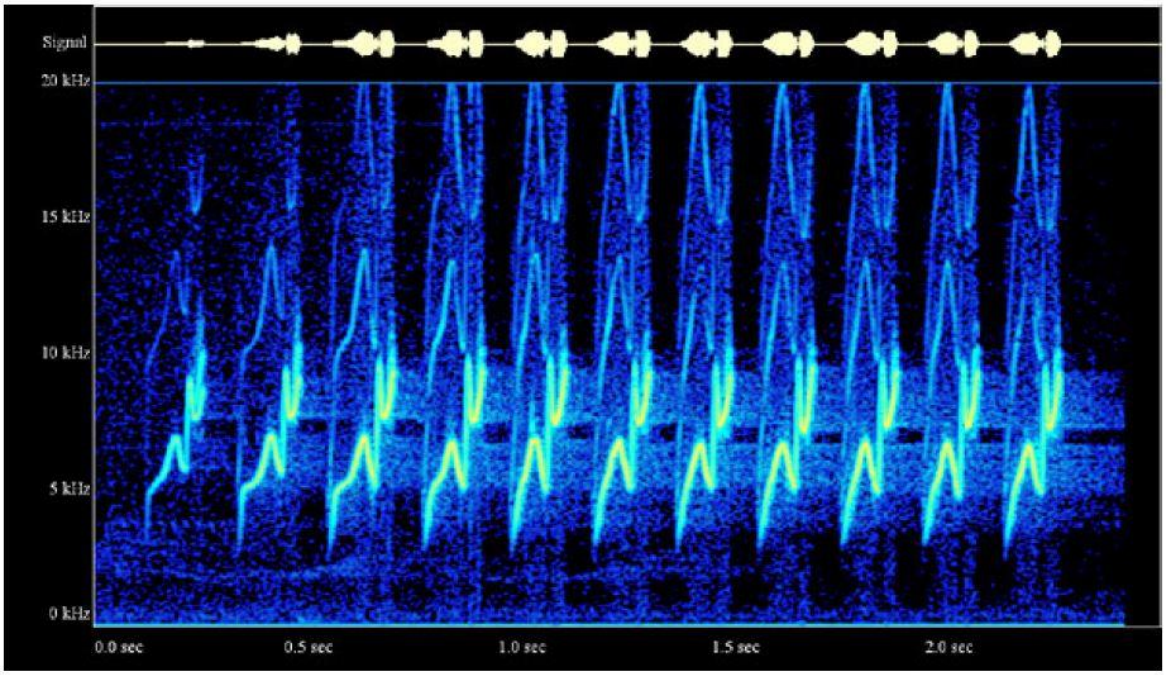
Физиолошка компонента препознавање гласа се односи на физички облик вокалног тракта појединца, која се састоји од дисајних путева и меког ткива, шупљине од које производи звук. Да би се произвео говор, ове компоненте раде у комбинацији са физичким кретањем вилице, језика и гркљана и резонанције у назалним путевима. Акустичност говора настаје из физичких карактеристика дисајних путева. Покрети из уста, изговор и понашање су главне компоненте овог биометријског система.

Постоје две врсте система препознавања гласа:

- ✓ Ограничени систем који зависи од текста (енг. *text dependent*)
- ✓ Неограничени систем који не зависи од текста (енг. *text independent*)

Код биометријских система препознавања гласа, који зависе од изговореног текста, од корисника се тражи да изговори своју лозинку или нпр. неке насумичне бројеве које бира систем. Овакав начин аутентификације показује одличне перформансе упоређивања корисника из базе података. Биометријски систем који не зависи од изговореног текста нема напредна сазнања о кориснику, тј. нема своју базу података са већ унапред снимљеним фразама. Овакав систем је јако флексибилан у случајевима када особе не желе да буду снимљене или не знају да их неко снима.

Снимљени узорци гласа су таласни облици који се могу представити тако да се на хоризонталној оси види време, а на вертикалној јачина звука. Биометријски систем препознавања гласа ради тако што анализира фреквенцијски садржај говора и пореди карактеристике као што су квалитет, трајање, интензитет, висина тона и карактеристике тона. [6]

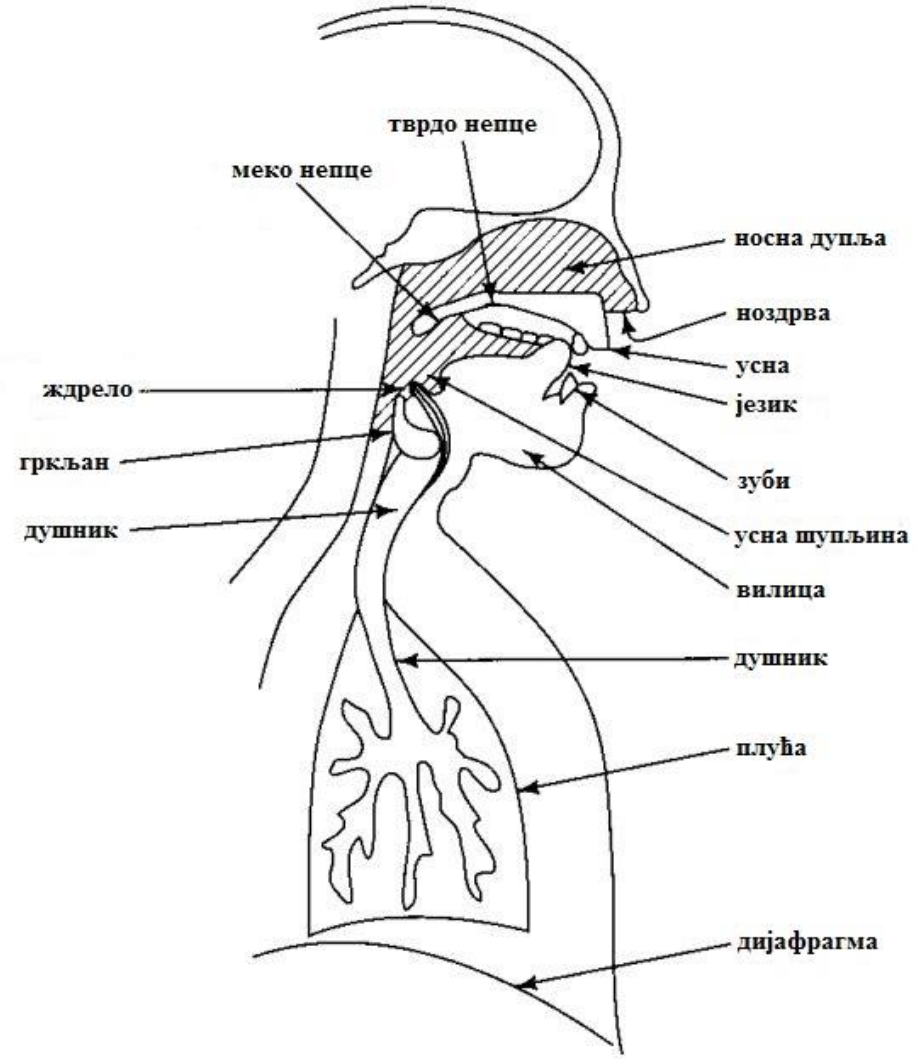


Слика 21 - Узорак снимљеног гласа

На овој фигури примећујемо да се на врху слике види јачина звука улазног сигнала која је приказана у временском домену. Дречаво плава боја у дну слике приказује спектралне информације овог говорног сигнала. Ове информације се уцртавају у временском домену у односу на фреквенцијске варијације.

