

ÓBUDAI EGYETEM

---

Keleti Károly Gazdasági Kar  
Vállalkozásfejlesztés és Infokommunikációs Intézet

# SZAKDOLGOZAT

ÓE-KGK  
2023

Hallgató neve:  
Hallgató törzskönyvi száma:

Kovács Gergő  
T007988/FI12904/G

### KONZULTÁCIÓS NAPLÓ

**Hallgató neve:**  
Kovács Gergő

**Neptun kód:**  
[REDACTED]

**Tagozat:**  
Nappali

**Szak:**  
Gazdaságinformatika

**Szakirány vagy gazdasági modul:**  
Vállalatinformatikai specializáció

**Telefon:**  
[REDACTED]

**Levelezési cím:**  
[REDACTED]

**Szaktervezési cím magyarul:**

Banki tevékenységekhez tartozó biometrikus azonosítási lehetőségek vizsgálata.

**Szaktervezési cím angolul:**

Exploring Biometric Identification for Banking

**Intézményi konzulens:**

Bálint Krisztián

**Külső konzulens:**

Alk.	Dátum	Tartalom	Aláírás
1.	2023.09.06	Követelmények áttekintése.	Bálint Krisztián
2.	2023.09.27	Elméleti bevezető, hivatkozások.	Bálint Krisztián
3.	2023.10.31	Empirikus bevezető, elemzések.	Bálint Krisztián
4.	2023.12.02	Összegzési önéletrajz ellenőrzése	Bálint Krisztián

A Konzultációs naplót összesen 4 alkalommal az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a „Szaktervezési” tantárgy aláírási követelményét teljesítette.

Bálint Krisztián  
Intézményi konzulens

Budapest, 2023. év 12 (hó) 05 (nap)



Óbudai Egyetem  
Keleti Károly Gazdasági Kar  
Vállalkozásfejlesztés és Infokommunikációs Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Kovács Gergő

Szaktervezési szám: [REDACTED]

Törzskönyvi száma: T007988/F112904/G

Neptun kódja: [REDACTED]

Szak: Gazdaságinformatikus

Specializáció: Vállalatinformatikai specializáció

**A dolgozat címe:** Banki tevékenységekhez tartozó biometrikus azonosítási lehetőségek vizsgálata

**A dolgozat címe angolul:** Exploring Biometric Identification for Banking

**A feladat részletezése:**

1. Végezzen elméleti kutatást a banki tranzakciók során használt biometrikus azonosítási folyamatokról és az azokban rejlő lehetőségekről!
2. Végezzen primer kutatást a biometrikus azonosítás hatásáról és annak előnyeiről a mindennapi életben végrehajtott banki tranzakciók során!
3. Tegyen javaslatot, miként lehetne tovább fejleszteni ezt az azonosítási módszert és ez miként segíthetne a mindennapok során a banki felhasználóknak!
4. Összegezze a kapott kutatási eredményeket, vonjon le következtetéseket, valamint fogalmazzon meg további lehetséges kutatási célokat!

**Intézményi konzulens neve:** Bálint Krisztián

**A kiadott téma elévülési határideje:** 2024. 12. 15.

**Beadási határidő:** 2023. 12. 15.

A szakdolgozat: Nem titkos.

Kiadva: Budapest, 2023. 10. 31.

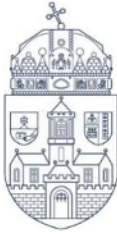
A dolgozatot beadásra alkalmasnak találtam.



[Signature]  
Intézetigazgató

[Signature]  
Bálint Krisztián  
belső konzulens

[Signature]  
külső konzulens



## HALLGATÓI NYILATKOZAT

Alulírott Kovács Gergő (Neptunkód: ██████████) hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2023.11.26.

-----  
hallgató aláírása

# Tartalomjegyzék

1. BEVEZETÉS .....	2
1.1. A kutatási téma időszerűsége .....	2
1.2. A témaválasztás indoklása .....	3
1.3. A téma kutatásának hipotézisei.....	3
1.4. Célkitűzések .....	4
1.5. A kutatás felépítése .....	4
1.6. A kutatás során használt módszerek .....	4
1.7. Kutatási probléma .....	5
2. Napjainkban használatban lévő biometrikus azonosítási formák .....	6
2.1. Ujjlenyomat szkenneléses azonosítás .....	7
2.1.1. Ujjlenyomat szkennerek .....	7
2.1.2. Optikai ujjlenyomat olvasás.....	7
2.1.3. Kapacitív ujjlenyomat olvasás .....	8
2.1.4. Ultraszónikus ujjlenyomat olvasás .....	9
2.1.5. Ujjlenyomat, mint bankkártya .....	10
2.2. Arcfelismerés-alapú biometrikus azonosítás.....	12
2.2.1. A technológia fejlődése .....	13
2.3. Retinaszkennelés alapú azonosítás.....	14
2.3.1. Anatómia használata az azonosításhoz.....	15

2.3.2.	Retina szkennerek .....	16
3.	A biometrikus azonosítás szerepe a banki tranzakciók során.....	17
3.1.	Mobil banking .....	18
3.2.	Új ügyfelek fogadása.....	18
3.3.	Újra azonosítás .....	19
3.4.	Hagyományos banki tevékenység során .....	19
4.	Empirikus Kutatás.....	19
4.1.	A kutatásban részt vett személyek eloszlása.....	20
4.2.	A kutatásban részt vett személyek válaszai .....	20
4.2.1.	A válaszadók alkalmasságának vizsgálata.....	21
4.2.2.	A megkérdezettek mindennapi banki szokásai.....	22
4.2.3.	Azonosítási módszerek biztonsága .....	23
4.2.4.	Azonosítási módszerek megbízhatósága .....	26
4.2.5.	Biometrikus módszerek praktikuma a hétköznapi életben.....	28
4.2.6.	Emberek bizalma a hitelintézetek felé .....	29
5.	Kiaknázatlan lehetőségek .....	30
5.1.	Népszerűsítés.....	30
5.2.	Viselkedés alapú azonosítás.....	34
6.	Probléma felvetése .....	40
6.1.	Jelenlegi helyzet a probléma területén .....	40
6.2.	Biometrikus azonosítás bevezetése a készpénzfelvételi folyamatokba .....	41

6.3. Javaslatok kivitelezési tervezete .....	43
6.4. Hátrányok.....	44
7. A dolgozat hipotézisei .....	44
8. ÖSSZEFOGLALÁS .....	45
IRODALOMJEGYZÉK .....	47
TARTALMI KIVONAT.....	I
SUMMARY .....	I

