Óbudai Egyetem

Doktori (PhD) értekezés

A MULTIMODÁLIS BIOMETRIKUS AZONOSÍTÓ RENDSZEREK KOCKÁZAT ALAPÚ VIZSGÁLATA FUZZY LOGIKA ÉS NEURÁLIS HÁLÓZATOK SEGÍTSÉGÉVEL

Werner Gábor Ákos

Témavezető:
Dr. Hanka László

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Emeritus Dr. Berek Lajos, egyetemi tanár, ÓE BGK

Tagok:

Tóthné Dr. Laufer Edit, egyetemi docens, ÓE BGK

Dr. Kiss Sándor, egyetemi docens, NKE HHK

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Pokorádi László, egyetemi tanár, ÓE BGK

Titkár:

Dr. Szűcs Endre, adjunktus, ÓE BGK

Tagok:

Prof. Emeritus Dr. Berek Lajos, egyetemi tanár, ÓE BGK

Dr. Kiss Sándor, egyetemi docens, NKE HHK

Dr. Bartha Tibor, egyetemi docens, NKE HHK

Bírálók:

Tóthné Dr. Laufer Edit, egyetemi docens, ÓE BGK

Dr. Balla József, egyetemi docens, NKE RTK

Nyilvános védés időpontja:

TARTALOMJEGYZÉK

BEVEZETÉS, KUTATÁSI TERÜLET ISMERTETÉSE

A doktori értekezésemet két meghatározó tudományterület, a matematika és a biztonságtudomány összefüggései mentén vezettem végig, mindvégig törekedve a kellő egyensúly fenntartására. Az értekezésben a biometrikus azonosító rendszerek biztonságtudományt érintő gyakorlati kihívásaira adott elméleti megoldások matematikai értelmezésével foglalkoztam.

A biztonságtudomány fontos kérdései közé tartozik, hogy miként szabályozható az egyes javakhoz, szolgáltatásokhoz vagy információkhoz történő hozzáférés, illetve a hogyan valósítható meg jogosult személyek gyors és hatékony azonosítása? A biztonságtechnikában a digitális biometrikus azonosítás a jogosultság-vizsgálati módszerek viszonylag modern ága. Azonban maga a biometria nem nevezhető modern tudománynak, hiszen mind az orvostudomány, mind a kriminológia évszázados múltú ismeretekkel rendelkezik arról, hogy miként lehet egyes testi/pszichikai jellemzők alapján személyeket azonosítani, csoportokba sorolni.

A biometria biztonsági, – vagy ahogy később nevezem – vagyonvédelmi értelmezésében azonban elmondható, hogy a korábbitól eltérő igények is felmerültek, mert az azonosítás vizsgálat körülményei egyes vonatkozásokban komoly korlátok közé szorulnak. A gyakorlati alkalmazásokban fontos szempont az idő- és a költségtényező, valamint az alkalmazkodási képesség is. Elmondható, hogy az alkalmazott biometriában a biztonsági színvonal mellett a rendszerek költsége, gyorsasága és megbízhatósága is összemérhető kell, hogy legyen egymással és más azonosítási megoldásokkal.

Míg ezen igények közül az első kettőt nem szükséges külön taglalni, addig megbízhatósághoz, azaz a zavarokkal szembeni toleranciához érdemes magyarázatot fűzni. A kérdéskör egzakt tárgyalása tulajdonképpen nem is olyan egyszerű, hiszen amíg az idő és a költség egy jól megfogható és érzékeltethető fogalom, addig a zavartűrés mindig relatív. A zavartűrés számos más szinonim jelzővel is megjelenik például; megbízhatóság, teljesítmény, érzékenység, hibatolerancia és sorolhatnánk, de végezetül ugyanazt a halmazt árnyalnánk, amit jelenleg explicite nehéz definiálni, hiszen – ahogy ezt a későbbiekben taglalom –, nem áll rendelkezésre széleskörűen elfogadott és egzakt mérési módszer.

A zavartűrés javítása érdekében a kutatásaim során elsősorban a biometrikus azonosítás matematikai hátterét vizsgáltam, ezen belül a mintázat felismerést, összehasonlítást és a döntési folyamatokat. Olyan matematikai apparátusokat alkalmaztam, amik hasonló problémák esetében más területen már bizonyítottak. Az azonosítási hibák eredetének vizsgálatához a Bayes analízist és a béta-binomális eloszlást, míg a multimodiális azonosítás eredményeinek összesíthetőségéhez, illetve a mintázat felismeréshez a gépi tanulást, vagy ismertebb nevén a mesterséges intelligenciát (MI) hívtam segítségül.

A tudományos probléma megfogalmazása

A vizsgált problémák a biometrikus azonosítási rendszerek minősítési kérdései, valamint a működési módok optimalizálásának lehetőségei által kirajzolt körbe csoportosíthatóak. A gyakorlati alkalmazások számára problémát jelent, hogy a biometrikus azonosító jegyek minősége időben változik. A digitális adathordozók öregedéséhez képest az emberi szervezet jelentősen gyorsabban képes megváltozni, elveszítve az azonosításhoz szükséges egyedi jegyek jellegzetes tulajdonságait. Valamint az azonosítás folyamata ki van téve olyan környezeti vagy felhasználói szokásokból származó zavaroknak, amelyek negatívan befolyásolják a megbízható működést.

A biometrikus azonosítási technológiák más módszerekkel történő összevetése után kézenfekvőnek tűnnek előnyeik, de a gyakorlati alkalmazásuk terjedését – a tapasztalatok szerint – több faktor is nehezíti; példaképen említhető az adatvédelmi szabályozás, az adatbiztonsággal kapcsolatos bizalmatlanság, vagy a megbízható működés kérdése. Ezen tényezők közül a kutatásom első sorban a műszaki megbízhatóságra fókuszált, ezen belül is a fajlagos, vagy elemi hibákkal szembeni tolerancia eredményességére.

Egy azonosítási folyamat függetlenül attól, hogy biztonsági beléptetésről van szó, vagy akár felhasználói azonosításról, komoly biztonsági kockázat-növelő hatású, ha az alkalmazott biometrikus eszköz működése megbízhatatlan. A kár vagy veszély mindenképpen jelentős, hiszen egyik esetben jogosulatlan személy tévesen hozzáférést kaphat védett tartalomhoz, míg másik esetben a jogosult személy nem fér hozzá a szükséges adatokhoz vagy javakhoz, így késedelem merül fel. A digitális biometrikus azonosítási technikák esetében a beállítások finomításával jellemzően e két tulajdonság

csak egymás kárára változtatható meg. A vizsgálataim során elsődleges feladatnak ezen viszony árnyalását tűztem ki főcélnak.

Kutatási célok definiálása

Kutatásom elsődleges célja annak megválaszolása volt, hogy mesterséges intelligenciák körébe sorolt lágy számítási módszerek és egyes statisztikus megoldások hogyan javíthatják az azonosítás hatékonyságát, különös tekintettel arra, hogy az automatizált rendszerek miként taníthatóak meg a megváltozott működési feltételek implementálására. A fő kutatási cél vizsgálata során felmerültek olyan kérdések is, amelyek megfelelő megválaszolása nélkül nem lenne teljes és kellően körültekintő e tudományos munka. Ennek érdekében az alábbi kutatási és vizsgálati részcélokat tűztem ki:

- biometrikus azonosítási módszerek matematikai modelljeinek megismerése a mintaazonosítástól a döntésig;
- a sikeres azonosítás feltételeinek feltárása, különböző módszerek szelektivitásának összehasonlítása;
- biometrikus azonosítási rendszerek működésének vizsgálata, gyakorlati hibajelenségek feltárása és tipizálása, megfigyelési egységek közötti struktúrák felépítése;
- mesterséges tesztelési környezet és javító algoritmusok hibamentes működésének optimalizálása.

A téma kutatásának hipotézisei

I. Ismert felhasználói kör és környezet esetén előzetes statisztikus eltérési vizsgálattal előre jelezhető az alkalmazott biometrikus azonosító eszköz valós működési teljesítménye, így jobban meghatározható a környezethez illeszkedő műszaki megoldás.

II. A fuzzy logika lágy vezérlési szekvenciájával javulhat a multimodális biometrikus azonosítás döntési folyamatának pontossága a klasszikus, összegező és statisztikus jellegű eljárásokhoz képest.

III. A mesterséges neurális hálózatok tanulási képessége a konvencionális minta-felismerési algoritmusokhoz képest növelheti a biometrikus minták

felismerésének hatékonyságát, illetve a genetikus algoritmusokkal optimalizált mesterséges neurális hálózatok jól alkalmazhatók olyan problémák kezelésére, ahol a multimodális minták minősége nem állandó, a felhasználói kör vagy környezet változik.

IV. Lágy számítási módszerek kombinálásával rövidíthető a multimodális biometrikus azonosítás folyamata, mindeközben a felismerés hatékonysága illetve egy komplex, mesterséges intelligenciát implementáló vezérlő képes lehet az emberi észleléshez hasonló logikával felismerési feladatokat végezni.

Kutatási módszerek bemutatása

A kutatási módszerek közül elsőként a szakirodalmi feldolgozást kell megemlíteni, aminek során elsősorban nemzetközi szakirodalmi forrásokat elemeztem és hasonlítottam össze. Ezzel párhuzamosan természetesen megvizsgáltam a témakör magyarországi forrásait is, amiről elmondható, hogy relevánsnak tekinthető a nemzetközi viszonylatban. Három alapvető témakör területeiről gyűjtöttem szakirodalmi forrásokat úgymint az alkalmazott matematika (ezen belül optimalizálási módszerek, lágy számítási módszerek és az algebra numerikus módszerei), a biometria (multimodális biometria, alkalmazott biometria), valamint az általános biztonságtudomány (objektumvédelem, kritikus infrastruktúrák védelme, kockázatelemzési módszerek).

A vizsgált problémák tárgyalása során áttekintettem a hazai és uniós szabályozást a biometrikus azonosítás minőségi jellemzőinek mérési és összehasonlíthatóságának nehézségei tekintetében.

A szakirodalom feldolgozásán túl, MATLAB (Matrix Laboratory Software) környezetben algoritmusokat készítettem az egyes hipotézisek igazolása céljából, amelyekkel vagy általam generált vagy nyilvánosan elérhető adatbázisok adatait elemeztem. A programozás során különleges célt állítottam magam elé, miszerint nem használtam úgynevezett toolbox-okat (eszközkészlet), hanem minden lépést analitikusan végigvezetve, külön-külön programoztam, így megadva a lehetőség arra, hogy minden beállítást tetszés szerint megváltoztathassak.

Bizonyos problémák esetében több matematikai modellt is megvizsgáltam, és témavezetőm útmutatása szerint az operációkutatáshoz hasonlatosan kerestem a legjobban illeszkedő matematikai modellt. A fentieken túl kvalitatív és kvantitatív kutatásokat végeztem egyes biometrikus azonosító eszközök működését illetően az Alkalmazott Biometria Intézetben, és az ebből származó kutatási adatokat a későbbiekben bemutatott modellekben feldolgoztam.

Megvizsgáltam, hogy egy multimodális biometrikus azonosító komplex modellje milyen rendszertechnikai elemekkel optimalizálható. Olyan mesterséges biometrikus azonosítási környezet hoztam létre, amelyben virtuális adatbázissal és eszközökkel automatizált teszteket tudtam lefuttatni. Végső soron kombináltam a multimodális vezérlési algoritmusokat, így egy komplex mesterséges intelligencia alapú vezérlőt készítettem, a kitűzött kutatási célok érdekében.

A kutatásaimban választ kerestem azokra a kérdésekre, amelyekkel a biometrikus azonosító eszközök gyakorlati alkalmazása során találkozhatunk, így egy igen komplex szemléletben vizsgáltam a biometrikus rendszereket a tervezéstől egészen a működtetésig.

Biometrikus azonosítás szabályozási hátterének bemutatása

A jogi háttér ismertetése során nem célom a jogi szabályozás részletekbe menő bemutatása, vagy a jogi környezet rendszerszintű működésének összefoglalása, mindazonáltal a jelen témát is érintő uniós jogharmonizáció okozta kihívások tekintetében a jogi környezet jelentős szakmai kihívásokat teremtő hatásait nem lehet említés nélkül hagyni.

A biometria a digitális személyazonosításban mint relatíve modern, interdiszciplináris vagy akár multidiszciplinárisnak nevezhető tudományág, amely folyamatos fejlesztéseket és változtatásokat igényel a felhasználói környezetet szabályozó társtudományok területén, így a jogtudományban is. A biometrikus adatok kezelésében évtizedeken keresztül kizárólag az ujjnyomatok és ujjnyomok voltak az egyetlen ismert, univerzális és magas szelektivitású egyedi azonosító jegyek. A digitális technikák fejlődésével ismertté váltak más egyedi azonosításra alkalmas biometrikus mintázatok, de a jogi szabályozás csak lassan követi le a technikai fejlődés adta sérülékenységi hézagok okozta jogi hiányosságokat. A következőkben röviden ismertetem a hazai és uniós szabályozás által érintett területeket, ennek célja, hogy tárgyalt műszaki megoldások értékét jobban érzékeltethessem a szabályozás tekintetében is.

Az Európai Unió szabályozásának hatásai

Az Európai Parlament és a Tanács 2016. április 27. napján elfogadta a természetes személyek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló általános adatvédelmi rendelet (a továbbiakban: GDPR). A GDPR az Európai Unió teljes területén alkalmazandó, felváltva a korábbi, irányelvek mentén kialakult helyi szabályozásokat. A GDPR értelmében biometrikus adatnak tekintendő minden olyan sajátos technikai eljárásokkal nyert személyes adat, ami egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozik, és amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását. Meg kell jegyezni, hogy a definícióhoz a korábbi jogi meghatározásokhoz képest jobban árnyalja a biometria jelentését, hiszen figyelembe veszi a dinamikus módszerekkel, viselkedésanalízissel történő azonosítást is [1].

A GDPR abból indul ki, hogy a személyes adatok különleges kategóriáinak és az ebbe a körbe tartozó biometrikus adatoknak tilos a kezelése, mert az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok, így egyedi védelmet igényelnek, hiszen az érintettek jogaira nézve a kezelésük körülményei jelentős kockázatot hordozhatnak [1]. A szabályozás célja, hogy a magánszemély kiszolgáltatottságának gátat szabjon, megelőzve a személyes adatok indokolatlan vagy gondatlan kezelését. Bár vélhetően az elkövetkező években lesznek pontosítások a rendelet végrehajtását illetően, az bizonyos, hogy minden biometrikus adatot különleges személyes adatként definiál, aminek oka, hogy azok egyediek és megváltoztathatatlanok. Ez a megkülönböztetés pedig szigorítást is jelent egyben, mert a biometrikus adatok korábban az általános személyes adatok kategóriába tartoztak [2].

2012. április 27-én a GDPR bevezetését megelőzően a 29-es Munka Csoport (aminek feladata volt a rendelet gyakorlati bevezetését megelőzően annak kidolgozása) kiadott egy kézikönyvet a biometrikus adatkezelésekhez fűződően. A Biometrikus Technológiák Fejlesztéséről Szóló Munkaanyag (Opinion 3/2012 on Developements in Biometric Technologies) felhívja rá a figyelmet, hogy a technikai fejlődés következtében a biometrikus adatok szerzése, tárolása és továbbítása sokkal kevesebb akadályba ütközik, így a személyiségek eltulajdonításának a lehetősége abszolút nem elképzelhetetlen. Tehát mindazonáltal, hogy a biometrikus adatokon alapuló azonosítás, vagy a biometrikus adatokat feldolgozó alkalmazások sok esetben kényelmesebbek, megbízhatóbbak, esetleg szórakoztatóbbak, megfelelő jogi alapok által kikényszerített technikai és szervezési intézkedések nélkül komoly adatbiztonsági aggályokat vetnek fel. A Munkacsoport rögzítette, hogy a biometrikus adatok kizárólag csak abban az esetben kezelhetők, ha rendelkezésre áll megfelelő jogalap és a gyűjtésük, illetve további kezelésük célja szempontjából a kezelés megfelelő, releváns és nem túlzott mértékű [1], [3].

Nemzeti szabályozás

A magyar jogrendszerben a biometria értelmezése és szabályozása a gyakorlati hasznosításhoz kötődően jelenik meg. Ennek megfelelően három olyan területet említhető, ahol a biometria megjelenik, de a mögötte lévő definíciók és szabályozás eltérő: az első ilyen terület az orvosi biometria, ami egészen más jelentéstartalommal

bír, mint a biztonsági területen megszokott definíciók. Ebben a kontextusban az orvostudomány matematikai statisztika alapú vizsgálatait értjük alatta. A másodikként említendő biometriával foglalkozó tudományterület, amely már közelebb áll a biztonságtudományokban klasszikusan használt értelmezésekhez, a határ- és rendvédelmi alkalmazás. Ezen területeken a biometrikus adatok kezelésének elsődleges céljai a kriminológiai, valamint idegenrendészeti feladatok ellátása. A harmadik területet nehezebb szűken körülhatárolni, mert igen széles körben jelennek meg felhasználási példák, így összefoglalóan nevezzük a továbbiakban vagyonvédelmi felhasználásnak, hiszen ebben a szegmensben a biometria célja, hogy a javakhoz történő hozzáférést az azonosítási folyamatok optimalizálásával könnyebbé tegye.

A szegmens szereplői számos céllal használhatnak biometrikus adatokat, és ennek megfelelően az eddigi jogi szabályozás leginkább a felhasználás célja szerint vizsgálta azt. Általánosan vonatkozó két főbb jogi szabályozást az adatvédelmi- (2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) és a személy- és vagyonvédelmi törvény (2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól) biztosította. Utóbbi kezeli az elektronikus biztonságtechnikai rendszerek által folytatott megfigyelés, adatrögzítés szabályait, bár részletesen csak a személyes adatokat tartalmazó kép- és hangfelvételek adatkezelését tárgyalja, de azt az adatvédelmi törvénnyel összehangolt módon.

A sportról szóló 2004. évi I. törvényt módosító 2014. évi XXVII. törvény nevezhető az első olyan magyar jogszabálynak, ami explicite definiált nem bűnügyi célú biometrikus személyazonosítási módszereket (képmásból, ujjnyomatból, íriszképből vagy érhálózatból képzett nem visszafejthető, alfanumerikus kód) és azok használatának módját. A stadionok és a sportrendezvények biztonságának céljából e-törvény okán vált lehetővé a biometrikus személyazonosítások alkalmazása az állami szektoron kívül, nem polgári jogi feltételek alapján.

A szabályozásból adódó kockázatok

Vélekedésem szerint a bevezetett általános adatvédelmi törvény jelen formában kettős kockázatot rejt a biometrikus rendszerek használatát illetően. Egyfelől a jogi környezet erősen korlátozza a vagyonvédelmi célú biometrikus azonosító rendszerek alkalmazását,

– ami a technikai fejlődésüket hátráltatja –, másfelől pedig nem definiálja pontosan, hogy a biometrikus mintakinyerési eljárások melyik módja, vagy a kinyerés milyen foka minősíthető még nem különleges személyes adatnak. E kettős kockázat a gyakorlati elterjedést bizonyosan hátrányosan érinti, főleg ha a biztonsági eszközök elrendeléséről döntést hozó vezetőknek mérlegelniük kell a GDPR által kilátásba helyezett bírságok figyelembe vételét is.

Fontosnak megjegyezni, hogy a jogalkotó által definiált kockázatok kezelését azonban nem lehet kiemelve tárgyalni, mert a társuló informatikai és műszaki rendszerek együttes összefüggéseit is figyelembe kell venni. A multimodális biometrikus azonosítás – ahogy ezt a későbbiekben ismertetem – alkalmassá teszi a biometrikus mintakinyerési és összevetési algoritmusokat arra, hogy több forrásból származó, de kevesebb fajlagos információval is kielégítően pontos eredményre vezessenek. Ennek következtében elérhető olyan működési mód, hogy a biometrikus mintaolvasó berendezés önmagában nem azonosítja a felhasználót, csupán olyan adatsort szolgáltat, amivel egy szűkebb osztályba történő besorolás valósítható meg. Több mintaolvasó adatsorának együttes értékelésével a személy egyedi azonosításához szükséges információ-tartalom már elérthető, viszont ennek visszafejtése elegendően bonyolult, hogy a visszaélés kockázata már elhanyagolhatóvá válhasson. Kiindulva azonban a GDPR mögött álló szándékokból, a technológiát megfelelő szabványokkal kell felvértezni, és ennek megfelelően szabványszerűen kell gondoskodni a minta kinyerés, titkosítás és a mesterséges intelligencia alapú értelmezés módjáról [4].

Biometria műszaki és minősítési hátterének ismertetése

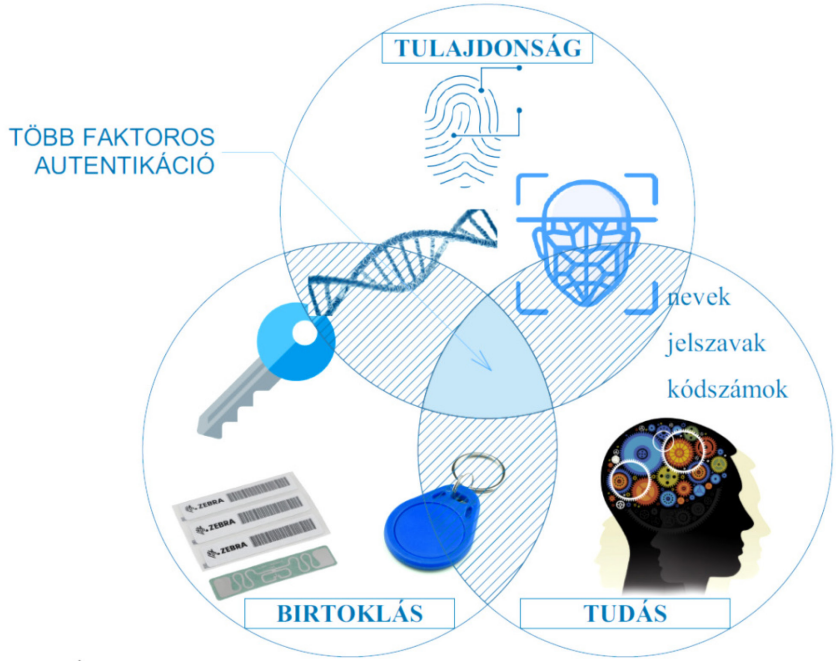
A biometrikus azonosítás módjainak ismertetése

A biometrikus azonosítási eljárásokban valamilyen egyedi jellemzők alapján kölcsönösen egyértelmű megfeleltetést hozunk létre az alany és a kinyert információ tartalma között. Meg kell jegyezni, hogy vannak olyan problémák, ahol elegendő kizárólag osztályozási feladatokat végezni és nem teljes azonosítást, ebben az esetben természetesen nincs kölcsönösen egyértelmű viszony, hiszen az adott minták alapján az egyén szintjén nem lehet visszakövetkeztetni (például: olyan szituáció, ahol csak a résztvevő nők és férfiak biometrikus megkülönböztetése a cél). Az általam vizsgált esetekben azonban mindig személyazonosítási feladatokkal foglalkoztam, így a kinyert

információnak elegendően részletesnek kell lennie az egyértelmű meghatározáshoz. Az, hogy mit jelent az "elegendő" már nehezebb pontosan megfogalmazni, mert függhet a vizsgált csoport nagyságától, a környezeti zajoktól, illetve magától a biometrikus azonosítás módjától is. Tulajdonképpen az értekezésem érdemi részében ezen "elegendőséget" fuzzyfikálom és magyarázom.

A biometrikus azonosítási módszerek műszaki szempontból szintén feloszthatóak, és ahogy ezt a későbbiekben látni fogjuk, kombinálhatóak. Jellemzően megkülönböztethetünk képalkotás alapú technológiákat (ujjnyomat-, írisz-, arc-, erezet-, kézgeometria azonosítás, archőtérkép, illetve aláírás vizsgálat) és nem közvetlen képalkotás módján működő technikákat (hangazonosítás, DNS vizsgálat, viselkedés elemzés illetve billentyű és aláírás dinamika). További megkülönböztetési szempont lehet az invazívitás és a kontaktus, ami szerint beszélhetünk kontaktusmentes (pl. arcazonosítás), vagy teljesen invazív (pl. DNS) elemzési módszerekről. A biometria hibaterhelése, ahogy erről a következő fejezet részletesen beszámol erősen függ a hibák forrásától. Amennyiben például rosszul pozícionáljuk a tenyerünket egy tenyérérhálózatot vizsgáló eszköz felületén, akkor az identifikációs minta összes eleme ugyanattól a hibafaktortól fog szenvedni.

A hibák csökkentése érdekében, illetve egyes objektumokban/felhasználásokban a különlegesen magas biztonsági igények okán úgynevezett többfaktoros azonosítást alkalmaznak. Ennek során több igazolási módszert együttesen kell figyelembe venni. Jellemzően ilyenen a kód+kártya, kártya+ujjnyomat, kulcs+kód megoldások. A módszer lényege, hogy ötvözze a tudás, a birtoklás és a tulajdonság alapú információkat (1. ábra).

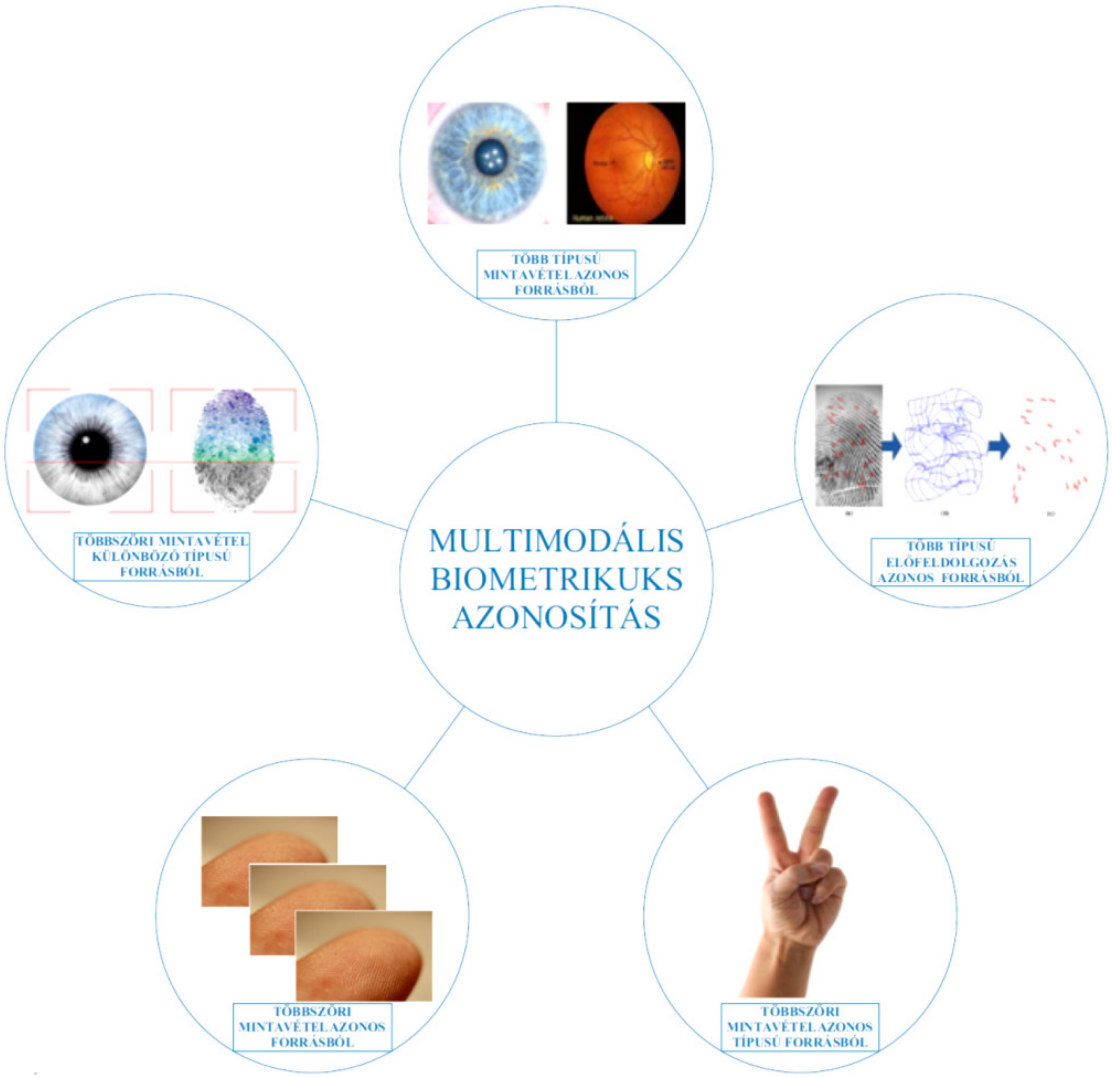


1. ábra: Több faktoros autentikáció

A multifaktoros azonosításhoz hasonlóan, lehetőség van a hibák fajlagos csökkentésének, vagy a biztonsági szint emelésének céljából, kizárólag biometrikus mintákon alapuló többszörös eljárásokra is. Ezt nevezzük multimodális biometrikus azonosításnak.

A multimodalitás többféleképpen megvalósítható, függően attól, hogy milyen eszközparkkal és programozási kapacitással rendelkezünk. Ahogy azt a 2. ábra is szemlélteti a legegyszerűbb esetben egyetlen eszközön ugyanazt a jellemzőt egymás után többször vizsgáljuk, valamivel összetettebb – mivel külön kell feltanítani a forrásokat –, ha ugyanazzal az eszközzel de két külön forrásból – de azonos alanytól származó – biometrikus mintát hasonlítunk össze. Amennyiben lehetőség nyílik a vezérlő algoritmus manipulációjára, akkor használhatunk olyan megoldást, hogy egyetlen olvasóval és azonos forrásból érkező mintákat több különböző algoritmus szerint értékeljük. Ennél bonyolultabb eljárás, amely során ugyan egy forrásból származó, de más típusú információkat olvasunk ki, amihez természetesen legalább két különböző típusú detektorra van szükség. Jó példa erre az írisz és retina szkennelés, vagy a kézgeometria és tenyérérhálózat párosítása, esetleg az ujjnyomat és ujjérhálózat kombinálása. A legösszetettebbnek tekinthető, de teoretikusan a legpontosabb, abszolút

különböző eredendő hibákkal terhelt módszer, ha különböző típusú biometrikus módszereket hasonlítunk össze [5].



2. ábra: Multimodális azonosítási megoldások

A minősítés során alkalmazható jellemzők

A biometrikus azonosítási rendszerek működési jellemzőinek minősítése az eljárások főbb fázisaihoz és folyamataihoz kapcsolódik. Ahogy azt A. K. Jain már a kétezres évek elején ismertette, számítható néhány olyan indexszám, amivel jól jellemezhető egy biometrikus azonosító eszköz működése. Ezek elsősorban a False Rejection Rate (téves visszautasítások aránya, továbbiakban FRR) és a False Acceptance Rate (téves felismerések aránya, továbbiakban FAR). Az előbbi a tévesen visszautasított – jogosultsággal rendelkező – ügyfelek, míg utóbbi a tévesen elfogadott – jogosultsággal

nem rendelkező – ügyfelek számarányát mutatja be. A számarányra tekinthetünk egyfajta valószínűségi együtthatóként is, ennek megítélése a tárgyalt szituáció függvénye [6].

Habár A.K. Jain eredetileg még más megnevezést használt, és első fajú hibaként az FRR-t False Non Match Rate-ként (téves nem egyezési arány) definiálta, míg a másodfajú hibaként azonosított FAR-t False Match Rate-ként (téves egyezési arány) nevezte el. Mára az FAR és FRR megnevezések váltak általánosan elfogadottá, ennek oka, hogy tulajdonképpen ezen megnevezések pontosabbak a rendszerszemléletű működést alapul véve, hiszen a Matching azaz a beolvasott mintából származó információ és a sablon összehasonlítása önmagában még nem képes teljes körűen jellemezni az eszköz, vagy a kialakított rendszer működését [6] [7].

A jelenlegi általános tudományos vélekedés szerint az FAR és FRR értékek között matematikai összefüggés tapasztalható, miszerint ezen értékek egymással fordított arányban állnak. Az FAR és FRR értékei együttesen vizsgálva (egymás függvényében) formálják az Olvasó Működési Karakterisztikát - azaz Receiver Operating Characteristics (továbbiakban ROC) vonalát, amely jól jellemzi egy adott biometrikus eszköz működését a környezeti körülmények tekintetében [8].

Jelen értekezés egyik fő hipotézise éppen ennek a vélekedésnek a megcáfolása, pontosabban átértelmezése annak a megközelítésnek, hogy amennyiben minél kisebb téves elfogadási arányt szeretnénk elérni, – azaz minél biztonságosabb rendszert akarunk működtetni –, annál több lesz a téves elutasítások aránya.

A bemutatott két mérőszám mellett további értékekkel is jellemezhető a biometrikus eszközök működése, ahogyan ezt Kovács Tibor, Milák István és Otti Csaba közös munkájukban ismertették. A biometrikus azonosító eszköz jellemezhető aszerint, hogy mennyire áll ellen az egyes minta-klónozó támadásokkal szemben, ez az ACOM szám (Anti-Cloning Operations Methods), és létezik index érték az eszközök célorientáltságának mérésére is ez a MOA (Mission Oriented Application) [9].

Ezek a módok úgynevezett puha értékeléssel jellemzik a biometrikus azonosítási rendszereket, mert a vizsgálatok során pontosabban kell felmérni a teljes működési környezetet és az alkalmazás feltételeit. A felsoroltakon kívül megemlítendő még az

azonosítási idő és az automatizálhatóság is mint összehasonlításokban szereplő egzakt jellemző.

További származtatott, puha jellemzőket is definiál a szakirodalom a különböző biometrikus azonosító eszközök összehasonlíthatósága végett. Ezen jellemzők skálázása – megfelelő szabvány hiányában – azonban szubjektív módon történik, így inkább kvalitatív mint kvantitatív eredményt adnak, annak ellenére, hogy legtöbbször diszkrét értéket rendelnek az egyes jellemzőkhöz. A biometrikus azonosítás során általánosan vizsgált összehasonlíthatósági szempontok az alábbiak [10]:

- **Egyediség:** minden mintának szükséges, hogy legyen egyedi azonosításra alkalmas mintázata, ami megkülönböztethető más mintákétól.
- **Állandóság**: a biometrikus minta egy bizonyos időszakon belül kellő mértékben változatlanul legyen kinyerhető.
- **Egyetemesség**: a vizsgált populációban a biometrikus minta minden alany esetében kinyerhető legyen.
- **Mérhetőség**: a gyakorlatban alkalmazható technikai módszerekkel jól mérhető az azonításra alkalmas egyedi azonosító jegyek sajátosságait kódoló egyedi jellemző.
- **Összehasonlíthatóság**: a rendszerben meglévő sablon könnyen összehasonlítható legyen a kinyert mintából származó adatokkal.
- **Kinyerhetőség**: ismert technikákkal jól előhívható a biometrikus minta által hordozott egyediséget kódoló információ.
- **Invazívitás**: az emberi test bevonása ne legyen túlzott mértékű az azonosítás folyamatába.
- **Teljesítmény**: együttes mérőszám a pontosság, sebesség és a biztonság vonatkozásában.
- **Elfogadottság**: a társadalom részéről ne legyen elutasított az alkalmazott eljárás.
- **Kijátszás**: ne legyen lehetőség az adott módszert megkerülni.

A felhasználási módtól függően változik, hogy az adott környezetben az azonosítási folyamat melyik érték irányában szenzitívebb. A kritikus infrastruktúrák esetében általában nem okoz problémát, ha nem sikeres minden esetben elsőre azonosítani magunkat, de egy jogosulatlan behatoló bejutása szigorúan elkerülendő, míg egy mobiltelefonos képernyőzár tekintetében a kevés jogosult, és a könnyű kezelhetőség érdekében fontosabb, hogy alacsony legyen a téves elutásítások száma, mégha az FAR ehhez képest relatíve magasabb is.

A **Kinyerhetőség** mint tényező a biometrikus azonosítási eszközök vizsgálata során kiemelten fontos ismertető. A gyakorlatban számos biometrikus rendszer működése nagyságrendekkel is eltérhet a gyártó által megadott és vállalt értékektől, aminek hátterében elsősorban a környezeti hatások (pl.: szenzorok elkoszolódása) és az ember-gép kapcsolat (pl.: rossz elhelyezés) okozta hibák állnak. Bizonyos esetekben az értékelésben figyelembe lehet venni a Failure to Acquire (továbbikaban FTA) értéket is, ami megmutatja, hogy milyen arányban sikertelen az azonosítható minta kinyerése [6]. Azon felhasználási körökben, ahol fontos az azonosítás gyorsasága jellemzően igen alacsony FTA értékkel működő rendszert kell kialakítani.

A jól kinyerhető minták mellett fontos jellemző marad az **Egyetemesség** is, hiszen a piaci környezetben olyan biometrikus azonosító jegyek állják meg a helyüket, amelyek lehetőleg a teljes populáció esetében hordoznak egyedi azonosításra alkalmas információt. Az Egyetemesség mérésére jól alkalmazható mérőszám a Failure to Enrol (továbbiakban FTE), amely megmutatja az adoutt popolációra vonatkoztatva, hogy milyen arányban fordulnak elő azon személyek, akik mintái a kérdéses biometrikus azonosítási technikával nem ismerhetőek fel, így már sablon kinyerése akadályba ütközik.

A kétezres évek végén kezdődött a a felhasználók klaszterekbe sorolása a biometrikus mintáik populáción belüli egymásra hatása tekintetében, így négy virtuális csoport alakítható ki, úgymint a "kecskék", "juhok", "bárányok", valamint "farkasok". A kecskék között magas az egyéni mintázatokban rejlő alapmotívumok közti különbözőség, a "juhok" mintái ezzel szemben sok azonos elemet tartalmaznak. A "bárányok" személyiségi jegyei mások mintáiban is gyakran előfordulnak, míg a

"farkasok" olyan mintázattal rendelkeznek, amiben mások mintázata is megtalálható, így ezeket kijátszhatják [11].

Norman Poh és Josef Kittler kutatásaikban vizsgálták, hogy a fenti klaszterek milyen mértékben fordulnak elő az egyes populációkban. Kutatásaikban különböző kvantitaív módszerekkel vizsgálták, hogy mennyire valószínű egy falhasználó "bárányssága" arc-, ujj- és íriszazonosítási rendszerek adatbázisaiban. Jelentős eredményként kell megemlíteni, hogy a fent említett csoportok aránya függ a vizsgált populációtól és a biometrikus azonosítás módszerétől is, ennek következtében amennyiben csökkenteni akarjuk egy személy besorolásának valószínűségét a bárányok csoportjába, azaz erősítenénk a személyhez füződő biometrikus azonosító jegyek egyediségét a kinyerhetőség szinten tartása mellett, akkor érdemes kvantatíve is megvizsgálni az azonosítási folyamatot, és multimodális biometrikus azonosítási technikát alkalmazni [12].

1 A BIOMETRIKUS AZONOSÍTÁS KVANTITATÍV VIZSGÁLATA

1.1 A kvantitatív módszerek hiba-terhelése

Ahogy az több szakirodalom is tárgyalja, és az Alkalmazott Biometria Intézetben végzett kutatások is bizonyítják, a tapasztalatok alapján a biometrikus azonosító eszközök gyártói által megadott FRR, FAR, FTA és FTE értékek sok esetben akár nagyságrendekben is különböznek a gyakorlati tesztek során mért eredményektől [13] [14] [15].