3.7 Настанак говорног сигнала

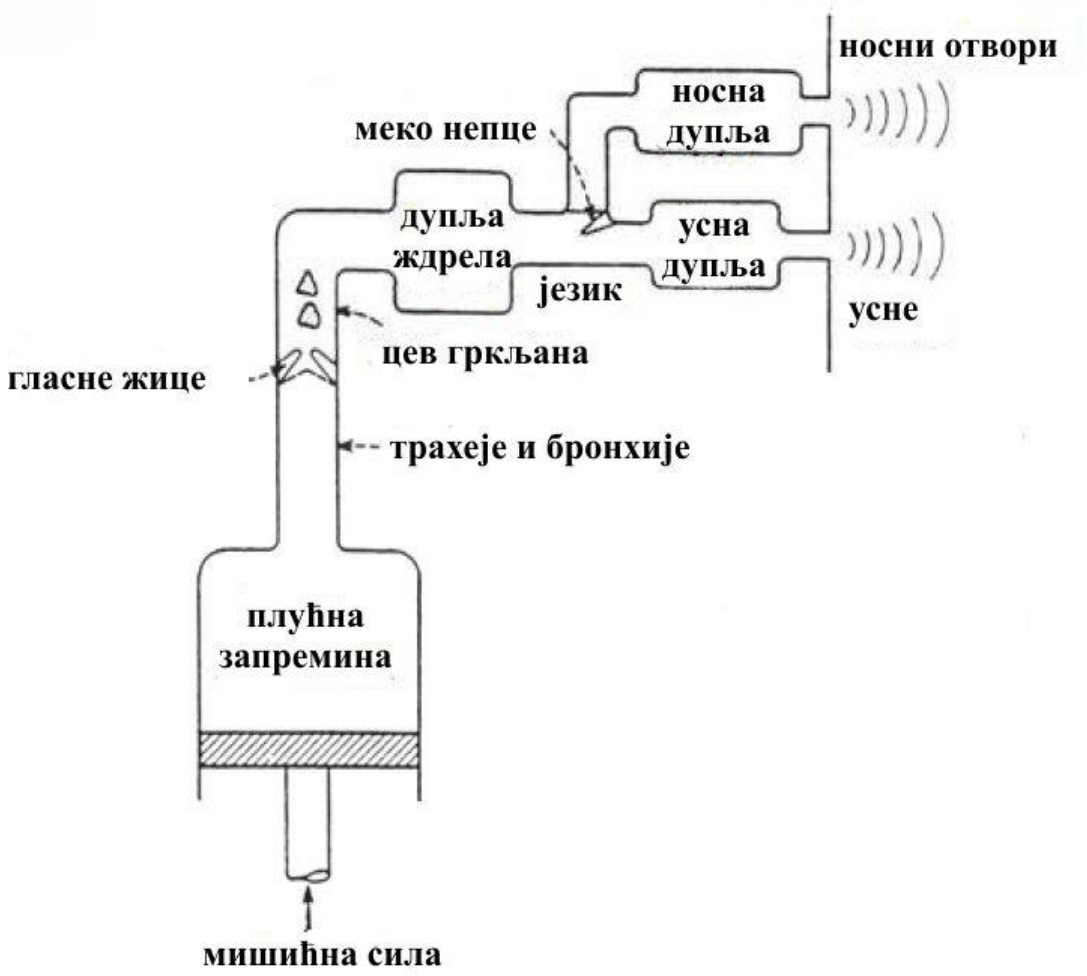
Приликом удисања када се плућа испуњавају ваздухом, нема производње говора. Приликом издисаја, ваздух из плућа, тј. ваздушна струја пролази кроз душник и изазива вибрације гласних жица у гркљану (те вибрације називамо Бернулијеве вибрације). Ваздушна струја је испрекидана и она формира квазипериодичне импулсе, који се фреквентно модулишу приликом проласка кроз ждрело, усну и носну дупљу. Позиције различитих артикулатора, као што су вилица, меко непце, тврдо непце, уста и усне, одређују различите звукове који при томе настају и конституишу акустички израз изговорене поруке. [5]



Слика 22 – Настанак говорног сигнала

3.8 Механизам производње говора

Плућа и одговарајући мишићи чине извор ваздушне побуде која побуђује вокални механизам. Мишићи избацују ваздух из плућа у бронхије и душник (веома слично као што клип потискује ваздух унутар цилиндра). Ако су ваздушне жице затегнуте, ова ваздушна струја изазива њихове вибрације, производећи вокализоване квазипериодичне звучне гласове. Са друге стране ако су гласне жице опуштене, ваздушна струја неометано пролази до вокалног тракта док не наиђе на сужења, што изазива турбуленције, које дају безвучне гласове (као што су у нашем језику: *с* и *ш*). Ваздушна струја такође може да наиђе и на препреке које потпуно затварају вокални тракт и на овај начин се прави пораст притиска док се препрека не отвори, након чега долази до наглог ослобађања ваздушног тока, чиме настају транзијентни гласови (као што су у нашем језику: *п*, *т*, или *к*). [5]



Слика 23 - Механизам производње говора

3.9 Предности и недостаци биометријских решења

Електронска повезаност људи у данашње време достиже ниво на коме је потребно константно радити и развијати нове технике система за аутентификацију и безбедност података. Постоји могућност да се аутентификујемо на основу три параметара: нечим што знамо, нечим што имамо и нечим што јесмо. Оно што јесмо се репрезентује нашом биометријом која је јединствена за сваку особу. Могућност коришћења биометрије у развоју система аутентификације има своје предности, као и неке недостатке у односу на класичне системе. Код класичних система аутентификације велики проблем настаје када је потребан висок ниво заштите података. Тада је потребно памтити, или безбедно ускладиштити комплексне лозинке. Обично се бирају слабије лозинке да би се лакше сачувале, као што су име, датум рођења, име неког од чланова породице итд. У испитивању у коме је анкетирано 1200 људи чак половина је користила неку од поменутих метода за генерисање своје шифре. Такве шифре је лако дешифровати, да ли простим погађањем, или нападом путем речника . Без обзира што је општа препорука да се за различите сервисе користе различите шифре, већина користи исту, тако да се компромитовања једне шифре угрожава безбедност свих сервиса . Корисници који користе комплексније шифре, или их записују, или небезбедно чувају. Шифровањем се може доћи до јаких шифара (шифарског кључа) које не морају да се памте, али оне су пак заштићене једноставном шифром, што доводи у питање сврху тог система. Велики проблем слабих шифара је тај што је нападачима довољно да дођу до једне шифре да би имали приступ неком интранету тако да је систем безбедан колико и најслабија шифра.

Коначно, ако се шифра дели са колегом, систем не може да препозна ко је корисник шифре. Приступ који је базиран на нечему што имамо је приступ уз помоћ токена, идентификационих картица, кредитних картица или кључева. Тада се јавља могућност компромитовања таквог система ако дође до губитка или крађе поменутих предмета.