## ÁBRAJEGYZÉK

1. ÁBRA. PÉLDA EGY BIOMETRIKUS AZONOSÍTÁS FOLYAMATÁRA.....	6
2.ÁBRA. AZ OPTIKAI UJJLENYOMATOLVASÓ MŰKÖDÉSE .....	8
3. ÁBRA. BIOMETRIKUS TOKEN ELKÉSZÍTÉSÉNEK FOLYAMATA. ....	11
4.ÁBRA. A SZEM ANATÓMIÁJA FORRÁS: (FARZIN, ABRISHAMI-MOGHADDAM, & MOHAMMAD-SHAHRAM, 2008) .....	16
5.ÁBRA. RETINA KÉPEK FORRÁS: (FARZIN, ABRISHAMI-MOGHADDAM, & MOHAMMAD- SHAHRAM, 2008) .....	16
6. ÁBRA. RENDELKEZIK ÖN BANKSZÁMLÁVAL? (N=107) .....	21
7. ÁBRA. MINDENNAPJAI SORÁN MILYEN BANKI TRANZAKCIÓKAT HAJT VÉGRE? (N=107) .....	22
8. ÁBRA. VOLT-E MÁR BANKI VISSZAÉLÉS ÁLDOZATA? (N=107) .....	24
9.ÁBRA. MIT GONDOL, MEGELŐZHETŐ LETT VOLNA AZ ESET, HA BIOMETRIKUS ADATTAL VÉDI MAGÁT? (N=107).....	24
10. ÁBRA. ELŐFORDULT MÁR ÖNNEL, HOGY A TRANZAKCIÓJA A BIOMETRIKUS RENDSZER MŰKÖDÉSI HIBÁJA MIATT NEM VALÓSULT MEG? (N=107).....	27
11. ÁBRA. ÖN SZERINT A HÉTKÖZNAPOKBAN PRAKTIKUSABB LENNE BIOMETRIKUS AZONOSÍTÁST HASZNÁLNI, MINT HAGYOMÁNYOSAT? (N=107).....	28
12. ÁBRA. HA A BANKJA KIVEZETNÉ A HAGYOMÁNYOS AZONOSÍTÁSI MÓDSZEREKET, ÉS BIOMETRIKUSRA CSERÉLNÉ AZOKAT, ÖNNEK CSÖKKENNE A BIZALMA FELÉJÜK?(N=107) .....	29
13. ÁBRA. ÖN ISMERI A BIOMETRIKUS AZONOSÍTÁST?(N=107).....	30
14. ÁBRA. NEM SZÍVESEN ADOM MEG BIOMETRIKUS ADATAIMAT A BANKOM SZÁMÁRA. (N=107) .....	33
15. ÁBRA. TARTOK ATTÓL, HOGY BIOMETRIKUS ADATAIMAT ELLOPJÁK ÉS FELHASZNÁLJÁK ELLENEM. (N=107).....	34
16. ÁBRA. A SÉTÁLÁS ALAPJÁN VALÓ AZONOSÍTÁS FOLYAMATA. FORRÁS: (LIANG, SAMTANI, GUO, & YU, 2019) .....	37
17. ÁBRA. ATM-BŐL TÖRTÉNŐ KÉSZPÉNZFELVÉTEL FOLYAMATA. ....	40
18. ÁBRA. AZ ÁLTALAM JAVASOLT FOLYAMAT ÁBRÁJA. ....	42
19. ÁBRA. ÜZEMELŐ ATM-EK MAGYARORSZÁGON.....	43

## TÁBLÁZATOK JEGYZÉKE

1. TÁBLÁZAT. A KITÖLTŐK ELOSZLÁSA VÁRMEGYÉK SZERINT .....	20
2. TÁBLÁZAT. MILYEN GYAKRAN HAJT VÉGRE BANKI TRANZAKCIÓKAT?.....	23
3. TÁBLÁZAT. MENNYIRE TARTJA BIZTONSÁGOSNAK A BIOMETRIKUS AZONOSÍTÁST? (N=107) .....	25
4. TÁBLÁZAT. AZONOSÍTÁSI HIBÁK MENNYISÉGÉNEK ÖSSZEHASONLÍTÁSA.....	27
5. TÁBLÁZAT. AZ ALÁBBI AZONOSÍTÁSI MÓDSZEREK KÖZÜL MELYIKEKKEL TALÁLKOZOTT MÁR? .....	31
6. TÁBLÁZAT. A VISELKEDÉS ALAPÚ AZONOSÍTÁS ÖSSZEFOGLALÁSA .....	39
7. TÁBLÁZAT. A HIPOTÉZISEK ÖSSZEFOGLALÁSA. ....	44

## **1. BEVEZETÉS**

Korunk talán leggyorsabban fejlődő iparága kétség nélkül az informatika. Azok a szektorok, és azon belül cégek, amelyek nem szeretnék piaci hátrányba kerülni versenytársaikkal szemben, kénytelenek meglovagolni ezt a hullámot, és élen járni a fejlesztésekben. Ez alól a bankszektor sem kivétel, hiszen ott is óriási szükség van a modern technológiákra. A kétezres évek elején egyre több helyen kezdték el bevezetni a biometrikus azonosítási módszereket. Elsőnek az ujjlenyomat szkennelést, majd ezt követték sorban a retina és arcfelismerő rendszerek. Mára már szinte megkerülhetetlen ezeknek a használata a banki tevékenységeink során, azonban rengeteg olyan kiaknázatlan lehetőség van még ilyen témakörökben, ami nagy előrelépés lehetne a bankok és az ügyfelek életében egyaránt. Ilyen lehetőség lehetne egy ATM-be vagy egy kártyaterminálba épített ujjlenyomatszkennel. Ezek a fejlesztések nemcsak biztonságosabbak lennének jelenlegi társaiknál, de praktikusabbak és meglehetősen gyorsabbak is.

### **1.1. A kutatási téma időszerűsége**

Témaválasztásomat azért találom időszerűnek, mivel napjainkban egyre nagyobb figyelmet fordítanak mind a bankok, mind az ügyfelek az adataik és értékeik biztonságára. Ebbe a témakörbe tartozik az általam kutatott azonosítási módszer is. Mivel a régi módszerek ellen egyre találékonyabbak és kifinomultabbak a csalók, gondolok itt például a PIN-kódra, amit könnyen le tudnak már másolni, és ezután ezt a károsításunkra felhasználni. Mindezek mellett társadalmunk jelenleg is egy nagy átalakulási folyamaton megy keresztül, amiben is a régebbi fizetési mód, vagyis a készpénzzel történő fizetésről állunk át a modernebb megoldások felé. Ugyan ez nem egy teljesen járatlan út, a fejlődésnek még bőven van helye. Új módszerek kiaknázása, vagy már létező módszerek más környezetben való használata nagy előrelépés lehet adatbiztonsági szempontból a bankok életében.