A különbségek nyilvánvalóan abból fakadnak, hogy a gyártói oldal és a felhasználói oldal nem egységes nézőpontból vizsgálja a működést. Míg előbbinek érdeke, hogy minél jobb színben tüntessen fel egy terméket, ami így a piaci konkurens eszközöknél jobb teljesítménytényezőkkel rendelkezik, addig utóbbi célja, hogy a beszerzett biztonságtechnikai eszközök valóban megfeleljenek a hozzájuk fűzött elvárásoknak, és minden működési körülmény esetén megbízhatóan teljesítsenek.

A gyártók által végzett tesztek során általában kvázi laboratóriumi körülmények között, ideális környezeti viszonyok mellett végzik a vizsgálatokat, esetenként virtuális adatbázisok felhasználásával. Ezzel szemben a gyakorlati alkalmazásoknál számos nem ideális körülmény is előfordul, amelyek zavaró hatása együttesen nagy mértékben befolyásolhatja a működést, így a teljesítménytényezőket is. Például egy hangfelismerő beléptető rendszer esetében nem mindegy, hogy csendes helyiségben vagy egy zajos folyosón alkalmazzák-e az eszközt, vagy esetleg egy arcazonosító eszköz alkalmazása során a teljesítménytényezők erősen függenek attól, hogy kellően tájékoztatták-e a felhasználókat a helyes fejtartásról, távolságról, illetve hogy milyenek a megvilágítás körülményei [16].

3. ábra: Példák biometrikus azonosítási módszerek hibaforrásaira

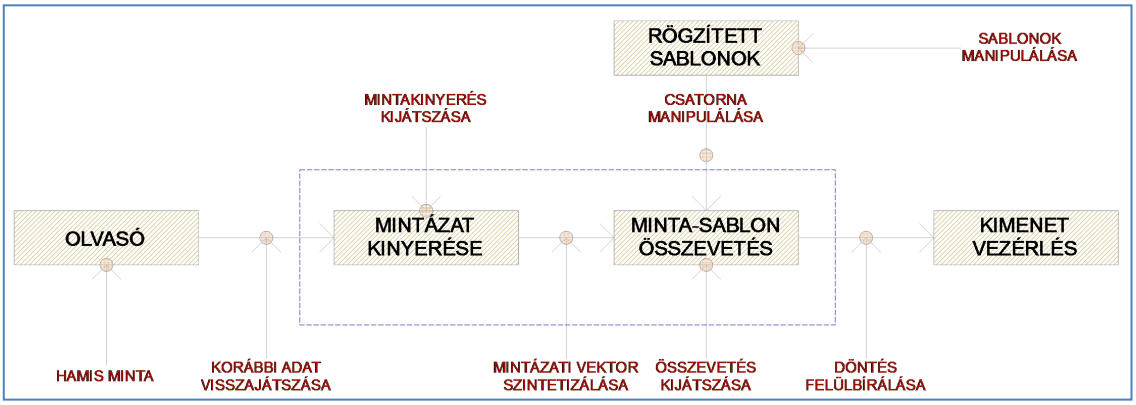
Ahogy a 3. ábra is illusztrálja, a használat során kifejezetten jelentős az időbeli teljesítményromlása azon érzékelőknek, amelyek optikai szenzora kontaktusba kerül a felhasználóval, ilyenek például az ujjnyomat olvasók, amelyek a mindennapi használatból fakadó szennyeződés során akár exponenciálisan rosszabb teljesítménytényezőkkel is működhetnek. Ennek pedig rendszerint kétféle következménye lehet: kikapcsolják az eszközt (esetleg más megoldással helyettesítik), vagy csökkentik az azonosítási küszöt, így viszont lecsökken a szelektivitás és nagymértékben megnő az FAR. A biometria mint tudomány fejlődése szempontjából mindkét lépés kifejezetten káros, hiszen a piaci keresletet hosszabb távon csökkenteni fogja, ami a fejlesztésekre fordított forrást és figyelmet is eliminálja.

Tehát fennáll a kérdés, hogy a biometrikus azonosító eszközök működését javító technikák milyen mértékben és ütemben kerülnek majd beépítésre? Illetve a teljesítménytényezőket melyik fél, esetleg egy független harmadik vizsgálati labor fogja-e elvégezni, illetve van-e egyáltalán piaci létjogosultsága a szigorúbb működési elvárások teljesítésének, amennyiben létezik olcsóbb alternatív biztonságtechnikai megoldás is. Szintén nem maradhat válasz nélkül, hogy a gyártóknak milyen mértékben kell figyelembe venni az alkalmazási körülményeket (populáció méret, környezeti feltételek, beléptetés rendje), amikor a gyári teljesítménytényezőket meghatározzák?

E kérdések megválaszolására nemcsak a nemzetközi szakirodalomban, hanem a hazai tudományos életben is igyekszünk válaszokat adni. Ahogy azt Kovács Tibor és Fialka György is vizsgálta az Alkalmazott Biometria Intézet eredményeit alapul véve. Arra jutottak, hogy a biometrikus azonosító eszközök nagyobb számú felhasználó esetében rosszabb teljesítménytényezőkkel (pl. hosszabb azonosítási idő, nagyszámú FRR) működnek. Ezek nagy mértékben javíthatóak, ha a mintavétel geometriai kialakítását módosítjuk. Például amennyiben a felhasználók rendszerbeli regisztrációjakor használt eszköz geometria elhelyezése hasonló a beléptetés során alkalmazott olvasókéval, akkor szignifikánsan redukálódik az FRR [17].

1.2 Kockázatcsökkentési lehetőségek ismertetése

A kockázat alapú megközelítés értelmében a hibacsökkentésre a teljes azonosítási folyamat tekintetében kell fókuszálni. E gondolat szellemében az értekezést megelőző kutatásokban elsősorban nem azt vizsgáltam, hogy adott biometrikus azonosítási módszer esetében miként javítható a teljesítménytényező, hanem rendszerszintű vizsgálatban – felhasználói populáció, működési körülmények, hibaterjedés, hibaesemények szuperpozíciója, kimeneti igények – miként javítható az azonosítás hatékonysága. Egy biometrikus rendszer működését számos ponton nyílik lehetőség megzavarni vagy kijátszani. Ennek megfelelően nyolc különböző támadási pont (4. ábra) definiálható, de nem csak az aktív manipuláció esetében érdemes ezen pontokat megjegyezni, hanem a véletlen hibák előfordulási lehetőségeként is.



4. ábra: Egy általános biometrikus azonosítási rendszer sérülékenységi lehetőségei [18]

A fenti modell (4. ábra) alapján elmondható, hogy a hibák kockázatának csökkentési lehetőségeit a biometrikus azonosítási folyamatban teljes körűen értelmezve kell

vizsgálni, beleértve a nem megfelelően biztonságos kommunikációs csatornákat, algoritmikus hibákat, vagy akár a fizikai kialakítás szabotázsvédelmét is.

Jelen értekezés megközelítésében az azonosítási folyamatot egy matematikai modellel leírható rendszerként definiálom, amelyben az egyes sérülékenységi pontokra számított kockázati értékek nem összeadódnak, hanem multiplikálódnak. Ezt a megközelítés alátámasztja Bayes függő valószínűségi elmélete, aminek előnyös következménye, hogy a logikai kapcsolatok könnyebben definiálhatóak a rendszerelemek közt, illetve egységesen vehetőek figyelembe az egyes sérülékenységek, függetlenül a biometrikus azonosítás módszerétől [4].

Kutatásaim során arra jutottam, hogy a biometrikus azonosító rendszerek különösen érzékenyek a fajlagos hibákra (adott mintavétel és azonosító vektor előállítása során végbemenő lépésekben bekövetkező hibák), amennyiben ezen fajlagos hibák a végeredményre ható befolyásolása csökkenthető, úgy szignifikánsan javítható az azonosítás hatékonysága. Az értékezés további fejezeteiben elsősorban olyan megoldásokat mutatok be, amelyek alkalmazásával ezen fajlagos hibák multiplikációs hatása mérséklődik. Az alábbi felsorolás négy ilyen megoldást említ, amik közül az első módszerrel csak a bemutatás szintjén foglalkozom, nevezetesen:

- független tesztelési és ellenőrzési szabványrendszer felállítása,
- béta-binomiális eloszlással történő populáció vizsgálat alapú működés,
- multimodális azonosítás alkalmazása,
- mesterséges intelligencián alapuló megoldásokkal történő optimalizálás.

1.2.1 Független tesztelési és ellenőrzési rendszerek születésének bemutatása

Általánosan elmondható, hogy a gyártók részéről megadott tesztek eredményei erősen árnyaltak, a pontosságot mérő értékek tekintetében az első generációs biometrikus eszközökről túlzóan optimisták. A legtöbb mérést ezen eszközök tekintetében a gyártók, forgalmazók végezték, saját laboratóriumban, kevés résztvevő alkalmazásával, így a hibák forrásai jelentősen redukálódtak, az eredmények szignifikanciája a valós működéssel szemben pedig csökkent. Ahogy Anil Kumar Jain is kutatásaiban szót ejt róla, a korai biometrikus azonosító eszközök esetében igen magas FTE értékek fordultak elő, habár sem az FTE sem az FTA értékek nem szerepeltek a gyártói jellemzésekben. Validált tesztek hiányában a mérési módszerek megismételhetőségének hiánya lehetetlenné tette az utólagos ellenőrzést [7] [15] .

A fentiek következményeként ezen rendszerek kiszolgáltatottá váltak a rosszindulatú támadásoknak is, aminek egyik fontos kivédési módszere az élőminta értékelés bevezetése volt. Emellett fontossá vált, hogy teszteket és ellenőrzéseket független külső szervezet végezze, amelyek igény szerint megismételhetők, kiterjednek az összes fontos teljesítmény tényezőre és az eredmények hozzáférhetők. E piaci nyomás következtében állami támogatással jöttek létre olyan szervezetek, amelyek zászlajukra tűzték a minősítés formalizálását: az Egyesült Államokban a Nemzeti Szabványügyi és Műszaki Intézet (National Institute of Standards and Technology) széleskörű vizsgálatokat folytat biometrikus azonosítási módszerek vizsgálatával, amelyek eredményei nyilvánosan megtekinthetőek. Hasonló erőfeszítéseket tettek Európában is az Európai Biometrikus Ellenőrzési Szervezet a BioTesting Europe 2006-os megalapításával, majd European Association for Biometrics 2012-es létrehozásával [7].

Az Egyesült Királyságban már 2000-ben megalakult a Biometria Munkacsoport (Biometric Working Group), kiadva a biometrikus rendszerek teszteléséhez használható legjobb gyakorlatok jegyzékét, amelyet 2002-ben ismét kiadtak egy újragondolt verzióban. A dokumentum három féle értékelési módszer-csoportot definiál (technológia, esemény és működés), amelyek közül ki kell emelni a működés alapú elemzést, mert ennek vizsgálata egy adott környezetre vonatkozik, a felhasználói csoport ismeretében [15]. Ahogy azt a következőkben ismertetem: a Béta-binomiális eloszlás alkalmazhatóságának vizsgálatakor szintén ilyen peremfeltételek mellett kezdtem meg a kutatást.

A nemzetközi tudományos nyomás hatására 2007-ben megszületett az ISO 24709 szabvány a biometrikus rendszerek megfelelőségének teszteléséről. A szabvány kihangsúlyozza, hogy fontos publikálni a részletes eredményeket, a tesztelő környezet pontos fizikai leírását, a vizsgált populáció demográfiai összetételét, és reprezentatív példákat az adatbázisból. Több egyéb ajánlás mellett hivatkozik rá, hogy a tesztelő csoport létszáma haladja meg a 200 főt, a felhasználók legyenek kiképezve a használatra, valamint a felhasználók köre ellenőrizzék kor és nemek megoszlásának tekintetében. A termékválasztási folyamatban kiemelt fontosságú, hogy olyan megoldásokat fontoljanak meg, amelyek megfelelnek a működési követelményeknek,

beleértve az FTE, FTA, FAR és FRR tényezőket is, valamint egyéb jellemzőket, mint például az átviteli teljesítmény és az adatbázis kapacitása [6] [7].

1.2.2 A kockázat alapú megközelítés valószínűségi modellje

Ahogy azt béta-binomiális eloszlás vizsgálatánál említettem, a hibák kockázatának egyik lehetséges megoldási módszere a környezet és a felhasználói kör alapos vizsgálata. Egy statisztikai adatbázis alkalmazásával előre becsülhető a zavaró hatások valószínűsége, és ennek következtében megfelelő módszer adható az azonosítás hatékonyságának növelésére. Mindazonáltal a legtöbb esetben a zavaró impulzusok nem folytonosak és kumulált hatásuk is nehezen becsülhető. Tehát, ha az adott fajlagos hibák nem minimálisak, akkor az eredmény érzékennyé válik a szélső értékekkel szemben, következésképpen megnő a téves elutasítások száma.

A fajlagos hibák hatásának csökkentése érdekében jó módszer, ha csökkentjük azok szerepét a végső értékelés tekintetében, azaz szétosszuk az egyes hibaforrások hatást befolyásoló tényezői értékét. Az elosztott fajlagos hibák módszerének egyik megvalósítása a multimodális biometrikus azonosítás alkalmazásával érhető el. A hatékonyság növelése érdekében vizsgált módszer bemutatását az azonosítási folyamat valószínűségi modelljének ismertetésével kezdem: alapvetően számos tényező együttes hatása van jelen a biometrikus azonosítási folyamatban, és ezek kumulált hatása jelenik meg a végeredményben is. Sztochasztikus rendszerekben nehezen becsülhető a tényezők elemi hatása, így abból kiindulva, hogy a vizsgált alany viselkedése, a környezeti tényezők és a természetes emberi változások miként változtatják meg a teljes folyamat végeredményét nem lenne célszerű kiindulni. Ellenben a folyamatok egymásra épülése miatt az egyes hatások között függő valószínűségi viszony van, így a kutatásban Bayes függő valószínűségi modelljét alkalmaztam. A Bayes analízis lefolytatva tudjuk, hogy az *a priori* paraméterek ismeretében statisztikus alapon is jobban becsülhető az *a posteriori* valószínűség. Ennek matematikai megfogalmazása halmazműveletekkel az alábbi [19]:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}; \quad P(B|A) = \frac{P(A \cap B)}{P(A)} \qquad \text{(1/a - 1/b)}$$

$$P(A|B)P(B) = P(B|A)P(A) \qquad (2)$$

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}, \tag{3}$$

ahol *P(A) = a priori* valószínűség, *P(B)= a posteriori* valószínűség.

A felírt függő valószínűségi rendszer kiterjeszthető teljes eseményrendszerre és többszörösen függő eseményvonalakra is, amelyek alkalmazása a mi esetükben is indokolt, mert a multimodális biometrikus azonosítás folyamatában – ahogy azt a későbbiekben ismertetem – akár kettőnél több mód és többszörös ok-okozati viszony is fennállhat.

Teljes eseményrendszer esetén:

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{P(B)} = \frac{P(B|A_i)P(A_i)}{\sum_i P(B|A_i)P(A_i)} \tag{4}$$

Többszörösen függő valószínűségek esetén:

$$P(X_1, \dots, X_n) = P(X_n) \prod_{i=1}^{n} P(X_i|parents(X_i)) \tag{5}$$

A Bayes elmélet jól alkalmazható a biometrikus azonosítás folyamatára, de a fenti modellel leírt rendszer pontossága javítható, amennyiben a béta-binomiális eloszlást alkalmazzuk az *a priori* paraméterekre [20]. A vizsgált populáció (felhasználói kör) mintáinak minőségi becslésével a Bayes analízis alkalmazása során nagyságrendekkel jobb biometrikus azonosítás is elérhető, ha a multimodális módon ellenőrizzük a jogosultságokat. Ennek korai kutatása 2000-es évek második felében a John Hopkins egyetemen kezdődött meg, ahol ismert statisztikai eloszlások alkalmazhatóságát vizsgálták az *a priori* paraméterek minősítésére [4].

1.2.3 A béta-binomiális eloszlás szerepe biometrikus azonosításban

További kutatások is igazolták, hogy az úgynevezett gamma eloszlás alkalmazása szignifikánsan javíthatja az azonosítás hatékonyságát, de fontos kitérni két matematikailag kezelendő nehézségre, így a kockázatokat meghatározó tényezők számítási módszerére és a multimodális részeredmények összesítésének számítási módjára [21]. Jelen munkában ezeket a III. fejezetben, a lágy számítási módszereknél tárgyalom.

A biometrikus azonosítás során nem olyan állandó paraméterekkel rendelkező azonosításra alkalmas jellemzőket vizsgálunk, mint a kártyás vagy kódos azonosítások során, hanem idővel változó és a környezeti tényezőkre is érzékeny biológiai tulajdonságokat. Ennek megfelelően egy adott felhasználói körben vizsgálva a biometrikus azonosítások hatékonyságát megfigyelhető, hogy egyes alanyok esetében az FRR értéke az átlaghoz képest jelentősen eltér. Az eltérés mindkét irányban előfordul, tehát vannak olyanok, akik könnyebben, mások nehezebben azonosíthatóak az adott körülmények között.

Nagyon fontos kihangsúlyozni, hogy az eltérést mindig relatíve kell vizsgálni, és tulajdonképpen ez a relativitás az, amit a kutatásom során megragadtam. A biometrikus azonosító eszközök egy élő, vagy mesterséges mintasorozat szerint kapják meg az alapbeállításokat, és ezen beállításokat jellemzően később nem lehet megváltoztatni. Azonban a gyárilag beállított értékek során alkalmazott körülmények és a felhasználói kör jellemzői közel sem biztos, hogy azonosak a későbbi alkalmazás körülményeivel. A feltételezésem szerint a fent bemutatott Bayes elmélet gyakorlati alkalmazása az adott körülmények között az alábbi mód szerint végső soron javítani fogja az átlagos FRR értékét.

A Bayes elmélet értelmében meg kell határozni, hogy a téves elutasítások esetében a tévesen azonosított valós minták előfordulása milyen valószínűséggel jelenik meg az ismert populáció és körülmények esetében. Jelen esetben általában igen kicsi értékekről beszélünk, amit általában Poisson eloszlással közelítünk, viszont a Poisson eloszlás tulajdonképpen a binomiális eloszlás egy határeloszlása aszimmetrikus valószínűségi tényezők esetében. Így jelen esetben a közelítést a binomiális eloszlással közelítettem, általánosítva és pontosítva a modellt.

A vizsgálat kulcsa az volt, hogy miként tudom meghatározni a binomiális eloszlás valószínűségi tényezőit a kis mintás kísérletben. Az *a priori* hiba eloszlást valójában azonban se Poisson, se binomiális eloszlással nem becsülhető, ezért bevezettük a béta-binomiális eloszlással történő közelítést. A béta-binomiális eloszlás alkalmazásával a binomiális eloszlásból ismert *p* valószínűségi változó értéke nem egy konstans, hanem paraméterekkel (*alfa* és *béta*) jellemezhető eloszlás. A Bayes elmélet tekintetében pedig

kimondható, hogy amennyiben az *a priori* eloszlás béta és az átviteli eloszlás pedig binomiális, akkor az *a posteriori* szintén béta [22].

A binomiális eloszlás szerint, amennyiben a minta számossága *n* és *x* azon esetek száma, amelyek során rendszer nem fogadott el valós (jogosult) mintát:

$$P(x) = \binom{n}{x} \cdot p^x \cdot (1-p)^{n-x} = f(x|n,p) \tag{6}$$

A fenti binomiális eloszlás *p* valószínűségi tényezője pedig az alábbi alfa és béta értékekkel paraméterezett eloszlást követi:

$$p(\alpha,\beta) = \frac{1}{B(\alpha,\beta)} \cdot p^{\alpha-1} \cdot (1-p)^{\beta-1} = f(p|\alpha,\beta) \tag{7}$$

A konjugált *a posteriori* béta eloszlás:

$$P(x|n,\alpha,\beta) = \int_0^1 f(x|n,p) \cdot f(p|\alpha,\beta)dp \tag{8}$$

A béta függvény kifejezhető a Gamma függvénnyel:

$$B(\alpha,\beta) = \frac{\Gamma(\alpha)\cdot\Gamma(\beta)}{\Gamma(\alpha+\beta)} \tag{9}$$

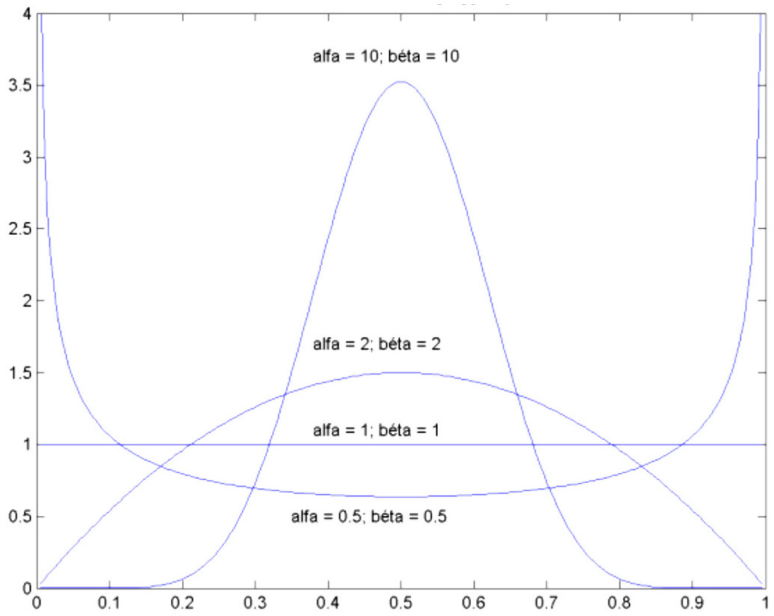
Végezetül, parciális integrálást követően megkapjuk a béta-binomiális eloszlást Gamma függvénnyel kifejezve:

$$P(x|n,\alpha,\beta) = \binom{n}{x} \cdot \frac{\Gamma(\alpha+x)\cdot\Gamma(\beta+n-x)}{\Gamma(\alpha+\beta+n)} \cdot \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} = f(x|n,\alpha,\beta) \tag{10}$$

Tehát levezethető, hogy az (α,β) paraméterekkel meghatározható a binomiális eloszlás sűrűségfüggvénye, habár ezen paraméterek definiálása komplex feladat. A paraméterek jelentősen eltérőek lehetnek a vizsgált populáció és környezet szerint, így fontos volt megtalálni azt az algoritmust, amellyel automatizálni tudtam a paraméterek kiolvasását a kísérletek során.

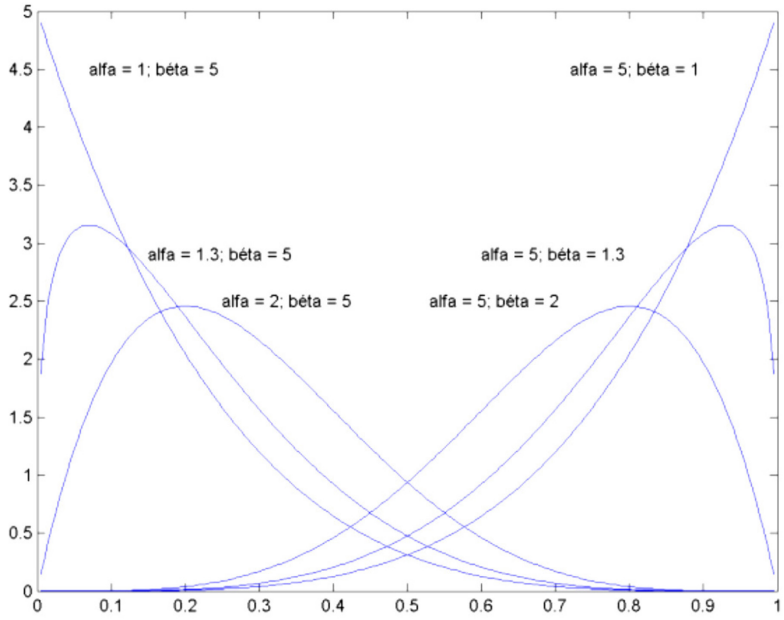
Ahogy az 5. ábra is látható, amennyiben az α és β paraméterek egyenlők ($\alpha = \beta$), akkor a sűrűségfüggvény szimmetrikus. Amennyiben pedig mindkét paraméter értéke egységesen egy, akkor a sűrűségfüggvény konstans. Ebben az esetben a *p* valószínűségi tényező értéke azonos valószínűséggel lehet bármekkora értékű a [0-1] intervallumon,

vagyis ez esetben az *a posteriori* valószínűség normál binomiális eloszlással meghatározható [22].



5. ábra: Béta eloszlás sűrűségfüggvénye azonos α és β paraméterek esetén [20]

Analizálva a biometrikus azonosítási módszer matematikai modelljét arra a következtetésre jutottam, hogy például a biometrikus minta beolvasása során egymás követő egyedi azonosító jegyek hibás azonosításának, vagy téves elutasításának valószínűsége eltérő, de ugyanez igaz makró szinten is, tehát például egy napi azonosítási sorozatban annak valószínűsége egy-egy felhasználót egymás után többször tévesen azonosít, vagy tévesen elutasít a rendszer más és más a valószínűsége. E megfigyelés igazolására a fenti matematikai módszerek alkalmaztam és készítettem egy algoritmust, amivel a béta-binomiális eloszlás paraméterei meghatározhatóak. A 6. ábra szemléltetem azokat az eseteket, amikor az α és β paraméterek eltérőek, így a valószínűségi érték sűrűségfüggvénye is aszimmetrikussá válik.



6. ábra: Béta eloszlás sűrűségfüggvénye eltérő α és β paraméterek esetén [20]

A felvázolt modellben az alapgondolat az, hogy amennyiben α és β paraméterek értéke ismert, akkor meghatározható az *a posteriori* eloszlás eredménye, azaz becsülhetővé válik, hogy a kérdéses biometrikus azonosító eszköz az adott környezetben, az aktuális felhasználói körrel milyen megbízhatósággal fog működni.

Ellenben az α és β paraméterek meghatározása matematikailag összetettebb feladat, a megoldását a maximum-likelihood becslési módszerrel végeztem, azaz ahol az alapfüggvény loglikelihood parciális deriváltja zérus, ott szélsőérték (maximum) van. Az alapfüggvényünk (10) logaritmizálása és parciális deriválása után az alábbi Jacobi-mátrixot kapjuk:

$$F(\alpha,\beta) = \sum_{x=1}^{n} f_x \cdot A(\alpha,x) - N \cdot A(\alpha+\beta,n) \qquad (11/a)$$

$$G(\alpha,\beta) = \sum_{x=1}^{n} f_{x-n} \cdot A(\beta,x) - N \cdot A(\alpha+\beta,n) \qquad (11/b)$$

ahol:

$$N = \sum_{x=0}^{n} f_x \qquad A(\alpha,x) = \frac{1}{\alpha} + \frac{1}{\alpha+1} + \cdots + \frac{1}{\alpha+x-1} \qquad (12)$$

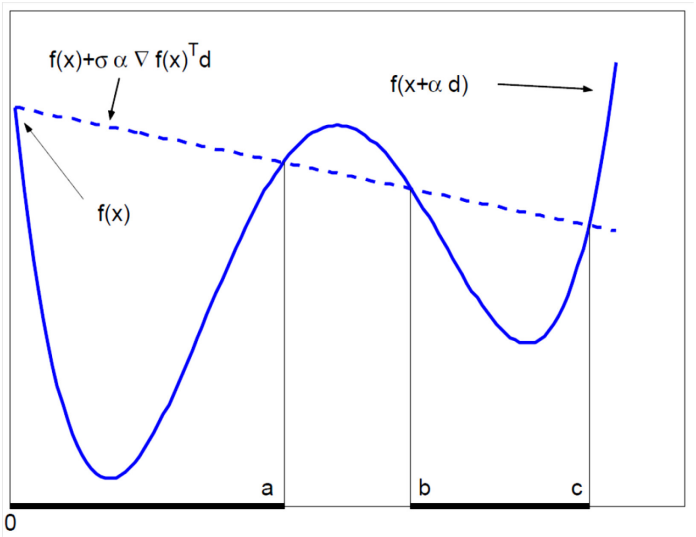
$$A(\beta,x) = \frac{1}{\beta} + \frac{1}{\beta+1} + \cdots + \frac{1}{\beta+n-x-1} \qquad (13)$$

$$A(\alpha+\beta,n)=\frac{1}{\alpha+\beta}+\frac{1}{\alpha+\beta+1}+\cdots+\frac{1}{\alpha+\beta+n-1} \tag{14}$$

Ahogy látjuk a paraméterek meghatározásához iterációra volt szükség. Több féle iterációs módszert is megpróbáltam, de sem a Newton-Raphson sem a fixpont iteráció nem vezetett eredményre, mert a konvergencia nem volt kvadratikus. Végül az Armijo-Goldstein féle gradiens módszer sikeresen konvergált. E módszer lényege, hogy a Jacobi mátrix gradiense nem negatív függvény (15), és ahol a gradiens a legnagyobb mértékben változik ott lesz az eredeti függvény szélsőértéke. A közelítés során be kell vezetni további két konstanst (ε,η) a lépésszám és a közelítés sebességének optimalizálására [23] [24] [25].

$$\underline{g}(\underline{x})=\underline{f}(\underline{x})^T\cdot\underline{f}(\underline{x})=\left|\underline{f}(\underline{x})\right|^2=F(\alpha,\beta)^2+G(\alpha,\beta)^2 \tag{15}$$

Ismeretes, hogy a közelítő függvény legmeredekebb iránya a konjugált gradiens, de hogy elkerüljük a túl nagy lépéseket és a túl kicsi közelítési sebességet az Armijo-Goldstein kritériumok (16) alkalmazását kell bevezetni [24].



7. ábra: Armijo-Goldstein kritériumok illusztrálása [24]

$$(1)\ \underline{g}\left(x-t\cdot\nabla\underline{g}(\underline{x})\right)\le\underline{g}(\underline{x})-\varepsilon\cdot t\cdot\left|\nabla\underline{g}(\underline{x})\right|^2 \tag{16/a}$$

$$(2)\ \underline{g}\left(x-\eta\cdot t\cdot\nabla\underline{g}(\underline{x})\right)\ge\underline{g}(\underline{x})-\varepsilon\cdot\eta\cdot t\cdot\left|\nabla\underline{g}(\underline{x})\right|^2 \tag{16/b}$$

A megfelelő konstansok, kezdőérték és megállási kritérium(ε, η, t_0, Δt) megadásával kellően pontosan meghatározhatóak az α és β paraméterek. A paramétereket ezután már csak be kell helyettesíteni az alábbi (17) egyenletbe és megkapjuk az *a posteriori* béta-binomiális eloszlás értékét.

$$P(x|n,\alpha,\beta) = \binom{n}{x} \cdot \frac{B(\alpha+k;\beta+n-k)}{B(\alpha,\beta)} \tag{17}$$

A kutatásom során a fent leírt matematikát első sorban a tévesen elutasított esetek vonatkozásában vizsgáltam. Ennek oka egyfelől az, hogy a téves elutasítások aránya minden típusú biometrikus azonosítási módszer esetében nagyságrendekkel magasabb a téves elfogadásnál, tehát jóval többször fordul elő. Otti Csaba vizsgálatai értelmében ez esetenként a felhasználói oldal részéről már nem elfogadható, így végső soron az eszközök mellőzéséhez vezet [13].

A kísérlet során nyolc önkéntessel folytattam le egy tíz sorozatból álló kísérletet. A résztvevők nem rendelkeztek számottevő tapasztalattal a biometrikus azonosító eszközök működése terén, vélhetően éppen ennek egyik eredménye, hogy idővel jelentős mértékben javult a téves elutasítások száma. Minden sorozatban tíz alkalommal kellett megkísérelniük az azonosítást. Az azonosítás környezete a kísérlet során nem változott, az elhelyezés és egyéb környezeti zavarok hatása állandónak tekinthető a teljes kísérlet során. A vizsgálat célja az volt, hogy igazolhatóvá váljon a feltevés miszerint a felhasználói kör biometrikus azonosíthatóságának ismerete javíthatja az azonosítás hatékonyságát. Fontos kiemelni, hogy nem a biometrikus azonosító eszköz működése jobb vagy rosszabb, hanem az adott körülmények és felhasználói körhöz képesti teljesítmény.

A vizsgálat során összehasonlítottam a hibák előfordulását jellemző egyéni sűrűségi eloszlásokat a felhasználói körre általánosan jellemző sűrűségi eloszlással, így megkaptam, hogy egy felhasználóra vonatkozó FRR várhatóan magasabb vagy alacsonyabb lesz. Meg kell jegyezni, hogy a nyolc önkéntes ujjnyomat mintáiból négy önkéntes mintázata olyan mértékben volt deformált vagy sérült, hogy az abból származó adatokat nem tudtam figyelembe venni, mert hatásuk nagyon jelentős mértékben torzította volna az eredményt. A deformáció mögött a vizsgált ujjak fizikai sérülése állt.

Az így kapott összes esetből (400 azonosítási kísérlet) közel 20%-ban (83 eset) a használt biometrikus azonosító eszköz (iEVO micro ujjnyomatolvasó[1]) nem fogadta el a mintát jogosult felhasználótól. Az első fejezetben már kifejtett okokból is következik, hogy ez az érték nagyságrendekkel tér el a gyártó által közölt teljesítmény tényezőtől, a gyári 0,1%-os értékekkel szemben 1-20%-os téves elutasítási arány is tapasztalható.

Az így vizsgált módszer alapján tehát béta-binomiális eloszlással előre becsülhető, hogy mekkora a valószínűsége az egyén, vagy a teljes felhasználói kör szintjén is a többszörös hibák bekövetkezésének, sőt megadható az eloszlás szórása is. (18) Ez ebben a formában egy sokkal egzaktabb, de összetettebb módja a biometrikus eszközök minősítésének [26].

$$FRR = \sum_{x=0}^{k-1} \binom{n-1}{x} \cdot p^{n-x-1} \cdot (1-p)^x \tag{18}$$

ahol: *k* a legkisebb száma az azonosításhoz szükséges egyedi azonosító jegyeknek, és *p* az azonosítás hibáinak valószínűsége. A Bayes-tétel alkalmazásával határozzuk meg az *a posteriori* eloszlást. Eltekintve a nevezőtől, mint normáló tényezőtől, a hiper-paramétereket is hangsúlyozva, írható, hogy [26]:

$$P(p|x,\alpha,\beta) = f(x|p,\alpha,\beta)P(p|\alpha,\beta) \sim \frac{n!}{k!(n-k)!} p^x (1-p)^{n-x} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{19}$$

Összevonva és a konstans szorzóktól eltekintve kapjuk, hogy:

$$P(p|x,\alpha,\beta) = \binom{n}{x} \frac{1}{B(\alpha,\beta)} p^{\alpha+x-1}(1-p)^{n-x+\beta-1} \sim \frac{1}{B(\alpha+x,\beta+n-x)} p^{\alpha+x-1}(1-p)^{\beta+n-x-1} \tag{20}$$

Ami ugyancsak béta eloszlás $\alpha + x$, $\beta + n - x$ paraméterekkel, tehát az *a posteriori* eloszlás: Beta($\alpha + x$, $\beta + n - x$). A fentiek következménye, hogy ha binomiális eloszlást alkalmazunk likelihood függvényként, és béta eloszlást *a priori* eloszlásként, az *a posteriori* eloszlás ugyancsak béta eloszlású lesz. Ez úgy is fogalmazható, hogy a binomiális eloszlás konjugáltja a béta eloszlás. Az *a posteriori* eloszlásból kapjuk a

[1]http://www.stanleypac.com/Products/iEVO/PDF%20Resources/PAC%20iEVO%20Fingerprint%20Reader%20Series.pdf

binomiális eloszlás *p* paraméterének frissített értékét. Így alkalmazhatóak a bemutatott paraméterek, amelyeknek aktualizált értéke [26]:

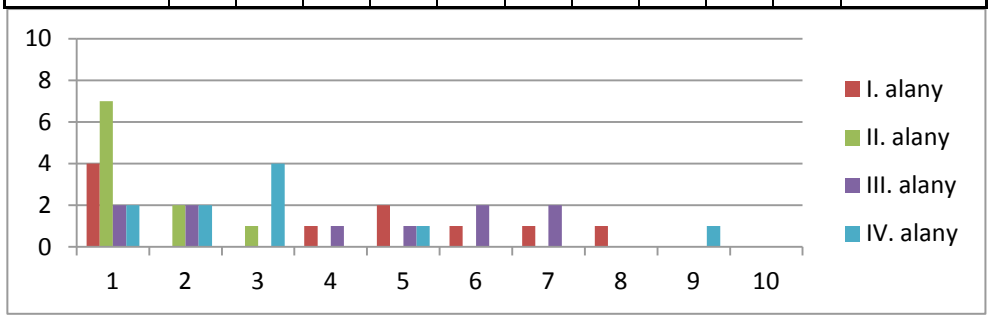
$$E' = \frac{\alpha+x}{\alpha+\beta+n}; Var' = \frac{(\alpha+x)\cdot(\beta+n-x)}{(\alpha+\beta+n)^2\cdot(\alpha+\beta+n+1)} \tag{21}$$

A fentiekből következik, hogy ha sok a mérési adat, kevésbé dominál a szubjektívnek tekinthető *a priori* béta eloszlás, a szubjektivitásnak pedig így egyre kisebb a hatása az *a posteriori* eloszlásra. Végül, ha n→∞, akkor tekintettel arra, hogy a szórásnégyzet (Var) nevezője az *n* magasabb fokú polinomja, mint a számláló, következik, hogy Var'→0, tehát az *a posteriori* becslés bizonytalansága egyre kisebb [26].

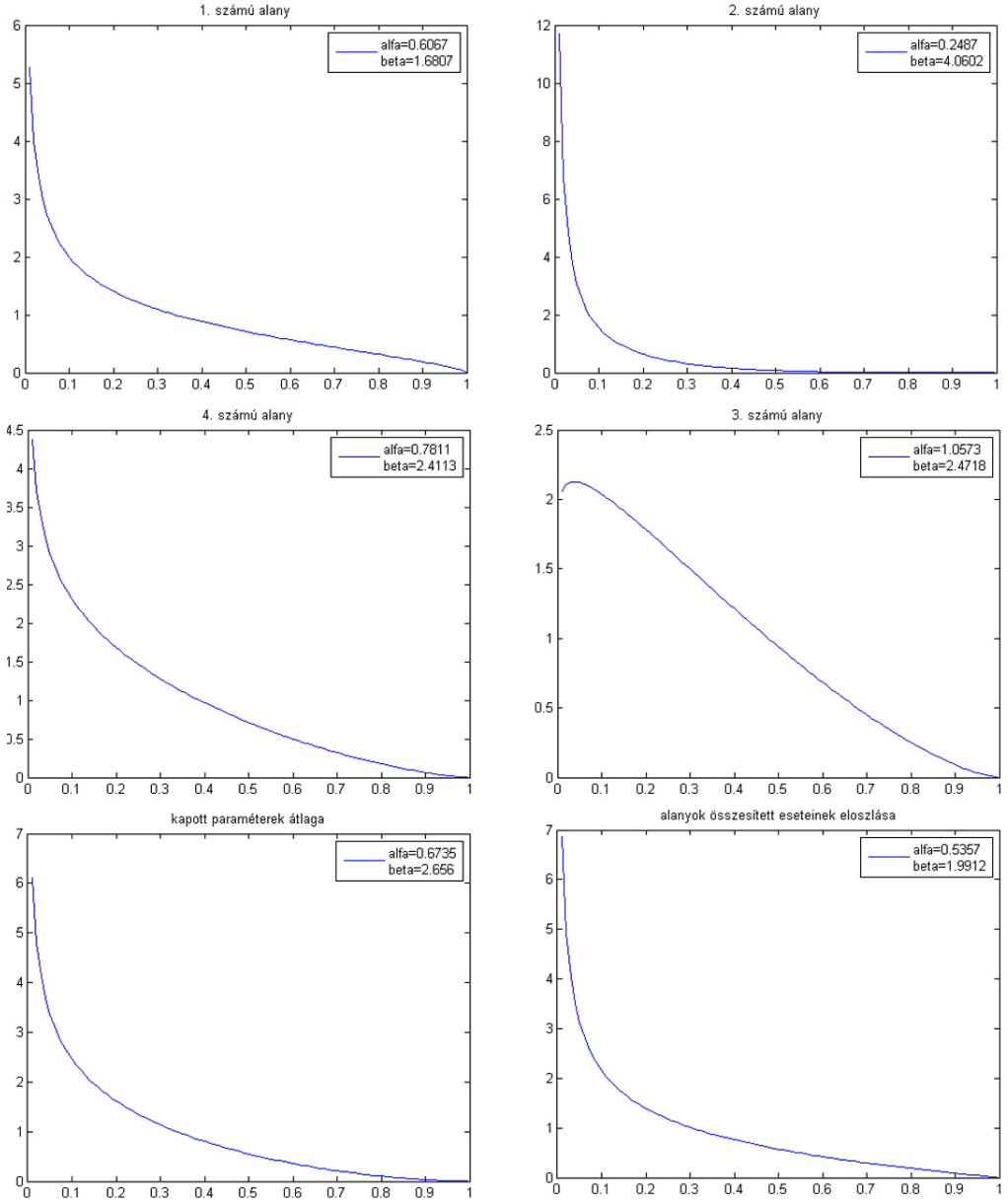
A kísérletből származó eredményeket az alábbi táblázat foglalja össze. Ebből jól látható, hogy bár eltérőek az értékek, tipikusan és empirikusan levonható, hogy a legjellemzőbb, hogy nincs, vagy egyetlen hiba volt az azonosítási sorozatban (tíz kísérlet). Természetesen fontos jelen pontnál megemlíteni, hogy a mért értékek relevanciáját is figyelembe kell venni, így módszer teljes körű validálásához szükségszerűen el kell végezni nagy mintás méréseket is.