Решење ових проблема се постиже коришћењем биометрије. Биометрију не можемо изгубити, увек нам је доступна, а не морамо је памтити. Ако посматрамо напад методом грубе силе на биометријски систем, шанса да ће такав напад успети зависи од тачности поклапања биометријских података. Претпоставићемо да је вредност ФМР-а 0001% за одређени биометријски систем. Са оваквим подешавањима неколико биометријских система (отисак прста или скенирање ириса) могу лако да буду на мање од 1% ФНМР-а. Ако је вредност ФМР- а подешена на 0001% онда је потребно да нападач тестира у просеку 100.000,00 узорака да би један био успешан. Ово се може поистоветити са сигурношћу шифре од 5 насумично изабраних бројева. Да би се напао биометријски систем потребно је генерисати велику количину биометријских узорака што је знатно теже него генерисати толико исто насумичних стрингова. Коначно, ФМР биометријског система се може редуковати тако да пружа већи степен сигурности што би опет довело до повећања ФНМР-а.

Међутим, постоји и низ недостатака који су специфични за употребу биометрије у процесу аутентификације. Један од највећих недостатака је тај да компромитовану биометрију не можемо заменити са новом, као што је то случај са шифрама или картицама. Узмимо за пример да се на аеродромима проверавају путници и тражи се 100 најтраженијих криминалаца (величина базе је дакле 100 узорака) користећи систем базиран на отисцима прстију који ради на параметрима од 1% ФНМР и 0.001% ФМР. Ако систем ради као верификациони у 1% случајева не би могао исправно да верификује исправног путника, док би у 0001% случајева погрешно пропустио траженог путника. Ако је тај исти систем постављен као идентификациони систем, онда би му параметри били ФНМР 1%, док би ФМР био 100 * 0.001 % = 0.1 %. Ово значи да постоји 99% шансе да се ухвати тражени криминалац, али има и велике шансе да дође до лажних аларма (имајући у виду да 200.000,00 људи користи главне аеродроме у Сједињеним Америчким Државама дневно дошло би до 200,00 лажних аларма).

Биометријски системи имају своја ограничења. Нека од најважнијих су:

Бука у осетљивим подацима - Осетљиви подаци могу бити пуни шума или изврнути. Отисак прста са ожиљком, или промукао глас су примери података са шумом. Такође постоји могућност да се шум појави због неисправно монтираних сензора (запрљани сензори), или лоших амбијенталних услова (лоше осветљење) приликом скенирања лица. Подаци са доста шума могу довести до погрешног одбијања.

Унутрашње варијације - Биометријски подаци исте особе се могу значајно разликовати, односно никад се не може добити идентичан узорак иако се ради о истој особи. Нпр. код узимања отиска прста положај прста никад није исти, такође није ни исти притисак на скенер, као и то што постоји разлика између самих скенера.

Особености - Како се очекује да се биометријске особине значајно разликују између појединаца, постоје велике унутрашње сличности групе својстава које исказују те особине.

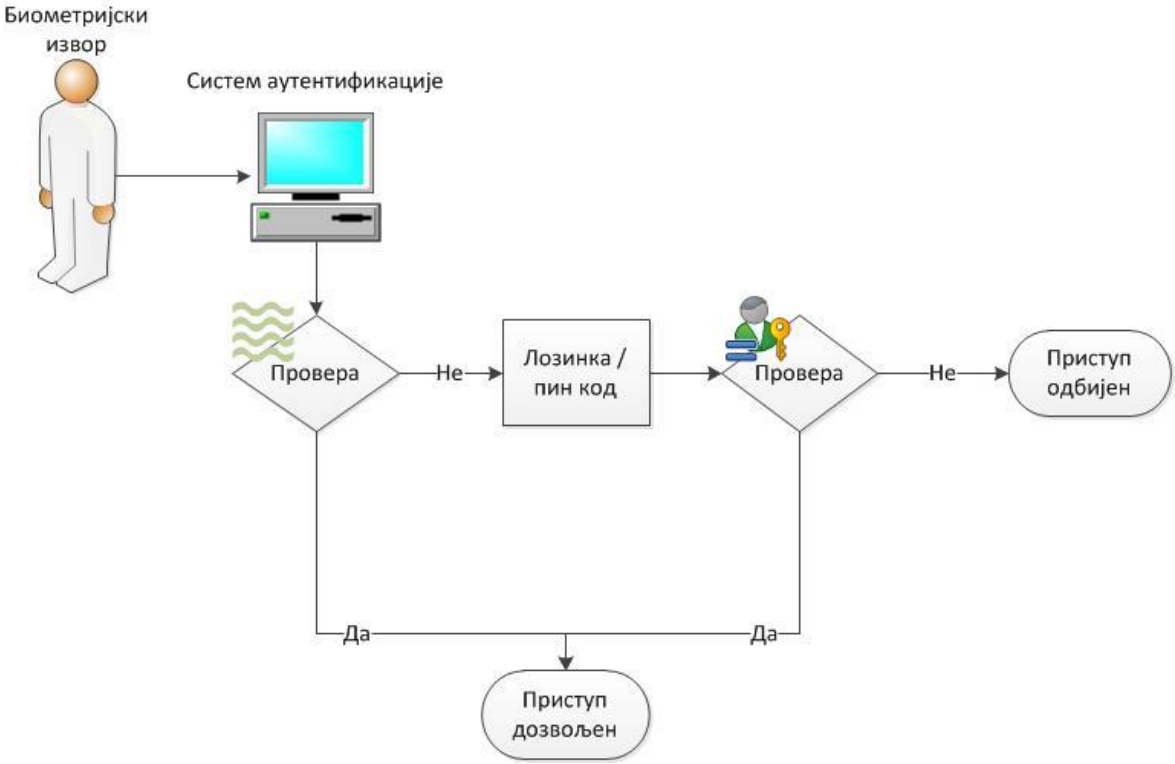
Неуниверзалност - Очекује се да сваки појединац има биометријске особине, али у стварности постоји група људи које не можемо идентификовати на основу неких биометријских узорака. Из неких отисака прстију није могуће извући карактеристичне информације које су нам потребне за идентификацију. Проблеми су лош квалитет гребена које поседује 4% становништва и код таквих особа није могуће са стандардним сензорима добити довољно квалитетну слику отиска прста.

Напади подметањем - Нападач је у могућности да подметне биометријски узорак легитимног корисника и на тај начин превари систем. Овакви напади су чести када је у питању биометрија гласа, или потписа. Такође могуће је и физичку биометрију подметнути. На пример, показано је да је могуће конструисати вештачки отисак прста за разумно време.

4 Преглед предложеног решења

4.1 Генеричка шема предложеног решења

Дво-факторска аутентификација као метод примене побољшава једно-факторске аутентификационе методе, стога смо се у овом раду и базирали на њој. Комбинацијом биометрије гласа са лозинком или пином унапређујемо систем аутентификације и смањујемо могућности грешке које се могу догодити. На следећој слици се јасно види генеричка шема предложеног решења.



Сл. 24 – Генеричка шема предложеног решења

- **Биометријски извор** – То је особа која изговара своју лозинку усмено у микрофон да би се аутентификовала пред системом.

- **Ситем аутентификације** – Систем снима изговорену реч да би је упоредио са унапред снимљеном гласовном секвенцом која се налази у бази података. За упоређивање гласовних секвенци користимо алгоритам који је написан у програмском језику Матлаб, а главну улогу у том алгоритму игра математичка функција крос корелације о којој ће касније бити више речи.