## **1.2. A témaválasztás indoklása**

Ezt a témát választottam, mivel személyes tapasztalatom alapján szinte elkerülhetetlen ezeknek a módszereknek az alkalmazása a mindennapi életünkben. Mérhetetlenül sok helyen könnyítik meg a dolgunkat, legyen ez akár a telefonunk feloldása, vagy éppen a témánkba vágó fizetési kérelem megerősítése egy banki tranzakció során. Mindezek mellett hihetetlen érdekesnek, és kiemelkedő fontosságúnak találom azt, hogy a pénzügyi intézetek ezt a fajta módszert választották, és fejlesztik évek óta ügyfeleik adatainak biztonságba tartására miközben kiemelkedő hangsúlyt fordítanak arra is, hogy időről időre kényelmesebb, és felhasználóbarát élményt nyújtsanak mindazon embereknek, akik bizalmat szavaztak számukra. Előző pontomban már bontogattam, hogy miért is időszerű ez a téma.

## **1.3. A téma kutatásának hipotézisei**

### ➤ Hipotézis 1

Feltételezhető, hogy a biometrikus azonosítási módszerek hatékonyabbak a banki tranzakciók során alkalmazott "hagyományos" azonosítási módszerekkel szemben.

### ➤ Hipotézis 2

Feltételezhető, hogy Magyarországon az alkalmazott biometrikus azonosítási lehetőségek közül legelterjedtebb az ujjlenyomattal történő azonosítás.

### ➤ Hipotézis 3

Feltételezhető, hogy a banki felhasználók körében igény lenne újfajta azonosítási módszerek bevezetésére és a bizalmuk sem csökkenne a bank irányába a mostani azonosítási rendszer leváltása esetén.

#### **1.4. Célkitűzések**

Szaktervezésem célja a biometrikus azonosítási módszerekben rejlő lehetőségek kutatása a banki tranzakciók során. Ezen belül célom a jelenleg Magyarországon használatos módszerek kielemezése biztonsági, gyorsasági, és megbízhatósági szempontból. A módszerek mellett a felhasználók véleményét, tudatosságát és a folyamatok felé tanúsított bizalmát is vizsgálom. A kapott eredményeket kielemezve teszek javaslatot a biometrikus azonosítási folyamatok fejlesztésére, azok hatékonyabbá tételére. Ezek nem csak a szolgáltatást nyújtók módszereire irányulnak, hanem a felhasználók látáspontjára is. Szeretnék kutatómunkám során olyan lehetőségeket feltárni, amikkel javítani tudom a felhasználói élményt a mindennapokban a banki tranzakciók elvégzése során amellet, hogy a módszerek egyéb tényezői nem romlanak, még inkább javulnak minden téren.

#### **1.5. A kutatás felépítése**

A kutatásomat a szekunder adatok gyűjtésével kezdtem. Egy erős elméleti háttérrel gyűjtöttem össze eddigi tudományos kutatásokból, könyvekből, hivatkozásokból. Ezzel párhuzamosan elkészítettem az online kérdőívemet is, amit a későbbiekben elemeztem. Mikor elegendő kitöltés jött már össze, illetve elkészültem az elméleti háttérrel, több szempont alapján elemezni kezdem a felhalmozódott adathalmazt. Célszerű olyan szempontok alapján elemezni, ami a későbbiekben alátámaszthatja, vagy cáfolhatja hipotéziseimet. Az elemzések után levonom a konklúziót, majd egy saját megoldást javaslok a problémára. A kutatásom végén összegzek.

#### **1.6. A kutatás során használt módszerek**

Kutatásom során primer és szekunder adatokkal egyaránt dolgoztam, a minél pontosabb és tényszerűbb eredmények elérésének érdekében. Szekunder adatokat aktuális, publikációkból, folyóiratokból, illetve statisztikai forrásokból gyűjtöttem. Primer adataimat egy kvantitatív kutatásból dolgoztam fel. Ezen információk segítettek abban, hogy hipotéziseim megerősítést, vagy ellenkező esetben megcáfolást nyerjenek. A kutatás ezen részét egy online formában létrehozott kérdőívvel tettem meg. A módszernek nagy előnye, hogy széleskörű kitöltőbázist érhet el, Magyarország minden részéről. A kérdésekre adott válaszok kielemezésére leíró statisztikai módszereket alkalmaztam, mint

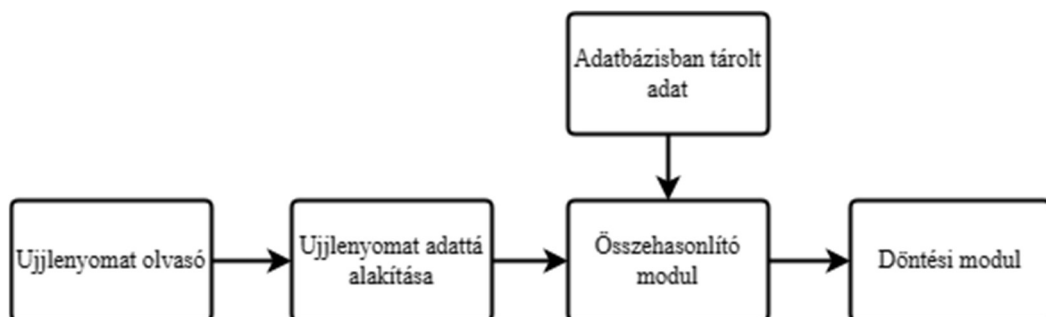
például átlag, modus vagy medián számítást. Ezek a statisztikai módszerek segítenek a kutatási eredmények megértésében, és könnyebbé teszik azok összehasonlítását. A kapott eredményeket próbáltam vizualizálással jobban érthetővé, informatívabbá tenni az olvasók számára. Grafikus módszereket használtam a céloom elérése érdekében. Ezek a következők voltak: kör, illetve oszlop diagrammok, táblázatok és folyamatábrák.

### **1.7. Kutatási probléma**

A problémafelvetésem során szeretnék egy olyan javaslatot tenni, ami egy biometrikus azonosítási folyamat segítségével tudná javítani a már meglévő, a mindennapokban a felhasználók által gyakran végrehajtott tevékenységet. A problémafelvetésemet a kvantitatív kutatásom eredményeire, illetve a saját magam által gyűjtött tapasztalatokra alapozom. Az általam felvetett probléma: Kézpénzfelvételi lehetőségek határai hazánkban, az ATM-ek használata során. Az adott témát a dolgozatom hatodik fejezetében fejtem ki.