1. táblázat: Azonosítási kísérlet során mért téves elutasítások száma (10x10 próbálkozásból)

VIZSGÁLAT SORSZÁMA	0	1	2	3	4	5	6	7	8	9	SZUM
I. alany	4	0	0	1	2	1	1	1	0	0	29
II. alany	7	2	1	0	0	0	0	0	0	0	4
III. alany	2	2	0	1	1	2	2	0	0	0	32
IV. alany	2	2	4	0	1	0	0	0	1	0	18
Átlagosan	3,75	1,5	1,25	0,5	1	0,75	0,75	0,25	0,25	0	20,75
Összesítve	15	6	5	2	4	3	3	1	1	0	83



A bemutatott matematikai módszertant alkalmazva felhasználónként és a teljes felhasználói körre is, meghatároztam az α és β paramétereket. Az eredményeket illusztrálja az alábbi 8. ábra.



8. ábra: A valószínűségi változó eloszlásfüggvényei a kapott α és β paramétereket alapján

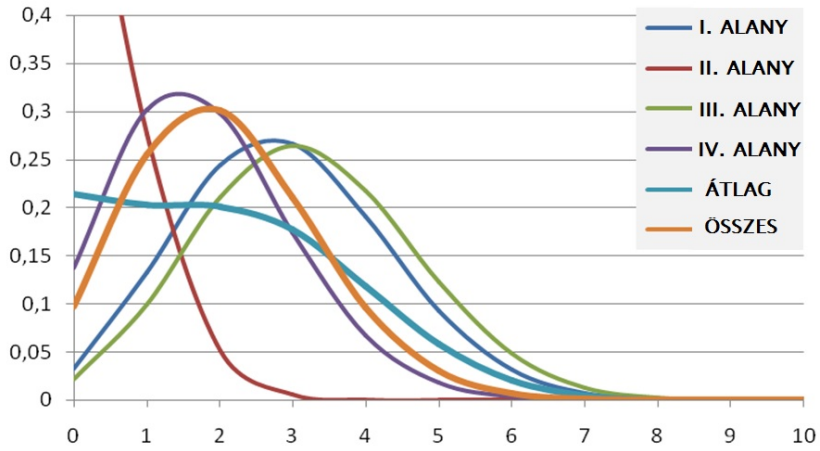
Az ismertetett matematikai módszert MATLAB környezetben komponált algoritmussal hívtuk életre, de a szignifikancia vizsgálat során meg kellett állapítani – bár az eredmények igazolják a hipotézist – a nagymintás vizsgálat lefolytatása megbízhatóbbá tenné az igazolást. 90%-os konfidencia szinten a Doddington féle 30-as szabály a kapott értékeket kielégítik, azaz az észlelt hibajelenségek száma elégséges a vizsgálathoz. Az értékek elfogadhatóságát igazolhatja kutatótársaim arcfelismerő berendezésen

folytatott, azonosan elfogadható eredményt hozó vizsgálata [27]. A kapott eredmények (7. ábra) elemzése során az alábbi következtetéseket lehet levonni:

- az elvárásoknak megfelelően, a felhasználónként számított valószínűségi eloszlások eltérőek. Van felhasználó, akinek az átlaghoz képest szignifikánsan jobb a biometrikus azonosítási hatékonysága (ennek oka vagy a helyesebb eszközhasználat, vagy a jobban beolvasható biometrikus minta lehet),

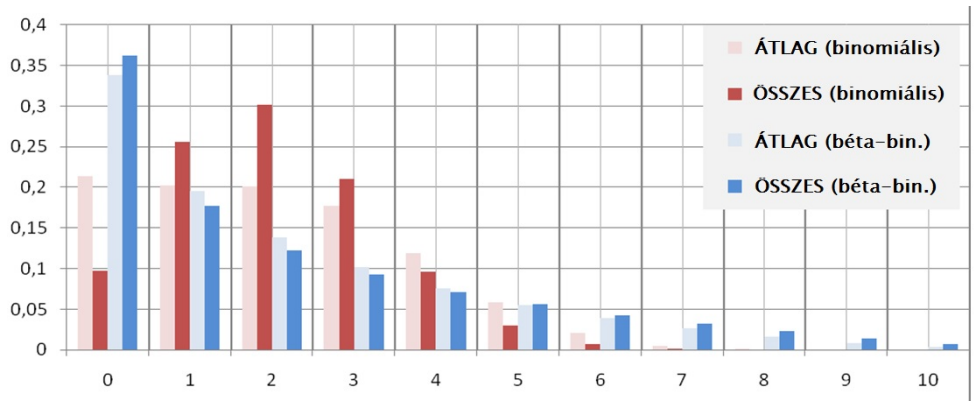
- általánosan számolva a zérus hiba valószínűsége 35%, szemben a normál binomiális közelítéssel, ahol ez az érték 10-15%, tehát a béta-binomiális közelítés jobban tükrözi a valóságos működést

- a normál binomiális eloszlással szemben a béta-binomiális eloszlás esetén a várható hibák valószínűségi értékének maximuma nem zéró hibánál, hanem 1-3 hiba esetén van, azaz valószínűbb, hogy a teljes sorozatban lesz, akár több hiba is, mint egy se.



9. ábra: Tapasztalati valószínűségi sűrűség eloszlás béta-binomiális eloszlás esetén

A fenti 9. ábra tekintetében meg kell jegyezni, hogy a feltüntetett értékek diszkrétek, így azokat helyesebb oszlopdiagramként bemutatni:



10. ábra: Tapasztalati valószínűségi értékek normál binomiális és béta-binomiális eloszlással számolva

1.3 Első főfejezet összefoglalása

A digitális biometrikus azonosítási módszerek fiatalsága és gyors fejlődése okán a tudományos kutatások eredményei nehezebben jutnak el az alkalmazási területet szabályozó ipari és jogi döntéshozókhoz. Az egyetlen olyan szabványcsalád, ami a biometrikus eszközök tesztelésével foglalkozik az ISO/IEC 24709-1:2017. Ennek megfelelősége azonban még mindig kérdéses, mert előírja ugyan kvantitatív módszerekkel igazolt vizsgálatokat, de pontos technológiai utasításokat nem tartalmaz a biometrikus azonosításra alkalmas eszközök minősítését illetően. A szabályozás hiányossága okán bevezetek egy új megközelítést, amiben a sérülékenységet kockázati alapon közelítem meg. Ennek következtében olyan kvantitatív modellt alkottam, amivel jobban összemérhetőek a biometrikus azonosító eszközök ismert környezetben.

A fejezetben kitérek rá, hogy Bayes függő valószínűségi elméletét alkalmazva a környezeti hatások zavarának együttes hatása leginkább kockázat alapú szemlélettel közelíthető. A felvázolt valószínűségi modell szerint béta-binomiális eloszlás alkalmazásával egy kismintás kísérletben választ kaphatunk, hogy egy adott populáció és környezet esetében melyik biometrikus azonosítási megoldás a legalkalmasabb. Meg kell jegyezni, hogy ez a megközelítés minden eddigi vizsgálati módszernél nagyobb tekintettel van a felhasználói kör és környezet hatásaira, sőt nem csak arra alkalmas, hogy összemérje a különböző módszereket, hanem a várható téves elutasítások vagy elfogadások számáról is szignifikáns eredménnyel szolgál.

2 LÁGY SZÁMÍTÁSI MÓDSZEREK ALKALMAZÁSA MULTIMODÁLIS BIOMETRIKUS AZONOSÍTÁSBAN

2.1 Alkalmazási lehetőségek általános ismertetése

Retter Gyula szavait idézve, a lágy számítások ismertetését érdemes azzal a frázissal kezdeni, hogy az emberiség a XX. század közepén újra felfedezte saját zsenialitását. A leírás roppant találó, mert a lágy számítások három fő csoportját alkotó módszer mind visszavezethető természeti folyamatokhoz, és tulajdonképpen így el is juthatunk a mesterséges gondolkodás fogalmához [28].

A lágy számítások közé sorolt legrégebbi módszer az emberi gondolkodás és döntéshozás szisztematikáját ragadta meg, ez a fuzzy logika. Az emberi agy biológiai működését és a tanulás folyamatát matematikailag is implementáló technikákat mesterséges neurális hálózatoknak nevezzük, míg a természetes kiválasztódás és az evolúció évmilliós optimalizálási eljárását a genetikus vagy más néven evolúciós algoritmusokkal lehet mesterséges módon modellezni [29].

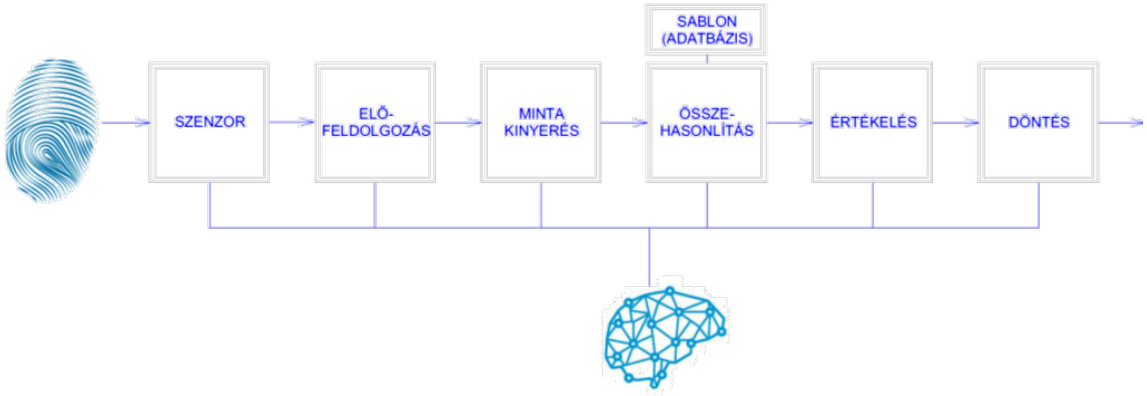
A fenti módszerek bizonyos kombinációja és kiterjesztése vezet el a gépi tanuláshoz (machine learning), vagy ahogy a szakirodalom ma ezt nevezi a *deep learning*-hez. Az általam korábban gépi gondolkodásnak nevezett módszertan pedig a megfelelő adatbázissal, a szükséges validálás és verifikáció után nevezhető mesterséges intelligenciának is (továbbiakban MI).

Meg kell jegyeznem, hogy a mesterséges intelligenciára számos definíció létezik, a maga módján sok találó, de jelen értekezés szempontjából maradnék az MI atyja, John McCarthy által definiált körülírásnál, miszerint, ha absztrakciók és nyelv használatával elérhető, hogy egy gép olyan problémákat oldjon meg, amiket embereket szoktak, és képes ennek fejlesztésére, akkor ezt a gépet intelligensnek nevezhetjük [30].

Az MI alkalmazásának korunkban számtalan példáját lehetne említeni, kezdve az autonóm járművektől, a szállásfoglalási weboldalakon át, a gyógyszer mellékhatás kutatásig. Általánosan elmondható, hogy az MI alkalmazása ma már elfogadottabb, és kevésbé ébreszt félelmet, mint évekkel ezelőtt a tudományos fantasztikus irodalom által keltett hangulatban. Ezzel együtt fontos kihangsúlyozni, hogy jelen pillanatban sincs

tudományosan elfogadott szabályozás alkalmazására. Bizonyos területeken ezzel együtt léteznek szabályozó előírások, példaképen említhető, hogy az 1968-as Bécsi Egyezmény tiltja a vezető nélküli, vagy a vezető által nem befolyásolható civil járművek közlekedését [31].

A biometrikus azonosítás folyamata során az MI tulajdonképpen mindegyik lépésben sikeresen alkalmazható, ilyen például a mintázat kinyerése (minta extraktció), a keresés optimalizálása az adatbázisban, a minták összevetése (matching), vagy a döntési szabály pontosítása az egyezésről, ezt illusztrálja a 11. ábra. Jelen munkában elsősorban döntési és mintakinyerési feladatokra alkalmaztam lágy számítási módszereket, ahogy ezeket a következő alfejezetekben ismertetem [32].



11. ábra: MI alkalmazhatósága a biometrikus azonosításban

A lágy számítási módszerek növekvő használatát figyelhettük meg az elmúlt években a biometria területén, ezeket a kombinációkat szokás lágy-biometriának is nevezni. Elsősorban annak köszönhető a gyors terjedés, hogy a lágy-biometria képes jól kezelni a változásokat és a bizonytalan adatokat, így ezen a területén használatuk különösen előnyös, hiszen [29]:

- A biometrikus mintáknak nincs tökéletesen ideális állapota, minden minta bizonyos mértékben különbözik a másiktól. A kutatásaim során arra a következtetésre jutottam, hogy amennyiben két biometrikus minta teljesen azonos, akkor az egyik bizonyosan hamis.
- A minták közti különbözőségeket nehéz matematikailag egzakt módon megfogalmazni, illetve ez a megfogalmazás bizonyos műveleti korlátokba is

ütközik (azonosítási idő véges hossza), így a nem analitikus módszerek előnyt élveznek az összehasonlítás során.

- Amennyiben egy minta egyedi azonosító jegyeinek azonosítása túl kritikussá válik, akkor csökken a rugalmasság (környezeti zajokkal szembeni tolerancia) és az általános összehasonlíthatóság elve.

2.2 Fuzzy logikai vezérlő alkalmazása multimodális döntési szituációban

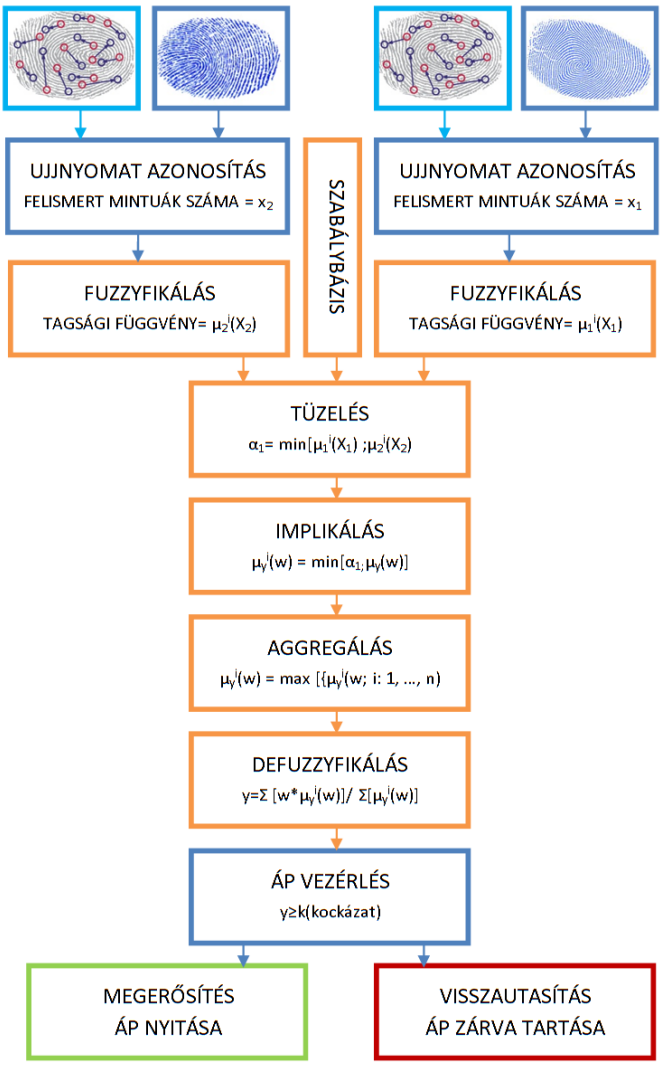
A lágy számítási módszerek első tagjaként az 1965-ben Lotfi A. Zadeh által bemutatott fuzzy logikát vizsgáltam. A "zavart halmazok" elmélete úgynevezett puha intuíciók és következtetések halmazán definiálja megfigyelt eseményteret. Az egyes, általában lingvisztikai változónak nevezett halmazokhoz minden eseményt egy tagsági függvény mentén rendelünk hozzá, majd ezekre külön szabálybázis szerint vizsgáljuk az egyes eredmények aggregált értékét. Az így kapott eredményeket összehasonlítottam több lineáris algebrai számítással és illusztráltam az eseménytér összes lehetséges kimeneti állapotát. A következőkben ismertetem egy általános fuzzy logikai vezérlő (Fuzzy Logic Controller - továbbiakban FLC) működését [33] [34].

2.2.1 Bimodális biometrikus fuzzy logikai vezérlő modellje

A digitális technika fejlődésével a felismerés folyamatát a beléptetési rendszerekben automatizálták, így védett objektumokban, államok határain, de akár hétköznapokban is találkozhatunk már ujjnyomat-olvasókkal. Tulajdonképpen a köztudatba 2004-ben robbant be a ThinkPad T42 beépített ujjnyomat felismerővel szerelt laptopjával, illetve 2007-ben dobta piacra a Toshiba a G500-as mobiltelefont, ami már beépített ujjnyomat azonosítóval rendelkezett. A széles körű elterjedést pedig minden bizonnyal az iPhone 5S-nek köszönhető, ami 2013-as debütálása után fél év alatt 500 millió példányban talált gazdára TouchID-re keresztelt ujjnyomat olvasó gombjával [35].

A 12. ábra egy bimodális, ujjnyomat érzékelőkkel párosított FLC kialakítást tüntettem fel, a faktorok száma azonban bizonyos szintig növelhető és igény szerint, a vizsgálandó biometrikus jellemző módosítható is. A bizonyítás során azért választottam az

ujjnyomatokat, mert a minutiae[2] vagy minutiák értékelésének viszonylag széles körben elfogadott módszertana van. Az összehasonlításnál pedig nyilvánvalóbb a két azonos jellemző mérésén alapuló módszertan különböző kiértékelési módszere közti különbség igazolása. A fenti egyértelműsítő rendelkezések ellenére a fuzzy logikán alapuló módszer alkalmazhatósági vizsgálatánál kitérek olyan eszközökre, amelyek javíthatják a beléptető rendszerek működési paramétereit [36].



12. ábra: Fuzzy logika alapú irányítási rendszer blokksémája

[2] minutiae: a daktiloszkópai értelmezésben az emberi ujj bőrredőzetének, fodorszálainak egyedi mintázata

Belátható tehát, hogy az általam meghatározott konstrukcióban a bemeneti eszközök változtathatóak, de figyelembe kell venni, hogy a felismert egyedi azonosító jegyek számának milyen az eloszlása. A fuzzy logika „zavart” karakterisztikájából adódóan több ponton is lehetőség van a vezérlési folyamat programozására. Befolyásolhatjuk a szabályrendszert, a tagsági függvények karakterisztikáját és számát, az aggregációs szabályokat, és a defuzzyfikálás függvényét, valamint annak értelmezését [37].

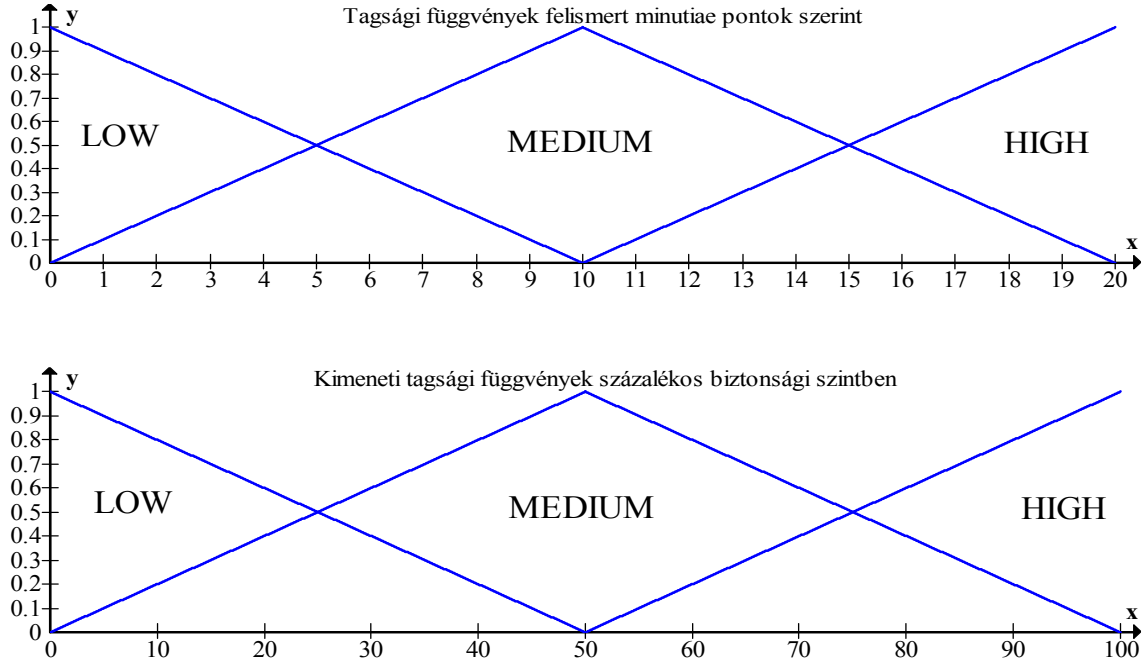
A fuzzy logikai vezérlő beállításainak módosításával végzett kísérleteim eredményei, a nemzetközi szakirodalommal összhangban, azt mutatják, hogy vannak olyan programozási pontok (pl:: tagsági függvények alakja), amelyek hatása nem különösebben változtatja meg a végeredményt, míg vannak olyan paraméterek, amelyek igen nagy hatással vannak az eljárásra. Ezen tulajdonságok következtében további vizsgálatok természetesen abszolút indokolttá váltak, hiszen fontos megismerni, hogy miképpen lehet optimalizálni a vezérlés működését [38] [34] [37] [39].

2.2.2 Ujjnyomat alapú bimodális azonosító rendszer FLC vezérléssel

A vezérlés modelljének készítése során arra törekedtem, hogy a fuzzy logika matematikai hátterét egy gyakorlati példákon keresztül szemléltethessem. A nemzetközi gyakorlatban a minutiák tekintetében a sikeres azonosításhoz bűnügyi esetekben nyolc, míg a beléptető rendszereknél tizenkettő pont egyezését kell bizonyítani. [40]

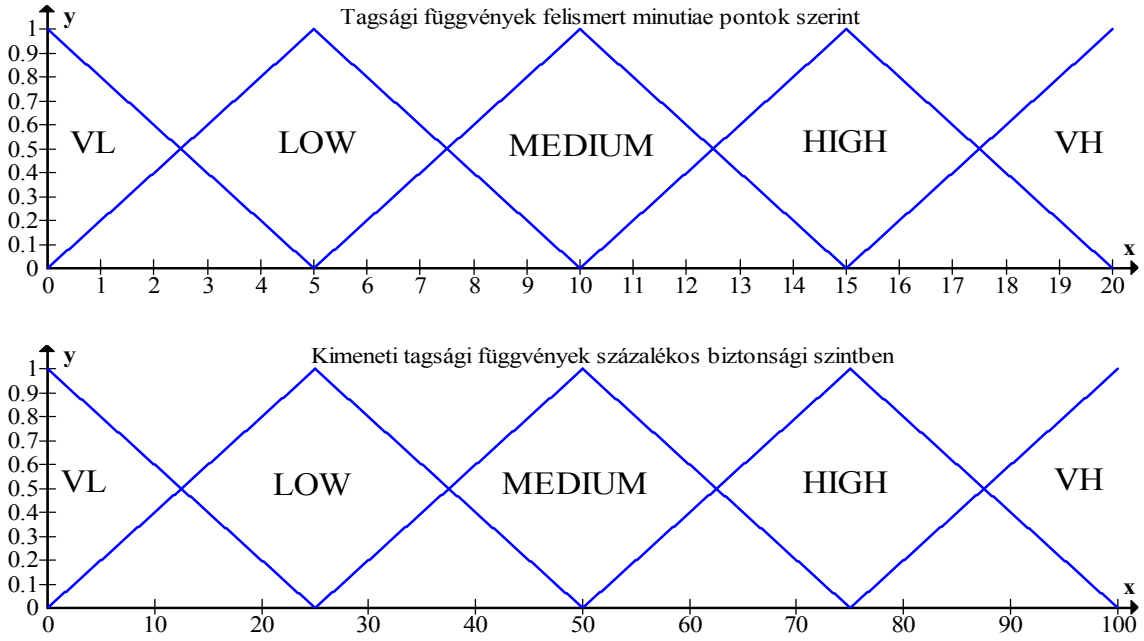
Egyes nemzetközi gyakorlatok ettől eltérnek, például az angolszász rendszerekben nem egy minimum érték, hanem egy szakértői vélemény támasztja alá az összevetést. Azonban a folyamatok automatizálásának elősegítése végett feltételezzük, hogy a [8-16] adja azt az intervallumot, ahol a minimális minutiae keresendő. Kiterjesztve a tagsági függvények értelmezési tartományát, a fuzzyfikálás előtti alaphalmazt ennek megfelelően az elegendően széles [1-20] intervallumra jelöltem ki. Abból kiindulva, hogy maga a minutiák felismerésének algoritmusa ismeretlen, bemeneti feltételnek azt adtam meg, hogy adott eszköz – ez esetben ujjnyomat olvasó – az adott intervallumon hány minutiae-t azonosított sikeresen. A megírt kódokban a skálák szélessége szabadon választható, így az könnyen alkalmazható más biometrikus azonosítási módszer, vagy minta extrakciós mód esetében is [40].

Az adott intervallumon ezek után tagsági függvényeket határoztam meg. A tagsági függvények száma attól függ, hogy mennyire szeretnénk finom beosztást. Gyakorlatilag ezek száma nagymértékben befolyásolja a rendszer számítási kapacitási igényét, hiszen a későbbiekben minden faktor összes definiált tagsági függvényét kombinálnom kell. A szemléltetést céljából definiáltam egy három és egy öt tagból álló tagsági függvény rendszert, ahol a nemzetközi alkalmazásokkal összhangban, illetve a MATLAB-ban történő kezelés megkönnyítése okán, a skála értékeket angolul definiáltam. Ezek az alábbi 13. ábra láthatóak:



13. ábra: Hármas tagolású bemeneti fuzzy halmaz és annak ötös osztású kimeneti halmaza

A gyakorlati szemléltetés során a bemeneti fuzzy halmazokat három és öt tagsági függvénnyel határoztam meg, amelyek közti különbségek jól láthatóak a kimeneti függvények által meghatározott felületeken. Ahogy azt a későbbekben látni fogjuk, a szabálybázisban meg kell határozni, hogy a kimeneti fuzzy halmazt hány tagsági függvény határozza meg. Mindkét esetben az ötös tagolást választottam (ismét angol skálát alkalmazva), ami már kellően nagy felbontást képes adni, de lényegesen nem bonyolítja a számításokat.



14. ábra: Ötös tagolású bemeneti fuzzy halmaz és annak ötös osztású kimeneti halmaza

A 14. ábra a minutiák számának tagsági függvényeit illusztrálja. A tagsági függvények halmaza (T_1; T_2) egy egyszerű háromszögfüggvénnyel is megadható, de közelíthetőek Gauss görbékkel, szinusz görbékkel, esetleg exponenciális függvényekkel is. A szakirodalom szerint a görbék alakja igen jelentéktelen hatással van a végeredményre a legtöbb esetben. A tagsági függvények megadják számunkra, hogy felismert minutiák adott száma mennyire tekinthető „jónak" a [0,1] intervallumon [41]. A biztonsági szint tagsági függvényei mutatják a kimeneti függvény, azaz a „*biztonsági szint*" „y(x)" a vezérlő által adott „jel jósága" lesz, amit későbbiekben a defuzzyfikiáció során átalakítunk, tehát a kimenő jel hasonló lesz ahhoz, mint amit egy bármilyen más detektor adhatna. A kimeneti jelet a [0, 100] intervallumon értelmeztem, így a százalékos szemléltetés látványosabb lehet. A minutiák számának tagsági függvényei és a biztonsági szint tagsági függvényei közti összefüggést határozza meg a szabálybázis[3].

A szabálybázis definiálása szakértői munkát kíván, hiszen ebben kell meghatározni azokat a hozzárendeléseket, ami alapján a különböző „jóságú" felismert minutiák

[3] A szabálybázis azon logikai kapcsolatok összessége, amelyek meghatározzák a bemeneti tagsági függvények különböző kombinációján értelmezett kimeneti tagsági függvényeket, ahol a szabályok numerikusan és lingvisztikailag is megadhatóak

halmaza meghatározza a biztonsági szintet. A rendszer lehetőséget ad arra, hogy ezt később megváltoztassuk, ami biztosítja az adaptív vezérlést és a rugalmas esetkezelést. Szemléltetésképpen az alábbi mátrixokban logikai formában érzékeltetem a szabálybázist:

T_1/T_2	LOW	MED	HIGH
LOW	VL	L	M
MED	L	M	H
HIGH	M	H	VH

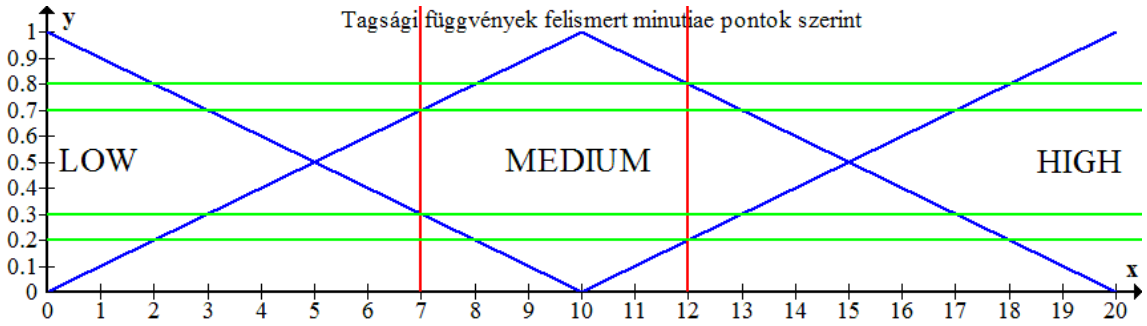
T_1/T_2	VL	LOW	MED	HIGH	VH
VL	VL	VL	L	L	M
LOW	VL	L	L	M	H
MED	L	L	M	H	VH
HIGH	L	M	H	H	VH
VH	M	H	VH	VH	VH

15. ábra: A szabálybázist kódoló mátrixok

A szabálybázis meghatározza a fuzzy halmazok adott tagági függvényei közti relációkat, de a logikai formát át kellett ültetni olyan analitikus formába, ami a MATLAB matematikai tervező szoftver kezelni képes. Analitikus parancsként jelen esetben a két változó *minimumát* határoztam meg, így a lehetséges tagsági függvény párosítás esetében a kisebbik határozza meg az adott kombináció értékét. A fuzzy logikában a *minimum* jelenti a logikai „*és*” avagy a *metszetképzés* analógiáját. Természetesen elméletileg lehetőségünk van más analitikai hozzárendelés megadására is (pl. szorzás), de a gyakorlatban ez az egyik legelterjedtebb megoldás. A továbbiakban a szemléltetés és összehasonlíthatóság céljából két konkrét bemeneti értékre végeztem el a vizsgálatokat, tehát tekintsük bemeneti értékként x_1=7 és x_2=12f eseteket, azaz az egyik ujj leolvasása során hét, míg a másik esetében tizenkét minutiae-t ismert fel sikeresen az olvasó.

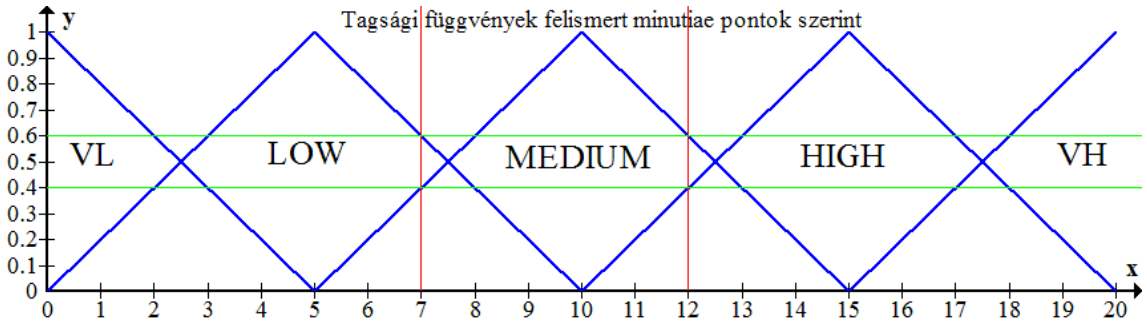
Az alábbi ábrákon (16. ábra,17. ábra, 18. ábra) látható, hogy a tagsági függvények közül a fenti két konkrét érték esetében melyik tagsági függvény értéke tér el zérustól, azaz "*tüzel*". A logikai kapcsolat szemléltetéséhez el kellett készíteni két tagsági függvény összes lehetséges párosítását x_1=7 és x_2=12 esetekben (a lehetséges kombinációk száma minden esetben a bemeneti tagsági függvények számosságának szorzata), amely az általam vizsgált konkrét alkalmazások esetében kilenc, illetve huszonöt lehetséges esetet

ad. Jelen esetben, a *minimum függvény* következtében, amennyiben egy függvénypáros valamelyik tagja nem *tüzel*, akkor a kombináció analitikusan zérus eredményt ad. A részletes ábrázolásnál kizárólag a hármas tagolású fuzzy halmazokat mutatom be, de az ötös osztású halmaz esetében is hasonló logikával kell eljárni.



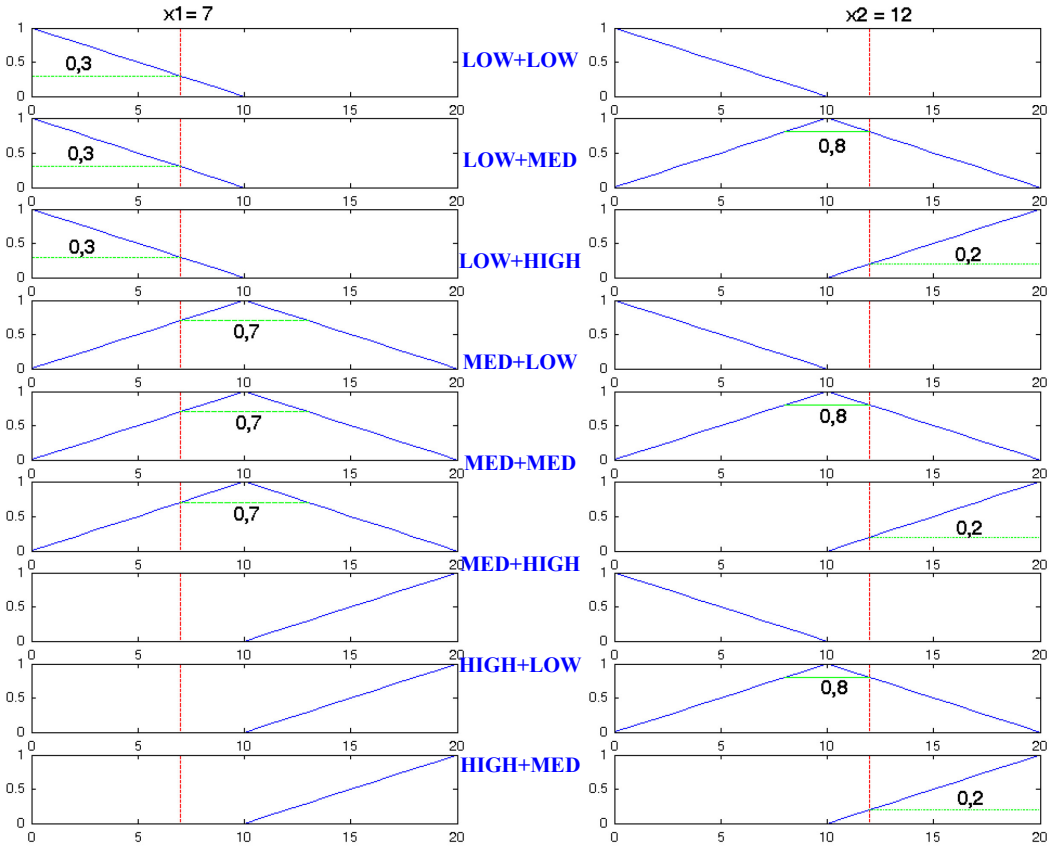
16. ábra: Tüzelő fuzzy függvények x_1=7, x_2=12 esetén, három osztású halmazban

A 16. ábra látható, hogy az x_1=7 esetén kizárólag a *LOW* és a *MEDIUM* tagsági függvények tüzelnek, míg x_2=12 esetén csak a *MEDIUM* és a *HIGH* tagsági függvények tüzelnek. Mind kombinatorikailag, mind logikailag könnyen belátható, hogy a kilenc lehetséges kombinációból összesen négy párosítás esetében lesz együttes tüzelés. Ennek szemléltetése látható a 17. ábra.