- **Провера** – Провера се врши тако што се две секвенце упореде и над њима се изврши функција крос корелације. Ако се после упоређивања добијена вредност међусобне корелације ова два сигнала не поклапа са унапред дефинисаном граничном вредношћу, корисник се није успешно аутентификовао пред системом и од њега ће бити захтевано да унесе лозинку или пин. Ако се вредност крос корелације поклапа са унапред дефинисаним границама, корисник ће се успешно аутентификовати.

4.2 Поставка и објашњење експерименталног окружења

- **Спецификација хардверске опреме која је коришћена**

  - Процесор – *"Intel E8400 3.0Ghz"*
  - Матична плоча – *"Intel Topsfield DP43TF "*
  - Оперативни систем – *"Windows7 x64"*
  - Рам меморија – *"4GB"*
  - Микрофон – *"A4 TECH 0907"*

- **Подаци о бази података која је коришћена**

  За потребе овог експеримента коришћена је наша база снимљених гласовних секвенци која се састоји од 8 особа које су рекле по 3 различите лозинке, али за овај експеримент у разматрање је узета једна лозинка која се састоји од три речи.

- **Подаци о развојном окружењу које је коришћено**

  Као развојно окружење коришћен је програмски језик *"Matlab R2010a"*

4.3 Спроведене анализе и експерименти који су претходили пројектовању целокупног решења

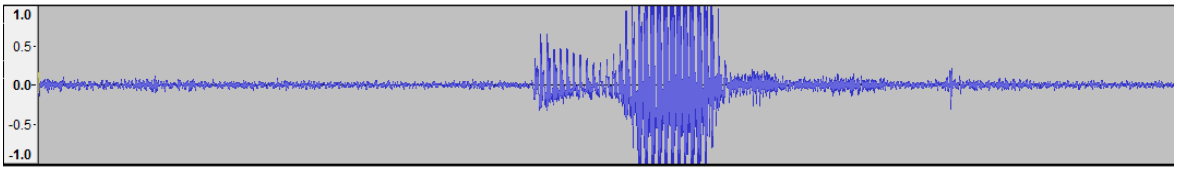
Током тестирања овог система вршени су разни експерименти. Врло нам је важно било да биометријски отисци гласовних секвенци говорника који ће служити за касније упоређивање буду снимљени са што мање шума у што бољим условима, али наравно не можемо утицати на све аспекте и околности. Ако би пак и дошло до шумова за потребе експеримента, тај шум је уклањан и резултати су се упоређивали са и без присутног шума у сигналу. Касније се могло доћи до закључка да приликом коришћења функције крос корелације присутни шум у сигналу прави велике разлике у величини опсега добијених резултата, али не утиче толико на утврђивање аутентификације појединца.

4.4 Процес снимања гласовних секвенци за потребе аутентификације

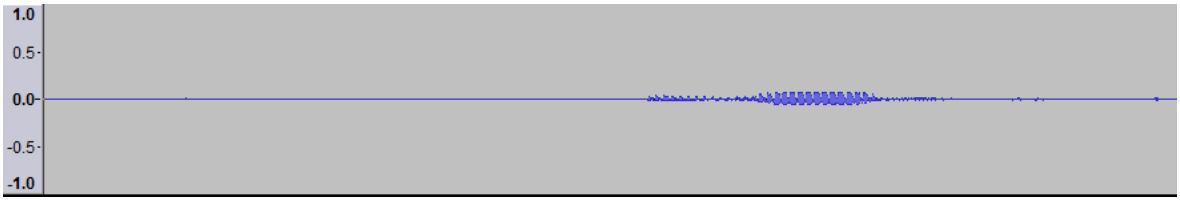
Све гласовне секвенце коришћене у овом пројекту су снимане у програмском језику Матлаб на „32 *bit*“-а, на фреквенцији *16000Hz*, у „*mono*“ режиму.

Као алат за снимање звука коришћен је обичан микрофон за рачунар „*A4 TECH 0907*“.

За потребе уклањања шума из гласовних секвенци коришћен је програм „*Audicity 2.0.0*“ и филтер „Noice removal “



Слика 25 – Гласовна секвенца са шумом



Слика 26 – Гласовна секвенца без шумом

4.5 Процес упоређивања гласовних секвенци за потребе аутентификације

Као што смо већ и поменули за потребе упоређивања гласовних секвенци коришћена је математичка функција крос корелација „*Cross-Correlation*“. Ова функција је имплементирана у програмски језик Матлаб и апсолутно је математички доказива.

4.6 Крос корелација „*Cross-Correlation*“

Како упоредити две гласовне секвенце које су настале од биолошког извора, а у себи поседују одговарајуће таласне форме? Ако су таласне форме јако сличне и варирају само у неким тачкама, онда се њихова корелација може добити тако што се рачуна производ парова тих тачака. Ова функција постаје још уверљивија када се посматрају две потпуно случајне и независне секвенце што нажалост није случај у нашем истраживању.

Крос корелација $r_{12}(n)$ за две секвенце података $x_1(n)$ и $x_2(n)$ које садрже N podataka може се написати као:

$$r_{12} = \sum_{n=0}^{N-1} x1(n)\, x2(n)$$

Оваква дефиниција крос корелације даје резултат који зависи од броја места и тачака које су узорковане.
Следећа формула је коригована за нормализацију резултата са бројем тачака које су дељене са N, а ово се може сматрати и просеком збира производа и пише се:

$$r_{12} = \frac{1}{N} \sum_{n=0}^{N-1} x1(n)\, x2(n)$$

Рачунање r_{12} је илустрован на слици испод, n је број тачака у секвенцама, а $x_1(n)$ и $x_2(n)$ су секвенце:

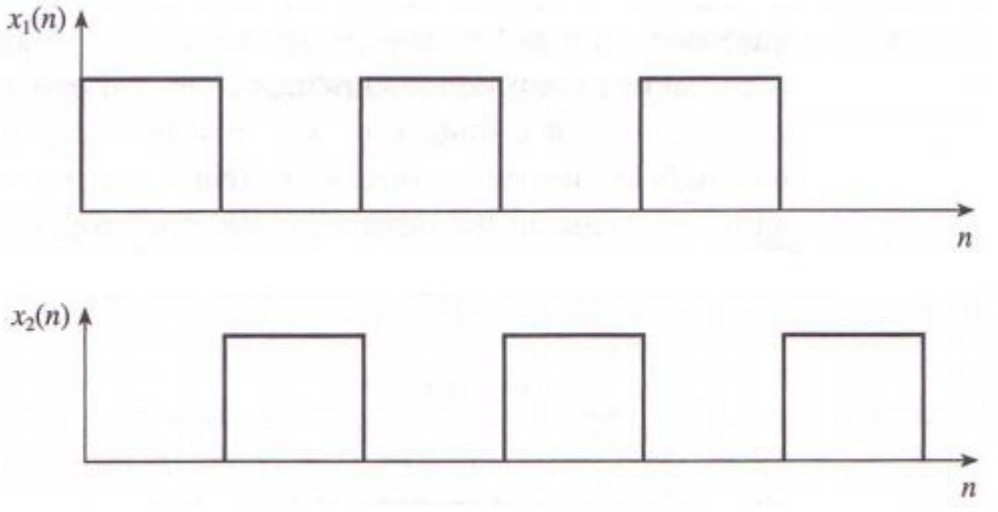
n	0	1	2	3	4	5	6	7	8
x_1	4	2	−1	3	−2	−6	−5	4	5
x_2	−4	1	3	7	4	−2	−8	−2	1