## 2. NAPJAINKBAN HASZNÁLATBAN LÉVŐ BIOMETRIKUS AZONOSÍTÁSI FORMÁK

Biometrikus azonosításnak azt nevezzük amikor egy adott személyt a viselkedése, illetve biológiai tulajdonságai alapján azonosítjuk automatizált módon. Ez a fajta rendszer a hagyományos azonosítási módszereket hivatott leváltani. Ahhoz azonban, hogy ezt sikeresen véghez tudja vinni, nagyon sok szempontot kell figyelembe venni. A két legfőbb ilyen szempont a pontosság és a biztonság. Az azonosítási folyamat során a biometrikus adatok szkennelése történik, annak érdekében, hogy egy úgynevezett biometrikus sablont hozzanak létre az illetőről. A későbbiekben ezt az adott mintát veti össze a rendszer az éppen leolvasottal, és ha egyezést talál, akkor sikeresen azonosította magát az illető. Az első ábrán egy ilyen folyamat látható. Ezeknek a sablonoknak a védelme különösen fontos, hiszen, ha egyszer egy ilyen sablont hackertámadás ér, és kitudódik, onnantól kezdve azt nem tudja az adott személy megváltoztatni. Ezáltal azt az adatát többé nem használhatja azonosításra, onnantól kezdve egyszerű préda lenne a támadóknak. Ennek a tényezőnek köszönhető az a tény, hogy ez a topik napjainkban is rendszeresen kutatott, és vélhetően a jövőben is nagy figyelmet fog kapni a biztonsági szakemberektől. (Sarkar & Singh, 2020)



1. Ábra. Példa egy biometrikus azonosítás folyamatára

## 2.1. Ujjlenyomat szkenneléses azonosítás

A mindennapi felhasználási területek terén az egyik legelterjedtebb azonosítási forma. Ezen folyamat során az ujj bőrfelületének barázdáltságát tárolja el a rendszer, amit úgynevezett fodorszálak és fodorvonalak alkotnak. Bár az egyik legősibb biometrikus technikaként tartjuk számon, azonban mai napig ez az egyik leginkább elterjedt módszer. Nagyjából tizenöt, húsz külső jellemzőt mérünk az azonosítás során. A mérés leggyakrabban nem érintésmentes. A föld népességének csupán 3-5% nem rendelkezik a mint vételre alkalmas ujjlenyomattal különböző okok miatt. Két tenyér vagy akár tíz ujj mintája áll rendelkezésre, de a vegyszerekkel végzett munka, vagy az építőipar bizonyos területein végzett fizikai tevékenység, hatására a tenyerek vagy az ujjak bőrrödözete könnyen roncsolódik, ami az ilyen jellegű azonosítást lehetetlenné teszi. Előfordul, hogy határátlépésnél az ujj(le)nyomatalapú azonosítás sikertelensége „érdekében” erős savakkal roncsolják a felső hámréteket, ezzel elkerülve az egyértelmű azonosíthatóságot. 18 hetes kortól már kialakul a minta és az évek során nem változik. Az egészségügyi területen történő felhasználás esetén az orvosi gumikesztyű használata kizáró ok lehet. (Ujhegyi , 2023)

### 2.1.1. Ujjlenyomat szkennerek

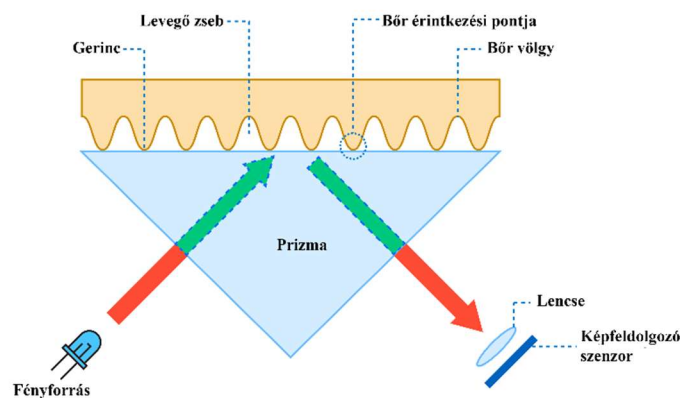
Az ujjlenyomat olvasóknak több különböző típusát fejlesztették ki mára. Most ezekből a mindennapjainkban leggyakrabban használt hármat fogom ismertetni. Ezek pedig a következők:

- Optikai ujjlenyomat olvasó
- Kapacitív olvasó
- Ultraszónikus olvasó

### 2.1.2. Optikai ujjlenyomat olvasás

A legrégebbi szkennelési módszer az optikai olvasás. Az optikai ujjlenyomat szkennerek az Abszolút Belső Visszaverődés (Total Internal Reflection, TIR) elvén alapul. Egy ilyen szkennerek esetében egy üvegprizmát használnak az TIR elősegítéséhez. Egy LED (általában kék színű) fényét engedik be az egyik prizma felületén egy bizonyos szögben,

hogy a visszaverődés végbe mehessen. A visszaverődött fény kijut a prizmából a másik felületén, ahol egy lencse és egy képérzékelő (lényegében egy kamera) található. Amikor nincs ujj a prizmán, a fény teljesen visszaverődik a felületről, egy sima képet létrehozva az képérzékelőben. Amikor az TIR megtörténik, egy kis mennyiségű fény szivárog ki a külső közegbe, ezt Evanescent Hullámnak nevezik. Az anyagok különböző törésmutatóval (RI) különböző módon reagálnak az evanescens hullámra. Amikor érintjük az üvegfelületet, csak a felszint érintő bemetszők lépnek kapcsolatba vele. A völgyek levegő tasakokkal vannak elválasztva a felülettől. A bőrünknek és a levegőnek különböző törésmutatója van, és így különböző módon befolyásolják az evanescens mezőt. Ezt az effektust Frustrált Abszolút Belső Visszaverődésnek (Frustrated Total Internal Reflection, FTIR) nevezik. Ez az effektus megváltoztatja a belsőleg visszaverődött fény intenzitását, és azt az képérzékelő észleli. Az képérzékelő adatait feldolgozzák, hogy előállítsanak egy magas kontrasztú képet, ami az ujjlenyomat digitális változata lesz. A bemutatott szkennelés a második ábrán látható. (MOHANAN, 2021)