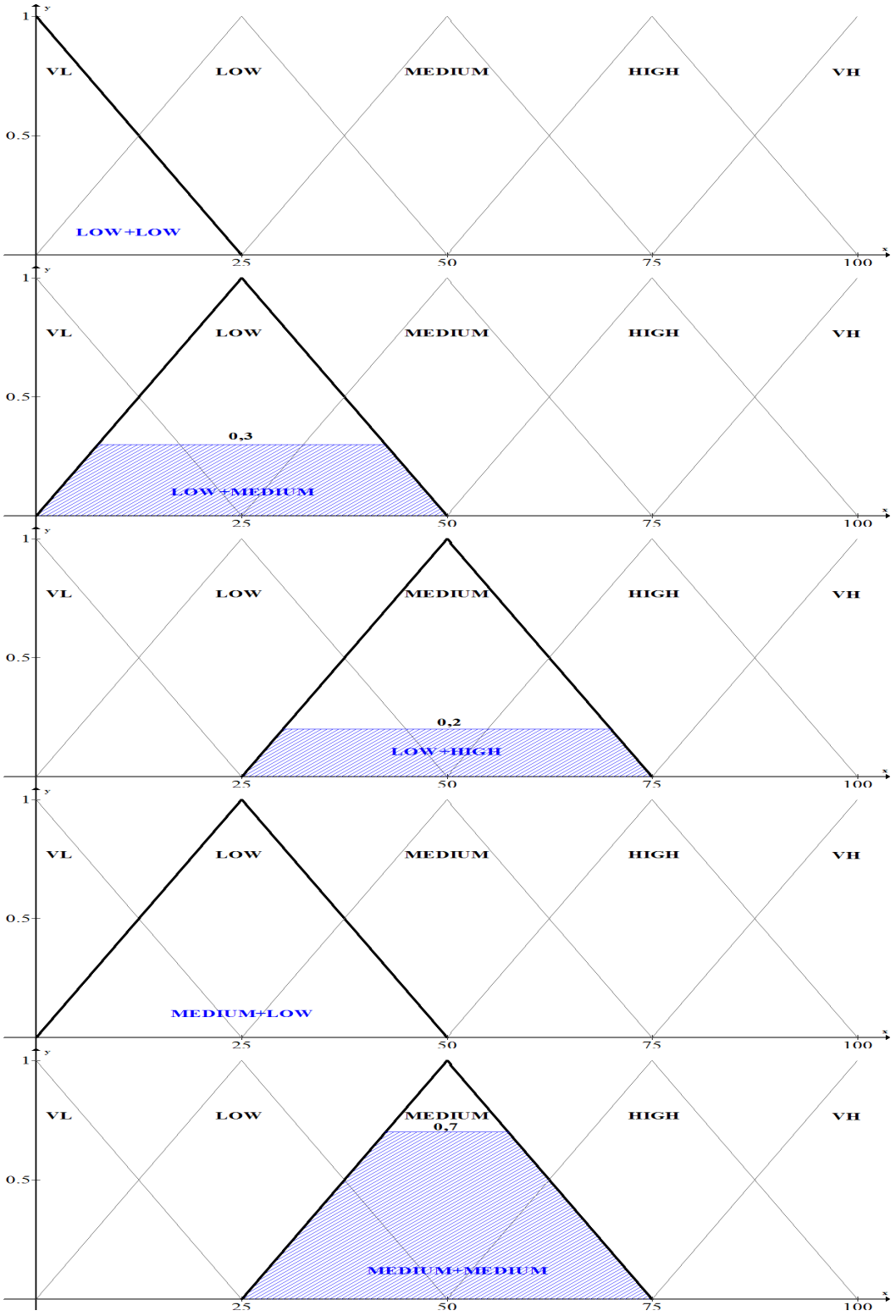
17. ábra: Tüzelő fuzzy függvények x_1=7, x_2=12 esetén, öt osztású halmazban

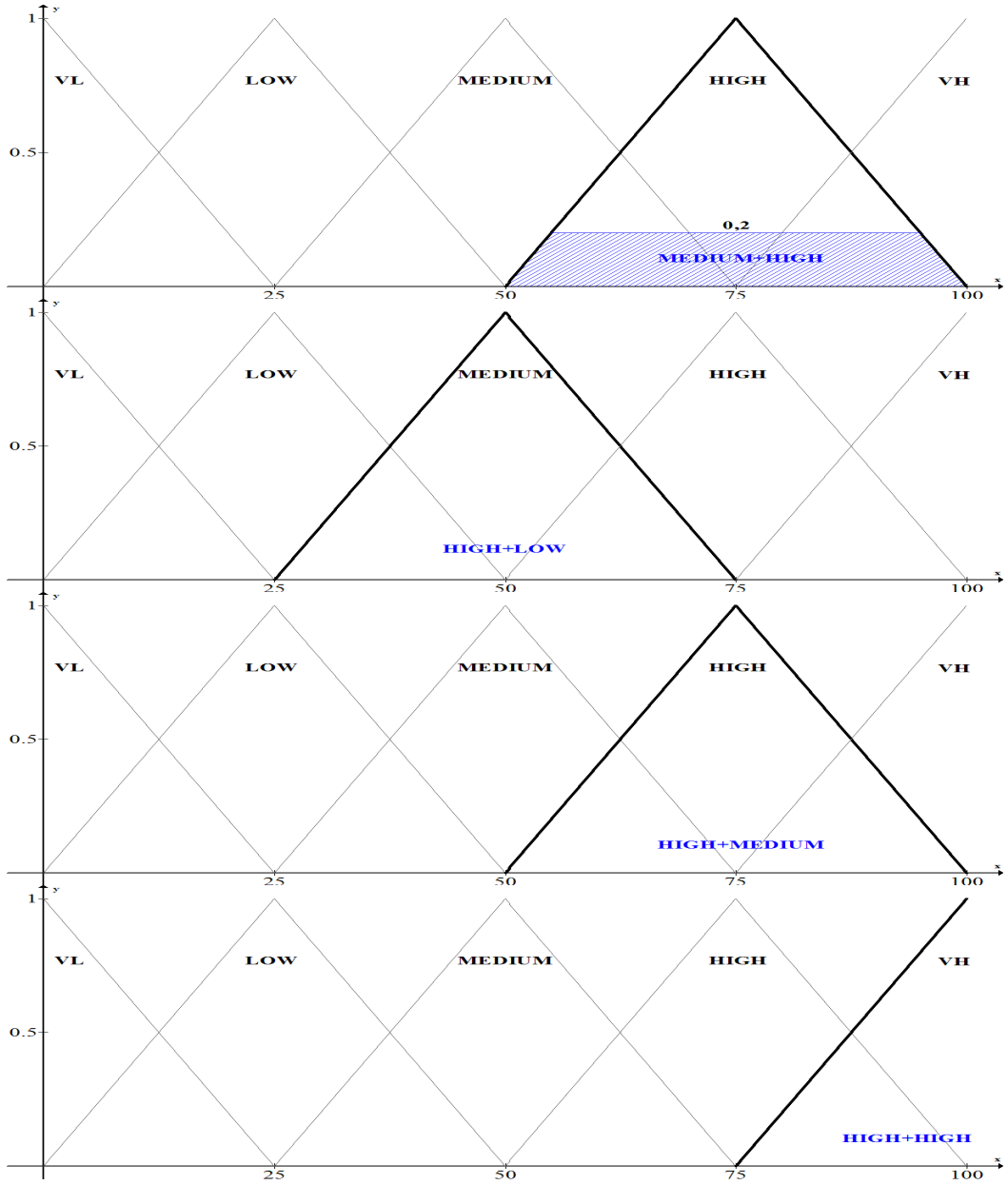
A 18. ábra látható az öt részre osztott bemeneti fuzzy halmaz, amin észrevehetjük, hogy x_1=7 és x_2=12 esetében az előzőekhez hasonlóan tüzelnek a tagsági függvények. Terjedelmi okokból ennek részletesen ábrázolásától tekintsünk el. Az alábbi ábrán (18. ábra) a kibontott tagsági függvényei szerepelnek, x_1=7 és x_2=12 számú sikeresen felismert minutiae esetén.



18. ábra: Fuzzy függvények tüzelése és azok súlyai hármas tagolású halmazban

A fenti fuzzy szabályok szerint csak akkor lesz a logikai kapcsolatokban szereplő kimeneti tagsági függvény értéke zérustól eltérő, ha mind a két a bemeneti tagsági függvény tüzel. A fenti kilenc lehetséges kombináció közül ez mindössze négy esetben fordul elő, tehát a kimeneti fuzzy halmazt e négy kimeneti tagsági függvény fogja meghatározni. A kimeneti fuzzy függvények alább láthatók (19. ábra).


VL
LOW
MEDIUM
HIGH
VH
LOW+LOW
0,3
LOW+MEDIUM
0,2
LOW+HIGH
MEDIUM+LOW
0,7
MEDIUM+MEDIUM
0.5
1
25
50
75
100

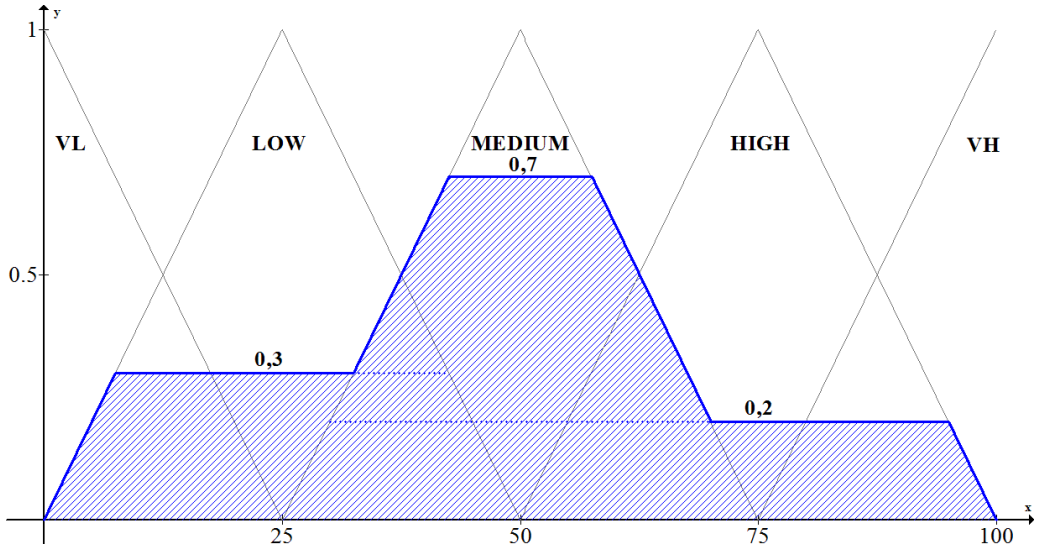


19. ábra: A kimeneti tagsági függvények a bemeneti kombinációk szerint

A fuzzy logika alapú vezérlés matematikai modelljének következő lépése szerint, aggregálni kell a kimeneti tagsági függvényeket egyetlen fuzzy halmazba. Jelen esetben az értelmezési tartományon a maximumát vettem az összes kimeneti tagsági függvénynek, mert az egyesítés vagy unióképzés műveletének ez az egyik fuzzy féle megfelelője, de a szakirodalomban több alternatív hozzárendelés is elfogadott [39].

Az aggregált kimeneti tagsági függvény tehát egy összetett függvény, amit az elemi kimeneti tagsági függvények halmaza határoz meg. Megmutatja, hogy a

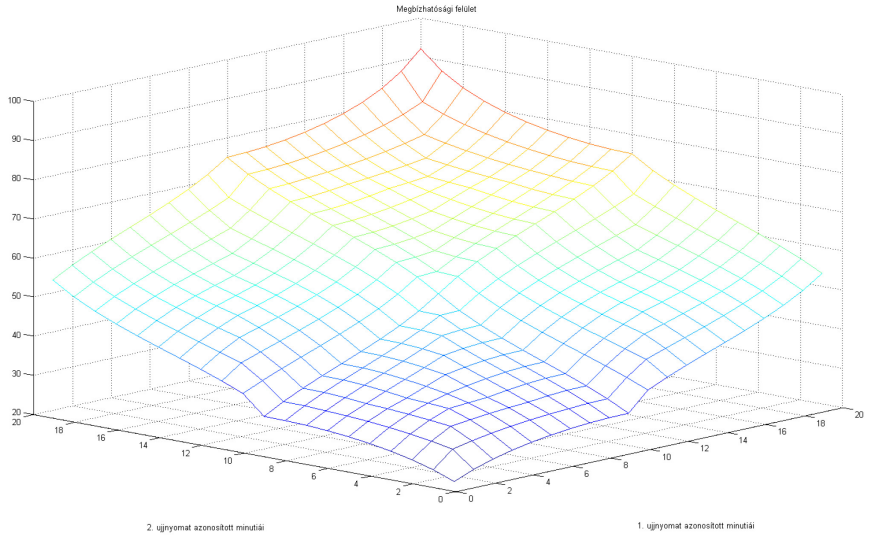
szabálybázisban definiált logikai kapcsolatok szerint milyen a kimeneti függvények jóságának összessége. A következő ábrán (20. ábra) az x_1=7 és x_2=12 esetekben tüzelő kimeneti tagsági függvényekből aggregált függvény látható:



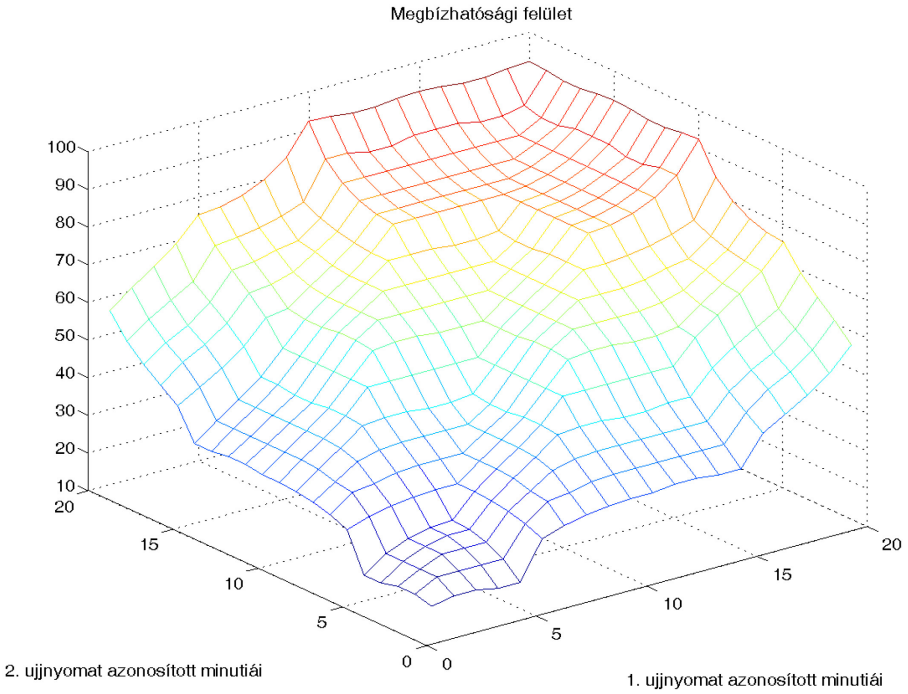
20. ábra: A kimeneti tagsági függvények aggregált függvénye

Az utolsó lépésben az aggregált kimeneti tagsági függvényt defuzzyfikálni kell. Ennek során valamilyen matematikai módszerrel olyan módon transzformáljuk a kimeneti tagsági függvények összevont halmazát, hogy az egy valós számot adjon. A defuzzyfikáció során is több matematikai módszert lehet alkalmazni, én jelen esetben, a gyakorlatban igen elterjedt, a súlypont meghatározásán alapuló módszert alkalmaztam [37]. A súlypont módszer megadja a 20. ábra poligonjának súlypontját, és ennek helyzete alapján osztályba sorolja.

A defuzzyfikáció során az a korábbiakban vázolt gondolatmenet alapján generált algoritmus képes kiszámítani az összes lehetséges esetre az aggregált kimenetei függvények súlypontját, ami két bemeneti változó esetén egy térbeli felületen szemléltethető. A bemeneti változók számának növelésével az azonosítás hatékonysága növelhető, tehát a téves elfogadás aránya (*FAR*) és a téves visszautasítás aránya (*FRR*), valamint a téves azonosítás aránya (*False Identification Rate – FIR*) csökkenthetőek, azonban a számítási feladatok és a rendszer átláthatósága is jelentősen nehezednek. A 21. ábra és 22. ábra illusztrálja azon felületeket, amiket a három illetve öt részre tagolt bemeneti halmazok alapján határoz meg a program [41] [42].



21. ábra: A felismert minutiák által meghatározott defuzzyfikált kimeneti felület, hármas tagolású bemeneti halmaz esetén



22. ábra: A felismert minutiák által meghatározott defuzzyfikált kimeneti felület, ötös tagolású bemeneti halmaz esetén

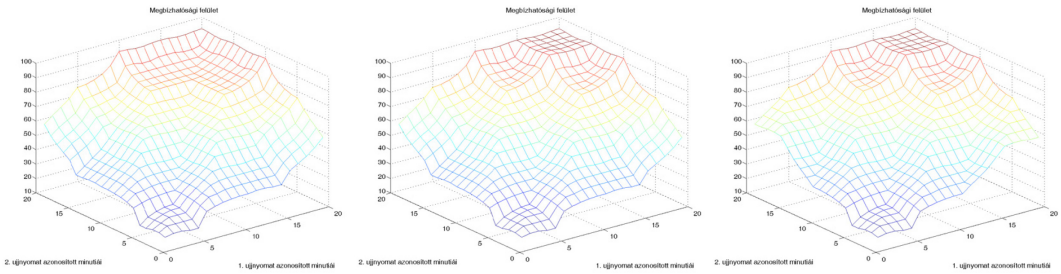
A felületeket megadó mátrixok az értekezés I. mellékletében találhatóak meg, de az ábrákon is jól követhető, hogy az összefüggések nem lineáris és inhomogén eloszlású

eredményt adnak, azonban a rendszer megőrizte szimmetriáját. A két ábra közti különbség arról tanúskodik, hogy a bemeneti tagsági függvények számának növelésével finomítható a felbontás, azaz egyes eredmények jobban elválaszthatóak egymástól. Ahogy azt már említettem, több ponton is lehetőség van a beállításokat megváltoztatni. A szabálybázist definiáló mátrixok elemeinek logikai következményeit kismértékben megváltoztatva kapjuk a látható módosulásokat:

T_1/ T_2	VL	L	M	H	VH
VL	VL	VL	L	L	M
L	VL	L	L	M	H
M	L	L	M	H	VH
H	L	M	H	H	VH
VH	M	H	VH	VH	VH

T_1/ T_2	VL	L	M	H	VH
VL	VL	VL	L	L	M
L	VL	L	L	M	H
M	L	L	M	H	VH
H	L	M	H	VH	VH
VH	M	H	VH	VH	VH

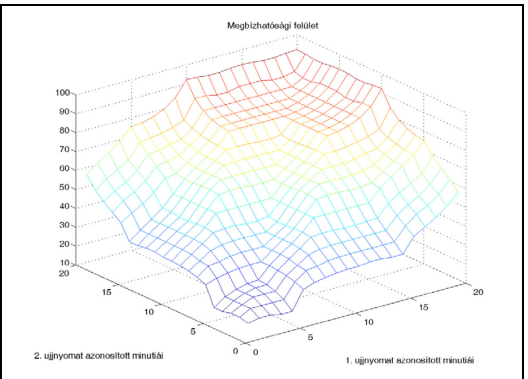
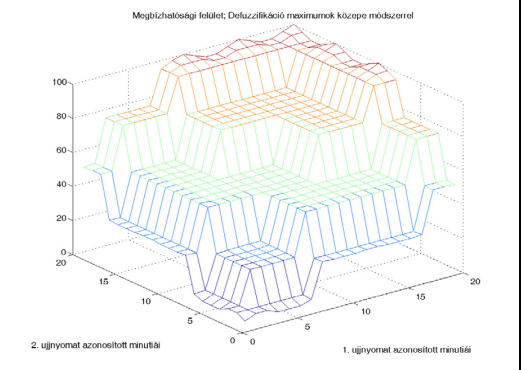
T_1/ T_2	VL	L	M	H	VH
VL	VL	VL	L	M	M
L	VL	L	L	M	H
M	L	L	M	H	VH
H	M	M	H	VH	VH
VH	M	H	VH	VH	VH



23. ábra: A szabálybázis logikai értékeinek megváltozása során tapasztalható változások

Az utolsó „beállítási” pont a módosításával, tehát a defuzzyfikációs függvény megváltoztatásával bizonyos mértékben szintén meg lehet változtatni a kimeneti értékeket, de ez a művelet az összes értéket megváltoztatja. A szakirodalomban általában a Center of Gravity – COA (súlypont) módszer a legelterjedtebb, de megemlíthetőek a Mean of Maxima – MOM (maximumok közepe), a Center of Area – COA (területi középpont) és a Center of Maxima – COM (középső maximum) módszerek [37] [39].

Összehasonlításképpen szemléltetem a COG és MOM módszerek közti különbséget [37]:

COG	$y_{COG} = \frac{\sum_{i=1}^{r}(y_i^* \cdot w_i^*)}{\sum_{i=1}^{r} w_i^*}$	
MOM	$y_{MOM} = \frac{\sum_{y \epsilon MAX(B^*)}^{r} y}{\lvert MAX(B^*) \rvert}$	
COA	$y_{COA} = \frac{\sum_{i=1}^{m} B^*(y_i) y_i}{\sum_{i=1}^{m} B^*(y_i)}$	
COM	$y_{COM} = \frac{min\{y_k \lvert y_k \epsilon M\} + max\{y_k \lvert y_k \epsilon M\}}{2}$	

24. ábra: A defuzzyfikációs módszerek és eredményeik

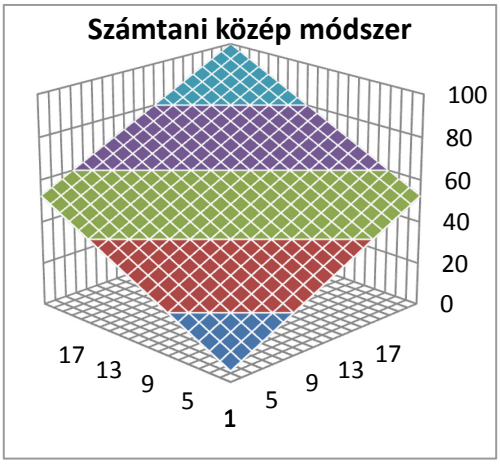
A 24. ábra jól látható, hogy súlyponti módszer alkalmazása előnyösebb, mert a maximumok közepe módszer töredezettebb eredményt ad, ami az irányítási és vezérlési feladatok során kevésbé jól alkalmazható. A COA módszer hasonló a súlyponti módszerhez, de nem veszi figyelembe az átlapolásokat, ami ez esetben igen jelentős különbséget adna. A középső maximum (COM) módszer igen könnyen számolható, de a MOM-hoz hasonlóan nem töredezett eredményt ad.

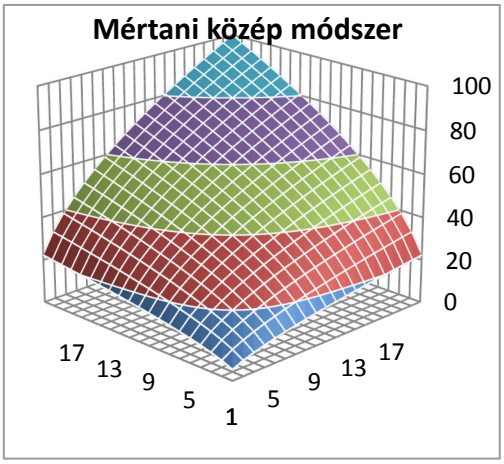
2.2.3 A fuzzy logika alapú és a klasszikus vezérlés összehasonlítása

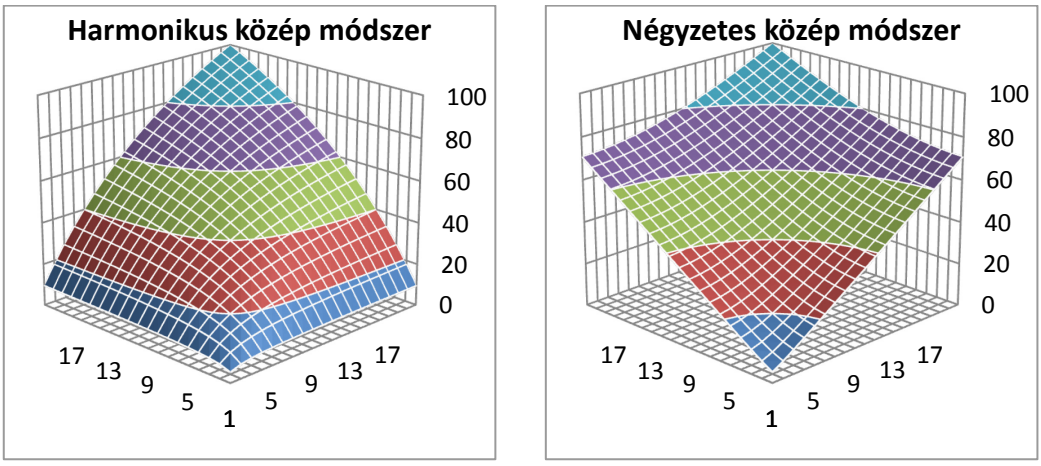
Az előző fejezetben láttuk, hogy a fuzzy logika alkalmazása olyan előnyökkel jár, mint az adaptív vezérlés lehetősége és a rugalmasság, ellenben nagyobb szakértelmet és több számítás igényel, mint a több változó együttes figyelembevételére gyakorlatban elterjedten használt statisztikus módszerek.

A következőkben arra a kérdésre adok választ, hogy a fuzzy logika alapú vezérlés milyen mértékben növelheti egy beléptető rendszer hatékonyságát. Az összehasonlításhoz a legegyszerűbb esetet választottam, így két azonos biometriai módszert vetettem össze, de eltérő felületeken vizsgálva, így kiküszöbölhettem az eltérő módszerek különbözőségéből fakadó aszimmetrikus hatásokat. Ezzel együtt meg kell jegyeznem, hogy a fuzzy logika alkalmazása éppen a különböző biometrikus azonosítási módok együttes vizsgálata során ajánlatos, hiszen a szabálybázis definiálása során könnyebben kezelhetőek az aszimmetriák, mint más konvencionális megoldással.

Azt a kérdést vizsgáltam meg, hogy két különböző ujjról sikeresen beolvasott minutiák számának statisztikai közepe hogyan viszonyul a fuzzy logika alapján végzett bimodális elemzéshez. A sikeresen beolvasható minutiák számát ez esetben is [1-20] intervallumon értelmeztem. A statisztikai eredményeket pedig a [0, 100] intervallumra normáltam, hogy jól összemérhetőek legyenek a fuzzy eredményekkel. A különböző módszerek eredményei a 25. és 26. ábra láthatóak.

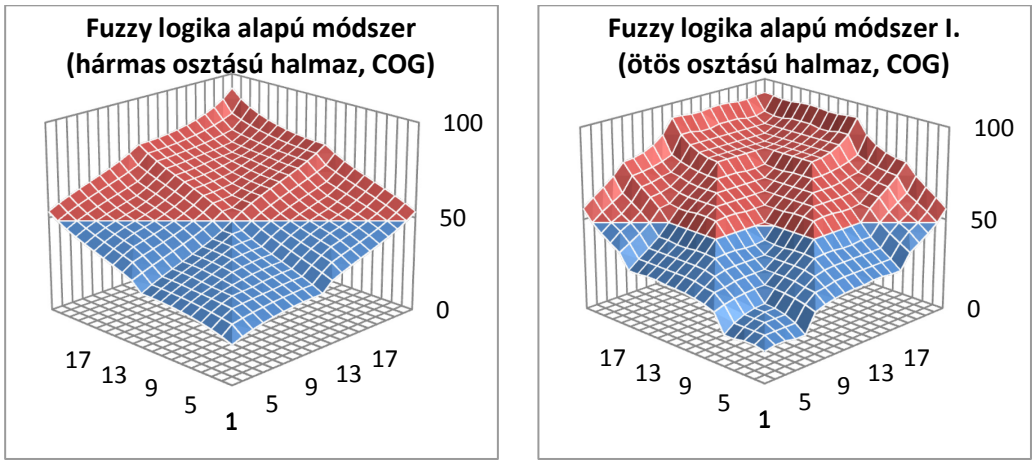


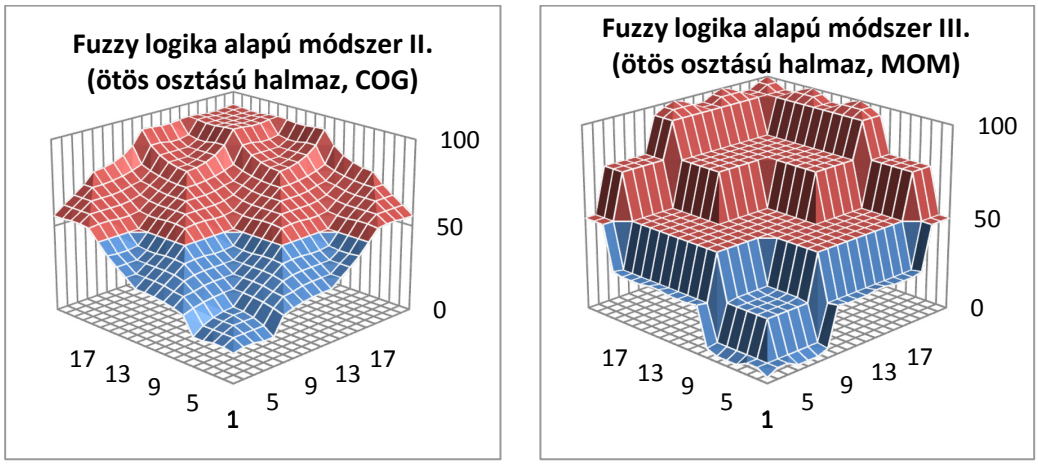




25. ábra: Statisztikai középértékek felületei

A fuzzy logikára épülő számítások eredményei által kirajzolt felületek az első esetben a hármas-, a többi esetben az ötös tagolású bemenetei tagsági függvényhez tartoznak. Utóbbiak esetében az I. és a II. a fenti szabálybázis első és utolsó felvázolt logikai kapcsolatait tükrözik, míg a III. felület az első szabálybázis alapján, de a *maximumok közepe* módszerrel defuzzyfikált megoldást szemlélteti.

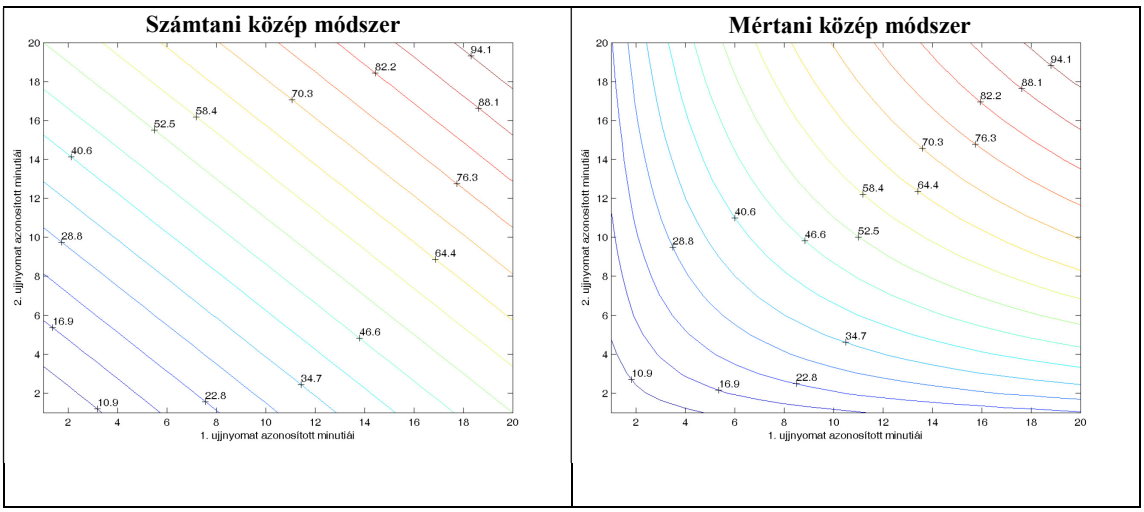


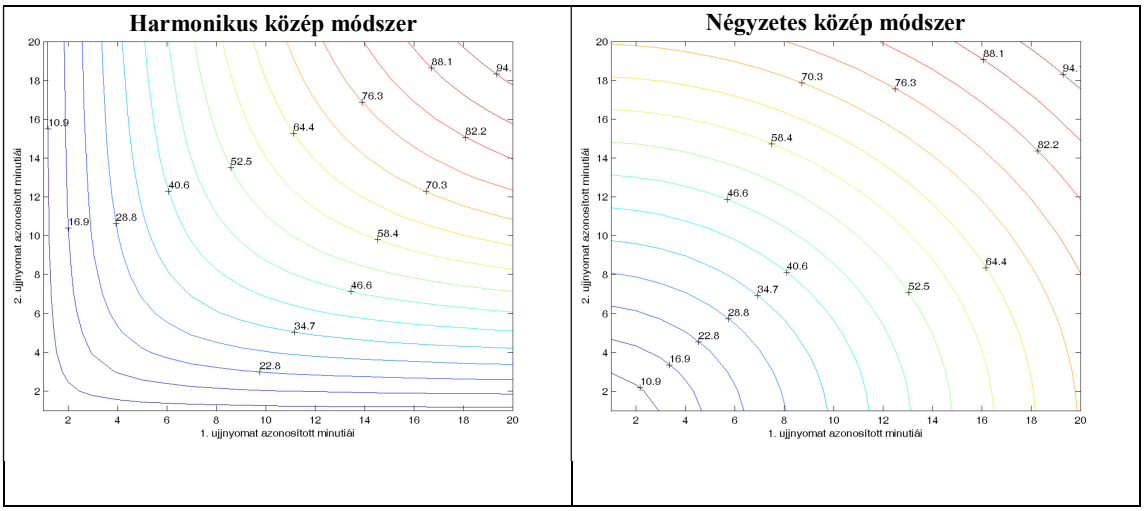


26. ábra: Fuzzy felületek

A két ábracsoport közti különbségek jól megfigyelhetőek. Amíg a statisztikai közelítés által kapott középértékek eloszlás egyenletesebb – aminek oka az első és másodfokú polinomok által meghatározott függvények folytonos jellege –, addig a fuzzy logika eredményei valamivel diszkrétebb eredményeket adtak – ennek oka az, hogy a fuzzy halmazok tagsági függvényeinek száma egy kis természetes számmal adandó meg. A *Fuzzy logika alapú módszer III.* című ábra felülete a defuzzyfikációs eljárás módosítása miatt vált lépcsőzetessé.

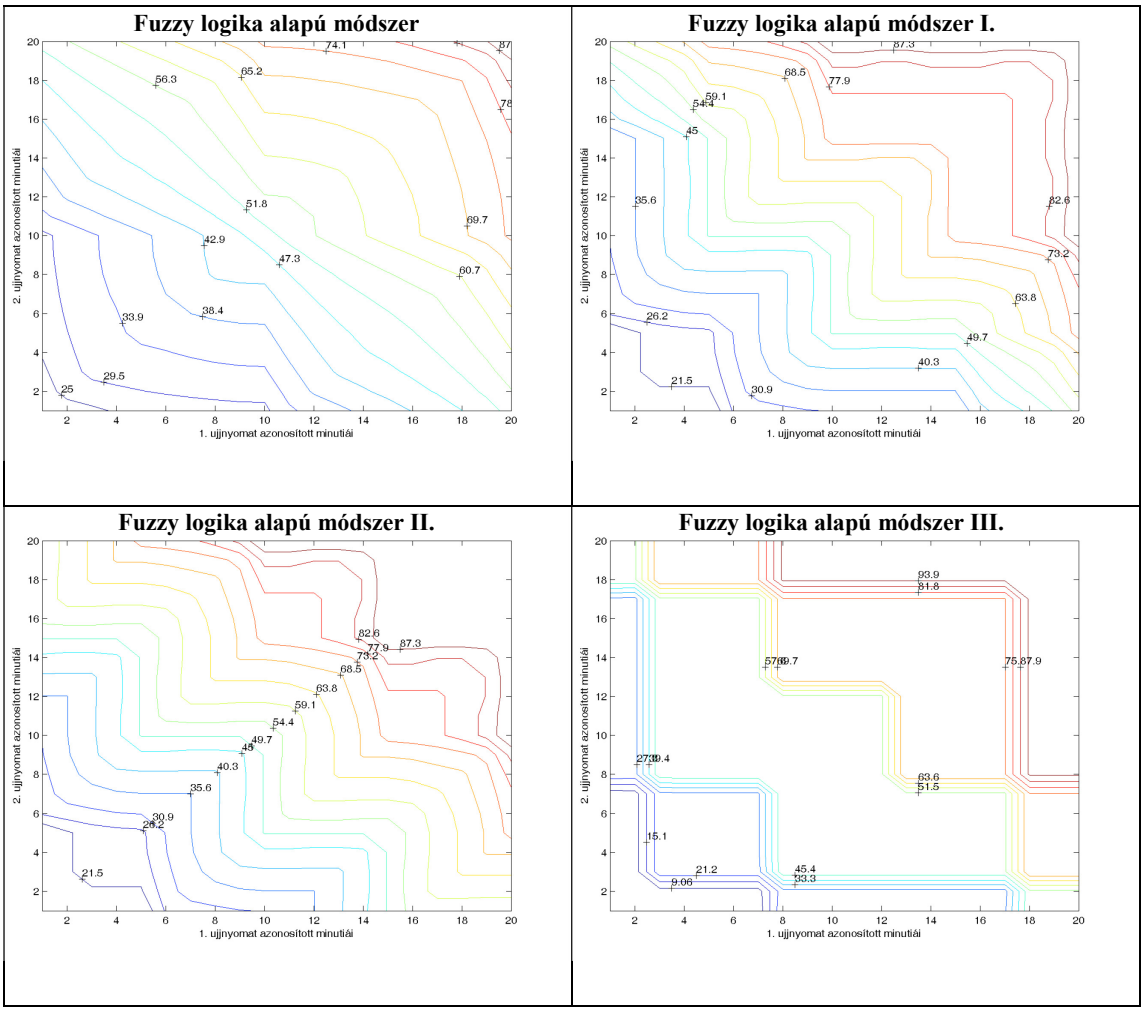
Kvantitatív szempontból érdemesnek tartom bemutatni, a nyolc fenti esethez megrajzolt szintvonalakat, illetve a kategorikus biztonsági szintekhez (25%, 50% és 75%) tartozó metszeteket. Az 27. ábra a MATLAB által készített szintvonalakat ábrázoltam tizenötös szintű felbontásban.





27. ábra: A statisztikus módszerek szintvonalai

A matematikai statisztikából ismerjük, hogy a statisztikai középértékek adott sokaságra vonatkoztatva mindig egy bizonyos nagyságrendi relációt követnek. Adott sokaság esetében a középértékek a következők szerint viszonyulnak egymáshoz: $y_{harmonikus} < y_{mértani} < y_{számtani} < y_{négyzetes}$. Hasonló szabályszerűség a fuzzy logikán alapuló kimeneti eredmények esetében természetesen már nem fedezhető fel, hiszen az algoritmust több ponton is megváltoztathatjuk és ezek hatása együttesen érvényesül. Az alábbi ábrákon azonban látható, hogy az egyes módosítások milyen jellegű hatással bírnak a végeredmények tekintetében.



28. ábra: A fuzzy logika alapú módszerek szintvonalai

Míg a 27. ábrán a statisztikus módszerekhez tartozó szintvonalak eloszlása relatíve egyenletes, pontosabban a szintvonalak eloszlása jól tükrözi az analitikus kapcsolatot a változók között, addig a 28. ábrán jól kivehető, hogy a szintvonalak eloszlása nem egy algebrai viszony, hanem a diszkrét – lingvisztikailag meghatározott – szabálybázis manifesztációja.