$$r_{12} = \frac{1}{9}(4 \times -4 + 2 \times 1 + -1 \times 3 + 3 \times 7 + -2 \times 4 + -6 \times -2 + -5 \times -8 + 4 \times -2 + 5 \times 1)$$

$$= 5$$

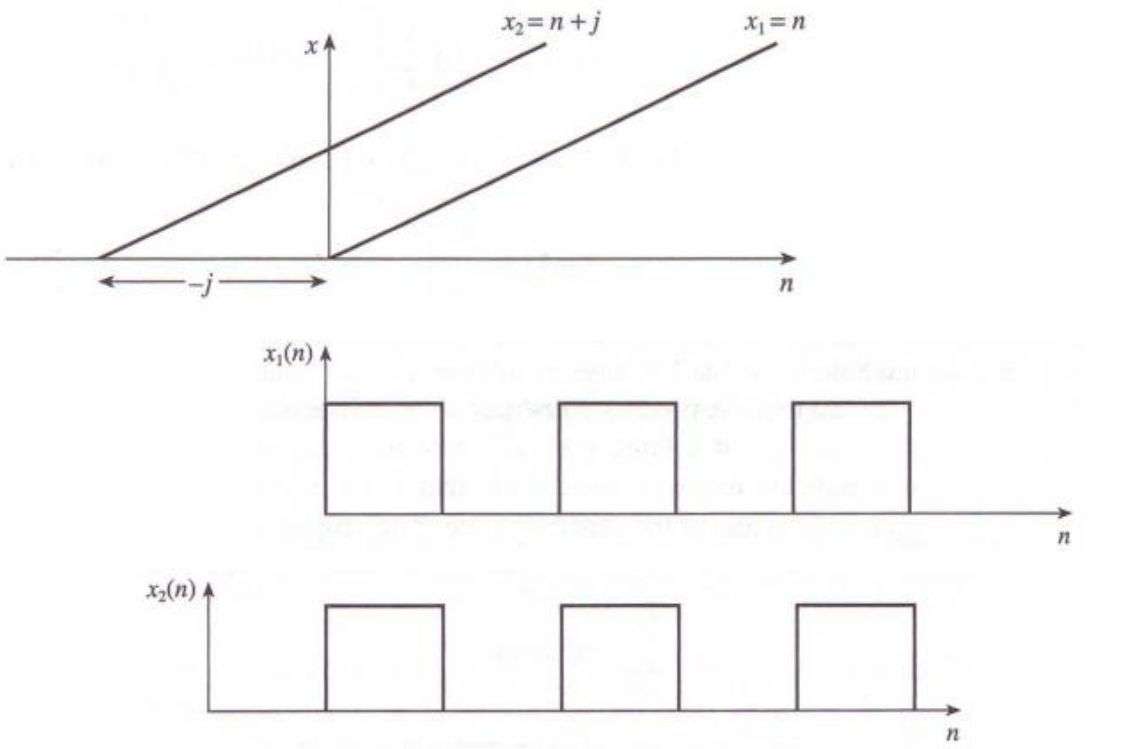
Слика 27 – Рачунање r_{12}

Међутим, ова дефиниција мора да се модификује да би могла да се искористи. У неким случајевима то може да указује на нулту корелацију и ако су две таласне форме у корелацији од 100%. То се може десити када су две таласне форме изашле из фазе и то изгледа овако:



Слика 28 – Таласне форме ван фазе

На овој слици се види да је сваки пар производа у нултој корелацији, одатле следи да су и та два заједно нула, па им је и корелација једнака нули. Међутим, таласни облици изгледају идентично, иако су излетели из фазе. Разлог оваквог случаја може бити зато што је x_2 у односу на x_1 закаснио са емитовањем. Да би се превазишле овакве фазне разлике, неопходно је да се сигнал, тј. талас помери за тај корак закашњења, да би ушао у исту фазу као свој претходник. На следећем примеру видећемо како да x_2 померимо у лево за корак који је довољан да буде у истој фази као x_1:



Слика 29 – Померање x_2 у лево

Ово је еквивалентно мењању $x_2(n)$ у $x_2(n+j)$ где j представља број кашњења, што је број узорака који треба да се помери у лево. На исти овакав начин x_1 може да се помери у десно.

Формула за крос корелацију сада постаје:

$$r_{12}(j) = \frac{1}{N}\sum_{n=0}^{N-1} x1(n)\, x2(n+j) =$$
$$r_{21}(-j) = \frac{1}{N}\sum_{n=0}^{N-1} x2(n)\, x1(n-j)$$

У пракси, када су две таласне форме у корелацији, њихов однос фаза највероватније неће бити познат. Дакле, корелација се обрачунава за више различитих заостања у циљу успостављања највеће вредности корелације, која се затим узима као тачна вредност. [4]

Када се за претходно израчунату корелацију x_1 и x_2 дода кашњење $j=3$ добијени резултат изгледа потпуно другачије:

n	0	1	2	3	4	5	6	7	8
x_1	4	2	−1	3	−2	−6	−5	4	5
x_2	7	4	−2	−8	−2	1			

$$r_{12}(3) = \frac{1}{9}(4\times 7 + 2\times 4 + -1\times -2 + 3\times -8 + -2\times -2 + -6\times 1)$$

$$= 1.33$$

Слика 30 – Рачунање r_{12} са кашњењем

Крос корелацијска вредност израчунавана по следећој формули зависи од апсолутних вредности података:

$$r_{12}(j) = \frac{1}{N}\sum_{n=0}^{N-1} x1(n)\, x2(n+j)$$

Крос корелацију је често потребно мерити за фиксне померање који се крећу у распону од -1 до +1.
Код рачунања крос корелације постоје три могућа исхода:

- +1 Значи да су секвенце у 100% корелацији.
- -1 Значи да секвенце 100% нису у корелацији (ово је случај искакања из фазе).
- ≈0 Значи да су извори сигнала потпуно независни и случајни.

4.7 Евалуација предложеног окружења са приказом експерименталних резултата

У овом делу биће приказани резултати упоређивања гласовних секвенци. Резултати су изражени у максималним вредностима крос корелација. Лозинка која је изговарана, снимана и упоређивана је: „Заштита у информационим системима“.
Следећи резултати су упоређене гласовне секвенце са шумом.