2.Ábra. Az optikai ujjlenyomatolvasó működése

### 2.1.3. Kapacitív ujjlenyomat olvasás

A félvezető technológia fejlődésével, és a hitelesítő eszközök mobil eszközökbe, például okostelefonokba és integrált áramkör kártyákba kerülve olcsó, kompakt csomagolást igényelnek, megjelenne a kapacitív leolvasó rendszerek. Alapelvben a kapacitív és induktív ujjlenyomat szenzorok "lapos" lemezzel rendelkeznek, amelyen száz szintetikus eszköz és egy, általában néhány mikron vastag felületi réteg található. Az ujjlenyomat kisebb vagy nagyobb emelkedéseinél, valamint az ujjlenyomat érintkezési pontjai közötti

távolság változik, amikor az ujjat a kapacitív szenzor felületére helyezik, ami különböző kapacitásértékeket eredményez. A kapacitásértékeket áram vagy feszültségértékekké alakítják át, amelyeket az ADC (analóg-digitális átalakító) által digitális adattá alakítanak. Minél közelebb van az ujjhegy a felülethez, annál erősebb az ujjlenyomat lenyomata. A szenzor az összegyűjtött eredmények átlagolásával fejezi be az ujjlenyomatgyűjtési folyamatot.

Vannak olyan szenzorok, amiket saját ellenállásra alapoznak. Ilyenkor egy mérőtű és a tápellátó egység közötti ellenállást mérik. A folyamat a következő módon néz ki. Ahogyan az ujjunkat ráhelyezzük a szenzorra, abban a pillanatban megváltozik az ellenállás, illetve a mért feszültség. Ennek köszönhetően lehetővé tevődik az ujj érzékelése. Ezeknél a rendszereknél az egységcella jellemzően egy áramkörből áll, ami az Si (System integrator) technológiát alkalmazza. A szenzor ellenállása közvetlenül, és függetlenül érzékelhető. Ezzel a folyamattal készült ujjlenyomat érzékelők csak olyan szilícium lapkákra gyárthatók, amelyek áttetszők, törékenyek és rugalmatlanok. Ezek a lapkák pedig csak merev dolgokba építhetők be, annak érdekében, hogy elkerüljük azok sérüléseit. Ilyen hely lehet például az okostelefonok gombjai. A rendszer nem alkalmas a többérintéses leolvasásra. (Yu, és mtsai., 2023)

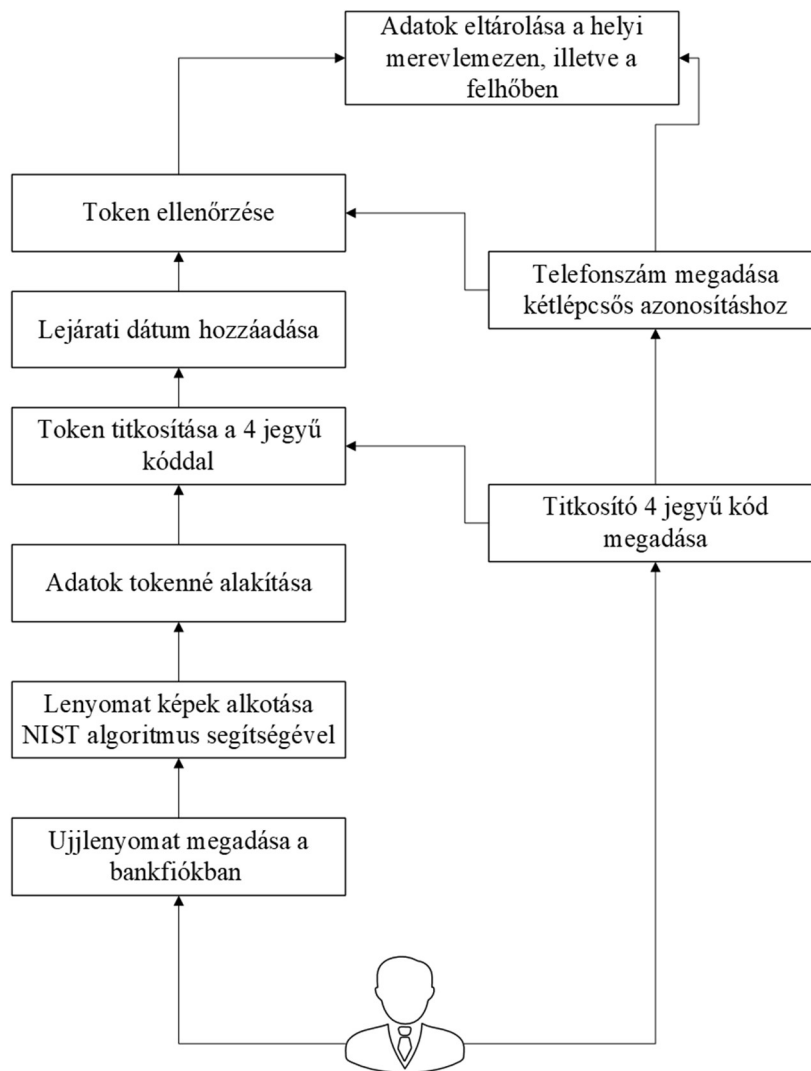
#### 2.1.4. Ultraszónikus ujjlenyomat olvasás

Az ultraszónikus ujjlenyomat olvasó a leggyorsabb és emellett a legprecízebb eszköz a kívánt képek elkészítéséhez. A technológiában két fő képalkotási módszer létezik: az úgynevezett pulzus-visszhang (pulse-echo), illetve az impedancia képalkotás. Ahogy a neve is mutatja, a módszer az ultrahang visszaverődésén alapul. A mobiltelefon alapul véve, amikor a kijelzőre helyezzük az ujjunkat, a nyomásérzékelő jelet küld a szenzornak, hogy működésbe lépjen. Ekkor ez egy elektromos impulzushullámot bocsáj ki. Az emberi szövet és a levegő közötti akusztikai impedancia különbsége miatt az emberi szövet visszaverődési amplitúdója nagyobb, mint a levegőé, ezért a szövetmintát az egyes pontokon történő visszaverődési amplitúdó meghatározásával lehet elkészíteni. A szenzor ultrahangos sugarai hasonlítanak az orvosi vizsgálat során használtakéhoz, így ez nem ártalmas az emberi szervezet számára. Köszönhetően az ultrahang erősségének, ezek a hullámok képesek keresztülhatolni anyagokon, mint például az üveg, a műanyag, az acél,

vagy a zafír. Ennek köszönhetően a szerkezet, jelen esetben a telefon belsejébe is van lehetőségünk beépíteni az olvasót, így annak megnövelhető a várható élettartama, biztonsága. Természetesen ezek után egy kis kosz sem lehet akadály, így akkor is pontosan lehet használni az olvasót, ha a bőrünk felületén szennyeződés, vagy adott esetben víz maradt. (Yu, és mtsai., 2023)