Összehasonlítva e két matematikai módszert, megállapítható, hogy a kisebb felismerési intervallumokban a fuzzy logika megengedőbb, azaz két kevésbé jól felismert jellemző fuzzy alapú bimodális kimeneti értéke magasabb, mint e jellemzők statisztikai közepe, illetve a fuzzy logika a finomabb felosztású felismerési intervallumokban szintén kevésbé szigorú. A fuzzy logika legnagyobb előnye azonban az, hogy e kritikus és megengedő tulajdonságok dinamikusan és egymástól függetlenül megváltoztathatóak, szemben a statisztikai közepek statikus függvényeivel.

2.3 Mesterséges neurális hálózat alkalmazása ujjnyomat azonosítási feladatok hatékonyságának növelésére

A mérnöki világban a mesterséges neurális hálózatokat (Artificial Neural Networks, továbbiakban ANN) már közel három évtizede alkalmazzuk mintázat-felismerési problémákra, mert univerzális approximátorok lévén jól taníthatóak és relatíve kis hibával képesek felismerni mind az egyszerűbb (pl. rendszámfelismerés) mind az összetettebb mintázatokat (pl. önvezető személygépjárművek).

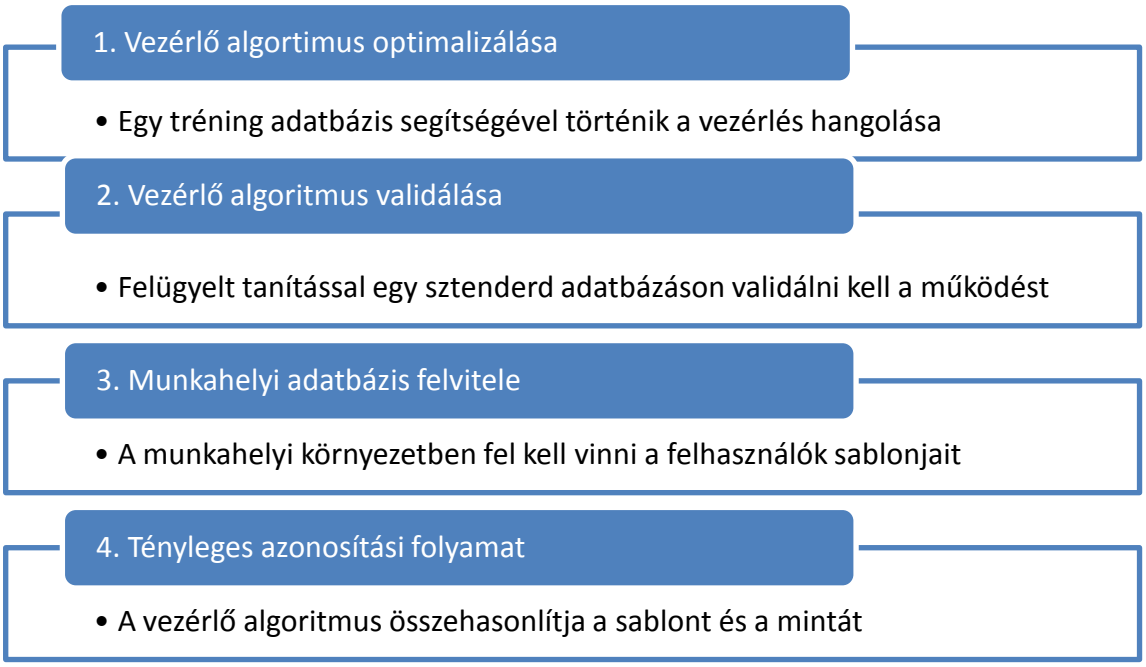
Meg kell jegyezni, hogy miként a természetes neurális rendszernek is szüksége van tanulásra és a megfelelő "működési beállítások" megtalálására, úgy a mesterséges neurális hálózatoknak is. Az emberi szervezet már magzati korban elkezdi megkeresni a "megfelelő beállításokat", mégpedig úgy, hogy egy olyan feldolgozó központ alakul ki, ami önmagában az általános "napi" problémák megoldásánál sokszorta összetettebb feladatokra is képes. A mesterséges neurális hálózatok struktúráját ma még csak korlátozottabb számú paraméterrel tervezhetjük, de a fejlődési irányok kedvező utat mutatnak. A jelenlegi korlátok legfőbb oka az, hogy a mesterséges neurális hálók tanítása és működtetése is olyan számítási kapacitást igényel, ami technikai korlátokba ütközik. Érdemes megjegyezni, hogy e területen a Google, az IBM Watson és Tesla vezető helyen járnak a számítógépek és hálószerkezetek fejlesztésében. A technikai nehézségeink a klasszikus Neumann féle számítógép architektúra korlátaira vezethetőek vissza. A jelenlegi fejlesztések, például az IBM TrueNorth chipje (4096 magon) szakítva a hagyományos memória és feldolgozóközpont elrendezéssel a lehető legközelebb hozza egymáshoz a feldolgozandó adatot és a feldolgozást végző mikro tranzisztorokat (5.4 milliárd), úgy hogy köztük 256 millió szinapszist alakít ki [43].

Ahogy ezt az első fejezet elején említettem, fontos gyakorlati probléma, hogy a biometrikus azonosító eszközökhöz megadott gyártói értékekhez képest szignifikánsan nagyobb a téves elutasítások tapasztalati aránya az általam vizsgált eszközök tekintetében. Ennek oka sok esetben arra vezethető vissza, hogy a beolvasott minták egyedi azonosító jegyeit nem sikerül kellően pontosan felismerni. Számos technika létezik az azonosító jegyek kiolvasására és összehasonlítására. A következőkben egy általam készített, nem lineáris és a maga módján nem hagyományos, hanem a mesterséges neurális hálózatokon alapuló módszert és ennek eredményeit ismertetem.

2.3.1 Ujjnyomat minták azonosítási folyamatainak modellezése

Attól a pillanattól kezdve, ahogy a felhasználó (aki éppenséggel valójában lehet egy imposztor[4] is) azonosítás céljából megérinti az ujjnyomat olvasó biometrikus azonosító eszközt egy komplex folyamat indul el. Meg kell jegyezni, hogy az azonosítás folyamatot ténylegesen nem itt kezdődik el, hanem korábban, az adatbázis és a vezérlő algoritmus optimalizálása során.

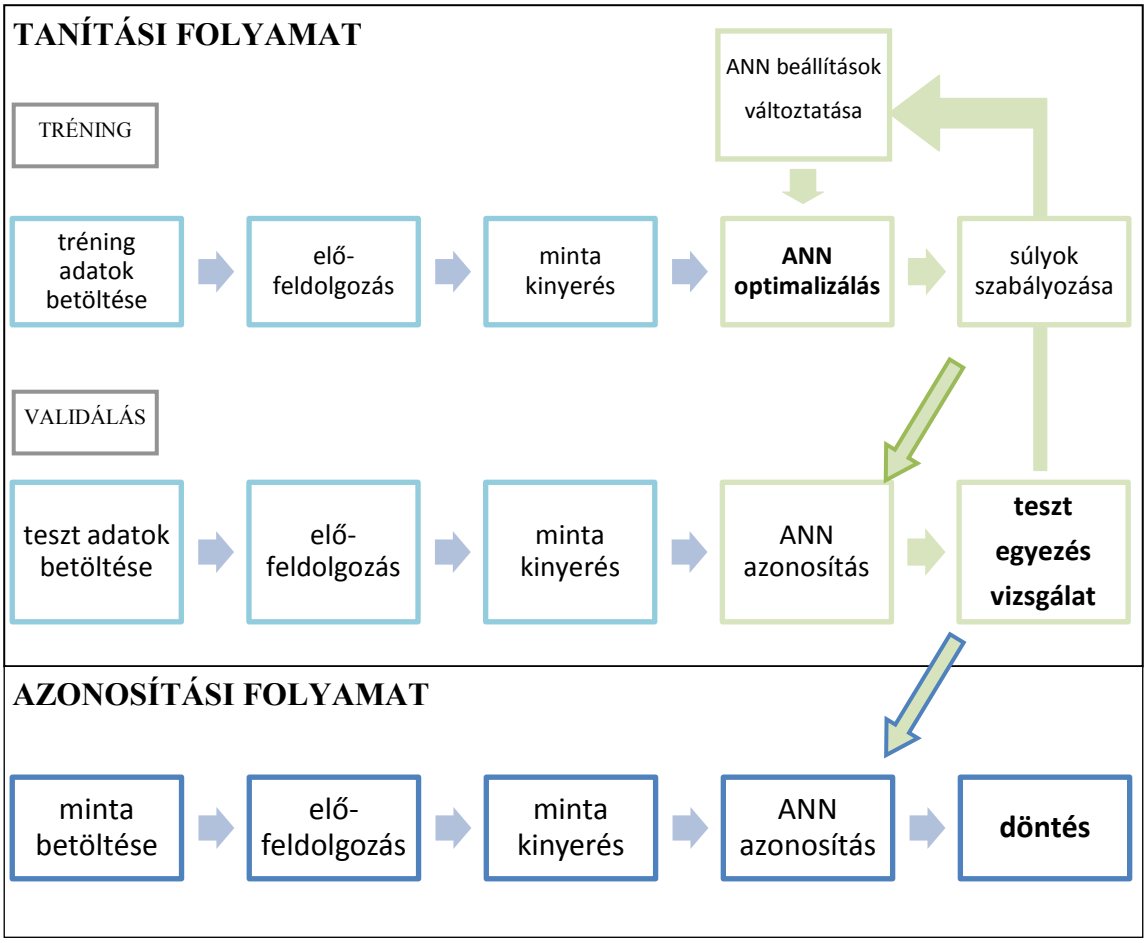
A biometrikus eszközök használatának, életútjának négy jól elkülöníthető fázisát tudjuk megkülönböztetni (29. ábra). Ezek közül kettőt a legtöbb esetben a gyártó végez, kettőt pedig a felhasználó/telepítő. A korábbi fejezetben említettem, hogy ez az éles szétválasztás a jövőben talán némiképpen finomítható, amennyiben lehetőség lesz a környezeti zajok és a kérdéses felhasználói körre jellemző eltérések implementálására, például a béta-binomiális eloszlás alkalmazásával.



29. ábra: Biometrikus azonosító eszköz életútjának fázisai

[4] felhasználói adatbázisban nem szereplő, jogosultsággal nem rendelkező személy

A kutatásban azt vizsgáltam, hogy egy többszörös sablonkészletből álló adatbázis alapján lehetséges-e a vezérlő algoritmust optimalizálni, így a fenti lépéseket összevonva kapjuk az alábbi működési blokkábrát (30. ábra) [44]:



30. ábra: ANN tanítási és azonosítási folyamatának blokksémája

Ahogy az a fenti ábrán is látszik, érdemes ketté választania a működést. Az első részt nevezzük tanítási folyamatnak, amely során meg kell, hogy történjen a vezérlő algoritmus tréningje és a működési beállításainak validálása. A kísérletekben ezt egy keretprogramba integrálva vizsgáltam MATLAB környezetben. Amennyiben a tanítás sikeres, az eszköz alkalmazható azonosítási folyamatokra is éles környezetben.

Jelen értekezés szempontjából a fő kérdés a tanítási folyamat optimalizálásnak a kérdése. Ennek részletes vizsgálatához először olyan adatokra volt szüksége, amik jellemzik a beolvasott mintákon lévő minutiákat, vagyis a felhasználók egyedi azonosító jegyeit.

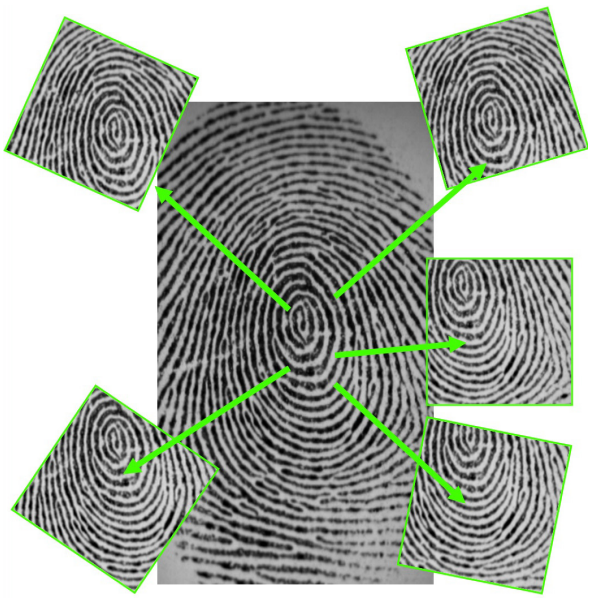
2.3.2 Egyedi azonosító jegyek kinyerésének és összehasonlításának vizsgálata

Az egyedi azonosító jegyek kinyerése többlépcsős folyamat. Minden lépcsőben más matematikai műveletek alkalmazására kerül sor, amivel közelebb jutunk a jelen szempontból értékes adatokhoz. Az adatok kinyerését a legegyszerűbben egy piaci forgalomban is megvásárolható ujjnyomat azonosító eszközön keresztül lett volna érdemes elvégezni, de ezen termékek működése biztonsági okokból kellően zárt ahhoz, hogy ilyen információkat – a rendelkezésemre álló technikával – ne tudjak kinyerni. Ennek következtében, részben meglévő, részben saját fejlesztésű apparátussal készítettem egy ujjnyomat olvasó programot MATLAB környezetben. Az alkalmazás során pedig törekedtem rá, hogy a modell leegyszerűsítése csak kutatási céllal összhangban történjen, így reprodukálhassam azokat a hibajelenségeket, amik téves elutasítás mögött állnak.

A program ugyanolyan jellegű lépéseket végez el, mint a többi kereskedelmi forgalomban is kapható társa, annyi különbséggel, hogy nincs benne optikai szenzor, így a szürkeskálás képeket egy külön adatbázisból olvassa be. Az adatokat az FVC 2002 adatbázisából hívtam le [45]. Meg kell jegyezni, hogy a konkrét matematikai műveletek és azok implementációja az egyes eszközök keretprogramjában értékes ipari titok, így minden gyártó igyekszik ezt valamelyest egyedivé tenni. A saját programomban is választani kellett egy módszert arra, hogy pontosan mik legyen azok a sajátosságok, amik egyedi azonosításra alkalmassá teszik az ujjnyomatot, illetve hány ilyen jegyet vegyek figyelembe az azonosítás során. Igyekeztem a program összes lehetséges lépésében nagy szabadsági fokot megadni, így a későbbiekben könnyen állíthatóak, finomíthatóak a beállítások.

A kutatásom során azt is figyelembe kellett venni, hogy az egyes lépések ne torzítsanak a köztes eredményeken, félrevezetve így a mesterséges neurális hálózat vizsgálatát. Ennek következtében úgy döntöttem, hogy a felhasználóhoz tartozó mintákat úgy állítom elő, hogy egy jó felbontású, nagyobb méretű ujjnyomatból (296 px × 560 px) egy vágóablakkal kisebb ujjnyomatokat készítem (200 px × 200 px). Ezek egymáshoz képest jól szimulálják az eltolásból és elforgatásból eredő torzításokat, de más környezeti vagy felhasználói hiba nem terheli őket. A mintákban az ujjnyomat közepe nagy valószínséggel fordul elő, mert a tapasztalat szerint ez gyakran szerepel a

valóságos adatbázisokban is, és fajlagos itt a legnagyobb az egyedi azonosító jegyek előfordulásának valószínűsége. A 31.ábra látható az adatbázisba kerülő minták generálásának illusztrációja. A felhasználóhoz köthető adathalmaz számára összesen tizennégy ujjnyomatot vágtam ki, amiből négyet minta sablonként az ANN tréningje során használtam fel, tíz mintát pedig később, a teszteléshez [46]:



31.ábra: Ujjnyomatok készítése a keretprogram adatbázis részére

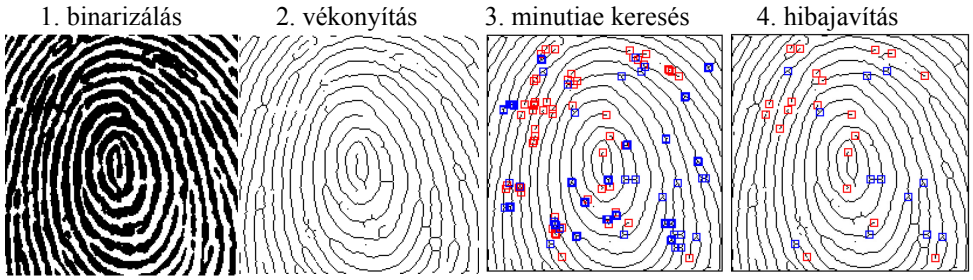
A következő lépés az ujjnyomat képek feldolgozása volt. A daktiloszkópia tudománya már régóta vizsgálja, hogy milyen egyedi jellemzők figyelhetőek meg a fodorszálak[5] között [47]. Jelen vizsgálatban nem foglalkoztam a fodorszálak makró szintű geometrikus elrendezésével, csak a minutiákkal (32. ábra), de meg kell említeni, hogy sok ujjnyomat azonosító eszköz ezt is figyelembe veszi. Bizonyos eszközök a fodorszálak fő geometrikus mintázatai alapján először csoportba sorolják az újjnyomat mintákat, majd már a szűkebb csoportokon belül keresik az egyezést, csökkentve ezzel tulajdonképpen az azonosítási időt. Ez a megoldási módszer a multimodális biometrikus megoldások közé sorolható, hiszen két különböző vizsgálati módszer egyszerre zajlik le az azonosítási ciklus során.

[5] A fodorszálak az ujjakon és a tenyéren futó bőrredők, az fodor szálak végződése, elágazása és találkozása jellemző mintákat, minuitiákat alkot

32. ábra: Fodor szálak által kirajzolt minutiae típusok [38]

A minutiae pontok felismeréséhez úgynevezett előfeldolgozáson kell keresztül esnie a képeknek. Ehhez a nyers, szürkeárnyalatos képet először át kell alakítani fekete-fehér képpé, majd a fodorszálak lenyomatát el kell vékonyítani. A karcsúsítás egészen addig tart, amíg egyetlen pixel vastagságúvá válnak. Ehhez a "*im2bw*" és a "*bwmorph*" parancsokat használtam (33. ábra). Az így kapott "csontvázon" már könnyebben lehet elvégezni a minutiák keresését. Nem az összes minutiae-t kerestem, csak a bifurkációkat és a végződéseket, mert a szakirodalom szerint ezek az azonosítás szempontjából legjobban használhatóak [48].

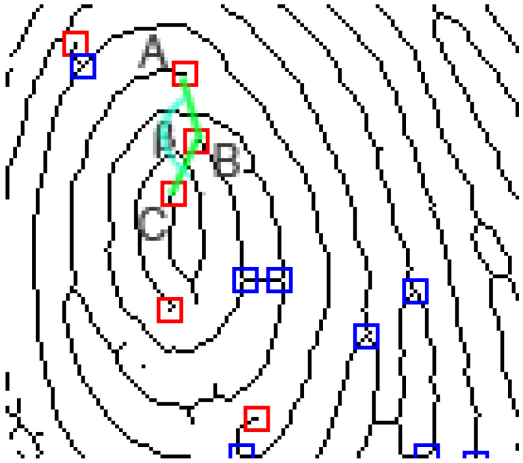
A kereséshez a Sudiro és Yuwono által részletesen leírt módszert a "keretező számok módszerét" (crossing number) használtam. Ez a módszer minden egyes pixel esetén megvizsgálja, hogy hány fehér és hány fekete pixel veszi körül, illetve ezek hogyan követik egymást. A vizsgált kilenc db pixel fekete vagy fehér mivoltának üteme fogja megadni, hogy a vizsgált pixel minutiae pont-e vagy sem [48].



33. ábra: Ujjnyomatok feldolgozásának lépései

Az előfeldolgozás részeként az azonosított minutiák közül ki kell szűrni azokat, amelyek hibásan lettek minutiaként azonosítva. Ennek egyik hatékony módszere, hogy az egymáshoz közel eső minutiaként észlelt pontok esetében mindkét pontot töröljük. Ennek oka, hogy ilyen esetekben egyfelől lehet szennyezés vagy sérülés a háttérben, illetve az újbóli azonosítási procedúra során a kis távolságokon még a kis mértékű torzítás is nagy relatív hatással bír. Ennek megfelelően az egymástól hat pixelnyi euklideszi távolságra lévő minutiaként azonosított pontok mindkét tagját kivettem a potenciális egyedi azonosító jegyek halmazából. Ez a lépés 60-80%-kal csökkentette a halmazok számosságát. Ezt a számosságot pedig tovább csökkentettem azzal, hogy kiszűrtem a legnagyobb torzító hatást elszenvedő pontokat is. Ennek során kijelöltem a számomra matematikailag érdekes területet (Region of Interest - továbbiakban ROI), és csak az ebben lévő pontokat vittem tovább az ANN felé. A ROI-t úgy határoztam meg, hogy a már csökkentett számú minutiae pontok közül tekintsük a súlyponti eloszlás szerinti középső minutiae-t és az ehhez legközelebb eső (euklideszi távolság szerint) további 14 minutae pontot. Így tehát generáltam 15 minutae pontot, ami bizonyosan kevesebb torzítást szenved el, mint távolabbi szomszédjai, de nagy valószínűséggel azonosításra is kerül az ujjnyomat kiolvasása során. Természetesen közel sem biztos, hogy minden esetben ugyanaz a 15 pont kerül azonosításra, de ennek a problémának a kezelését már az ANN-re bíztam.

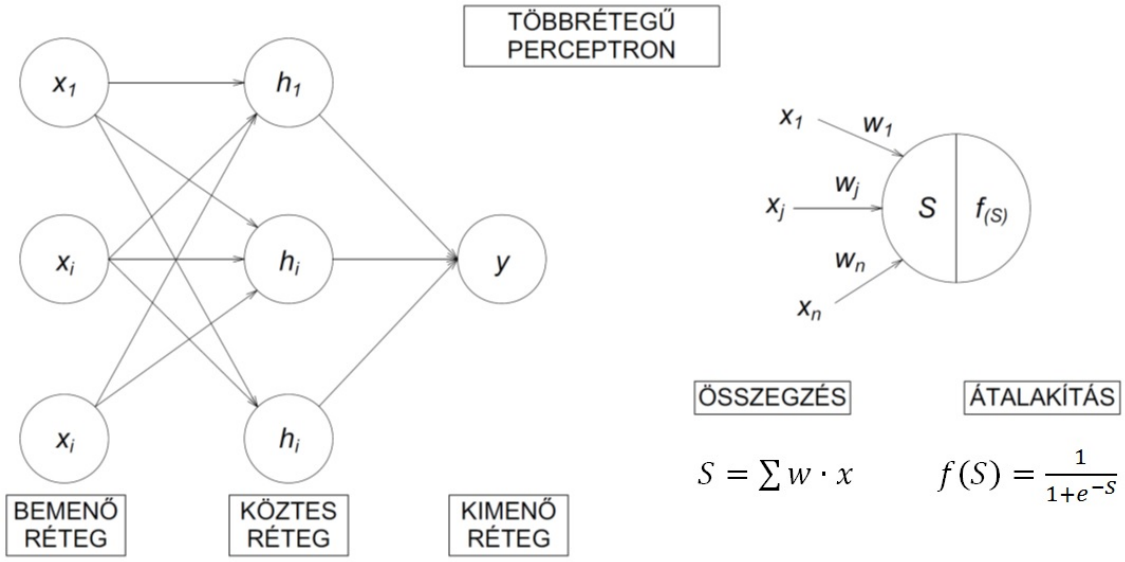
Mielőtt az ANN bemeneti rétegére küldhettem volna a minutiae pontokat még egy feladatot kellett elvégezni az előfeldolgozás részeként, ez pedig az egyedi azonosítási információk explicit meghatározása. Ebben a lépésben nem Sudiro és Yuwono által ismertetett utat követtem, hanem Ravi és kollégái által bemutatott – matematikailag könnyebben kezelhető – közeli szomszédok módszerét vettem alapul [49]. Megkerestem minden minutiae pont (B_i) esetében a két legközelebbi szomszédot (A_i ; C_i), és meghatároztam az euklideszi távolságokat (;) illetve a közbezárt szöget (β) (34. ábra). Minden egyes pont esetében ezt a három adatot előállítva egy 45 elemű adatsort kaptam ujjnyomatképenként. Az adatokat egy tulajdonság vektorként (feature vector) definiálva vittem tovább az ANN számára.



34. ábra: Egyedi azonosító jegyekből az egyediséget kódoló információ kinyerése

A kinyert adatsor értékeit a továbbiakban tanításra és tesztelésre használtam fel, amit egy mesterséges neurális hálóval végeztem. Ahogy a bevezetőben szó esett róla az ANN tulajdonképpen az emberi neurális hálózathoz hasonlóan működik, de a matematikai implementációja megkövetel egy bizonyos struktúrát. Ebben a struktúrában minden esetben van egy bemeneti és egy kimeneti réteg, illetve a kettő között lehetséges rejtett rétegeket is beiktatni. Az egyes rétegekbe véges számú neuront kell rendelni, és ezek, illetve a rejtett rétegek száma az, ami végső soron meghatározza, hogy milyen összetett problémát tud kezelni a hálózat. Amennyiben túldimenzionált hálózatot alkotunk, akkor sok tanító adatra és nagy számítási kapacitásra van szükség, amennyiben pedig túl kicsi hálózatot konstruálunk, akkor nem lesz képes felismerni a mintázatot. A kérdéses méret meghatározása kritikus feladat, és nehezen automatizálható, de ahogy azt a későbbiekben ismertetem, a feladat jól kezelhető az ANN paraméterek genetikus algoritmusokkal történő automatikus optimalizálásával.

Minden egyes neuron hálózati szerepe kettős, mindegyik egyfelől összegzi a beérkező értékeket a vele kapcsolatban lévő bemeneti neuronoktól, és súlyozza ezeket a két neuron közti súlyértékek alapján, másfelől bizonyos szinten aktiválódik a beérkező "jelek" függvényében. Ehhez általában egy szigmoid (pl. tangens hiperbolicus) aktivációs függvényt használunk, aminek aktivációját a bemenő, súlyozott értékek határozzák meg. Egy többrétegű percepotron általános modelljét illusztrálja a 35. ábra [28].



35. ábra: Többrétegű perceptron általános modellje [50]

Ahogy a fuzzy logikában, úgy a mesterséges neurális hálózatok esetében is vannak olyan beállítási lehetőségek, amelyek érdemes kipróbálni. Így megvizsgáltam, hogy az unipoláris vagy bipoláris aktivációs függvény-e az alkalmasabb. Az algoritmus sajnos csak a bipoláris aktivációs függvény esetében vezetett eredményre, így végül kizárólag a tangens hyperbolicus függvényt használtam hálózatokban.

A neurális hálózat mint univerzális approximátor jól alkalmazható olyan feladatokra, ahol a bemenetek és kimenetek közti összefüggés összetett, és lineáris algebrai eszközökkel nehezen kezelhető. Jelen esetben az azonosítás modelljében az összehasonlítást úgy kell elképzelni, hogy a tárolt sablonokhoz tartozó tulajdonság vektorok egy kvázi "átlagos" értékét vetjük össze az azonosítás során beolvasott mintából kinyert tulajdonság vektorral. Ezen vektorok összehasonlítása természetesen nem csak lágy számítási módszerekkel oldható meg, jó megoldásra vezethet a klaszter-analízis egy kiterjesztése is, de a tanulási képesség és a változások figyelembe vétele az ANN esetében különösen jó eredményeket mutat a szakirodalom szerint [51].

Az ANN szerkezeti kialakítása során nem tértem el az ajánlásoktól, de az algoritmust nem MATLAB TOOLBOX-szal, hanem külön erre a célra készített programsorral kódoltam. Az alapstruktúra egy előre csatolt többrétegű perceptron, amit úgynevezett hiba-visszaterjesztési (error back-propagation) módszerrel tanítottam, Milan Hajek könyvében leírtak szerint [52].

Ahogy arra már utaltam a hiba-visszaterjesztéssel történő tanítás a példákból okul. A tanítási fázis tulajdonképpeni célja, hogy az ANN szabad paraméterei, tehát a neuronok közötti összeköttetés erősségét szimbolizáló súlyok elérjék a legjobb beállítást, pontosabban egy olyan beállítást, ami mellett a háló már kellő biztonsággal használható. A tanítás során úgynevezett tanulási ciklusokat (epoch) kell lefuttatni, ami egy iterációs folyamat útján az elvárt és az aktuális kimenet közti különbséget visszaterjeszti minden egyes réteg súlyvektorába (22,23).

$$E = \frac{1}{2}(d_i - o_i)^2 \tag{22}$$

$$E = \frac{1}{2}[d_i - f(w^t x)]^2 \tag{23}$$

Ismerve az eltérést az elvárt (desired - d_i) és az aktuális kimenet (output - o_i) között, elindítható az súlyok javítása a súlymátrixban. Ezzel együtt meg kell jegyezni, hogy a megoldás erősen függ két beállítástól. Egyfelől a kutatásom eredménye – a nemzetközi szakirodalommal összhangban – azt mutatta, hogy a teljes rendszer rendkívüli módon érzékeny súlymátrixban szereplő kezdeti értékektől. Amennyiben ezen értékek kezdeti kiosztásában egy adott mintázat vagy szabályosság figyelhető meg, akkor a konvergencia nagyon lassú, sőt esetenként nem is sikerült a tanítás [51] [52].

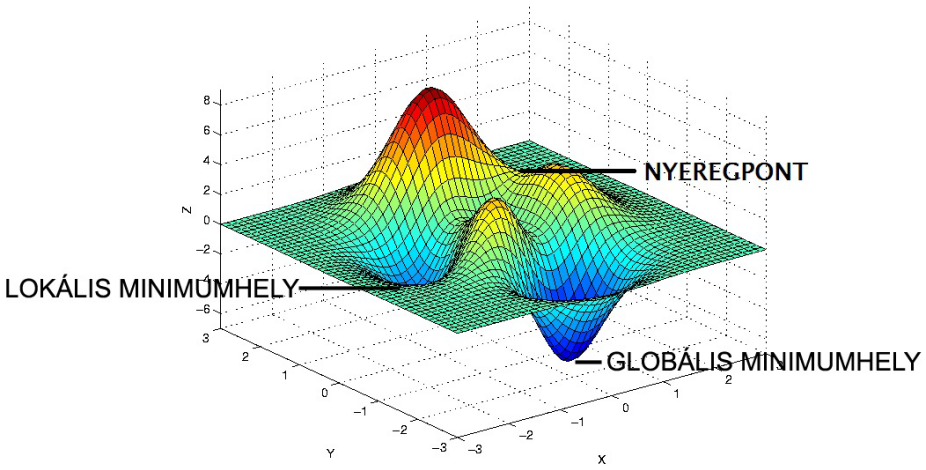
A kezdeti értéke okozta torzítások kompenzálására a súlymátrix megadásánál választottam egy kezdeti eltérési értéket is (bias), hogy a közelítés pontosabb legyen. A súlymátrix javításánál ezt az értéket is minden körben frissítettem (25). A másik erős limitáló tényező a tanulás sebességét meghatározó paraméterek kérdése (24). Amennyiben a tanítási paramétereket úgy állítjuk be, hogy gyors legyen a konvergencia, előfordulhat olyan eset, hogy a "túl nagy ugrások" miatt a közelítés megragad egy lokális minimumhelyen (local minima) [51] [52].

$$\Delta w_{ji}(n+1) = \eta \delta_j(n) y_i(n) + \Delta w_{ji}(n) \tag{24}$$

$$\Delta b_i(n+1) = \eta \delta_i(n) + \Delta b_i(n) \tag{25}$$

Ahogy azt a béta-binomiális eloszlás bizonyításánál is bemutattam, a megfelelő módszerek alkalmazása segíti megtalálni a megfelelő konvergenciát. Több kezdeti módszer mellett a Newton-Raphson féle iterációs módszert is megpróbáltam alkalmazni

de ez több okból kifolyólag sem vezetett sikerre. Egyfelől, ha a távoli az iteráció kezdőpontja, akkor a túl gyors lépések okán a konvergencia elmarad, illetve ha lokális minimumhelyre érkezik a derivált zérus lesz, és így a konvergencia ismét nem kvadratikus.



36. ábra: Lokális minimumhely és nyeregpont szemléltetése nem lineáris eseménytérben

Ebben a megközelítésben olyan megoldást kellett választani ami általánosan jól konvergál és számítási formájában is kezelhető a tanító algoritmus számára. A választás ez esetben is az iránymenti deriválttal számított, Martin Riedmiller által is leírt gradiens ejtési (gradient descent) módszerre esett, amely speciális módon, úgynevezett rugalmas hiba visszaterjesztéssel (26) (resilient error back-propagation - Rprop) módszerrel valósítottam meg [53] [54].

$$\Delta w_{ijk}^{(t)} = \begin{cases} -\Delta_{ijk}^{(t)}, \ if \ \ \frac{\partial E^{(t)}}{\partial w_{ijk}} > 0, \\ +\Delta_{ijk}^{(t)}, \ if \ \ \frac{\partial E^{(t)}}{\partial w_{ijk}} < 0 \\ 0, otherwise \end{cases} \tag{26}$$

$\Delta w_{ijk}^{(t)}$: súlyok frissítésének iránya

$E^{(t)}/w_{ijk}$: parciális deriváltak összesített értéke

A hiba visszaterjesztésnek ez a típusa nem a parciális deriváltak értékét hanem irányát vizsgálja, ami tulajdonképpen meghatározza a súlyok módosításának irányát ($\Delta w_{ijk}^{(t)}$). Természetesen fontos megtalálni a lépés mértékét is, amit az alábbi egyenlet (27) ír le. A lépés ez esetben függ a frissítés irányától, azaz a gradiens előjelétől és a η^- és η^+

faktoroktól, amik jelen esetben 0,5 és 1,2 értéket kaptak a vonatkozó szakirodalommal egybevetve [53] [54].

$$\Delta_{ijk}^{(t)} = \begin{cases} \eta^{+}\Delta_{ijk}^{(t-1)}, \ if \ \frac{\partial E^{(t-1)}}{\partial w_{ijk}} \cdot \frac{\partial E^{(t)}}{\partial w_{ijk}} > 0 \\ \eta^{-}\Delta_{ijk}^{(t-1)}, \ if \ \frac{\partial E^{(t-1)}}{\partial w_{ijk}} \cdot \frac{\partial E^{(t)}}{\partial w_{ijk}} < 0 \\ \Delta_{ijk}^{(t-1)}, \ otherwise \end{cases} \tag{27}$$

A tanító algoritmus leprogramozása után, készítettem egy validáló programrészt is, ami az ismert adatsorokon egy ciklikus tesztsorozat lefuttatásával egy statisztikailag elfogadható eredményt ad. A teszt során tíz valódi mintából származó – korábban kinyert – biometrikus tulajdonságvektorral és tíz véletlenszerűen generált tulajdonságvektorral vizsgáltam a tanítást és az algoritmus működését.

A mesterséges neurális hálózatok tanítása szempontjából kritikusan fontos, hogy a súlymátrix kezdeti értékei kellően aszimmetrikus eloszlást kövessenek. Ennek érdekében egy random generátort használtam, aminek két paraméterét – optimalizálási céllal – változtathatónak hagytam meg. A tanítást akkor tekintettem sikeresnek, ha az egyes tanító ujjnyomat illeszkedésének értéke elérte a 99,5%-os küszöböt, azaz a tanítás után átlagos eltérés *epsilon* < 0,005. Az így "feltanított" algoritmusok minden esetben egy kissé eltérő módon jutottak el a célállapothoz, van, amelyik már öt *epoch*, de volt amely csak 13 *epoch* után. A teljes súlymátrixok elemei ennek megfelelően, ugyan kis mértékben de eltérőek. Ezen eltérések vizsgálatának célja éppen a tesztelés, hiszen annak ellenére, hogy a tanítás az ismert mintákra 99,5%-nál magasabb ugyan, de nem biztos, hogy a tanító mintákból kinyert információ és maga a konvergencia elégséges a hatékony gyakorlati működéshez.

2.3.3 A mesterséges neurális hálózat tanításának eredményei

A MATLAB környezetben egyedi kódolással készített előrecsatolt, többrétegű perceptron modell tanítását tehát két lépésben kellett elvégezni. Egyfelől olyan tréningeken esett át az algoritmus, ahol ismert torzítási hibákkal rendelkező ujjnyomatokkal végeztem el a súlymátrix hangolását. Tíz alkalommal hangoltam újra az algoritmust, random kezdeti súlymátrixszal, de a tanítás hatékonyságának küszöbértékén, a tanító sablonokon és az iterációs folyamatot befolyásoló egyéb

paramétereken (momentum paraméter, eta tanítási koefficiens, epsilon, hálóstruktúra) nem változtattam. Ezzel együtt meg kell jegyezni, hogy ezen paraméterek tudatos megválasztása, optimalizálása nagy mértékben segítheti a hatékonyabb tanítást és a gyakorlati működést, azonban a változók relatív magas száma és a keresési tér kiterjedtsége nagy mértékben nehezíti a vizsgálatot, sőt belátható, hogy analitikus módon a feladat nem optimalizálható. Ezen paraméterek optimalizálásának kérdését szintén genetikus algoritmusokra érdemes bízni.

A mintasorokból a négy tanító sablon minutiáinak egyedi azonosító jegyeit kódoló információkat (4 db 45 elemű tulajdonságvektor) az algoritmus együttesen tanulta meg. Ez a módszer a természetes neurális hálók működéséhez hasonlóan, erősítette a "könnyen" előhívható minutiák adatait, így szelektívebbé válhatott az azonosítás, azonban rugalmasabban is kezelte a beolvasott minutiák által hordozott információt, így nagyobb hibatoleranciát sikerült elérni. A tíz ellenőrző teszt összesen húsz elemű adatsorát lefuttatva az adott kezdeti feltételekkel tréningelt hálózaton, a következő három esetet adta:

- egyfelől bizonyítottan előállt olyan eset, ahol az általam készített ujjnyomatolvasó program és az ANN kellően szelektív módon meg tudta különböztetni a felhasználói és a mesterséges tulajdonságvektorokat, ezen esetekben az egyezőség mértéke a hamis és az eredeti adatok esetén nem egy nagyságrendbe esett,
- másik esetcsoportban előfordult olyan eset, hogy a mesterségesen előállított értékek közül a háló tévesen elfogadott mintákat, aminek oka lehet, hogy a véletlenül generált minta éppen egyezett a felhasználóra egyébként jellemző mintázattal, de valószínűbb, hogy úgynevezett túltanított háló jött létre, azaz a nehéz kezdeti feltételek kompenzálása okán egy olyan erős konvergenciát kellett véghezvinni a hiba visszaterjesztése során, hogy a súlymátrix elvesztette szelektivitását,
- a harmadik csoportba sorolhatóak azon eseteket, amikor az eredmények ütközést mutattak, azaz a mesterséges és eredeti tulajdonságvektorok felismerése egy nagyságrendbe került, tehát jellemzően megszűnt a megkülönböztethetőség a valós és az idegen minták között.

A teszt eredményeit a II. és III. melléklet táblázatai foglalják össze, de fontos kiemelni, hogy teszt kiterjesztése nagyobb elemű adatsorokra, illetve egyes változók számának bővítése (több tanító minta, több felhasználótól származó mintasor együttes vizsgálata) tovább árnyalná a képet. Jelen tézisben arra fókuszáltam, hogy egy-az-egyhez típusú ellenőrzés esetében az ANN egyes tulajdonságai milyen módon lehetnek hatással a biometrikus minták automatikus azonosításának hatékonyságára.