лозинка = ЗИС	Милош
крос корелација(са шумом)	**максимална вредност**
Милош и Милош'	482.0616
Милош и Јован	174.7155
Милош и Бранислав	145.5694
Милош и Душан	223.1209
Милош и Марија	43.5324
Милош и Марко	144.6834
Милош и Миломир	73.3554
Милош и Никола	75.5891

Табела 2 - Милош

лозинка = ЗИС	Јован
крос корелација(са шумом)	**максимална вредност**
Јован и Јован'	354.8073
Јован и Милош	174.7155
Јован и Бранислав	179.5763
Јован и Душан	89.9403
Јован и Марија	37.0590
Јован и Марко	122.3858
Јован и Миломир	79.4408
Јован и Никола	38.5063

Табела 3 – Јован

лозинка = ЗИС	Бранислав
крос корелација(са шумом)	**максимална вредност**
Бранислав и Бранислав'	125.7427
Бранислав и Милош	145.5694
Бранислав и Јован	179.5763
Бранислав и Душан	73.8962
Бранислав и Марија	30.2933
Бранислав и Марко	126.5475
Бранислав и Миломир	51.3775
Бранислав и Никола	43.5850

Табела 4 – Бранислав

лозинка = ЗИС	Душан
крос корелација(са шумом)	**максимална вредност**
Душан и Душан	134.3252
Душан и Милош	223.1209
Душан и Бранислав	73.8962
Душан и Јован	89.9403
Душан и Марија	20.3084
Душан и Марко	70.1127
Душан и Миломир	60.9255
Душан и Никола	27.7371

Табела 5 – Душан

лозинка = ЗИС	Марија
крос корелација(са шумом)	**максимална вредност**
Марија и Марија'	15.7424
Марија и Милош	43.5324
Марија и Јован	37.0590
Марија и Бранислав	30.2933
Марија и Душан	20.3084
Марија и Марко	53.9454
Марија и Миломир	13.9833
Марија и Никола	16.2368

Табела 6 – Марија

лозинка = ЗИС	Марко
крос корелација(са шумом)	**максимална вредност**
Марко и Марко'	103.1175
Марко и Милош	144.6834
Марко и Јован	122.3858
Марко и Бранислав	126.5475
Марко и Душан	70.1127
Марко и Марија	53.9454
Марко и Миломир	42.7581
Марко и Никола	39.6978

Табела 7 – Марко

лозинка = ЗИС	Миломир
крос корелација(са шумом)	**максимална вредност**
Миломир и Миломир'	24.0696
Миломир и Милош	73.3554
Миломир и Јован	79.4408
Миломир и Бранислав	51.3775
Миломир и Душан	60.9255
Миломир и Марија	13.9833
Миломир и Марко	42.7581
Миломир и Никола	33.4080

Табела 8 – Душан

лозинка = ЗИС	Никола
крос корелација(са шумом)	**максимална вредност**
Никола и Никола'	19.1148
Никола и Милош	75.5891
Никола и Јован	38.5063
Никола и Бранислав	43.5850
Никола и Душан	27.7371
Никола и Марија	16.2368
Никола и Марко	39.6978
Никола и Миломир	33.4080

Табела 9 – Никола

Следећи резултати су упоређене гласовне секвенце без шума.

лозинка = ЗИС	Милош
крос корелација(без шума)	**максимална вредност**
Милош и Милош'	5.3458
Милош и Јован	0.6859
Милош и Бранислав	0.5792
Милош и Душан	0.8877
Милош и Марија	0.1730
Милош и Марко	0.5721
Милош и Миломир	0.2915
Милош и Никола	0.3014

Табела 10 – Милош без шума

лозинка = ЗИС	Јован
крос корелација(без шума)	**максимална вредност**
Јован и Јован'	1.4107
Јован и Милош	0.6859
Јован и Бранислав	0.7144
Јован и Душан	0.3580
Јован и Марија	0.1478
Јован и Марко	0.4844
Јован и Миломир	0.3167
Јован и Никола	0.1532

Табела 11 – Јован без шума

лозинка = ЗИС	Бранислав
крос корелација(без шума)	**максимална вредност**
Бранислав и Бранислав'	0.5005
Бранислав и Милош	0.5792
Бранислав и Јован	0.7144
Бранислав и Душан	0.2943
Бранислав и Марија	0.1206
Бранислав и Марко	0.5035
Бранислав и Миломир	0.2044
Бранислав и Никола	0.1733

Табела 12 – Бранислав без шума

лозинка = ЗИС	Душан
крос корелација(без шума)	**максимална вредност**
Душан и Душан	0.5347
Душан и Милош	0.8877
Душан и Бранислав	0.2943
Душан и Јован	0.3580
Душан и Марија	0.0793
Душан и Марко	0.2783
Душан и Миломир	0.2427
Душан и Никола	0.1103

Табела 13 – Душан без шума

лозинка = ЗИС	Марија
крос корелација(без шума)	**Максимална вредност**
Марија и Марија'	0.0627
Марија и Милош	0.1730
Марија и Јован	0.1478
Марија и Бранислав	0.1206
Марија и Душан	0.0793
Марија и Марко	0.2147
Марија и Миломир	0.0560
Марија и Никола	0.0649

Табела 14 – Марија без шума

лозинка = ЗИС	Марко
крос корелација(без шума)	**максимална вредност**
Марко и Марко'	0.4103
Марко и Милош	0.5721
Марко и Јован	0.4844
Марко и Бранислав	0.5035
Марко и Душан	0.2783
Марко и Марија	0.2147
Марко и Миломир	0.1701
Марко и Никола	0.1574

Табела 15 – Марко без шума

лозинка = ЗИС	Миломир
крос корелација(без шума)	**максимална вредност**
Миломир и Миломир'	0.1480
Миломир и Милош	0.2915
Миломир и Јован	0.3167
Миломир и Бранислав	0.2044
Миломир и Душан	0.2427
Миломир и Марија	0.0560
Миломир и Марко	0.1701
Миломир и Никола	0.1315

Табела 16 – Миломир без шума

лозинка = ЗИС	Никола
крос корелација(без шума)	**максимална вредност**
Никола и Никола'	0.0763
Никола и Милош	0.3014
Никола и Јован	0.1532
Никола и Бранислав	0.1733
Никола и Душан	0.1103
Никола и Марија	0.0649
Никола и Марко	0.1574
Никола и Миломир	0.1315

Табела 17 – Никола без шума

Као што сте може приметити из табела, резултати нису успешни за све учеснике у овом експерименту, тј. функција крос корелација није успела успешно да аутентификује оригиналне говорнике, већ је дошло до грешака. Узмимо нпр. прву аутентификацију где особа 1, у овом случају Милош треба да се аутентификује пред системом. Максимална вредност крос корелације када се упоређују два говорна сигнала са шумом чији је биометријски извор био Милош је 482.0616., сви остали резултати као што можете приметити у табели испод су далеко ниже вредности. Разлог за овако добар резултат је у томе што је оба пута биометријски извор био исти, висина тона је била иста, лозинка је изговорена на исти начин у истом временском периоду без кашњења и заостатака у гласовним секвенцама.

лозинка = ЗИС	Милош
крос корелација(са шумом)	**максимална вредност**
Милош и Милош'	482.0616
Милош и Јован	174.7155
Милош и Бранислав	145.5694
Милош и Душан	223.1209
Милош и Марија	43.5324
Милош и Марко	144.6834
Милош и Миломир	73.3554
Милош и Никола	75.5891