#### 2.1.5. Ujjlenyomat, mint bankkártya

Az utóbbi évtizedben a hitel- és bankkártyák nagyon kényelmes és praktikus fizetési módussá váltak a lakosság körében. Ez az eszköz nagy kényelmet biztosít akár bolti vásárlás, akár online vásárlások folytatásakor. Az utóbbi folyamat során a fizető és a fogadó fél között hatalmas távolságok is lehetnek. Ez növeli a hitelkártyák kiberbiztonsági támadásoknak való kitettségeinek esélyét, különösen akkor, ha a tranzakció összege elég nagy. Egy másik probléma, ami felmerül, az a potenciális csalás, ha egy tolvaj megpróbál a személyes adatainkkal visszaélni. Ezeknek az akadályoknak a leküzdése érdekében egy új, a biometrikus adatra épülő sémát mutatnék be, amely az ujjlenyomatot biotokenként használja fel a jelenleg használatban lévő műanyag hitelkártya helyett. A séma a biometrikus adatokat (ujjlenyomat), visszavonható ujjlenyomat biotokeneket használja fel a magas biztonsági szint eléréséhez. A folyamat során a felhasználtól begyűjtjük a biometrikai adatait(például az ujjlenyomatát), majd négyjegyű biztonsági kódokat ágyaz az átkódolt biometrikus adat kódjai közé. Végül ezeket, a négyjegyű biztonsági kódokat, illetve az összekevert kódot is, egymástól jól elkülönítve tárolja el a felhőben. A fizetés folyamatában a felhasználó az ujjlenyomatát adja meg a tranzakció végrehajtásához. A bemutatott módszert a hármas számú ábra jeleníti meg. (Alsolami, 2019)



3. Ábra. Biometrikus token elkészítésének folyamata.

A folyamat megkezdése hasonló, mint amikor egy ügyfél csak simán bankszámlát szeretne nyitni, vagy új hitelkártyát szeretne intézni magának. Az ügyfélnek be kell fáradnia a bankfiókba, hogy egy ügyintéző felvehesse adatait, köztük a biometrikus adatát is, azaz az ujjlenyomatát. Ezt követően a BioPay nevezetű algoritmus követi a NIST Bozort Matcher algoritmust ahhoz, hogy pontos adatokat rögzítsen, majd ezekből egy képet alkosson, amit egy galéria táblázatban tárol el. Ezt követően egy folyamat során a biometrikus képi adatokat az algoritmus átalakítja visszavonható tokenekké, titkosítja, majd eltárolja az átalakítás során használt transzformációs adatokat. Ezekből az adatokból készíti el a felhasználó számára a saját maga BioPay tokenjét. Miután ez a token elkészült, megkérlik az ügyfelet, hogy adjon meg egy négy számból álló kódot, hasonlóan a PIN-

kódhoz. Ezt a kódot rejtik el a tokenné alakított biometrikus adatokban, hogy azt majd később az azonosítás során fel tudják használni. Ezt követően egy véglegesítő lépésként megadja még az ügyfél a telefonszámát, egy kétlépcsős azonosítás felállításához, majd letesztelik a tokenet. Ha minden rendben ment a felhasználó saját tokenje elkészült, és ezt követően a lejárat dátumig bezárólag biztonságban tudja használni azt, mindenféle banki tranzakció során. Legyen az online fizetés, banki átutalás, vagy éppen készpénz felvétel az egyik bankautomatából. (Alsolami, 2019)

## **2.2. Arcfelismerés-alapú biometrikus azonosítás**

Az ujjlenyomat után korunk egyik legismertebb és leggyakrabban használt biometrikus módszere. Ez annak is köszönheti, mivel a mostani telefonok, tabletek és notebookok túlnyomó többsége is képes ezen módszer alapján azonosítani a felhasználót. Ma már szinte minden kamerás rendszer ajánl valamiféle arc alapú biometrikus azonosítást. A technika elfogadottsága tehát magas. Külső paraméterek alapján mér, ezáltal nem igényel fizikai kontaktot például az ujjlenyomattal szemben. Ezt leszámítva több tényező is befolyásolja az azonosítás sikerességét. Ilyenek például a személy és a kamera távolsága, azok szöge, elhelyezkedése egymáshoz képest, és a megvilágítás is. Nem kell a személy beleegyezése vagy együttműködése a sikeres azonosításhoz, ami alkalmassá teszi a megoldást többcélú és rejtett felhasználásra. Az azonosítás során a minták összehasonlítása nem feltétlenül az adatkezelés céljához hozzájárult felhasználók regisztrált adatbázisával történhet. Mozgóképből kivett vagy letöltött kép alapján is működhet az azonosítás, és mesterséges intelligenciával támogatott megoldások esetén még a kamerába nézni sem szükséges, meglepően kevés paraméter alapján is lehet sikeres a felismerés. A technológia az emberi arc jellegzetes pontjait figyeli, az azok közötti távolságot, arányukat. Anyajegyek, sebhelyek, tetoválások, ráncok és a bőrpólusok is nagyban elősegítik az azonosítás sikerességét. Ezek alapján a sikerességen felül akár az illető kora is megállapítható lehet. Mindezek mellett a technológia pontossága alacsony, sérülékenysége igen magas. Könnyen elérhető, hogy jó minőségű, nagy felbontású képek alapján, maszkok használatával fizetési vagy azonosítási szolgáltatások sérülékenységi kihatásait kihasználják. A rendszerek általában nem tartalmazzak élőminta felismerést segítő hardver-szoftver megoldásokat. (Ujhegyi, 2023)