2.4 A második főfejezet összefoglalása

A fejezetben a Mesterséges Intelligencia alapját jelentő lágy számítási módszerek közül részletesen foglalkoztam a Fuzzy Logikával és a Mesterséges Neurális Hálókkal. Mindkét területen megvizsgáltam az alkalmazható matematikai hátteret, és egy-egy önálló programot készítettem, míg előbbinél egy bimodális biometrikus vezérlő döntési algoritmusát, addig utóbbinál egy mintafelismerési feladat tanulásra képes értékelő algoritmusát készítettem el. A Fuzzy Logika esetében bizonyítást nyert, hogy a fuzzy alapú, összetett döntési modell szegmentáltabb eredményhalmazt konstruál, mint a középértékekkel történő következtetés (pl.: átlagolás). A Mesterséges Neurális Háló alkalmazása pedig segítette a biometrikus mintákban bekövetkező minorális változások azonosításra kiható befolyásának szignifikanciáját, javítva így a felismerés hatékonyságát a klasszikus torzítások (eltolás, elforgatás) esetében.

3 KOMBINÁLT LÁGY SZÁMÍTÁSI MÓDSZEREK ALKALMAZÁSA MULTIMODÁLIS BIOMETRIKUS AZONOSÍTÁSI FELADATOKRA

3.1 Genetikus algoritmussal optimalizált mesterséges neurális hálózattal végzett biometrikus mintafelismerés

3.1.1 Összetett problémák kezelése GA alkalmazásával

Az előző fejezetben bemutatást nyert a mesterséges neurális hálózatok szerkezete, működése és alkalmazásának feltétele a biometrikus azonosításban. Láttuk, hogy az ANN tanulási képesség előrelépést jelent a mintázatok rugalmasabb felismerésében, a szelektivitás megőrzése mellett. Azonban azt is láthattuk, hogy sajnos számos olyan paramétert kell beállítani, ami alapvetően határozza meg a háló és a tanulás működését.

A problémakör komplex vizsgálata során megállapítható, hogy amíg az elméleti megközelítés oldaláról erősen limitáló tényező, hogy legyen kellően bonyolult a háló (összetett súlymátrix), legyen képes a magas szelektivitásra, és a kezdeti súlyok megválasztása valóban véletlenszerű legyen, addig a gyakorlati alkalmazás oldaláról általában négy limitáló tényezőt kell figyelembe venni,: a biztonságot, az időtényezőt, a technológiai igényt, és az ezeket tulajdonképpen közvetve magába foglaló gazdasági szempontokat. Figyelembe véve a limitáló tényezőket, hamar belátható, hogy a megfelelő háló architektúra és egyéb működési beállítások egy NP-teljes problémát alkotnak. Az NP teljes problémák esetében pedig ismeretes, hogy megoldásuk időben nem polinomiális, vagy olyan számítástechnikai háttér kell, aminek feldolgozási kapacitása a bemeneti adatok számával exponenciális viszonyú, ilyen pedig nem áll rendelkezésre. Nehezen képzelhető el olyan piaci modell, ami egy nagyteljesítményű úgynevezett szuperszámítógép bevonását igényli a tanítási fázisban, hogy végig lehessen próbálni a működési beállítások összes lehetséges kombinációját [55].

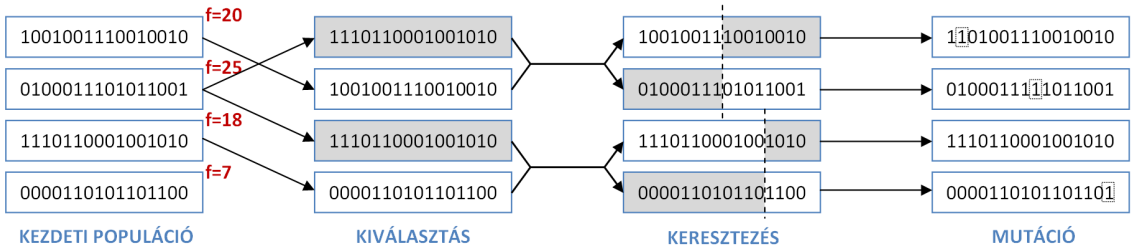
Így matematikai szempontból jobban kezelhető optimum keresési eljárásra van szükség. Habár meg kell jegyezni, hogy ma már több olyan szolgáltató van, aki az alkalmazott MI technológiákat számítógépes hardverrel kínálja szolgáltatásként, ilyen például a Google Cloud AI & Machine Learning Products vagy az Amazon ML & AI Services.

Míg a korábbi fejezetben a szakirodalmi javaslatokat és heurisztikus megközelítéseket alkalmaztam a háló megfelelő beállításainak megtalálására, addig ebben a fejezetben azt bizonyítom, hogy a genetikus algoritmusokkal hatékonyan megtalálhatóak azok a működési beállítások, amelyekkel a tanulás kellően hatékony. Sőt, a megoldandó biometrikus feladat jellegétől függően az ANN beállításai újrahangolhatóak az adott problémára, így megőrizve a mesterséges hálók univerzális approximátor tulajdonságát is.

A Lágy Számítási Módszerek eddig nem tárgyalt ága a három alaptechnika közül a legmodernebb. Ez az Evolúciós Számítások csoportja és ezen belül a Genetikus Algoritmusok. A munka során a Genetikus Algoritmusok klasszikus definíciója szerint értelmezett formáját használom, bár meg kell említeni, hogy a GA optimalizált ANN rendszereket szokás Evolúciós Mesterséges Neurális Hálóknak is hívni (Evolutionary Artificial Neural Networks - EANN) [56]. Ahogy a többi lágy számítási módszer, a GA is a természetből eredeztethető, mégpedig a Charles Darwin által leírt evolúciós megfigyelésekből, miszerint a természet is igyekszik a genetikai állományunk javítására, optimalizálására. Már most különösen fontos megjegyezni, hogy ez az optimum mindig relatív, hiszen a környezeti feltételek megváltozása során az optimális pont, helyesebben optimális működési intervallum is változik.

John Holland 1975-ben ismertette a GA matematikai interpretációját, aminek lényege, hogy az optimalizálandó elemeket kromoszómaként kódoljuk egy string-en. A kódolásra általában egy bináris kód a legalkalmasabb, azzal később könnyebb a genetikus átvitelek elvégzése. Minden stringhez rendelni kell egy úgynevezett fitnesz értéket, amely az adott környezeti feltételek tekintetében jellemzi a hordozott információk jóságát. Ez a fitnesz érték sokszor egy összetettebb eredménysorozat során adódik ki (ahogy erre a saját programomban is példát mutatok), de amennyiben a fitnesz érték meghatározása összetett, az nagymértékben lassítani fogja az optimum megtalálását is. Ahogy az a természetes evolúció során is zajlik, ez esetben is egy kompetitív szituáció áll elő az egy populációba rendelt, egymástól kissé eltérő kromoszómákkal rendelkező egyedek között. A GA lényege pedig az, hogy ez a verseny milyen módon zajlik le [57].

Az optimalizálás folyamata során minden populáció egy-egy generációt él meg, így a keresés generációról-generációra történik, ameddig elérjük azon stringek tömegét, amelyek a legjobb fitnesz értékkel rendelkeznek. Egy populáció tagjaival a generációs váltás során – a természettel analóg módon – három féle módosulás történik (lásd 37. ábra). Egyrészről kiválaszthatjuk (selection) a legjobb fitnesz értékkel rendelkező egyedeket, amelyek nagyobb valószínűséggel kerülnek be a következő populációba, másfelől keresztezhetjük (crossover) is a sikeresebb kromoszómájú egyedeket, kicserélve így bizonyos genetikai állományukat egymással, harmadrészről pedig véletlenszerűen megengedhetjük, hogy egy-egy tulajdonság mutációt szenvedjen (mutation) úgy, hogy minden bit kis valószínűséggel megváltozhat [28].



37. ábra: A genetikus algoritmus során lezajló változások

3.1.2 Az alkalmazott GA kiválasztása és illesztése az ANN optimalizáláshoz

Számos módszer létezik a kiválasztás és a keresztezés megvalósítására, jelen vizsgálathoz a tournament (lovagi torna) módszert választottam, amelynek során minden új helyért a következő generációban a korábbi populáció két, véletlenszerűen kiválasztott tagja vív meg egymással (a magasabb fitnesz értékű nyer). A kereszteződés függ néhány kezdeti feltétel megadásától, és egy véletlenszerűen választott kereszteződési valószínűségtől. Jelen esetben a keresztezéshez egy különleges keresztezési módszert definiáltam, ami nem csak az adott string keresztezését dönti el véletlenszerűen, hanem a keresztezési pont kijelölése is egy randomgenerátor szerint történik. Itt meg kell jegyezni, hogy a keresztezés ebben a formában jelentősen egyszerűbb a biológiai változatnál, hiszen, ott egyfelől kvadratikus a kódolás a nukleinsavak miatt, másfelől csak értelmes szekvencia töredéket lehet másolni és átemelni, szemben a fenti módszerrel, ami adott esetben az egyes tulajdonságokat kódoló, összetartozó biteket figyelmen kívül hagyja. Ellenben ez a megoldás lehetőséget ad rá, hogy a teljes string kicserélődjön, így adott esetben véletlenszerűen ne legyen

kereszteződés. A mutációs rátát egy változtatható paraméterrel állítottam be, mert a szakirodalmi vélemények szerint ennek értéke erősen hatással lehet a GA működésének sikerére [58] [28].

Ahogy azt az ANN tanításánál láttuk, több olyan fontos paraméter van, aminek optimalizálása kritikusan fontos a működés szempontjából. A biometrikus minták jellegétől függően optimalizálandó a tanulás mértéke (η), illetve a lendület paramétere (m_0). A tanulás sebességének (η) 0 és 1 között kell lennie, ha az érték kisebb, akkor a súlymátrixok elemei lassabban változnak, a pálya ugyan simább, de a konvergencia lassabb. Ha az eta (η) túl közel van az egyhez, akkor a konvergencia gyorsabb, de az algoritmus könnyen instabillá válik, oszcillálhat. Az oszcilláció elkerülése érdekében lehetőség van a delta szabály módosítására, amely technikailag az alábbiakat jelenti:

$$\Delta w_{ji}(n) = m_0 \Delta w_{ji}(n-1) + \eta \delta_j(n) y_i(n) \tag{28}$$

A súlymátrixok (Δw_{ij}) elemeinek megváltoztatása az előző változás momentummal történő szorzatának és az aktuális réteg helyi gradiensének összege. A gradiens ejtési módszerrel végzett hiba vissza-terjesztés gyorsabbá teszi a konvergenciát és védelmet nyújt az oszcilláció ellen [52].

Az ANN összes említett paraméterére vonatkozóan megállapíthatjuk, hogy azok számos lehetséges beállítást és megszámlálhatatlanul sok lehetséges beállítási kombinációt adnak. Ezért szisztematikus módszert kell találni azok optimalizálására. Az empirikus tapasztalataim szerint az egyik legnagyobb nehézség a súlymátrixok kezdeti beállítása. Ha szimmetria vagy kezdeti minta fedezhető fel a véletlenszerű kezdeti súlyértékek mátrixában, akkor a súlymátrixok helyi minimumokhoz vezetnek, és a tanítás nem lesz sikeres. Hajek szerint a szokásos gyakorlat az, hogy a hálózatok összes szabad paraméterét egyenletesen elosztott véletlen számokra állítjuk be [52].

Alapvetően a túl kicsi kezdeti súlyokat azonban el kell kerülni, mert δ-val szorozva a gradiens túl kicsi lesz. Az sem megfelelő, ha a kezdeti súlyok értékei túl nagyok, mert ez korai telítettséghez vezethet. Ebben az esetben a neuron kimenete megközelíti a sigmodialis funkció határait, és csak kis változás következik be a súlyokban. A jelenség megfelel a hibafelületek nyeregpontjának (lásd 36. ábra).

A második fejezetben ismertetett, mintázatok felismerésére készített ANN manuális hangolása megmutatta, hogy a különböző rétegekben a súlyok kezdeti eloszlása (w_0 = bemeneti réteg; w_1 = az első rejtett réteg; w_2 = második rejtett réteg; w_3 = kimeneti réteg) másnak kell lennie. Ez azt jelenti, hogy a véletlenszerűen választott súlyok intervallumának határértékeit és hosszát másként kell kiválasztani. Ahhoz, hogy ezek a különbségek lehetségesek legyenek, a véletlen generátorokat különböző paraméterekkel kell beállítani. Valójában a GA egyik legfontosabb feladata az, hogy ezeket a beállításokat optimalizálja [58].

```
W0=a0+b0*randn(1,N+1)

W1=a1+b1*randn(k0+1,k1)

W2=a2+b2*randn(k1+1,k2)

W3=a3+b3*randn(1,k2+1)

,ahol:

N=tréning vektor mérete

k0= bemeneti réteg neuronjainak száma

k1= első rejtett réteg neuronjainak száma

k2= második rejtett réteg neuronjainak száma
```

A véletlenszerű súlyok generátorainak összesen nyolc paramétere van. Négy súlymátrixunk van (minden rétegben egy), egy paraméter a véletlenszerűen választható számú intervallumának szélességet, a másik az intervallum kezdőpontját határozza meg. Jelen esetben a súlymátrix kezdeti beállítására összpontosítottam, mivel ez döntő fontosságú, azonban a GA egyéb paramétereit is érdemes vizsgálni az optimum megtalálása szempontjából.

3.1.3 GA optimalizált ANN tanítási eredményeinek összefoglalása

Ahhoz, hogy megtaláljam a GA elemi beállítását, mielőtt az ANN optimalizálásához használnám, egy nyolc változóval rendelkező komplex függvényt használtam. A változók kezdeti értékeit a változók nullától való torzítása adta, mert olyan függvényt alkalmaztam, amelynek nulla értéke egy maximális pont (29).

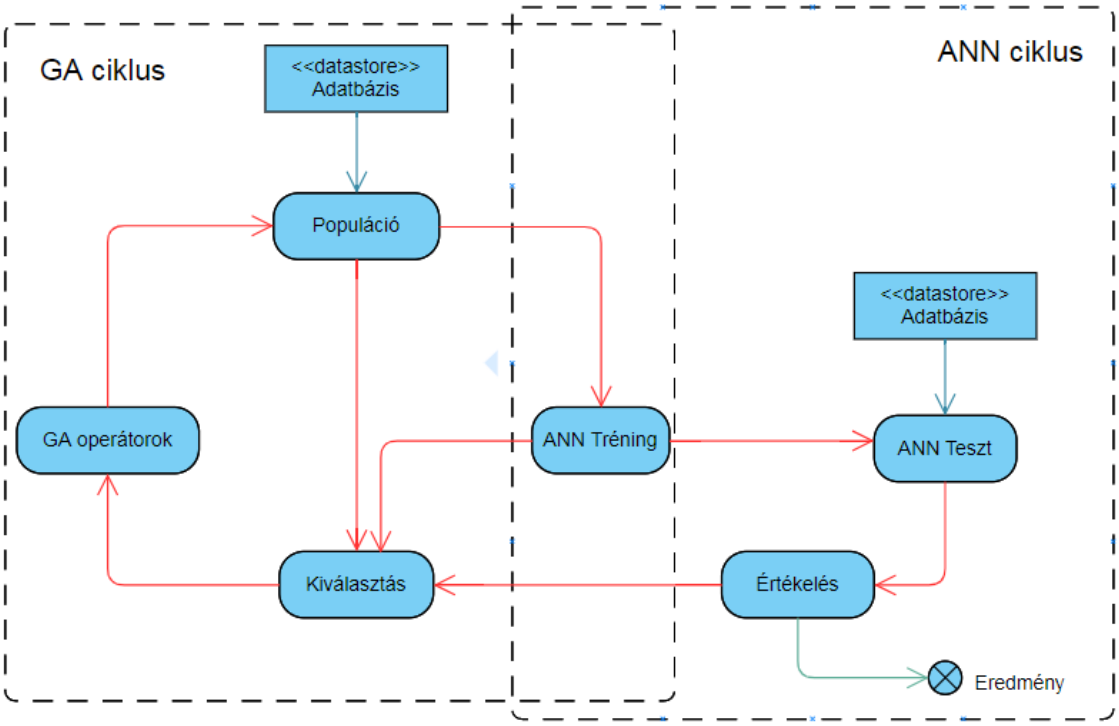
$$f(x_1, \dots, x_8) = \sum_{i=1}^{8} x_i^2 + \sum_{\mathrm{i}\neq\mathrm{j}}^{8} \mathrm{x_i x_j} \tag{29}$$

Egy küszöbértéket állítottam be a változók optimálishoz viszonyított átlagos hibáira vagy távolságaira. Amikor az algoritmus elérte ezt a küszöböt, akkor a program futása megállt, és megmutatta, hogy hány generáció szükséges ahhoz, hogy elérje ezt. A változókat 0,1 , ... , 0,8 értékekre állítottam, így a küszöbértéket alapvetően 0,05-re választottam, de néhány kisebb küszöbérték is várható volt. Az eredmények szerint 0,035, 0,04, 0,045 vagy 0,05 között nem volt szignifikáns különbség. Azonban minél alacsonyabb a küszöbérték, annál kisebb a valószínűsége annak, hogy a GA képes azt elérni. Azt is meg kell állapítani, hogy a küszöb elérhetősége nem 100%, néha az algoritmus lokális maximumot talál és így elakad. A tapasztalati értékek következők:

2. táblázat: A tesztciklusok és a generációszámok viszonya adott küszöbértékek esetén

Küszöb	0,05	0,045	0,04	0,035
Általános generációszám	23	26	33	54
Teszt ciklus	400	300	250	250

A fenti súlymátrix beállítása természetesen csak abban az eseten célszerű, ha az ANN alapstruktúráját már ismerjük. Egy ANN méretét alapvetően a vizsgált probléma bonyolultsága határozza meg. A neurális hálók bemeneti és kimeneti oldala könnyebben kezelhető, mert a legtöbb probléma esetén az adatsorok és a kimeneti értékek alakíthatóak úgy, hogy a bemeneti oldal neuronjainak száma az adatforrásokhoz igazodjon, míg a kimeneti oldal a kívánt eredmények jellegéhez. A problémát alapvetően a rejtett rétegek mennyiségének és az ezekben lévő neuronok számának meghatározása jelenti. A szakirodalom szerint léteznek ugyan ökölszabályok ezek meghatározására, de rendszer kevés neuronnal nem jut el odáig, hogy képes legyen megkülönböztetni az elvárt kimeneteket, míg túl sok neuronnal túltanítottá válik és bármilyen inputra ugyanolyan eredményt ad. A rejtett rétegekben lévő neuronok és a feladatra alkalmas ANN struktúra meghatározásához az alábbi (38. ábra) algoritmust készítettem:



38. ábra: GA optimalizált ANN algoritmusának modellje

Láthattuk, hogy a mesterséges neurális hálózatok működését számos paraméter együttesen határozza meg, és ezeknek létezik olyan részhalmaza, ami a hatékony működés szempontjából nagyobb jelentőséggel bír. Amennyiben olyan probléma esetében alkalmazunk ANN-t, aminek nem ismert az összetettsége, akkor a használat előtt genetikus algoritmus segítségével, felügyelt tanulással optimalizálni kell a hálózat topológiáját (rejtett rétegek száma, neuron száma a rétegekben).

Ezen paraméterek bináris kódolásával egy tetszőlegesen választott széles skálán vizsgáltam a megfelelő hálótopológiát. Fontos következtetésként állapítható meg, hogy a GA optimalizálási eljárás csak akkor vezetett eredményre, ha a hiba-visszaterjesztés során alkalmazott epszilon (υ) és az éta tanulási paraméter (η) azonos nagyságrendbe estek. Szintén jelentős eredményként kell kiemelni azon megfigyelést, hogy a hálózat topológia akkor stabil, ha a bemeneti réteg neuronjainak száma egyenlő, vagy közel azonos a vizsgált egyedi azonosító jegyek számával.

3.2 ANFIS adaptálása multimodális szabálybázis inicializálására

3.2.1 A neuralizált fuzzy rendszerek előnyei

Az előző fejezetekben felvetettem, hogy a mind a fuzzy logika, mind a mesterséges neurális hálózatok jól alkalmazhatóak a biometrikus azonosítási folyamat egy-egy főbb lépésének hatékonyabb alkalmazása céljából, viszont e két módszer együttes úgynevezett hibrid megoldása különösen célravezető. Ismételten ki kell hangsúlyozni, hogy a biometrikus azonosítás egyik központi problematikája a változó minta és az ehhez fűződő egyéni azonosító jegyekhez tartozó adatok rugalmas kezelése.

Értelemszerűen az egyéni azonosító jegyek száma és vizsgálatuk módja függ az azonosítási folyamat struktúrájától is. Így amennyiben úgynevezett egy-a-sokhoz (one-to-many) azonosítási folyamatot vizsgálunk akkor több egyéni azonosító jegyet kell megkeresni és összehasonlítani, mint ha egy-az-egyhez (one-to-one) hitelesítést hajtunk végre. Az utóbbi megoldás használata ritkább, hiszen ebben az esetben kell, hogy legyen egy előfeltétel, miszerint a vizsgálandó mintához tartozó sablon időben és térben egyértelműen rendelkezésre áll, például egy adathordozón. Alapvetően tehát az azonosítás során nagyobb számú egyéni azonosító jegyet kell összehasonlítani. A multimodális azonosítással elérhető, hogy több mintavételi lépést kelljen elvégezni, így egy lépés által bírt hibaterhelés fajlagos súlya csökkenthető. Kérdés viszont, hogy ez hogyan tud megjelenni az azonosítási algoritmus teljes folyamatában?

A lágy számítási módszereknek számos kombinált hibridje létezik. A fuzzy logika és mesterséges neurális hálózatok kombinációi közül manapság a neuralizált fuzzy rendszerek a legelterjedtebbek, ezeken belül is az integrált megoldások. A 80-as évektől számos kutatás foglalkozott a témával főleg optimalizálási eljárások vizsgálata alkalmával. A neurális-fuzzy kombinációk a legtöbb esetben olyan fuzzy következtető rendszerek, amelyek neurális hálózattal javítanak. Tehát van egy alapvetően jól követhető, könnyen programozható fuzzy struktúra, aminek ismeretlen paramétereit (szabályok, tagsági függvények, stb.) neurális hálóval kell optimalizálni. Ezen ismeretlenek finomhangolásával nagymértékben csökkenthetőek a futási idők, és ezzel párhuzamosan a költségek is. A neuralizált fuzzy rendszerek legnagyobb előnye, hogy képes tanulni, és az új ismeretek implementálásával a meglévő folyamatokat optimalizálni vagy új megoldásokat találni [28], [59].

3.2.2 A neuralizált fuzzy rendszerek és az ANFIS struktúra bemutatása

Szabályozási célra alapvetően három típusú neuralizált fuzzy változat létezik, amelyek főleg az implikációs struktúrában térnek el, így megkülönböztethetünk a Mamdani, Takagi-Sugeno és Tsukamoto típusú rendszereket. A szakirodalom vizsgálata során arra jutottam, hogy a Takagi-Sugeno féle megoldás érdemes választani, ahol a szabályok kimenete a bemeneti függvények lineáris kombinációja (30), aminek következtében a defuzzyfikálás lépése elhagyható [28].

$$y_i = a_i + b_i x_1 + c_i x_2 \tag{30}$$

Jyh-Shing Roger Jang és munkatársai 1991-ben ismertették megoldásukat az ANN és fuzzy implikáció ötvözésére. A konstrukció az Adaptive Neuro-Fuzzy Inference System (Alkalmazkodó Neuro-Fuzzy Következtető Rendszer továbbiakban ANFIS) nevet kapta, illetve meg kell említeni ennek többszörös kimenettel is megbirkózó változatát is a Multi Adaptive Neuro-Fuzzy Inference System-t (továbbiakban MANFIS) [60] [61].

Az ANFIS szerkezetében a fuzzy tulajdonságok a premissza (31) és a következtető (32) paraméterekben jelennek meg, míg a választott következtetés Sugeno típusú, a háló pedig egy ötrétegű előrecsatolt MLP (Multi Layer Perceptron). A tanulás ez esetben is hiba-visszaterjesztéssel (Error Back-propagation) történt, a már ismertetett okoknál fogva szintén konjugált gradiens módszerrel iterált tanítással. Jellegzetessége az ANFIS rendszernek, hogy a szabályok kívánt számát előre kell definiálni, így a rendszer tulajdonképpen csak paraméter tanulást végez [61] [62].

Premissza paraméterek:

$$\mu_{A_i}(x) = \frac{1}{1+\left|\frac{x-c_i}{a_i}\right|^{2b_i}} \tag{31}$$

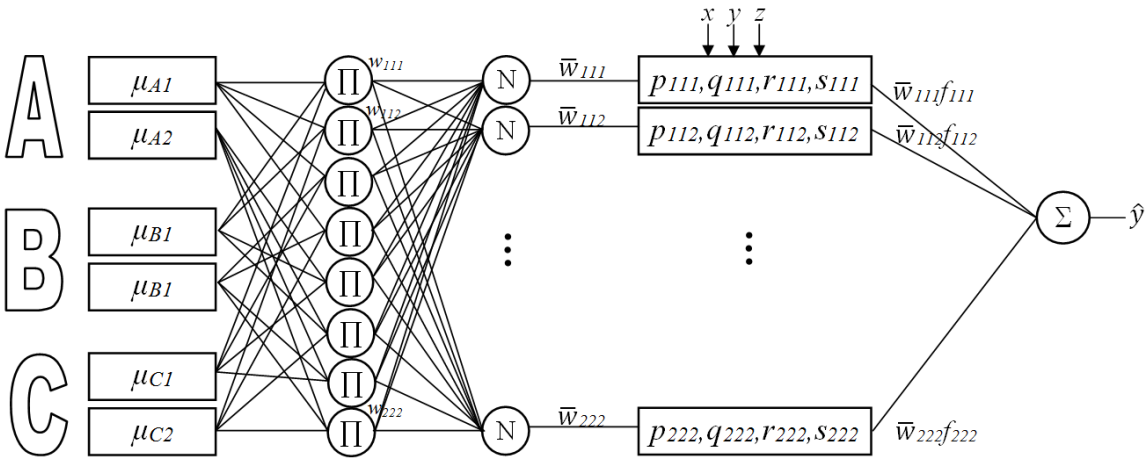
ahol A meghatározza a bemeneti halmazt (A;B;C) és i jelöli a tagsági fgv. felbontást (i=2 jelen konstrukcióban)

Következtető paraméterek:

$$f_{ijk} = p_{ijk}x + q_{ijk}y + r_{ijk}z + s_{ijk} \tag{32}$$

ahol i,j,k jelöli a fuzzy halmazok felbontását (i,j,k=2)

Az alábbi 39. ábra illusztrálja az általam is kódolt ANFIS szerkezetét, amiben fuzzy tagsági függvényeket Gauss görbékkel definiáltam, ezeket jelölik a a_{ijk}, b_{ijk}, c_{ijk} adaptív *premissza paraméterek*.



39. ábra: A megvalósított ANFIS struktúrája

A második rétegben $\prod$ mint összefoglaló operátor áll, feladata, hogy összegezze tüzelő tagsági függvények értékét. A második réteg kimeneti értéke w_{ijk} számítja ki a tüzelő tagsági függvények erősségét (33).

$$w_{ijk} = \mu_{A_i}(x) \cdot \mu_{B_i}(y) \tag{33}$$

A harmadik (rejtett) rétegben a neuronok feladata a második rétegből származó információk összegzése és normálása ($\overline{w}_{\text{ijk}}$) (34):

$$\overline{w}_{ijk} = \frac{w_{ijk}}{\sum_1^{ijk} w_{ijk}} \tag{34}$$

A negyedik rétegben történik meg tulajdonképpen a Sugeno típusú következtetés, ami egyfelől az eredeti változókat (*x, y, z*) másfelől a harmadik réteg kimenetén kapott normált tüzelési értékeket kombinálja (35) az alábbiak szerint:

$$\overline{w}_{ijk} f_{ijk} = \overline{w}_i (p_{ijk} x + q_{ijk} y + r_{ijk} z + z_{ijk}) \tag{35}$$

ahol p_{ijk}, q_{ijk}, r_{ijk} and s_{ijk} a lineáris kombináció premissza parmatérei

Az utolsó, ötödik rétegben mindössze egyetlen neuron van, aminek feladata az eddigi értékek összegzése az alábbi (36) összefüggés szerint:

$$o_{ANFIS} = \sum_1^{ijk} \overline{w}_{ijk} f_{ijk} \tag{36}$$

3.2.3 Az ANFIS szerepe a multimodális biometrikus azonosítási folyamatban

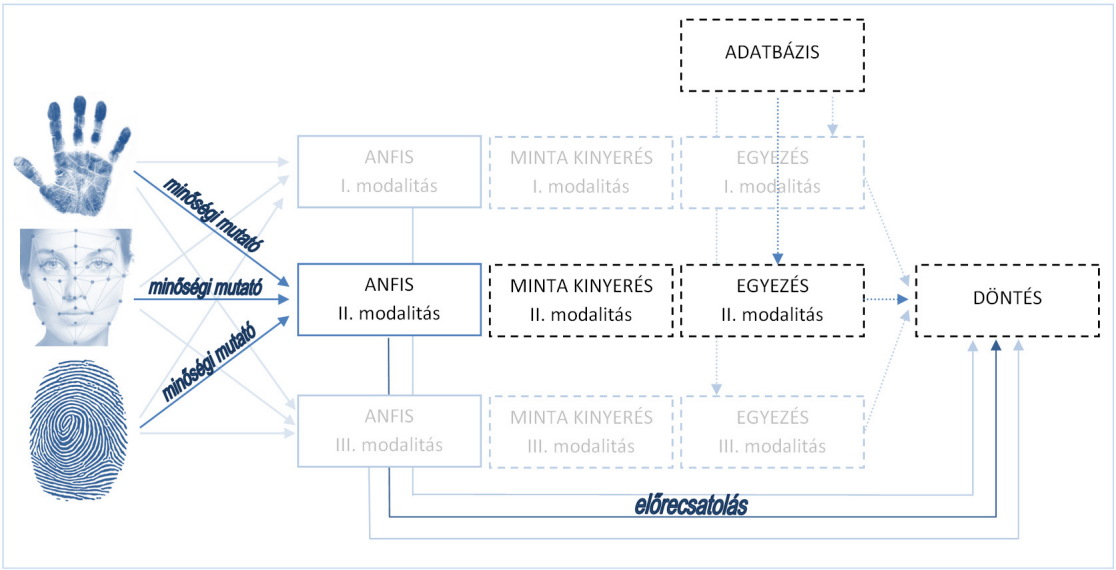
Az általam készített algoritmusban három különböző bemenetet definiáltam, így akár három biometrikus eszközből származó információ együttes elemzése is megvalósítható. A rendszer kialakítása végett működőképes – további átalakítás nélkül – két biometrikus minta alkalmazásával is, azaz bimodális módban. Illetve belátható, hogy korlátosan, de bővíthető a módok száma, azonban ennek határát és korrelációját jelen értekezés kapcsán nem vizsgáltam, de meg kell jegyezni, hogy a három bemeneti változó nem feltétlenül jelenti, hogy három különböző biometrikus módszert kell alkalmazni, hiszen a multimodalitást alkalmazó technikák megengedik, hogy akár egyetlen biometrikus forrást akár sorozatban vizsgáljunk, és az így kapott eredményeket, mint különálló, de mégis e tekintetben összetartozó mintaként kezeljünk [63].

Wang és Elhang tanulmánya alapján a fuzzy halmazok granulációját alacsonyra állítottam be, így tulajdonképpen minden fuzzy halmazhoz összesen két tagsági függvényt definiáltam. Belátható, de bizonyítását jelen értekezésben nem taglalom, hogy a tagsági függvények számának növelése bizonyos szinten túl nem segíti elő sem a gyorsabb sem a pontosabb tanulást [64] [65]. Az így kapott 18 változó adja tehát a premissza paraméterek halmazát, amelyet '`premise`' mátrixként definiáltam.

A Sugeno típusú következtetés értelmében a következtető paraméterek halmazát a '`consequent`' mátrixot a p_{ijk}, q_{ijk}, r_{ijk}, és s_{ijk} paraméterek – összesen 32 db – adják. A tanulás során tulajdonképpen e két mátrix változóit kell optimalizálni, aminek több jó megközelítése is létezik. A tanítás kulcsfontosságú lépés, ahogy azt az ANN hangolása fejezetben ismertettem.

Ez esetben is, több megoldás vizsgálata után a rugalmas hiba-visszaterjesztés (resilient error back-propagation) mutatkozott a leghatékonyabb iterációs módszernek. Az eljárás a korábbiakkal egyezően (26) és (27) egyenletek szerinti szabály alapján, a gradiens változásának előjelétől és az η^- és η^+ faktoroktól függ. A korábbi tézisponttal ellentétben ebben a vizsgálatban a mesterséges neurális hálózatot nem közvetlenül mintázat felismerési feladatra használtam, hanem egy minőségellenőrzéssel optimalizált döntési folyamati előszűrőjeként. Efféle szűrőként a beérkező előminősített azonosítási információk alapján – amelyeken az azonosítás maga még nem történ meg, csak az

azonosíthatóság foka került vizsgálatra – súlyozni képes a későbbi eredmények relevanciáját a döntési folyamatban, sőt a hatékonyság növelése érdekében, akár ki is hagyhat egy-egy azonosítási eljárást, amennyiben annak előminősített értéke a többi értékhez képest elhanyagolhatóan alacsonynak mutatkozik. Ebben a formában tulajdonképpen egy MANFIS mint előszűrő elem épült be az előminősítés és az azonosítás közé, a felvázolt program szerkezetét illusztrálja az alábbi 40. ábra.



40. ábra: Multimodális azonosító program szerkezete MANFIS szűrővel

Az előszűrés során valamilyen előzetes minősítési értéket kell felhasználni, így szükséges feltétel a program indulásához, hogy rendelkezzünk egy olyan index számmal, ami valamilyen módon a kinyerhető azonosítójegyek azonosításra alkalmas mivoltát értékeli. Sok biometrikus azonosítási módszer során valamilyen vektort vagy vektorrá konvertálható minutiae térképet generál az algoritmus, amelyek méret alapján már jó minőségi jellemzést is adhatnak, hiszen, minél több egyedi azonosító jegyet sikerült felismerni annál hatékonyabb az azonosítás. Természetesen vannak megoldások amelyekbe korlátozó szűrőket szerelnek, így még azok előtt kell kinyerni ezt az információt. Az alábbi táblázat többféle biometrikus azonosítási módszer minőségi elemzéséhez használható technikáit hasonlítja össze.

3. táblázat: Biometrikus azonosítási módszerek összehasonlítása a kinyert tulajdonságok szerint

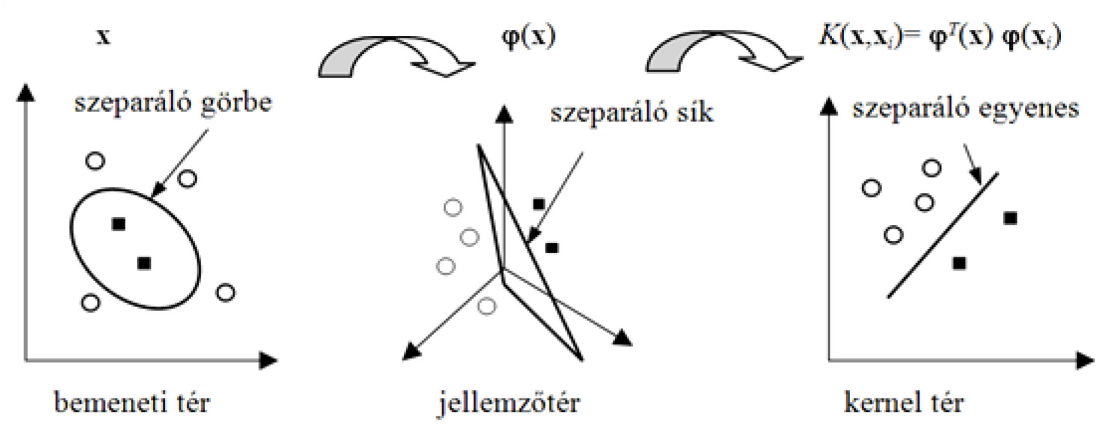
Azonosítási technika megnevezése	Biometrikus módszer	Tulajdonság kinyerés	Átalakítás	Kinyert tulajdonságok reprezentációja
Biohashing PalmHash	Arc, tenyér-, ujjnyomat	Vektor (Fisher Discriminant Features)	Véletlen mátrix szorzat	Vektor
BioPhasor	Ujjnyomat	Vektor (FingerCode)	Nem-lineáris	Vektor
Cancelable Face	Arc	Vektor (FaceImage)	Véletlen mátrix keverés	Vektor
Robust Hash	Arc	Vektor (Face Image Matrix)	Lágy multimodális elemzés	Vektor
Class Distribution Preserving Transformation	Arc	Vektor (Fisherface tulajonságok)	Halmaz pontok tulajdonságvektorai -nak elemzése	Vektor
Cancelable Iris	Írisz	Vektor (Log-Gabor válasz)	Körkörös eltolás és kombináció, új mintát adva	Vektor
Histogram of minutiae triangle	Ujjnyomat	Vizsgálati pont	Minutiae háromszögek hisztogramjának elemzsése	Vektor
Symmetric Hash	Ujjnyomat	Vizsgálati pont (Minutiae mint komplex szám)	Invariáns minutiae függvények halmaza	Minutiae térkép
Cancelable Finger Prints	Ujjnyomat	Vizsgálati pont (Minutiae térkép)	Image folding	Minutiae térkép
Alignment free cancelable fingerprint	Ujjnyomat	Vizsgálati pont (minutiae térkép, iránymezők)	Minutiae átalakítás környező iránymező szerint	Minutiae térkép
Cuboid based Minutiae Aggregates	Ujjnyomat	Vizsgálati pont (Minutiae térkép)	Aggregált minutiae tulajdonságok választása véletlen területből	Vektor

Kryszcuk és Drygajlo kutatásához kapcsolódva elmondható, hogy több lehetőség is kínálkozik olyan mutató számok kinyerésére, amelyek alkalmasak az azonosítás jóságát minőségileg érzékeltetni. A szokásos biometrikus osztályozás során a minőséget két egymást kiegészítő módszerrel szokás vizsgálni, az egyik az alapvonali értékek a másik pedig a minőségmérés.

Az alapvonali értékek az osztály-szelektív nyers biometrikus mintákból osztályozó operátorokkal nyerhető ki, ezzel szemben a minőségi mérés során a minták kinyerése során fellépő zajok hatását kell vizsgálni, ami osztálytól független mérést tesz lehetővé. A vizsgálat első részét mondhatjuk kvázi kvalitatív módszernek, amelynek során a kinyert információ mennyiségi elégségét vizsgáljuk, míg a második lépés inkább kvantitatív, hiszen a jel/zaj viszony lesz a meghatározó [66].

Több módszer ismeretes a minőségi mutatók szerinti osztályozására, megemlítendő a hozzáadott zaj alapú modell (Additive Noise Model - ANM), vagy a multiplikatív zaj model (Multiplicative Noise Model - MNM), amelyek a következő módszereket használják osztályozásra; lineáris diszkrimináns elemzés (Linear Discriminant Analysis - LDA) vagy a kvadratikus diszkrimináns alapú elemzés (Quadratic Discriminant Analysis - QDA). Ezeken felül használatosak a Bayes osztályozó módszerek is, amik egy kevert gauss modelt (Gaussian Mixture Model) alkalmazva, eloszlási reprezentáció alapján különböztetik meg az értékeket, ilyen például a radiális bázisfüggvényekkel optimalizált tartóvektor gépek módszere (Support Vector Machines - SVM) [67].