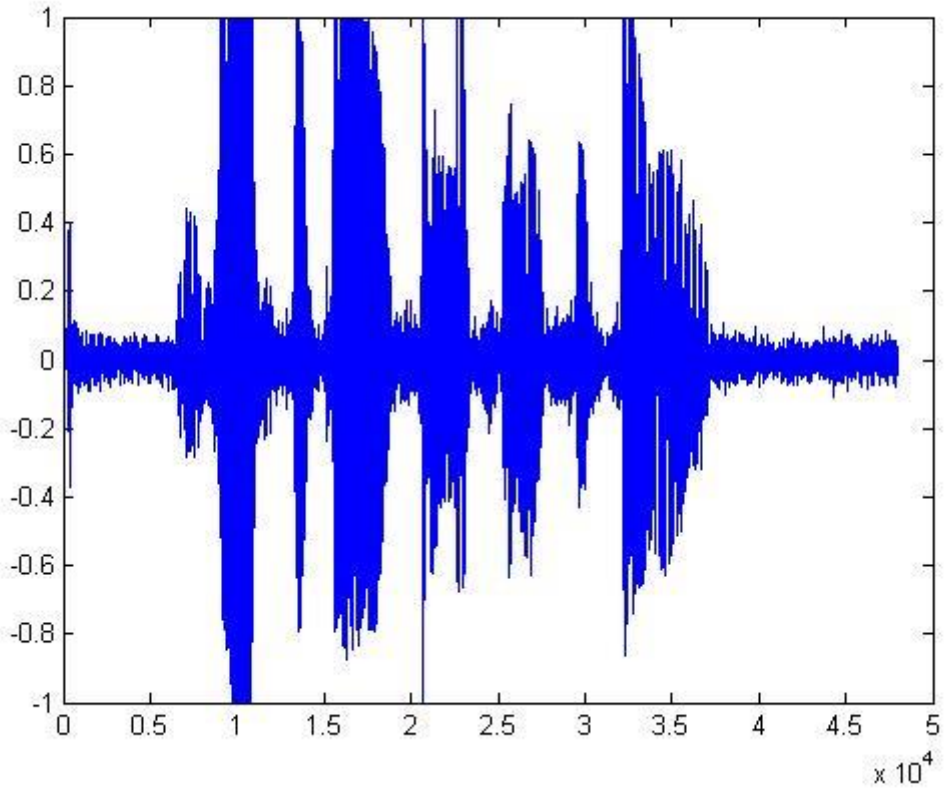
Табела 19 – Милош са шумом

Када смо применили филтер за уклањање шума на све снимљене гласовне секвенце, добили смо сличне резултате, нпр. код аутентификације првог говорника, резултат је био 5.3458, сви остали говорници који су били упоређивани са овим говорником имали су далеко нижи резултат.

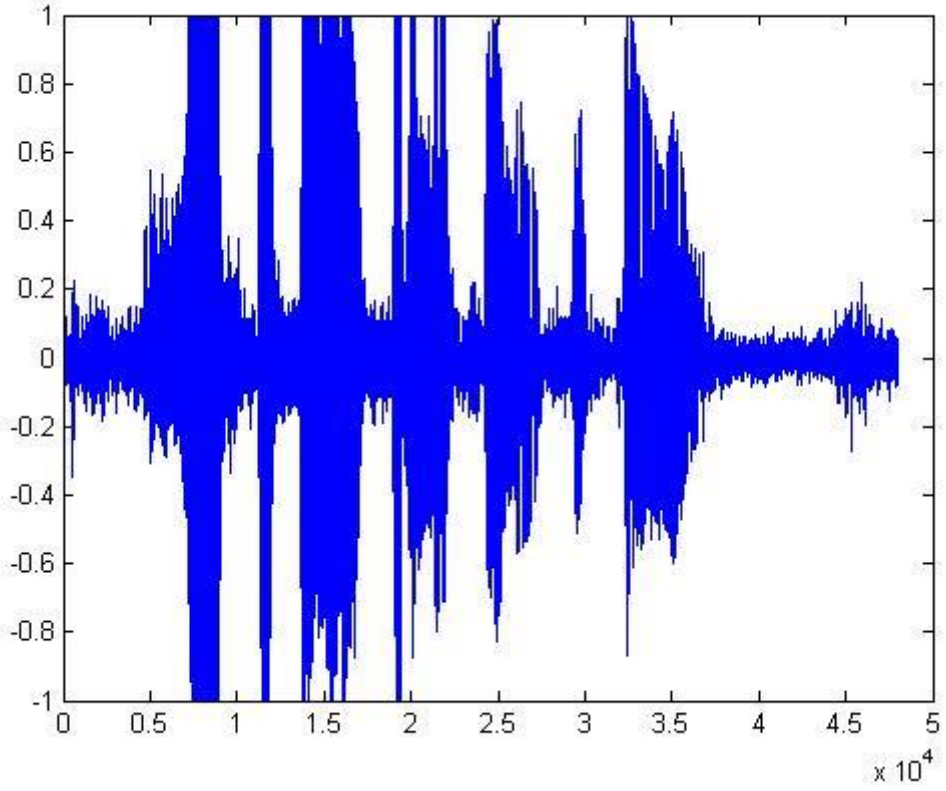
лозинка = ЗИС	Милош
крос корелација(без шума)	**максимална вредност**
Милош и Милош'	5.3458
Милош и Јован	0.6859
Милош и Бранислав	0.5792
Милош и Душан	0.8877
Милош и Марија	0.1730
Милош и Марко	0.5721
Милош и Миомир	0.2915
Милош и Никола	0.3014

Табела 20 – Милош без шума

На следеће две слике видећемо графички приказан снимак обе гласовне секвенце. Примећујемо да су јако сличне.



Слика 31 - Милош



Слика 32 – Милош’

Узмимо у разматрање неког другог говорника, нпр. Марију. Резултат упоређивања две гласовне секвенце ове особе је 15.7424, када смо једну од те две говорне секвенце упоредили са осталим учесницима у експерименту, добили смо веће вредности сличности сигнала.

лозинка = ЗИС	Марија
крос корелација(са шумом)	**максимална вредност**
Марија и Марија'	15.7424
Марија и Милош	43.5324
Марија и Јован	37.0590
Марија и Бранислав	30.2933
Марија и Душан	20.3084
Марија и Марко	53.9454
Марија и Миломир	13.9833
Марија и Никола	16.2368

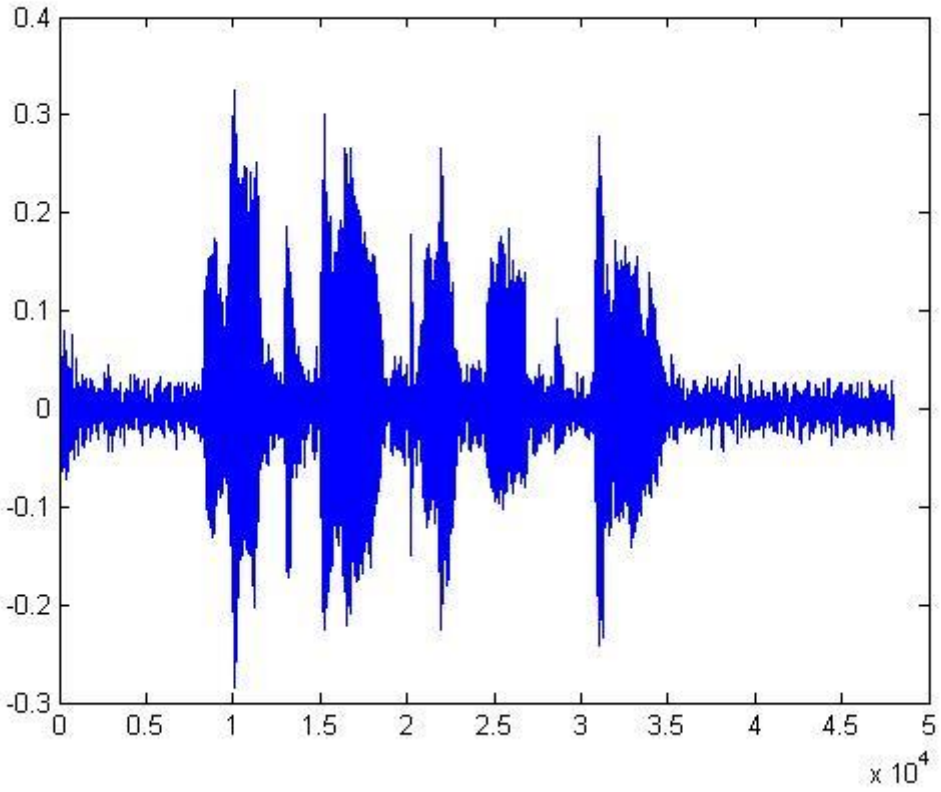
Табела 21 – Марија са шумом

Слични резултати су и када је уклоњен шум из сигнала.