### 2.2.1. A technológia fejlődése

Az arcfelismerés alapú azonosítás először az 1960-as években került a felszínre. A témában úttörők voltak Woody Bledsoe, Helen Chan, és Charles Bisson. Ők elsőnek használtak számítógépeket arra, hogy felismerjék az emberi arcot, mindezt 1964 és 1965 között. Projektjük anyagi finanszírozása egy név nélküli hírszerzési ügynökséghez köthető, ennek köszönhetően sok részlet a kutatásaikból sosem látotta napvilágot. Akárhogy is, a későbbiekben kiderült, hogy kezdetleges munkáik magukban foglalták az arcon manuálisan meghatározott iránypontokat használtak, ilyenek voltak például a szemek, az orr hegye, vagy éppen az alany szája. Ezeket ezt követően egy számítógép matematikailag elforgatta, hogy korrigálni tudja a fej helyzetének változását. Az előbb már említett iránypontok változásának távolságait is számítógépek segítségével számolták ki, és hasonlították össze a személy azonosításának érdekében. A korukhoz képest nagy előrelépés volt ez, azonban a technológia nem volt elég fejlett ahhoz, hogy tovább tudják fejleszteni a megkezdett módszerüket. Az 1970-es években az ő munkájukat folytatták, Goldstein, Harmon és Lesk. Ők hárman kiterjesztették a vizsgált pontok számát huszonegy pontra. A bővítésbe beletartozott például a hajnak a színe, illetve az ajkaknak a vastagsága. Céljuk a folyamat teljes automatizálása volt. Ezt ugyan nem sikerült elérniük, mivel a pontokat továbbra is kézzel kellett beállítani és lemérni. De részleges sikert értek el, mivel a módszer pontossága nagyban javult az elődéhez képest. Ezután egy nagyobb csend következett a kérdéses technológia fejlődésében, ugyanis a nagyobb előrelépésre majd húsz évet kellett várni. Ekkor is két kutató, Sirovich és társa Kirby nekiálltak lineáris algebrát használni az arcfelismerés problémájában. A módszert, amit használtak, Eigenface-nek nevezték el. Ez a rendszer azt mutatta, hogy egy gyűjtemény az arcokról készített ábrákról, képes egy bizonyos csoportot felállítani az alapvető vonásokról. Azt is bebizonyította ez a módszer, hogy kevesebb mint száz elem elég ahhoz, hogy egy normalizált arcképet készítsenek. 1991-ben Turk és Pentland folytatták tovább a kutatást, és ők sikeresen azonosítottak egy arcot képről. Ezzel utat törtek az automatikus arcfelismerésnek. Azonban mint már elődjeiket is, őket is hátráltatta a kor technológiájának fejlettségi szintje, és így nem voltak képesek a módszert kivitelezni éles körülmények között, de a későbbi nemzedék számára kaput nyitottak a siker felé. Az ezredfordulón az úgynevezett Védelmi Kutatási Projektet Ügynöksége (angolul DARPA) és a National Institute of Standards and Technology (NIST) elindította

a FERET nevű projektet, annak érdekében, hogy ösztönözze a kereskedelmi szektorban az arcfelismerés alapú azonosítást fejlesztő cégeket. A projekt magában foglalta egy adatbázisnak a létrehozását, ahol 2413 statikus fényképet tároltak, és ezek 856 embert képviseltek. Ezzel a terv az volt, hogy egy ilyen adatbázis ösztönzően hathat a kutatókra, és ennek segítségével, egy erősebb és pontosabb arc alapú azonosítási rendszert tudnak majd létrehozni. A NIST ezt követően még több ilyen programot is indított. Ilyen volt például az FRVT rövidítésre hallgató program. Ennek a programnak a célja az volt, hogy az amerikai kormány és a hírszerzés a legnaprakészebb technológiákkal rendelkezzen az arcfelismerés terén, és cserébe független értékelést és támogatást kínáltak a kereskedelmi gyártóknak a projektjeikhez. 2006-ban került napvilágra egy olyan szoftver, ami már háromdimenziós arcképeket, és szemírész azonosítást is használt a folyamat során. Ez az algoritmus nagyjából tízszer pontosabb volt a 2002-ben kiadott elődjénél, és majd százszor az 1995-ben kiadottnál. 2010-ben az akkori kor legnagyobb socialmedia platformja, a Facebook is beszállt a versenybe. Ők folyamatosan elemezték, és tárolták a felhasználók által a platformra feltöltött képeket. Itt hatalmas adatbázis képződött, hiszen a felhasználók naponta több mint 350 millió képet töltek fel. Ezzel, ha ugyan csak közvetve is, de mindennapi életünk részévé vált ez a technológia. A nagy áttörés akkor jött el, amikor az Apple 2017. szeptember 12.-én bemutatta az Iphone X-et, amit már általuk FaceId-nak nevezett technológiával lehetett feloldani. Ez nem volt más mint a telefon előlapi kameráján keresztül üzemelő többdimenziós arcfelismerő szoftver. A fejlődés azonban mint sok más téren, itt sem áll meg napjainkban sem. Hatalmas ipari verseny alakult ki a téma körében, ahol cégek ezrei versenyeznek a legjobb kormányzati és egyéb megbízásokért annak reményében, hogy ők fogják megtalálni a következő áttörést, az újabb nagy technológiai előrelépést. (NEC, 2022)

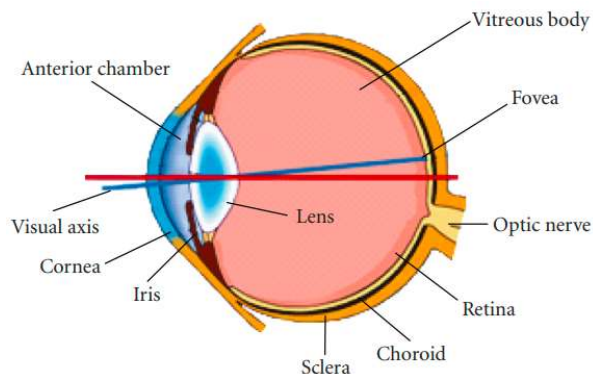
### **2.3. Retinaszkennelés alapú azonosítás**

Az eddig felsoroltak közül talán a legbiztonságosabb azonosítási forma a retinaszkennelés. Ezt részben köszönheti a velejáró méreteinek a csalással szemben, kiemelkedő egyediségének és stabilitásának. A retina egyedisége annak tetején futó vérerek mintázatából nyeri. Mindezek mellett a retina megy keresztül a legkevesebb változáson élete során. Hogy miért nem jobban elterjedt módszer ez napjainkban? Ez nem másnak köszönhető, mint a technológia költségességének. Az iparban hiányában voltak

az olcsón előállítható retinaszkennereknek, és sorozatgyártásban nem érte meg készíteni és árusítani a drága változatokat. Az első kereskedelemben is használt retinaszkennert 1976-ban mutatta be egy EyeDentify Company nevezetű cég. Zöld árnyalatú retinaképeket használtak, majd meghatároztak egy vektor görbét a vérerek vázának. Ezután meghatároztak egy sor jellemző vektort minden kép esetében, ideértve a jellemző pontokat, irányokat és méretezési faktort. A módszerükben a jellemzők párosítását az alkalmazott és a legmegfelelőbb találatként azonosított kép közötti affin transzformációs paraméterek megtalálása jelentette. Ennek az algoritmusnak a legnagyobb hátránya a számítási költsége, mivel számos merev mozgási paramétert kell kiszámítani az összes lehetséges megfeleltetés esetében a lekérdezés és az adatbázisban található képek között. Xu és munkatársai a módszerüket egy 200 képet tartalmazó adatbázison értékelték, és nullás hamis azonosítást értek el 38 hamis elutasítás mellett. (Farzin, Abrishami-Moghaddam, & Mohammad-Shahram, 2008)