A Support Vector Machine (SVM) tulajdonképpen egy speciális neurális hálózat, azonban szokás a statisztikus tanulási elméleti módszerek közé sorolni. Az elméleti besorolás kérdésétől függetlenül az SVM az utóbbi idők egyik fontos gyakorlati eszköze lett az osztályozási feladatok körében. és egyben mély elméleti kutatások tárgyává vált. A fentiekben bemutattam, hogy egy MLP-vel is jól közelíthetőek ismeretlen, nem lineáris függvények, de a tartóvektor gépek esetében az optimális megoldást nem elég megközelíteni, hanem egzakt módon meg is kell tudni határozni. Amennyiben olyan problémára kell alkalmazni az SVM módszert, ahol az osztályozandó elemek dimenziótere kiterjedt, akkor a komplexitásból fakadó nehézségék miatt előnyös lehet kernel reprezentáció alkalmazása (41. ábra), például egy véges tartójú radiális bázisfüggvénnyel [68].



41. ábra: SVM módszer illusztrációja kernel reprezentáció alkalmazásával [68]

3.2.4 Az alkalmazott MANFIS eredményeinek ismertetése

Jelen esetben nem egy pusztán neurális rendszerrel, hanem a már ismertetett neuro-fuzzy hibriddel, a MANFIS algoritmussal végeztem el a minőségi mutatók közti osztályozási feladatot, mert ennek alkalmazása az adott környezetben előnyösebb. Három különböző bemeneti halmaz lett definiálva, amelyek a három biometrikus modalitást reprezentálják. Tulajdonképpen mindegyik modalitáshoz egy ANFIS-t rendeltem, amiben az adott modalitás többihez viszonyított teljesítményét hasonlítottam össze. Ezen ANFIS-ok bemenetére tehát az egyes előfeldolgozások minőségi mutatóinak értéke kerül, míg a kimeneti érték meghatározza, a további feldolgozási lépéseket. Beállítási értékektől függően változik a kinyert egyedi azonosító jegyek feldolgozásának folyamata, így elképzelhető olyan eset, amelynek során akár nincs is szükség további feldolgozásra az adott modalitás tekintetében, mert az ANFIS eredménye szerint annak relevanciája a teljes azonosításra vetítve elhanyagolható.

A MATLAB környezetben készített algoritmus a teljes azonosítási folyamatból az ANFIS-ra fókuszált, így az eredmények között az ANFIS mint osztályozó szűrő tanulási képességét ismertetem. A rugalmas hiba visszaterjesztéshez használt η^- és η^+ faktorokat 0,5 és 1,2 értékre állítottam, az adatok pedig három különböző ujjnyomat azonosító eszköz feldolgozási adataiból származnak (BioEntry+, iEVO, Bioscrypt).

Az Alkalmazott Biometria Intézetben számos módszerrel és mérőszámmal jellemezzük az egyes biometrikus azonosító eszközöket. Az egyik jellemző az azonosítási idő, ami mint származtatott minőségi mutató is alkalmazható, hiszen minél rövidebb ideig tart az

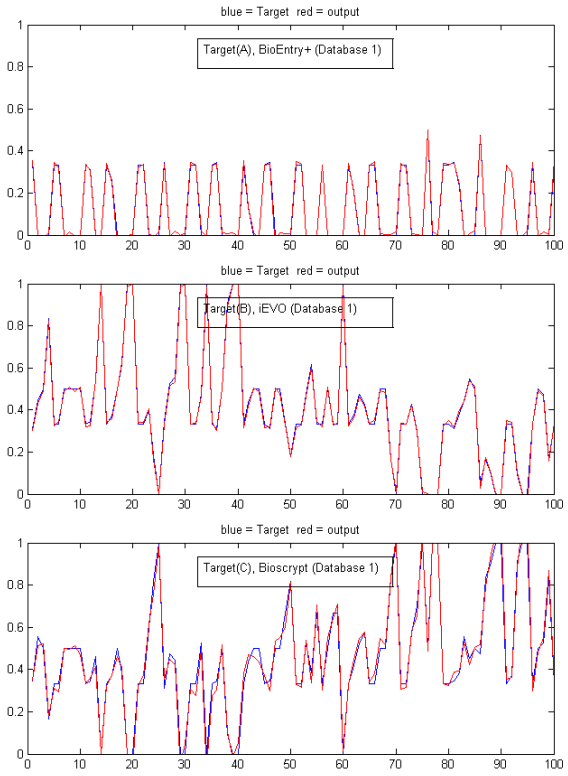
egyedi azonosító jegyek kiolvasása annál könnyebben zajlik az azonosítás a vizsgált eszközök esetében. Az azonosítási idő maximumát (kellően sok tartalékkal) 15 másodpercnek állítottam be, míg az egyes modalitásokhoz tartozó ANFIS-ok célfüggvényeit az alábbi összefüggések írják le (37/a-b-c).

$$target_A = \frac{1-FRR_A}{(1-FRR_A)+(1-FRR_B)+(1-FRR_C)} \quad (37/a)$$

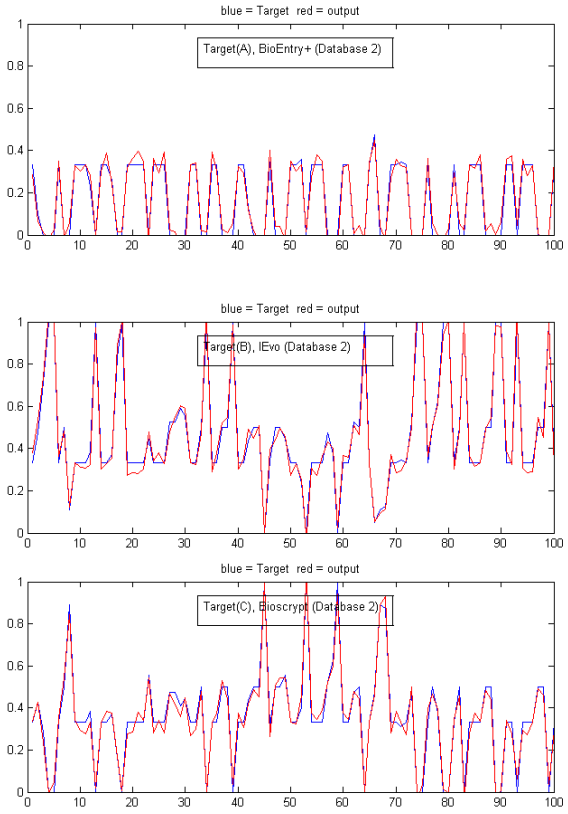
$$target_B = \frac{1-FRR_B}{(1-FRR_A)+(1-FRR_B)+(1-FRR_C)} \quad (37/b)$$

$$target_C = \frac{1-FRR_C}{(1-FRR_A)+(1-FRR_B)+(1-FRR_C)} \quad (37/c)$$

Az egyes modalitások fajlagos "jóságát" az 1-FRR értékek relatív mutatója adja, minden idő és FRR adatpár egy tízes próbasorozat eredményét tükrözi, ennek következtében igen diszkrét értékeket kapunk, a vizualizált ábrák pedig csúcsosak. Az adatbázis ujjnyomat olvasónként 200 adatpárt tartalmaz azaz, 2000 próbát minden modalitás esetében. Az adatbázist ketté választva végeztem el a "tanítás és a tesztelést" 100-100 adatpáron, (3000 eredeti adattal). Az alábbi ábrákon (42. ábra, 43. ábra) látható, hogy a megfelelő tanítás során elért beállításokkal a tesztek eredményei magas fokú egyezést mutatnak, az elvárt és a valós kimeneti értékek szinte egybevágóak.



42. ábra: Elvárt és valós kimeneti értékek az egyes modalitás esetében (1. adatbázis)



43. ábra: Elvárt és valós kimeneti értékek az egyes modalitás esetében (2. adatbázis)

3.3 Komplex, MI alapú biometrikus azonosító rendszer modellje

3.3.1 A természetes és mesterséges intelligencia szerepe az azonosításban

Az előzőkben olyan példákat mutattam be, ahol a mesterséges intelligenciák csoportjába sorolt lágy számítási módszerekkel javult a biometrikus azonosítás hatékonysága. Az egyes lágy számítási módszerek önmagukban kétség kívül alkalmasak lehetnek az azonosítási folyamat egy-egy lépésében jól szerepelni. Láttuk, hogy a GA segít megtalálni az optimális beállításokat egy túldimenzionált vizsgálati térben, az ANN jól alkalmazható mintázat felismerési problémákra, míg egy FLC jól szerepel a döntési helyzetekben. A kérdés azonban az, hogy létezik-e olyan alapvetően mesterséges intelligencia alapú vezérlés, ami alkalmas a biometrikus azonosítás teljes rendszerét irányítani.

A technikai lehetőségek ismertetése előtt, röviden érdemes áttekinteni a természetes intelligencia biometrikus azonosítási rendszerét, ugyanis ennek megértése nagymértékben segíthet a megfelelő mesterséges változat modelljének megalkotásában. Az emberi érzékelésből elsősorban a látás az, amelyik a személyazonosítási feladatokért felelős, ami természetesen annak is köszönhető, hogy az emberi agy számára a legtöbb feldolgozandó információ a szemen keresztül érkezik, de meg kell említeni, hogy a hallásunk és szaglásunk is szerepet kaphat a személyek azonosításában [69].

Az azonosítás folyamata összetett neurobiológiai kölcsönhatások lépésének sorozata, amelynek részletes bemutatása jelen értekezésnek nem képezi tárgyát. Érdemes azonban ismertetni Sekuler és Blake által vázolt rendszert, amiben élesen elválasztják a közeli és távoli érzékelés formáit, miszerint a közeli érzékelés formái az ízlelés, tapintás és a szaglás is – hiszen ez az orr nyálkahártyájában zajló biokémiai reakciókon alapuló folyamat –, míg a távoli érzékeléshez sorolható a látás és a hallás, mert azok valamilyen közvetítő közegen keresztül érkeznek az érzékszerveinkhez. A szerzők által nem említett érzékelési módok közül érdemes lehet külön kiemelni a hőérzékelést, – amelyet korunk tudományos vélekedése alapján el kell választani a tapintástól –, mert mind közeli, mind távoli érzékelést lehetővé tesz, és létezik mesterséges változata is a hőarctérkép alapú azonosítási technika esetében [69].

A mesterséges azonosítás szemszögéből az információ kizárólag valamilyen közvetítő közegen keresztül jut a feldolgozásért felelős központba, de a azonosítandó személyére irányuló attitűd vizsgálatok azt mutatják, hogy a mesterséges azonosításban is lényeges szerepe van a térnek. A biometrikus eszközöket használó személyek sokkal együttműködőbbek olyan biometrikus azonosító eszközökkel, amelyek távoli érzékelés módján működnek. A pontos távolságok nagymértékben függnek a pszicho-szociális és kulturális adottságoktól, de általánosan elmondható, hogy a mesterséges azonosítás gyakorlati megvalósítása során két jelentős szempontból is előnyt élvezhetnek a távolibb érzékeléssel operáló megoldások. Egyfelől lényegesen nagyobb tér fedhető le távolabb helyezett mérőeszközzel (pl. nagyfelbontású kamera, puska-mikrofon), másfelől nagyobb együttműködésre és elfogadásra lehet számítani, mint a közeli érzékelési technikáknál. Ezzel együtt figyelembe kell venni, hogy a közvetett tér miatt zajterhelés szignifikánsan nagyobb lesz [70], [71] .

Az észlelés mögöttes pszichofizikai modelljének igen leegyszerűsített, de a valósághoz közel álló modelljét vázolja Sekuler és Blake, akik egy kvázi körfolyamatban írják le az észlelés és felismerés folyamatát. Az észlelés egy kvázi reflex szerű folyamat, amelynek során a környezet felől érkező ingerek az érzékszerveken generált elektromos jellé, ingerületté vállnak, és bizonyos torzítás és jelvesztés után az adott érzékszerv számára kijelölt agyi feldolgozó központba jutnak. Az észlelés során az agyunk figyelmet fordít néhány kiemelt eseményre abból a több ezer különböző jelből, ami másodpercenként éri, nevezzük ezeket a komplex primer kép részeinek. A komplex primer kép nyilvánvalóan nem csak vizuális inger során alakul ki, és ugyan a zajból kiemelkedik, a teljes asszociációhoz általában elégtelen. A figyelem kulcsfontosságú jelenség a felismerésben. A figyelem kialakulásának van azonban néhány fontos feltétele, úgymint, a megfigyelendő esemény jelszintje szelektíven elválasztható kell legyen a környezeti zajtól, másfelől a feldolgozásért felelős agyi központ legyen megfelelő állapotban, valamint a megfigyelendő jel váltson ki valamilyen asszociációt, tehát legyen ismerős számunkra [69].

A figyelem kiváltása során megkezdődik valamilyen kategorizációs, illetve asszociációs tevékenység, de a legtöbb esetben itt még nem áll rendelkezésre elegendő információ ahhoz, hogy pontos képet kapjunk az eseményről. Ennek következtében a figyelem egy

koncentrált megfigyelésre irányítja érzékszerveinket, jellemzően úgy, hogy ezzel párhuzamosan igyekszik csökkenteni a többi érzékszerv felől érkező felesleges zajt, elindítva ezzel egy automatikus visszacsatolást. A koncentrált figyelem során többnyire egy részletekben gazdagabb ingerület sorozat kerül továbbításra az agyi feldolgozó központok felé. Az esetek nagy részében ez elegendő információval szolgál valamilyen másodlagos asszociációhoz, vagy a felismeréshez, amit nevezzünk szelektív szekunder képnek [69].

Habár eddig az észlelés humánbiológiai és pszichológiai hátteréről esett szó, annak ismerete nem elhanyagolható a mesterséges modell megalkotásához. A mesterséges modell alapvetően három fő részre tagolandó. Egyfelől az emberi érzékszervekhez hasonlóan szükség van olyan detektorokra, amik egyúttal képesek a komplex primer és szelektív szekunder képek érzékelésére. Másfelől a detektált ismeretet valamilyen módon kódolni kell, és ezt a kódot el kell juttatni a központi feldolgozóegységhez, harmadrészről olyan központi feldolgozó egységre van szükség, amely az emberi észleléshez és gondolkodáshoz hasonlatosan működik. A biológia neurális rendszerünk működését segíti megérteni Bechtel és Abrahamsen tanulmánya a neurális hálózatok működéséről. A szerzők az agyi neurális rendszert mint idegsejtek és az idegsejteket összekötő, strukturált hálózatot tekintik, ahol a kognitív tudás a hálózat szerkezetében rejlik [72].

A mesterséges felismerés modelljében a mesterséges intelligencia eszközeit kell alkalmaznunk, amelyeket tulajdonképpen a lágy számítási módszerek egzakt matematikai megoldásira épülnek. Ahogy Amit Konar könyvében kifejti, a lágy számítási módszerek közé tartozó fuzzy logika (FL), mesterséges neurális hálók (ANN) és a genetikus algoritmusok (GA) jól alkalmazhatók a emberi észlelés, felismerés és a kognitív gondolkodás egyes folyamatainak modellezésére [73].

3.3.2 Kombinált lágy számítási módszerek a multimodális azonosításban

A két alaprendszer az FLC és ANN kombinálásának alapjai a közös vonások és, hogy mindkettő képes ugyanazt a problémát megközelíteni de eltérő módon. Mindkét megoldás képes javítani a zajos környezet káros hatásait, és tetszőleges pontossággal közelíteni nemlineáris problémákat. Számos lehetőség nyílik a kombinálásukra, de a leggyakoribb a fentebb is bemutatott neurális ruhába öltöztetett fuzzy következtető

rendszer, azaz a neuralizált fuzzy logika. Előnyös tulajdonsága, hogy megtartja a fuzzy következtetés jellegét, de tanulási képességgel vértezi fel, így működése adaptívabb lehet. Egy neuralizált fuzzy rendszer képes megtanulni a modellezett rendszer működését, azt reprezentáló numerikus példákból, illetve alkalmas a tudás szintézisre lingvisztikai változók szabályaira építve [28].

Szintén láttuk, hogy a genetikus algoritmusok képesek olyan összetett optimumkeresési feladatok megoldására is, mint amire a klasszikus operációkutatás már nem tud választ adni. Jól paraméterezett alapbeállításokkal szinte bármilyen optimalizálási feladat megoldható, vagy található olyan megoldás, ami már kellően kielégítheti a kezdeti feltételeket. A GA és az ANN keresztezése hasznos és szükségszerű is, amennyiben szeretnénk megőrizni az ANN univerzális approximátor jellegét, hiszen láthattuk, hogy egy adott struktúrájú ANN nehezen birkózik a jelentős rendszerszintű változásokkal. Példaként megemlíthető, hogy az egy-az-egyhez típusú és az egy-a-sokhoz típusú azonosítási eljárásokhoz igen más karakterisztikájú ANN-re van szükség, de a módosítások manuális állításával ez belátható időn belül nem lehetséges.

Az alábbi táblázatok összefoglalják a Retter Gyula által vizsgált lágy számítási módszerek alaptulajdonságait:

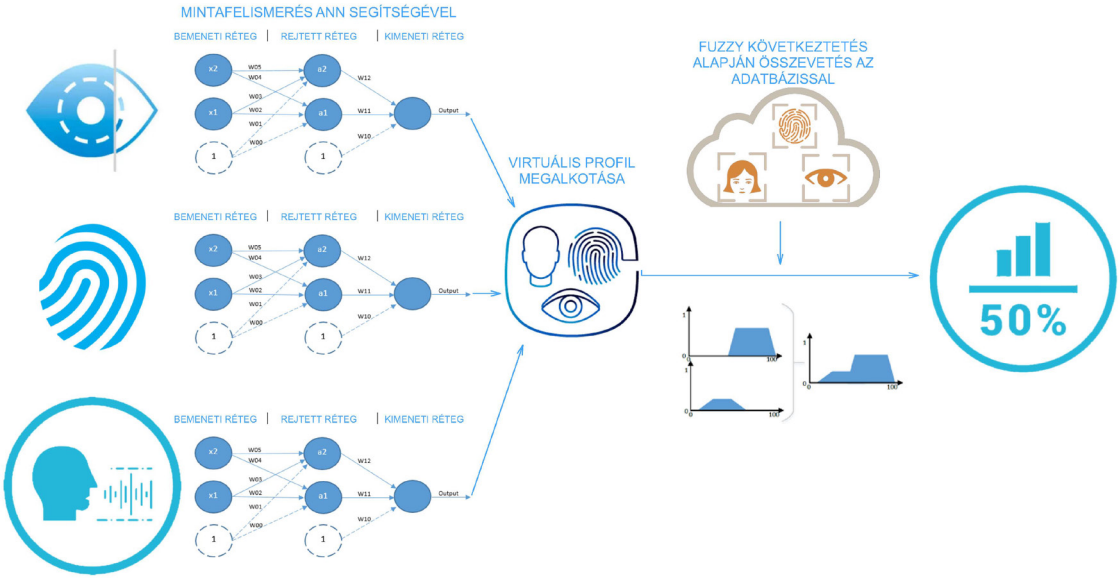
4. táblázat: A lágy számítási módszerek közös tulajdonságainak összehasonlítása [28]

KÖZÖS TULAJDONSÁGOK	FUZZY	NEURÁLIS	GENETIKUS
Inferencia	közelítő	közelítő	Közelítő
Általánosítás	jó	nagyon jó	jó
Hiba toleranica	jó	nagyon jó	gyenge
Bizonytalansági tolerancia	jó	jó	jó
Valós idejű működés	jó	nagyon jó	gyenge
Nonlinearitás	jó	jó	jó

5. táblázat: A lágy számítási módszerek kiegészítő tulajdonságainak összehasonlítása [28]

KIEGÉSZÍTŐ TULAJDONSÁGOK	FUZZY	NEURÁLIS	GENETIKUS
Tudás reprezentálás	jó	rossz	nagyon gyenge
Tanulási képesség	nincs	nagyon jó	gyenge
Értelmezhetőség	nagyon jó	nincs	gyenge
Szakértői tudás	nagyon jó	nincs	nincs
Numerikus adat	gyenge	nagyon jó	jó
Matematikai modell	nagyon jó	gyenge	gyenge
Optimalizálási képesség	gyenge	nagyon jó	jó

A lágy számítási módszerek kombinációja természetesen úgy is lehetséges, ha azokat nem hibrid formában, hanem egymás mellett, a teljes azonosításban integrált formában alkalmazzuk. Ilyen megoldás például. ha egy ANN mintafelismerését egy FLC vezérlő értékeli ki. Sánchez és Melin cikkükben egy ilyen írisz, fülgeometria és hangazonosító rendszert alkottak meg moduláris neurális hálók és fuzzy integrátor segítségével (44. ábra). Szintén felismerve, hogy az ANN egyes paraméterei állításával az azonosítás hatékonysága javítható, néhány paraméter (neuron száma a rejtett rétegekben, tanító algoritmus típusa, elérhető hiba) optimalizálását genetikus algoritmus segítségével végezték el. Megoldásukban tehát ötvözték az egymásba oltott és az egymás mellett működő lágy számításokat [74]:

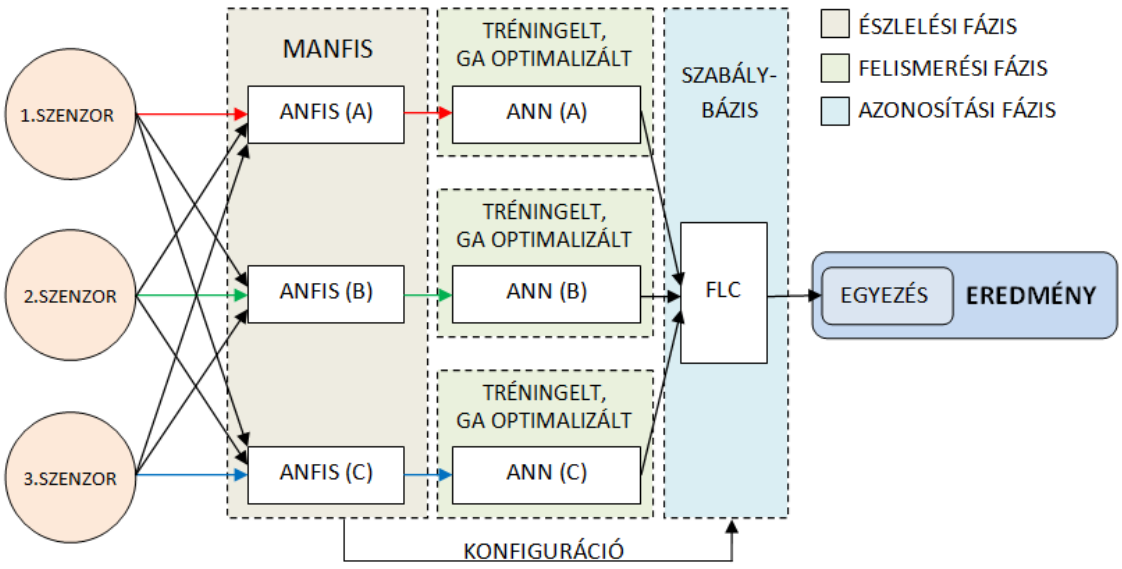


44. ábra: Multimodális azonosítás ANN és fuzzy integrátor kombinációjával

Továbbgondolva a modellt, olyan komplex vezérlő megalkotásába kezdtem bele, ami hasonlóan jól kezeli a multimodális biometria működési feltételeit, de alkalmas az alfejezet első részében említett asszociációs folyamatot is integrálni, így aszerint élesíteni az egyes megfigyeléseket, hogy az előminősítések értékei hogyan alakulnak.

3.3.3 Komplex MI alapú vezérlő működésének ismertetése

A humán percepció mesterséges megvalósítása során törekvéseim arra irányultak, hogy annak hármas tagoltságát és logikáját a legkevesebb változtatás nélkül tudjam átültetni a gyakorlatba. Így az észlelés, a felismerés és az azonosítás fázisai az alábbiak szerint modellezhetők:



45. ábra: Az emberi észlelés mesterséges modellje lágy számítási módszerek alkalmazásával

Az ábrán különböző sorszámmal jelölt szenzorok nem feltétlenül jelentik azt, hogy ezek eltérően működő mesterséges érzékszervek, azonban fontos különbség, hogy a beolvasott információk valamilyen tulajdonságukban különbözőek. A gyakorlati megvalósítás szempontjából elképzelhető három ugyanolyan kamera, ami három különböző irányból figyeli az azonosítandó személyt, de elképzelhető más multi-modális azonosítási megoldás is, amelynek során három különböző biometrikus mintát beolvasva kezdődik meg az identifikációs eljárás [75].

A fuzzy logikán alapuló következtető egység beállításainak meghatározási nehézségei miatt érdemes segítségül hívni a mesterséges neurális hálók és a fuzzy logika előnyeit együttesen reprezentáló megoldást, az Adaptív Hálózat Alapú Fuzzy Következtető Rendszert, pontosabban ennek többszörös kimenetet is kezelni képes megoldását a multi ANFIS-t, vagy MANFIS-t. E modulnak az legfőbb feladata, hogy adaptív módon, tehát a tanítási fázisban érkező információk alapján a fuzzy következtetés néhány beállítását a tapasztalat szerint igazítsa. Így a tagsági függvények alakját meghatározó premissza paramétereket és az ANFIS-ban használt Sugeno típusú implikáció paramétereket [37].

Az ANFIS modul szerepe, hogy a különböző szenzorok felől érkező minták azonosíthatóságát összevesse, úgy, hogy a rendszer képes megtanulni, hogy a melyik érzékszervére támaszkodjon. A tanítást – ahogy ezt korábban a mesterséges hálók tanításánál bemutattam – konjugált gradienssel iterált hiba vissza-terjesztéses (error

back-propagation) módszerrel érdemes végrehajtani. A minták felismerése egy későbbi lépésben történik meg, de előzetesen el kell dönteni, hogy melyik "érzékszervre" milyen mértékben hagyatkozzon a rendszer. Tulajdonképpen a modell intelligenciája ebben a szakaszban bontakozik ki, hiszen a modul adaptív módon dönt a szenzorok felől érkezők jelek feldolgozásáról a beérkező jelek minőségi értékelése alapján [75].

Jelen formában három szenzort nevesítettünk és ennek megfelelően három kimenettel kell számolni, azaz három párhuzamos ANFIS modult építettünk be. Mindegyik ANFIS modul megvizsgálja, hogy a beérkező mesterséges ingerek együttes értékelése alapján érdemes-e az adott kimenetet továbbvinni. Tehát minden ANFIS modul kimenete egy-egy szenzorból érkező jel továbbvitelét indukálhatja, sőt az összevetés eredménye később hatással van a végső összegző fuzzy következtetés szabálybázisára is, így egy többszörösen előrecsatolt rendszer jött létre [75].

Az ANFIS modul szerepe kimondottan a bonyolultabb minta-felismerési problémákban hatékony, amikor a mesterséges neurális háló (ANN) alkalmazása nem feltétlenül vezet pontos megoldáshoz, vagy az azonosítási idejét nagyon meghosszabbítja. Az ANFIS modul alkalmazásával biztosítható, hogy azok a mesterséges ingerületek, amelyek a többinél szignifikánsan jobban értelmezhetőek (pl. több egyedi azonosító jegy ismerhető fel rajtuk), kitüntetett szerepet kapnak a mintafelismerésben. Szélsőséges esetben akár mellőzhető a többi szenzorból származó információ további feldolgozása. Ennek éppen ellenkezője az az eset, ha a konvencionális azonosításhoz képest sokkal rosszabb az összes minta felismerhetősége, de az együttes vizsgálat és a párhuzamos mintafelismerések csökkenteni képesek a bizonytalanságot.

Fontos megjegyezni, hogy a mintafelismerésre alkalmazott ANN-eket szintén tréningezni kell. Ennek során egy genetikus algoritmuson alapuló javító automatikával meghatározható az ANN néhány kritikus beállítása, például a rétegekbe sorolt neuronok kezdeti súlymátrixa, amelynek optimalizálása azért fontos, mert az ANN tanulása érzékenyen függ a kezdeti súlymátrix értékeitől.

Az egyes ANN modulok eredményeit az utolsó blokkban működő fuzzy logikai vezérlő veti össze az előzetesen definiált szabálybázis alapján. A szabálybázis előzetes, de automatikus konfigurációja tulajdonképpen azt határozza meg, hogy az adott

körülmények között melyik mesterséges érzékszervre érdemes támaszkodni. A konfiguráció eredménye alapján előfordulhat, hogy minden érzékszervet azonos mértében kell figyelembe venni, de előfordulhat egy-egy modalitás teljes kizárása is. Az emberi percepcióban nem ismerjük a végső döntések és a érzékszervi ingerek feldolgozásának eredménye közti relációt, de vélhetően a fuzzy implikációk jobban közelítik ezt, mint bármely más lineáris, algebrai modell.

A végső eredmény tekintetében az adott problémára adandó válasz szerint számos kimeneti értéket tudunk megjelentetni. Megadható, hogy az adott személyt a rendszerünk felismerte vagy sem, megadható, hogy kikhez hasonlít a legjobban, de akár azt is fel tudjuk tüntetni, hogy hány százalékos az egyezés a korábban eltárolt felhasználókhoz képest.

3.4 Harmadik főfejezet összefoglalása

Az értekezés harmadik főfejezete részletesen foglalkozik a lágy számítási módszerek kombinálásával, és azok alkalmazási lehetőségeivel a biometrikus azonosításban. Egzakt példákon került bemutatásra a Fuzzy Logika, a Mesterséges Neurális Hálók és a Genetikus Algoritmusok esetleges kombinációinak előnye.

Az első ismertetett kombinációban azt vizsgáltam meg, hogy a Mesterséges Neurális Hálók számos változtatható beállítási paraméterének optimalizálása hogyan automatizálható Genetikus Algoritmus segítségével, így elősegítve a szükséges számítási kapacitás igénybevételének minimalizálását. A második ismertetett eljárásban egy neuralizált fuzzy rendszer használatának előnyeit vizsgáltam multimodális biometrikus döntési szituációkban, ahol akár az előértékelés alkalmazásával gyorsítható az eljárás. Végezetül, összesítve az alkalmazott modelleket, olyan komplex, multimodális vezérlő és értékelő algoritmust ismertetettem, ami az emberi asszociatív tanuláshoz hasonlóan képes fejlődni.

KUTATÁSI EREDMÉNYEK ÖSSZEFOGLALÁSA

A doktori iskolában eltöltött évek alatt megismerkedtem az alkalmazott matematika és a programozás adta lehetőségekkel, amik jelentős mértékben segítettek hozzá a biometrikus azonosításban általam tárgyalt problémák, és az ezekhez fűzött megoldási javaslatok vizsgálatához. A cél, a részcélok és az egyes hipotézisek tekintetében széles körben tájékozódtam a kapcsolódó, releváns és újszerű kutatások eredményeiről. E nemzetközi kutatói közösség tagjaként pedig jómagam is rendre publikáltam a vizsgálataim eredményét. A béta-binomiális eloszlással történő előminősítés és a mesterséges neurális hálók hangolása több nemzetközi tudományos mű forrásává vált, így igazolva ezen munkák értékét.

A disszertációmban a kutatásaim olyan területeinek bemutatására szorítkoztam, amelyeket különösen fontosnak tartok a biometria tudományos hátterének építésében, emellett kézzel fogható eredménnyel, vagyis valós tudományos újdonsággal bírnak.

Az értekezésem elején négy hipotézist fogalmaztam meg, amelyet a gyakorlatban hat kutatási feladattal igazoltam, összevonva a kombinált lágy számítási módszerek együttes alkalmazását. Az értekezésben e hat egység önállóan kerül bemutatásra, de végigkövethető az a lineáris logikai kapcsolat ami a modulokból végezetül elvezet egy komplex vezérlő algoritmusig.

A kutató munkám elején, a biometrikus azonosítás matematikai modellezése során arra következtetése jutottam, hogy az azonosítási folyamat során a hibák hatása multiplikatív, és e tulajdonságánál fogva alkalmazható Bayes függő valószínűségi tétele. A biometrikus azonosító eszközök működési eredményeit összefoglaló statisztikák kvantitatív vizsgálata során olyan modellt készítettem, ami kezelni képes a környezeti hatások okozta elemi hibák változó bekövetkezési valószínűségét. Az erre felírható algoritmus alapját a béta-binomiális eloszlás adja, aminek alkalmazásához meg kell ismerni a béta paramétereket. Tulajdonképpen ez a gyakorlatban úgy képzelhető el, mint egy próbaüzemű használat, aminek során kiderül, hogy a kérdéses műszaki megoldás mennyire alkalmas az adott környezetben és felhasználói körben.

A kockázat alapú modell felállítása után arra jutottam, hogy a fajlagos hibák minimalizálásnak legjobb módszere, ha diverzifikáljuk a hibák forrását. Így a

figyelmemet a multimodális azonosítási módszerek irányába tereltem. Azonban ezen technikák eredményeinek kiértékelése a biometrikus azonosítás területén nem egyszerű középérték számításokkal a leghatékonyabb, mert éppen a változó emberi tényező jelentős befolyásoló hatással bír. Ennek következtében alkalmaztam a Lotfi Zadeh nevéhez fűződő zavart halmazok logikáját, azaz a fuzzy logikát. Ennek egyik legfontosabb előnye, hogy úgynevezett lingvisztikai változók mentén adhatjuk meg egy érték egy adott halmazhoz tartozását, illetve maga a kiértékelés sem a bináris logika éles megkülönböztetésén alapul, tehát lehetőség van a halmazok között átfedéseket definiálni, sőt, a szabályrendszerek módosításával lekövethetjük az emberi tulajdonságok változását is. Az értekezésemben egy konkrét példán, egy általam készített bimodális ujjnyomat alapú fuzzy logikai kontrolleren mutatom be a vezérlési algoritmus előnyeit.

Bár a doktori iskolai tanulmányaim elején még kevésbé volt közismert a mesterséges intelligencia biometrikus azonosításban történő alkalmazhatósága, úgy döntöttem, hogy e technikák mélyebb ismerete, megértése és használata segíthet a célom elérésében. E módszerek egyik képviselője a mesterséges neurális hálózatok, amelyek jól alkalmazhatóak minta-felismerési feladatokra. Ennek következtében készítettem el én is azt az ujjnyomat azonosító algoritmust, amivel a mesterségesen kinyert egyéni azonosító jegyek felismerésének hatékonyságát tudtam vizsgálni. Eredeti terveim szerint biometrikus azonosító eszközökből kinyert egyedi azonosító jegyeket vizsgáltam volna, viszont ez az eszközök zártsága és a gyártók bizalmatlansága miatt meghiúsult. Viszont a szakirodalom tanulmányozása során arra jutottam, hogy az egyéni azonosító jegyek kinyerésének számos módja létezik, igen széles matematikai paletta áll rendelkezésre. Így elkészítettem a saját ujjnyomat olvasó és kiértékelő algoritmusomat, ami felügyelt tanítás mellett egyre jobb felismerési arányt produkált elsősorban a téves elutasítási arány tekintetében.

A ujjnyomat olvasó és összehasonlító program azonban sok esetben megakadt és csak ismert számú bemeneti jegy esetében működött hatékonyan. Továbbgondolva a folyamatot arra jutottam, hogy optimalizálnom kell a háló topológiáját. E feladat azonban igen összetett, mert nagy számú paramétert kell szimultán, széles keresési univerzumban optimalizálni. Ekkor került képbe a mesterséges intelligenciák harmadik

altípusa a genetikus algoritmus, ami pontosan ilyen feladatok megoldására alkalmas. Egy általam készített programban beágyaztam a genetikus algoritmussal történő optimalizálást a mesterséges neurális háló felügyelt tanítási ciklusába. Ennek okán olyan algoritmus született, ami egy rövid optimalizálási ciklussal képes megváltoztatni a mesterséges neurális háló szerkezetét, hatékonyabbá téve így az erőforrások kihasználását, és jobb arányban képes elkerülni lokális szélsőértékek okozta megakadást.

Retter Gyula olvasmányosan ismerteti könyvében a lágy számítások további kombinálási lehetőségeit, amik közül új véltem, hogy a neuralizált fuzzy következtetési rendszer a biometrikus azonosítás területen komoly sikerrel alkalmazható, hiszen a felvázolt modellemben pontosan azokat az ismeretlen paraméterek definiálhatjuk fuzzy következtetéssel, amelyek biológia sajátosságainkból fakadnak. E sajátosságok változását pedig a neurális tulajdonságok kódolják, így a modell alapján készített adaptív neuro-fuzzy következtető rendszerem képes megtanulni a felhasználói sajátosságokat és ennek megfelelően súlyozni a döntést egy multimodális döntési szituációban.

Az értekezésemet egy olyan komplex modell ismertetésével zárom, ami tulajdonképpen kombinálja a korábbi modulokat. Alapul véve az emberi észlelést és a kognitív asszociációt, egy-egy modult a megfelelő biológiai folyamathoz társítottam. Így az észlelést egy multi-adaptív neuro-fuzzy következtető algoritmussal, a minta-felismerést genetikus algoritmusokkal tréningelt neurális hálózatok csoportjával, míg az azonosítást egy visszacsatolt fuzzy következtető rendszerrel modelleztem.

A kitűzött cél tekintetében elmondható, hogy a téves elutasítás és elfogadás bűvös fordított arányú kapcsolata igenis feloldható, ha a feladatra optimalizált lágy számítási módszereket vagy ezek megfelelő kombinációját alkalmazzuk.

ÚJ TUDOMÁNYOS EREDMÉNYEK

I. A béta-binomiális eloszlással számított kismintás tesztek eredményei alapján jól felmérhető egy adott biometrikus azonosító eszköz alkalmazhatósága ismert felhasználói kör és környezet esetében.

II. A bemutatott bimodális biometrikus fuzzy logika alapú vezérlés képes adaptív módon alkalmazkodni a megváltozott körülményekhez, így amennyiben változik a felismerési karakterisztika, akkor a szabálybázis változtatásával korrigálható egy esetleges torzító hatás is.

III. A vizsgált egy-az-egyhez típusú azonosítási módban az ANN megfelelő hangolása és tanítása során olyan mintafelismerő algoritmus készült, ami a biztonsági színvonal változása nélkül kevesebb téves elutasítással képes működni.

IV./A Genetikus algoritmus alkalmazásával sikerült olyan működési beállításokat találni, amelyek az ANN működését tekintve adott működési körülmények esetében optimálisnak tekinthetőek. Így a tanulás konvergenciája folyamatos és gyors.

IV./B MANFIS alkalmazása multimodális biometrikus azonosítási problémák esetében szignifikánsan javítja az egyes módok kihasználtságát és a teljes azonosítás pontosságát. Ezzel párhuzamosan az azonosítás ideje csökkenthető, így jogosultsági folyamat ellenőrzése rövidíthető.

IV./C Az emberi észlelés és felismerés folyamatát alkalmazva, lágy számítási módszerek kombinációjával lehetséges megalkotni egy olyan algoritmust, ami az emberhez hasonló motorikus és kognitív képességekkel bír.

KÖVETKEZTETÉSEK

A digitális biometrikus azonosítás gyakorlatában eddig nem született széles körűen elterjedt, és elfogadott explicit formula, amivel előre becsülhető az eszközök működése ismert környezetben és felhasználói körben. Ennek következtében a minősítés és a működési teljesítmény értékelése támogatásra szorul. Az általam ismertetett megoldás alkalmazása segítheti a beruházókat, hogy a célra alkalmas eszközöket vásároljanak, illetve azokat a megfelelő körülmények szerint alkalmazzák.