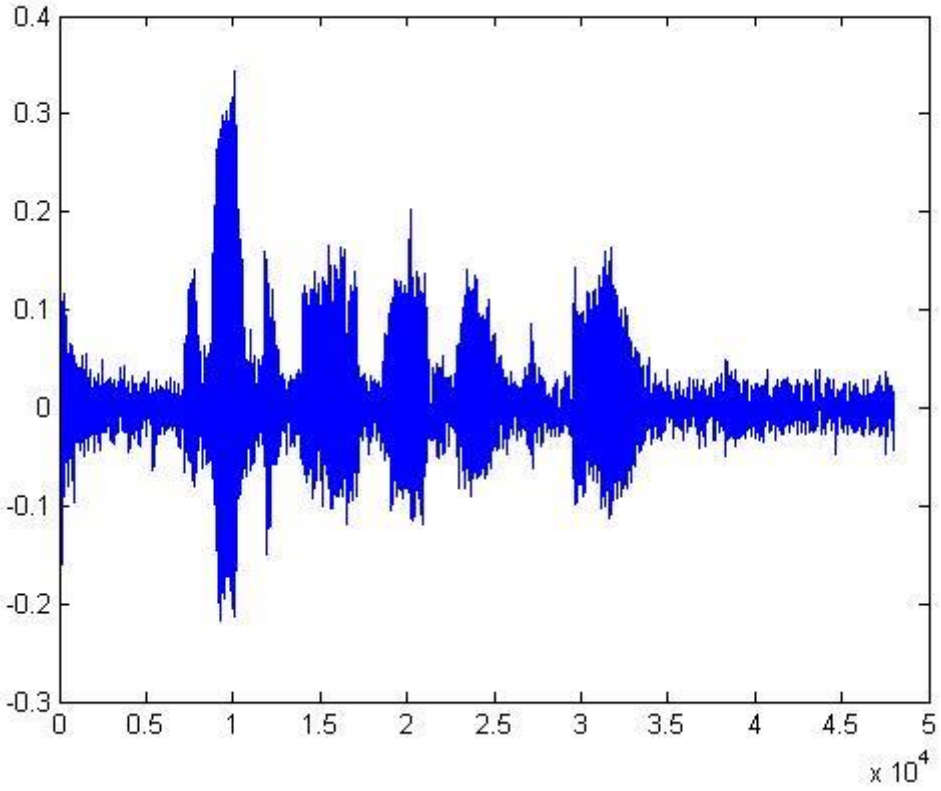
лозинка = ЗИС	Марија
крос корелација(без шума)	**максимална вредност**
Марија и Марија'	0.0627
Марија и Милош	0.1730
Марија и Јован	0.1478
Марија и Бранислав	0.1206
Марија и Душан	0.0793
Марија и Марко	0.2147
Марија и Миломир	0.0560
Марија и Никола	0.0649

Табела 22 – Марија без шума

На следеће две слике видећемо графички приказан снимак обе гласовне секвенце. Примећујемо да су јако различите, иако их је иста особа изговорила.



Слика 40 - Марија



Слика 40 – Марија

4.8 Област примене предложеног решења

Аутентификација базирана на биометрији може обезбедити погодну и сигурну проверу идентитета корисника која се може одвијати у локалном окружењу и на интернету. Уколико се захтева висок ниво аутентификације, онда биометрију можемо да комбинујемо са другим параметрима као што су лозинка или пин. Систем које је предложен у овом раду се може користити у тим окружењима за потребе аутентификације корисника.

5 ЗАКЉУЧАК

5.1 Сумарни циљеви рада

Циљеви који су постигнути у овом раду су засновани на практичном решењу. На крају се испоставило да због функције крос корелације која је коришћена за потребе упоређивања говорног сигнала резултати ниси испали очекивано добри. Идеја овог рада је да се направи систем аутентификације на основу биометрије гласа који ће бити лак за имплементацију и неће захтевати велике финансијске издатке.

5.2 Остварени резултати

Резултати који су остварени у овом раду су нажалост лошији од радова који се баве сличном или истом темом. Због не тако репрезентативних резултата које је показала коришћена функција, уводи се други фактор аутентификације. Систем је замишљен да ради тако да када се деси грешка код аутентификације на основу биометрије гласа, тј. резултатати максималне вредности крос корелације буду мањи од у напред задатих, од корисника се захтева да унесе лозинку или пин ручно како би систем био сигуран да је то особа баш она за коју се представља.

5.3 Предлог за будући рад

Побољшање перформанси и унапређење предложеног система је могуће унапређивањем начина на који би се аутентификација вршила. То је могуће урадити тако што би се пре рачунања корелације гласовне секвенце уједначиле, тј. треба подесити гласовне секвенце тако да у њима нема заостатака и кашњења (енг. *lags*).

Матлаб команде које су коришћене:

- voicein = wavrecord(intval*fs,fs, 'int16'); - Снимање говорног сигнала
- wavplay(voicein,fs) – Преслушавање говорног сигнала
- wavwrite(voicein,fs, ИмеФајла.wav'); - Снимање говорног сигнала у базу
- kk=xcorr(wavread(ИмеПрвогФајла.wav'),wavread(ИмеДругогФајла.wav')); - Рачунање крос корелације две учитане говорне секвенце
- max(kk) – Рачунање максималне вредности крос корелације две учитане говорне секвенце

Литература

[1] Toeplitz - Based Voice Verification for Human Identification - Extensive Review Author: Saeed, Khalid, Source: Recent Patents on Electrical & Electronic Engineering (Formerly Recent Patents on Electrical Engineering), Volume 1, Number 3, November 2008 , pp. 238-243(6)
[2] Hidden Markov Models Estimation and control Author: Robert J. Elliot, John B. Morre, Laghdar Aggoun SBN: 978-0-387-94364-0 (Print) 978-0-387-84854-9 (Online)
[3] Speaker Verification Using Adapted Gaussian Mixture Models Author: Douglas A. Reynolds, Thomas F. Quatieri, Robert B. Dunn
[4] http://www.ee.up.ac.za/main/_media/en/undergrad/subjects/esp411/esp411_lecture13.pdf
[5] Криптологија 2, Лекција 14 Кодовање говорног сигнала Проф. Др Милан М. Милосављевић
[6] http://www.nist.gov/biometrics-portal.cfm
[7] http://biometrics.cse.msu.edu/
[8] http://www.bioconsulting.com/bio.htm
[9] http://www.bioconsulting.com/Bio_Tech_Assessment.html