A fuzzy logika alapú vezérlés előnye, hogy a bemeneti és kimeneti érték viselkedése alapján, empirikus módon is lehetőség van a működés optimalizálására, tehát pusztán a rendszer megfigyelése is segíthet az irányítási folyamatok hangolása során. A fuzzy logikának számos előnye mellett azonban tisztában kell lennünk a hátrányaival is. Olyan folyamatokban, amelyekben a bemeneti és a kimeneti változók között pontos analitikus kapcsolat áll fenn, nem érdemes a fuzzy logikát alkalmazni. Az analitikus kapcsolatok között bizonyosan pontosabban lehet megközelíteni az optimumot vagy kvázi optimumot, mint a fuzzy logikával közelíteni a szuboptimumot. A fuzzy logika tehát olyan biometrikus vezérlési és irányítási folyamatok esetében alkalmazandó, ahol nem ismerjük az analitikus megoldást, vagy az – annak összetettségéből fakadóan – a rendelkezésre álló időn belül, vagy számítási kapacitások korlátja miatt nem kezelhető. A fuzzy logikai vezérléssel egy multimodális biometrikus azonosítási rendszer felismerési hatékonysága jelentősen javítható.

A mesterséges neurális hálózatokat a gyakorlatban elterjedten használják osztályozási problémák megoldására, de egy strukturáltabb, többrétegű perceptron bonyolultabb mintázatok felismerésére is alkalmas lehet. Ennek alapján készítettem el azt az ujjnyomat azonosító algoritmusomat, ami a kinyert információt egy ANN segítségével hasonlítja össze a tárolt adatokkal. A hálózat tanítása különösen fontos feladat, amire az úgynevezett rugalmas hiba-visszaterjesztéses iterációt kellett alkalmazni. Ki kell emelni, hogy a mesterséges neurális hálózat számos olyan beállítással rendelkezik, amivel a felismerés hatékonysága növelhető, de ezek megkeresésre analitikus módon korlátozott, így összetettebb feladat esetében optimum kereső algoritmusokat kell alkalmazni.

A genetikus algoritmusok alkalmazásával gyorsan és a lokális szélsőértékek kikerülésével sikerült elérni olyan optimálisnak tekinthető működési beállításokat, amelyekkel az ANN működése stabilizálódott. Természetesen a GA által vizsgált paraméterek lehetősége is korlátos. A teljes rendszer szempontjából kell megvizsgálni az ideális működési intervallumot, valamint azt, hogy milyen jellemzőket lehet esetleg előzetesen megkeresni, és mik azok, amiket a kérdéses adathalmaz vizsgálata során szükséges optimalizálni. A GA alkalmazásának egyik legnagyobb előnye, hogy a moduláris algoritmus beállításainak megfelelő változtatásaival egymástól igen különböző típusú biometrikus azonosítási eljárások vizsgálatára is alkalmassá válik ugyanaz az algoritmus.

Felismerve, hogy a multimodális azonosítás egy bonyolultabb architektúrát jelent, egy adaptív neuro-fuzzy megoldással afféle előszűrési fázist építettem be a biometrikus azonosítási eljárásba. Ez az előfeldolgozás nem közvetlenül mintázat felismerési feladatot végez, hanem egy minőségellenőrzéssel optimalizált döntést hoz a további feldolgozási lépések szükségességéről és a végeredmények értékeléséről. A (M)ANFIS egységből érkező előminősített azonosítási információk alapján az algoritmus súlyozni képes a későbbi eredmények relevanciáját a döntési folyamatban, sőt a hatékonyság növelése érdekében, akár ki is hagyhat egy-egy azonosítási eljárást. Az egység alkalmazása különösen hasznos lehet olyan szituációkban, ahol a multimodális megoldások szerepe – felhasználói vagy környezeti szempontok miatt – folyamatosan változik.

A megvizsgált lágy számítási módszerek mindegyike segíti a biometrikus azonosítás hatékonyságának növelését, de érdemes ezen módszereket magasabb szinten is kombinálni és megvizsgálni, hogy ezek milyen analógiát mutatnak a természetes percepció folyamatával. Ezen vizsgálatok eredményeként fontos megállapítást nyert, hogy az emberi észlelés és felismerés folyamata egészen jól modellezhető, és az egyes modell egységek feladatát – természetesen bizonyos határok között – lehetséges a vizsgált módszerekkel helyettesíteni. E modell gyakorlati alkalmazásához és teszteléséhez a terjedelmes adatbázison kívül, nagy teljesítményű számítási kapacitással bíró számítógép bevonása is szükséges az egymásba ágyazódó ciklusok folytán.

IDÉZETT FORRÁSMUNKÁK

[1] Kovács T.; Miklós G., "A Biometrikus Adatok Kezelésének Jogi Szabályozása," *Hadmérnök,* vol. XIV., no. 1., pp. 8-16, 2019..

[2] Coseraru, R., "Facial Recognition Systems and Their Data Protection Risks Under the GDPR," Master Thesis Law and Technology LL.M., 2017, pp. 41-43.

[3] 29. WORKING PARTY, *Opinion 3/2012 on developments in biometric technologies,* http://ec.europa.eu/justice/data-protection/index_en.htm, 2012.

[4] Baker, J. P.; Maurer, D. E., "Fusion of biometric data with quality esitmates via a Bayesian belief network," vol. Proceedings of the Biometric Symposium, pp. 21-22, 2005.

[5] Jain, A. K.; Hong, L., Multimodal Biometrics, Boston: Springer, 1996.

[6] Jain, A. K.; Ross, A.; Prabhakar, S., "An Introduction to Biometric Recognition," *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY,* vol. 14 No. 1, pp. 4-19, 2004.

[7] Ahmad, S. M. S.; Ali, B. M.; Adnan, W. A. W., "Technical issues and Challanges of biometric Applications as Access Control Tools of Infromation Security," *International Journal of Innovative Computing, Information and Control,* vol. 8 No.11, pp. 7983-7999, 2012.

[8] Luis-García, R.; López, C. A.; Aghzout, O. A.; Alzola, J. R., "Biometric identification systems," *Signal Processing,* vol. 83 (12), pp. 2539-2557, 2003.

[9] Kovács T.; Milák I.; Otti Cs.;, "A biztonságtudomány biometriai aspektusai," in *Pécsi Határőr Tudományos Közlemények XIII. kiadvány - Tanulmányok a Biztonság Rendészettudományi Dimenziói - Változások és Hatások Című Tudományos Konfereneciáról ISSN 1589-1674*, 2012.

[10] Srivastava, H., "A Comparison Based Study on Biometrics for Human Recognition," *IOSR Journal of Computer Engineering,* Vols. e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 15, Issue 1 (Sep. - Oct. 2013), pp. 22-29.

[11] Yager, N.; Dunstone, T., "The biometric menagerie," *IEEE Transactions on Pattern Analysis and,* vol. 32 No. 2., pp. 220-230, 2010.

[12] Poh, N.; Kittler, J., "A methodology for separating sheep from goats for controlled enrolment and multimodal fusion," *Proceeding of the Biometric Symposiumm Tampa,* pp. 17-22, 2008.

[13] Otti Cs., Classification of Biometric Access Controll Systems Based on real-time Throughout, Pozsony, Szlovákia: REVIEWED PROCEEDINGS Fifth International Scientific Videoconference of Scientists and PhD. students or candidates: Trends and Innovations in E- business, Education and Security. 129 p. ISBN 978-80-225-4191-6, 2015.

[14] Werner G., Hanka L., "Using the Beta-binomial Distribution for the Analysis of Biometric Identification," Vols. ISBN 978-1-4673-9388-1, 2015.

[15] Mansfield, A.; Wayman, J. L., "Best Practices in Testing and Reporting Performance of Biometric Devices," Vols. Biometric Testing Best Practices, Version 2.01, no. ISSN 1471-0005, 2002.

[16] Jain, A. K.; Kumar, A. , "Biometrics of next generation: An overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, ISBN 978-97-007-3892-8, Springer, 2012, pp. 47-79.

[17] Kovács T.; Fialka Gy., "The Vulnerability of Biometric Methods and Device," *ANNALS of Faculty Engineering Hunedoara - International Journal of Engineering,* vol. 14, no. ISSN 1584-2673, pp. 45-48, 2016.

[18] Ratha, N. K.; Connell, J. H.; Bolle, R. M. , "An Analysis of Minutiae Matching Strength," *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01),* Vols. Halmstad, Sweden, June 2001, pp. 223-228,.

[19] Werner G.; Hanka L., "Risk-Adapted Access Control with AI based Multimodal Biometric Identification," in *European Smart, Sustainable and Safe Cities Conference 2019 Abstract Book*, Budapest, 2019.

[20] Hitchcock, D. C., Evaluation and Combination of Biometric Authentication Systems, USA: University of Flodria, 2003.

[21] Rodrigues, R. N.; Ling, L. L.; Gondaraju, V., "Roboustness of multimodal biometric fusion methods against spoof attacks," *Journal of Visual Languages and Computing,* vol. doi:10.1016/j.jvlc.2009.01.010, pp. 169-179, 2009.

[22] Navarro, D.; Perfors, A., "An Introduction to the Beta-Binomial Model," *Computational Cognitive Science,* 2012.

[23] Armijo, L., "Minimization of Functions Having Lipschitz Continous First Partial Derivates," *Pacific Journal of Mathematics,* vol. 16, no. 1, 1966.

[24] Hintermüller, M., Nonlinera Optimization, Humboldt University of Berlin.

[25] Galántai A., Optimalizálási Módszerek, Miskolc0: Miskolci Egyetemi Kiadó, 2004.

[26] Hanka L.; Balogh Zs., "Bayesian Analyzis in the Risk Asessment Applivation of Discrete Probability Distributions," *Statements in Aeronautics,* vol. 25, no. 2, 2013.

[27] Otti Cs.; Kolnhofer-Derecskei A., "Az emberek elfogadási küszöbe a biometrikus rendszerek megbízhatóságával szemben," *Katonai Nemzetbiztonsági Szolgálat,* vol. XVI., no. 3., pp. 133-148, 2018.

[28] Retter Gy., Kombinált Fuzzy, Neurális, Genetikus Rendszerek Kombinált Lágy Számítások, Budapest Műszaki és Gazdaságtudományi Egyetem ISBN 978 963 87401 0 6: Invesz Marketing Bt., 2007.

[29] Franke, K.; del-Solar, J. R.; Köppen, M., "Soft-Biometrics: Soft-Computing Technologies for Biometric-Applications," in *SPRINGER*, Berlin, 2002.

[30] McCarthy, J., "Artificial Intelligence, Logic and Formalizing Common Snese," in *Philosophical Logic and Artificial Intelligence*, University of PittsburghPhiladelphiaUSA, Springer ISBN 978 94 010 7604 3, 1989, pp. 161-190.

[31] Bradshow-Martin, H.; Easton, V., "Autonomus or 'Driverless' Cars and Diasability: a Legal and Ethical Analysis," *European Journal of Current Legal Issues,* vol. 20, no. 3, 2014.

[32] Werner G., "A mesterséges intelligencia szerepe a biztonságtudományban," in *XX. Tavaszi Biztonságtechnikai Szimpózium, Óbudai Egyetem*, Budapest, 2017.

[33] Werner G.; Hanka L., "A Fuzzy logika alkalmazása a multi-modális biometrikus azonosításban," in *KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI*, 2016.

[34] Zadeh, L. A., "Fuzzy Sets," *Information and Control,* Vols. doi:10.1016/S0019-9958(65)90241-X, pp. 338-353, 1965.

[35] [Online]. Available: https://in.pcmag.com/biometric-devices/118254/the-biometric-system-in-your-phone-has-come-a-long-way. [Accessed 15. február 2019.].

[36] Werner G.; Hanka L., "Optimization of Big Population's Multimodal Biometrical Identification with a Complex neuro-Fuzzy Logic Controller," in *Sixth International Scientific Videoconference of Scientists and PhD students or candidates : Trends and Innovations in E-business, Education and Security*, Budapest, 2016.

[37] Kóczy L.; Tikk D., Fuzzy Systems (Fuzzy Rendszerek), Budapest: Typotex, 2001.

[38] Werner G., "Fuzzy Logic Adapted Controller System for Biometrical Identification in Highly-Secured Critical Infrastructures," in *10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2015)*, Timisoara, Romania, 2015.

[39] Jager, A., Fuzzy Logic in Control, Delft, 1995.

[40] Polski, J.; Smith, R.; Garrett, R., The Report of the International Association for Identification, Standardization II Committee, 2011, pp. 28-29.

[41] Abdolahi, M.; Mohamadi, M.; Jafari, M., "Multimodal Biometric System Fusion Using Fingerprint and Iris with Fuzzy Logic," *Internationl Journal of Soft Computing and Engineering,* Vols. ISSN 2231-2307, no. 2, 2013.

[42] Contil, V.; Milici, G.; Ribino, P.; Sorbello, F.; Vitabile, S., "Fuzzy Fusion in Multimodal Biometric Systems," in *Knowledge-Based Intelligent Information and Engineering Systems*, Berlin, Springer, 2007, pp. 108-115.

[43] [Online]. Available: http://www.research.ibm.com/brain-chip.shtml. [Accessed 15 szeptember 2016].

[44] Werner G.; Hanka L., "A mesterséges neurális hálózatok alkalmazásának lehetőségei a biometrikus személyazonosításban," *XXI. FMTÜ Nemzetközi Tudományos Konferencia kiadványa - Proceedings of the XXI-th International Scientific Conference of Young Engineers,* pp. 441-444, 2016.

[45] "Fingerprint Veriification Competition 2002," [Online]. Available: http://bias.csr.unibo.it/fvc2002/. [Accessed 1. március 2019.].

[46] Werner G; Hanka L., "Tuning an Artificial Neural Network to Increase the Efficiency of a Fingerprint Matching Algorithm," in *SAMI 2016 : IEEE 14th International Symposium on Applied Machine Intelligence and Informatics*, Herlany, Slovakia, 2016.

[47] Kovács T., Milák I., Otti Cs., A Biztonságtudomány Biometrai Aspektusai, Pécs: Pécsi Határőr Tudományos Közlemények, XIII. kötet, HU ISSN 1589-1674, 2012.

[48] Sudiro, S. A.; Yuwono, R. T. , "Adaptable Fingerprint Minutiae Extraction Algorithm Based-on Crossing Number Method for Hardware Implementaion Using FPGA Device," *International Journal of Computer Science, Enigneering and Information Technology,* vol. 2, no. 3, 2012.

[49] Ravi, J.; Raja, K. B.;Venugopal, K. R., "Fingerprint Recognition Using Minutiae Score Matching," *Journal of Engineering, Science and Technology,* Vols. 1 ISSN 0975-5432, no. 2, pp. 35-42, 2009.

[50] "Artificial Neural Network - Perceptron," [Online]. Available: http://www.saedsayad.com/artificial_neural_network_bkp.htm. [Accessed 01. március 2019.].

[51] Ali, S.; Al-Omari, K.; Sumari, P.; Al-Taweek, S. A.; Hussain, A. J., "Digital Recogntion Using Neural Network," *Jorunal of Computer Science,* Vols. 5 ISSN 1549-3636, no. 6, pp. 427-434, 2009.

[52] Hajek, M., Neural Networks, University of KwaZulu-Natal, 2005.

[53] Weeraprajak, E.; Chacko E., "New Learning Algorithm for Adaptive Network Based Fuzzy Inference System in Application of Forecasting Chaotic Time Series," in *Universitiy of Canterbury*, Christchurch, New Zealand, 2007.

[54] Riedmiller, M., "Rprop - Description and Implemenations Details," in *University of Karlsruhe*, Karlsruhe, Germany, 1994.

[55] Katona Gy.; Recski A.; Szabó Cs., A számítástudomány alapjai, TYPOTEX, 2002.

[56] Yao, X., "A Review of Evolutionary Artifical Neural Networks," *Internatonal Journal of Intelligent Systems,* vol. 8, no. 4, pp. 539-567, 1993.

[57] Holland, J. H., Adaptation in Natural Artificial Sytems, Ann Arbor: University of Michigan Press, 1975.

[58] Werner G.; Hanka L., "Optimization of Artificial Neural Networks with Genegtic Algorithms for Biometric Pattern Recognition," *REVISTA ACADEMIEI FORTELOR TERESTRE / LAND FORCES ACADEMY REVIEW,* vol. 19, no. 3, p. 256, 2019.

[59] Jang, J-S. R.; Sun, C.H.; Mizutani, E., "Neuro-Fuzzy and Soft Computing-A Computational Approach to Learning and Machine Intelligence," vol. 42, IEEE Transactions on Automatic Control, 1997, pp. 1482-1484.

[60] Jang, J-S R., "Fuzzy Modeling Using Generalized Neural Networks and Kalman Filter Algorithm," *AAAI'91 Proceedings of the ninth National conference on Artificial intelligence,* vol. 2, pp. 762-767, 1991.

[61] Jang, J-S. R.; Sun, C-T.; Mizutani, E., Neuro-Fuzzy and Soft Computing; A Computational Approach to Learning and Machine Intelligence, Upper Saddle River: Prentice Hall, 1997.

[62] Jang, J-S. R., ANFIS: adaptive-network-based fuzzy inference system, USA: Dept. of Electr. Eng.& Compit. Sci., California Univ, Berkeley, p. 665-685, DOI: 10.1109/21.256541, 2002.

[63] Werner G.; Hanka L.; Őszi A., "Application of Adaptive Neuro-Fuzzy Inference System in Multimodal Biometrical Identification," *ÓBUDA UNIVERSITY E-BULLETIN,* vol. 9, no. 1, pp. 23-28, 2019.

[64] Wang, L. X.; Mendel, J. M., "Back-propagation fuzzy system as nonlinear dynamic system identifiers," *IEEE International Conference on Fuzzy Systems,* pp. 1409-1418, 1992.

[65] Wang, Y. M. ; Elhang, T., "An Adaptive Neuro-Fuzzy Inference System for Brdige Risk Assessment," *Expert Systems with Applications,* vol. 34, no. 4, pp. 3099-3106, 2008..

[66] Kryszczuk, K.; Drygajlo, A., "On Quality of Qiality Meusures for Classification," in *Biometrics and Identity Management*, Denmark, Roskilde Univesity, 2008, pp. 21-31.

[67] Abreu, M.; Fairhust, M., "An Empirical Comparison of Individual Machine Learning Techniques in Signature and Fingerprint Classification," in *Biometrics and Identity Management*, United Kingdom, University of Kent, 2008, pp. 133-143.

[68] Altrichter M.; Horváth G.; Pataki B.; Strausz Gy.; Takács G.; Valyon J., Neurális Hálózatok, Budapest: Panem Könyvkiadó Kft., 2006.

[69] Sekuler, P.; Blake, R., Perception (Észlelés), Budapest: Osiris Kiadó, 1994.

[70] Kovács T.; Földesi K., A biometrikus azonosítással kapcsolatos averziók rendőrök és egyetemi hallgatók körében, Budapest: Biztonságtechnikai Szimpózium, a Magyar Tudomány Ünnepe 2014 keretében: Óbudai Egyetem. 2015. pp. 1-12. ISBN 978-615-5460-30-2, 2014.

[71] Otti Cs.; Valociková C., "A Biztonsági Rendszerek Felhasználói Attitűdje, Értékelése és Befolyásolásának Lehetőségei," *Hadmérnök,* vol. 14, no. 1, pp. 32-41, 2019.

[72] Bechtel, W.; Abrahamsen, A., Connectionism and the Mind: an Intorduction to Parallel Processing in Networks, Cambridge, USA: Basil Blackwell, 1991.

[73] Konar, A., Artificial Intelligence and Soft Computing, Calcutta, India: Jadavpur University, CRC Press, 2000..

[74] Sánchez, D.; Melin, P., "Modular Neural Network with Fuzzy Integration and Its Optimization Using Genetic Algorithms for Human Recognition Based on Iris, Ear and Voice Biometrics," in *Soft Computing for Recognition Based on Biometrics*, Berlin, Springer, 2010, pp. 85-103.

[75] Werner G.; Hanka L., "Az emberi észlelésen alapuló mesterséges intelligencia modellezése a személyazonosításban," in *KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI*, Budapest, 2016.

PUBLIKÁCIÓS LISTA

Tézisekhez kapcsolódó publikációk

I. Werner G.; Hanka L.: Using the Beta-Binomial Distribution for the Analysis of Biometric Identification, in IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY), ISBN:978-1-4673-9388-1, pp. 209-215., 2015.

II. Werner G.; Hanka L.: Risk-Adapted Access Control with AI based Multimodal Biometric Identification, in European Smart, Sustainable and Safe Cities Conference Abstract Book, ISBN:978-615-5586-35-4, Budapest, 2019.

III. Werner G.: A mesterséges intelligencia szerepe a biztonságtudományban, XX. TAVASZI BIZTONSÁGTECHNIKAI SZIMPÓZIUM, Budapest, Óbudai Egyetem, 2017.

IV. Werner G.; Hanka L.: A Fuzzy logika alkalmazása a multi-modális biometrikus azonosításban, KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 8:(1-2), Szeged, ISSN:2064-437X, pp. 177-185., 2016.

V. Werner G.; Hanka L.: Optimization of Big Population's Multimodal Biometrical Identification with a Complex Neuro-Fuzzy Logic Controller, in Sixth International Scientific Videoconference of Scientists and PhD. Students or Candidates: Trends and Innovations in E-business, Education and Security, Budapest, Óbuda University, ISBN:978-963-449-014-2, pp. 108-123., 2016.

VI. Werner G.: Fuzzy Logic Adapted Controller System for Biometrical Identification in Highly-Secured Critical Infrastructures, in IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI) ISBN:978-1-4799-9910-1, pp. 335-340., 2015.

VII. Werner G.; Hanka L.: A mesterséges neurális hálózatok alkalmazásának lehetőségei a biometrikus személyazonosításban, MŰSZAKI TUDOMÁNYOS KÖZLEMÉNYEK, Kolozsvár, Románia, ISSN:2393-1280, pp. 441-444. 2016.

VIII. Werner G.; Hanka L.: Tuning an Artificial Neural Network to Increase the Efficiency of a Fingerprint Matching Algorithm, in IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herlany , Slovakia, ISBN:978-1-4673-8739-2, pp. 105-109., 2016.

IX. Werner G.; Hanka L., Optimization of Artificial Neural Networks with Genetic Algorithms for Biometric Pattern Recognition, in *REVISTA ACADEMIEI FORTELOR TERESTRE / LAND FORCES ACADEMY REVIEW,* Volume XXIV, No. 3(95), ISSN:2247-840X, pp. 256-264., 2019.

X. Werner G.; Hanka L.: Application of Adaptive Neuro Fuzzy Inference System in Multimodal Biometrical Identification, in Óbudai Egyetem e-Bulletin, Volume 9 Issue 1, ISSN:2062-2872, pp. 23-28., 2019.

XI. Werner G.; Hanka L.: Az emberi észlelésen alapuló mesterséges intelligencia modellezése a személyazonosításban, in KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 8:(1-2), Szeged, ISSN 2064-437X, pp. 187-197., 2016.

További publikációk

XII. Werner G.: A kritikus infrastruktúrák kockázatelemzési módszereinek újragondolása, különös tekintettel az ivóvízellátásra, 6. BÁTHORY-BRASSAI NEMZETKÖZI KONFERENCIA ELŐADÁSAIBÓL, Budapest, ISBN:978-615-5460-38-5, pp. 383-394., 2015.

RÖVIDÍTÉSJEGYZÉK

ACOM - Anti-Cloning Operations Methods

Másolás-Védelmi Végrehajtási Módszerek

ANFIS - Adaptive Neuro-Fuzzy Inference System

Alkalmazkodó Neuro-Fuzzy Következtető Rendszer

ANM - Additive Noise Model

Összegző Zajhatás Modell

ANN - Artificial Neural Network

Mesterséges Neurális Hálózat

BIPA - Biometric Information Privacy Act

Biometrikus Adatvédelmi Törvény

COA - Center of Area

Terület Közepe Módszer

COG - Center of Gravity

Súlypont Közepe Módszer

COM - Center of Maxima

Maximumok Közepe Módszer

FAR - False Acceptance Rate

Téves Elfogadás Aránya

FIR - False Identification Rate

Téves Azonosítás Aránya

FLC - Fuzzy Logic Controller

Fuzzy Logikai Vezérlő

FRR - False Rejection Rate

Téves Elutasítása Aránya

FTA - Failure to Acquire

Téves Mintakinyerés

FTE - Failure to Enrol

Téves Mintabeolvasás

GA - Genetic Algorithm

Genetikus Algoritmus

GDPR - General Data Protection Regulation

Általános Adatvédelmi Törvény

GMM - Gaussian Mixture Model

Gass Féle Keverékmodel

IBM - International Business Machines

Nemzetközi Üzleti Berendezések

LDA - Linear Discriminant Analysis

Lineáris Különbség Elemzés

MATLAB - Matrix Laboratory

Számítógépes program

MI - Mesterséges Intelligencia

AI Artificial Intelligence

MLP - Multi Layer Perceptron

Többrétegű Perceptron

MNM - Multiplicative Noise Model

Sokszorozó Zajhatás Modell

MOA - Mission Oriented Application

Célorientált Alkalmazás

MOM - Mean of Maxima

Maximumok Átlaga Módszer

QDA - Quadratic Discriminant Analysis

Kvadratikus Különbség Elemzés

ROC - Reciver Operating Characteristic

Eszköz Működési Karakterisztika

ROI - Region Of Interest

Vizsgálati Terület

SVM - Support Vector Machines

Tartó Vektor Gépek

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

MELLÉKLETEK

I. melléklet, kimeneti fuzzy felületeket kódoló mátrixok

Fuzzy logika alapú módszer (hármas osztású halmaz, COG, egészre kerekített)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	21	23	24	25	26	27	28	28	28	28	33	35	37	39	41	43	45	47	50	53
2	23	27	28	29	29	30	30	31	31	31	35	39	41	42	44	46	48	50	53	56
3	24	28	31	31	32	32	32	33	33	33	37	41	43	45	46	48	50	52	55	58
4	25	29	31	33	33	34	34	35	35	35	39	42	45	47	48	50	52	54	57	60
5	26	29	32	33	35	36	36	37	37	38	41	44	46	48	50	52	54	56	59	63
6	27	30	32	34	36	38	38	39	39	40	43	46	48	50	52	53	55	58	61	65
7	28	30	32	34	36	38	40	41	42	42	45	48	50	52	54	55	57	59	63	67
8	28	31	33	35	37	39	41	43	44	44	47	50	52	54	56	58	59	61	65	69
9	28	31	33	35	37	39	42	44	47	47	50	53	55	57	59	61	63	65	67	72
10	28	31	33	35	38	40	42	44	47	50	53	56	58	60	63	65	67	69	72	75
11	33	35	37	39	41	43	45	47	50	53	54	56	59	61	63	65	67	69	72	75
12	35	39	41	42	44	46	48	50	53	56	56	57	59	61	63	65	67	70	72	76
13	37	41	43	45	46	48	50	52	55	58	59	59	60	62	64	66	68	70	73	76
14	39	42	45	47	48	50	52	54	57	60	61	61	62	63	65	67	68	71	73	77
15	41	44	46	48	50	52	54	56	59	63	63	63	64	65	66	67	69	71	74	78
16	43	46	48	50	52	53	55	58	61	65	65	65	66	67	67	68	70	72	75	80
17	45	48	50	52	54	55	57	59	63	67	67	67	68	68	69	70	70	73	77	82
18	47	50	52	54	56	58	59	61	65	69	69	70	70	71	71	72	73	74	78	84
19	50	53	55	57	59	61	63	65	67	72	72	72	73	73	74	75	77	78	81	87
20	53	56	58	60	63	65	67	69	72	75	75	76	76	77	78	80	82	84	87	92

Fuzzy logika alapú módszer I. (ötös osztású halmaz, egészre kerekített)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	17	18	18	17	17	27	29	30	31	31	31	32	32	31	31	39	42	46	50	56
2	18	21	21	21	21	29	33	34	35	35	35	35	35	35	35	42	47	50	54	60
3	18	21	23	23	23	30	34	38	39	40	40	40	40	40	40	46	50	53	58	65
4	17	21	23	25	25	31	35	39	43	44	44	43	43	44	44	50	54	58	61	69
5	17	21	23	25	25	31	35	40	44	50	50	50	50	50	50	56	60	65	69	75
6	27	29	30	31	31	31	35	40	44	50	56	57	57	56	56	57	61	65	70	76
7	29	33	34	35	35	35	35	40	43	50	57	60	60	60	60	61	63	67	71	77
8	30	34	38	39	40	40	40	40	43	50	57	60	65	65	65	65	67	68	72	80
9	31	35	39	43	44	44	43	43	44	50	56	60	65	69	69	70	71	72	74	84
10	31	35	40	44	50	50	50	50	50	50	56	60	65	69	75	76	77	80	84	92
11	31	35	40	44	50	56	57	57	56	56	56	60	65	69	75	76	77	80	84	92
12	32	35	40	43	50	57	60	60	60	60	60	60	65	68	75	76	77	80	83	91
13	32	35	40	43	50	57	60	65	65	65	65	65	65	68	75	76	77	80	83	91
14	31	35	40	44	50	56	60	65	69	69	69	68	68	69	75	76	77	80	84	92
15	31	35	40	44	50	56	60	65	69	75	75	75	75	75	75	76	77	80	84	92
16	39	42	46	50	56	57	61	65	70	76	76	76	76	76	76	76	77	80	84	92
17	42	47	50	54	60	61	63	67	71	77	77	77	77	77	77	77	77	80	83	91
18	46	50	53	58	65	65	67	68	72	80	80	80	80	80	80	80	80	80	83	91
19	50	54	58	61	69	70	71	72	74	84	84	83	83	84	84	84	83	83	84	92
20	56	60	65	69	75	76	77	80	84	92	92	91	91	92	92	92	91	91	92	92

Fuzzy logika alapú módszer II. (ötös osztású halmaz, egészre kerekített)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	17	18	18	17	17	27	29	30	31	31	31	35	40	44	50	56	57	57	56	56
2	18	21	21	21	21	29	33	34	35	35	35	35	40	43	50	57	60	60	60	60
3	18	21	23	23	23	30	34	38	39	40	40	40	40	43	50	57	60	65	65	65
4	17	21	23	25	25	31	35	39	43	44	44	43	43	44	50	56	60	65	69	69
5	17	21	23	25	25	31	35	40	44	50	50	50	50	50	50	56	60	65	69	75
6	27	29	30	31	31	31	35	40	44	50	56	57	57	56	56	57	61	65	70	76
7	29	33	34	35	35	35	35	40	43	50	57	60	60	60	60	61	63	67	71	77
8	30	34	38	39	40	40	40	40	43	50	57	60	65	65	65	65	67	68	72	80
9	31	35	39	43	44	44	43	43	44	50	56	60	65	69	69	70	71	72	74	84
10	31	35	40	44	50	50	50	50	50	50	56	60	65	69	75	76	77	80	84	92
11	31	35	40	44	50	56	57	57	56	56	57	61	65	70	76	76	77	80	84	92
12	35	35	40	43	50	57	60	60	60	60	61	63	67	71	77	77	77	80	83	91
13	40	40	40	43	50	57	60	65	65	65	65	67	68	72	80	80	80	80	83	91
14	44	43	43	44	50	56	60	65	69	69	70	71	72	74	84	84	83	83	84	92
15	50	50	50	50	50	56	60	65	69	75	76	77	80	84	92	92	91	91	92	92
16	56	57	57	56	56	57	61	65	70	76	76	77	80	84	92	92	91	91	92	92
17	57	60	60	60	60	61	63	67	71	77	77	77	80	83	91	91	91	91	91	91
18	57	60	65	65	65	65	67	68	72	80	80	80	80	83	91	91	91	91	91	91
19	56	60	65	69	69	70	71	72	74	84	84	83	83	84	92	92	91	91	92	92
20	56	60	65	69	75	76	77	80	84	92	92	91	91	92	92	92	91	91	92	92

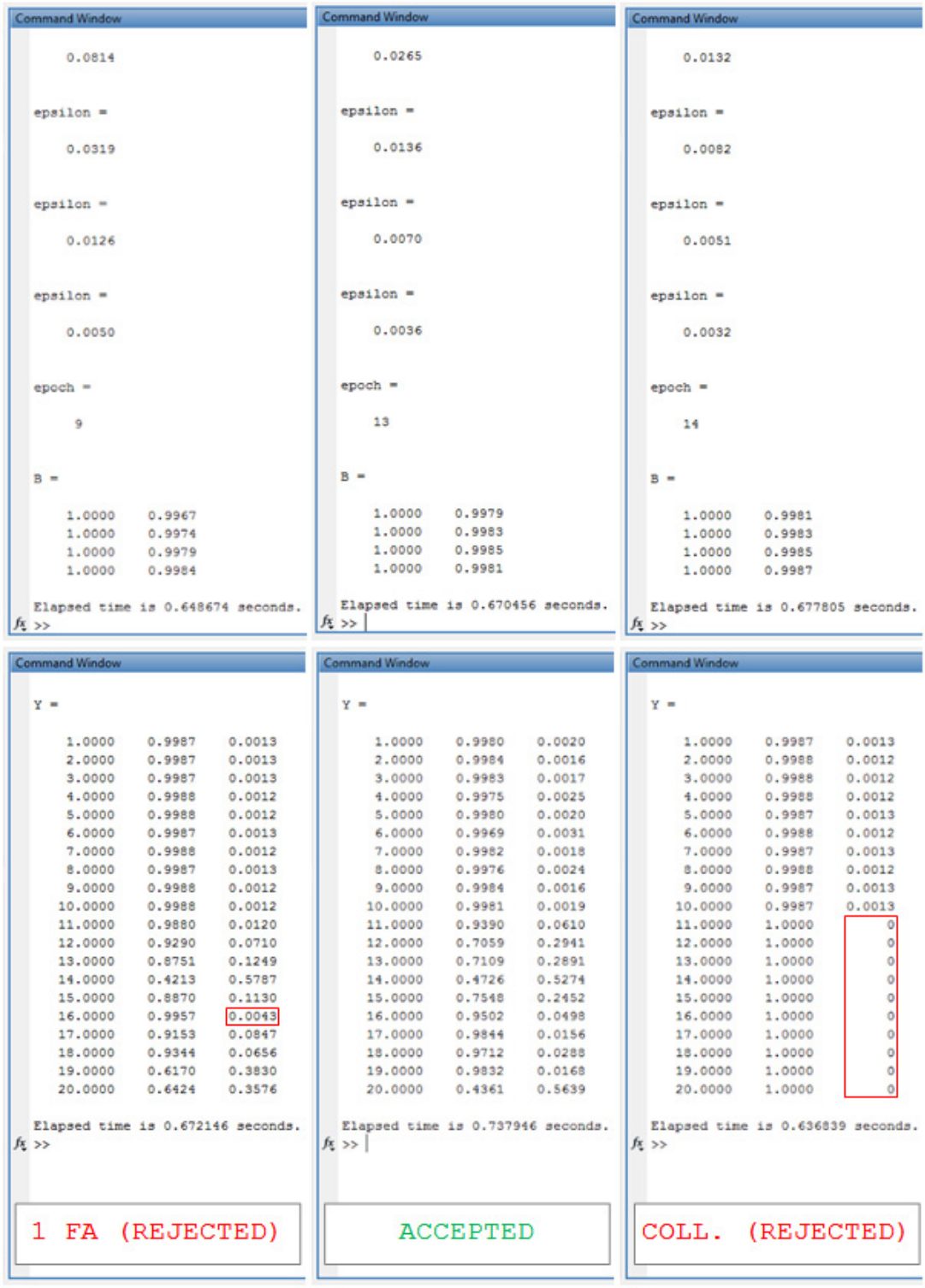
Fuzzy logika alapú módszer III. (ötös osztású halmaz, MOM)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	3	6	6	3	3	3	5	26	25	25	25	26	26	25	25	25	26	50	50	50
2	6	6	6	6	6	6	6	25	25	25	25	25	25	25	25	25	25	50	50	50
3	6	6	25	25	25	25	25	50	50	50	50	50	50	50	50	50	50	75	75	75
4	3	6	25	25	25	25	26	50	50	50	50	50	50	50	50	50	50	75	75	75
5	3	6	25	25	25	25	26	50	50	50	50	50	50	50	50	50	50	75	75	75
6	3	6	25	25	25	25	26	50	50	50	50	50	50	50	50	50	50	75	75	75
7	5	6	25	26	26	26	26	50	50	50	50	50	50	50	50	50	50	75	75	75
8	26	25	50	50	50	50	50	50	50	50	50	50	75	75	75	75	75	95	95	95
9	25	25	50	50	50	50	50	50	50	50	50	50	75	75	75	75	75	95	98	98
10	25	25	50	50	50	50	50	50	50	50	50	50	75	75	75	75	75	95	98	100
11	25	25	50	50	50	50	50	50	50	50	50	50	75	75	75	75	75	95	98	98
12	26	25	50	50	50	50	50	50	50	50	50	50	75	75	75	75	75	95	95	95
13	26	25	50	50	50	50	50	75	75	75	75	75	75	75	75	75	75	95	95	95
14	25	25	50	50	50	50	50	75	75	75	75	75	75	75	75	75	75	95	98	98
15	25	25	50	50	50	50	50	75	75	75	75	75	75	75	75	75	75	95	98	100
16	25	25	50	50	50	50	50	75	75	75	75	75	75	75	75	75	75	95	98	98
17	26	25	50	50	50	50	50	75	75	75	75	75	75	75	75	75	75	95	95	95
18	50	50	75	75	75	75	75	95	95	95	95	95	95	95	95	95	95	95	95	95
19	50	50	75	75	75	75	75	95	98	98	98	95	95	98	98	98	95	95	98	98
20	50	50	75	75	75	75	75	95	98	100	98	95	95	98	100	98	95	95	98	100

II. melléklet, ANN tréning után teszt eredmények

					m_0=0,5	EPS=0,005	ETA=0,025	k_0=1	k_1=6	k_2=4
TRIAL	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
TRAIN01.tif	0,9977	0,9983	0,9998	0,9981	0,9986	0,998	0,9979	0,9982	0,9969	0,9988
TRAIN02.tif	0,9979	0,9986	1	0,9984	0,9989	0,9983	0,9984	0,9985	0,9985	0,9991
TRAIN03.tif	0,9983	0,9988	1	0,9987	0,9991	0,9986	0,9987	0,9987	0,9976	0,9993
TRAIN04.tif	0,9985	0,9989	0,998	0,9999	0,9993	0,9988	0,999	0,9989	0,9986	0,9995
mean value	0,9981	0,9987	0,9990	0,9988	0,9990	0,9984	0,9985	0,9985	0,9979	0,9991
rel.stand. dev.	0,0365	0,0264	0,0971	0,0789	0,0299	0,0350	0,04697	0,0299	0,0806	0,0299
Epsilon	0,0038	0,0027	0,002	0,003	0,0021	0,0032	0,0031	0,0029	0,0044	0,0017
Epoch	11	9	5	10	10	10	8	9	13	9
time (s)	0,62	0,63	0,66	0,64	0,61	0,56	0,6	0,61	0,53	0,61
Test	REJECTED	ACCEPTED	ACCEPTED	1 FA	2 FA	5 FA	REJECTED	REJECTED	2 FA	REJECTED
test time(s)	0,58	0,58	0,58	0,58	0,62	0,6	0,55	0,56	0,55	0,58

III. melléklet, ANN tréning utáni teszt eredmények példái



KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném megköszönni családom, barátaim, valamint kollégáim támogatását és megértését, amivel hozzájárultak e munka elkészüléséhez. Kiemelt köszönettel tartozom Dr. Hanka Lászlónak, aki szakmai és emberi támogatása nélkül nem juthattam volna el ideáig, nemcsak oktatómként, de konzulensemként és témavezetőmként kísérte végig tanulmányaimat az Óbudai Egyetemen.

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

Alulírott, Werner Gábor kijelentem, hogy a „Multimodális Biometrikus Azonosító Rendszerek Kockázat Alapú Vizsgálata Fuzzy Logika és Neurális Hálózatok Segítségével" című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2019. november 29.

Werner Gábor