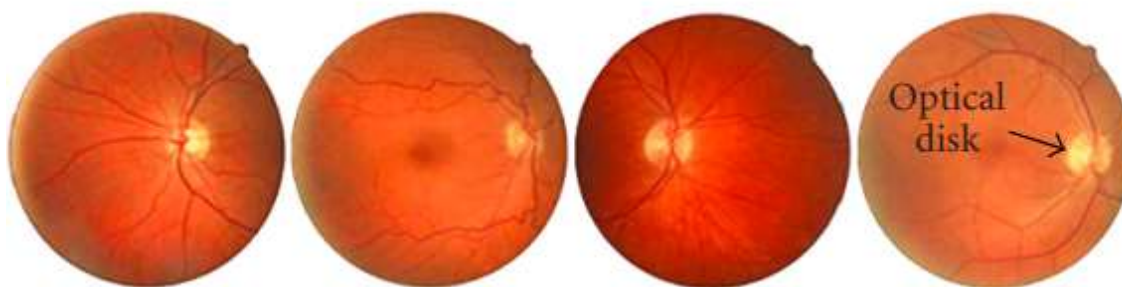
### 2.3.1. Anatómia használata az azonosításhoz

Amikor a szemről beszélünk biometrikus szempontból gyakran összekeverik a retinát és a szemíriszt, mivel ezeknek nagyon hasonlítanak egymásra. Bár egy biometrikus kategóriába soroljuk őket, feladatuk teljesen eltérő. Az írisz a szem pupilla és a szem fehér része (amit sklerának is neveznek) közötti színes terület. Az írisz fő szerepe a pupilla méretének tágítása és összehúzása. Ahogy az 4. ábrán látható, az írisz az elől található a szemben, míg a retina a szem hátsó részén található. Mivel a retina belső helyen található a szemben, nem érheti a külső környezet, így rendkívül stabil biometrikus adattal rendelkezik. A retina véredény-mintázata képezi a retinás felismerés tudományának és technológiájának alapját. Az 5. ábrán négy különböző retinát láthatunk, amelyeket négy különböző személyen rögzítettek.



4.Ábra. A szem anatómiája

Forrás: (Farzin, Abrishami-Moghaddam, & Mohammad-Shahram, 2008)



5.Ábra. Retina képek

Forrás: (Farzin, Abrishami-Moghaddam, & Mohammad-Shahram, 2008)

Két híres tanulmány erősítette meg a retina véredény-mintázat egyediségét. 1935-ben Simon és Goldstein publikáltak egy cikket, amelyben megírták, hogy minden retina rendelkezik egyedi és különböző véredény-mintázattal. Sőt, később egy olyan cikket is közzétettek, amely javasolta a retina véredény-mintázatának fényképekkel történő felhasználását az emberek azonosítására. A második tanulmányt az 1950-es években Dr. Paul Tower végezte. Ő azt fedezte fel, hogy még az azonos ikrek között is a retina véredény-mintázata egyedi és különböző. (Farzin, Abrishami-Moghaddam, & Mohammad-Shahram, 2008)

### 2.3.2. Retina szkennerek

Ahhoz, hogy a retina szkennelése sikeresen végrehajtható legyen, szükség van egy megfelelő hardveres eszközre is. Az ilyen irányú fejlesztéseket elsőnek 1972-ben kezdték meg. A témában élen járt egy EyeDentification nevezetű cég, akik megalkották az első ilyen kamerákat. Ugyan elsőkézből nem erre a célra készítették az eszközöket, hanem

szakorvosi célra, azonban kisebb módosításokkal képesek voltak retina képek készítésére is. Ezeket a kamerákat „fundus kameráknak” nevezték. A kezdeti technológiának azonban megvoltak a maga hátrányai. Első soron meglehetősen költséges volt előállítani, és kezelni is bonyolult volt. Másodrészt pedig a pácienseknek is kellemetlen volt a használata, ugyanis a fényképezésre használt fénysugarak nagyon erősek voltak, használat közben kellemetlenséget, fájdalmat okoztak. (Farzin, Abrishami-Moghaddam, & Mohammad-Shahram, 2008)

### **3. A BIOMETRIKUS AZONOSÍTÁS SZEREPE A BANKI TRANZAKCIÓK SORÁN**

A biometrikus azonosítás a bankszektorban a kétezres évek elején jelent meg. Az azonosítás során az eddigiekben már felsorolt metódusokat használják a bankok arra, hogy ügyfeleiket akár közvetlen, akár távolról azonosítani tudják. Gyorsan felismerték benne a potenciált, és a banki rendszerek mindennapi komponensévé vált, mind a mobilbankolás, mind az online tranzakciók során. Az alábbi pontokban összegyűjtöttem, és bemutatom néhány előnyét a biometrikus azonosítás során:

- Megnövekedett biztonság,
- Magasabb szintű kényelem,
- Magasabb szintű működési hatékonyság,
- Csökkentett visszaélési ráta.

Általában a banki biometrikai azonosító rendszerek két részből állnak. Van egy hardver, egy szkennert, ami szolgáltatja az adatokat, illetve egy szoftvert, ami feldolgozza azokat. A rendszer minősége, összetettsége nagyban függ az alkalmazott területtől. Lehet az például egy aprócska olvasó a telefonunk képernyőjébe integrálva, de akár egy professzionális az egyik bankfiókba. Miután a szkennert működésbe lépett, a beolvasott adatot egyből átalakítja digitálissá, és továbbítja azt a bank adatbázisa felé. Ha egyezést talál, akkor engedélyezi a hozzáférést, míg ellenkező esetben elutasítja azt. Ebben az esetben lehetőségünk van újra próbálkozni, vagy egy másik módon azonosítani magunkat. Összegezve a folyamat a következő lépésekből áll: beolvasás, tárolás, összehasonlítás. (Brezitska, 2023)

### **3.1. Mobil banking**

Az okostelefonok fejlődése egyre népszerűbbé, és többértévé tette azokat. Az emberek már régen nem csak telefonálásra vagy internetezésre használják a készülékeiket. Egyre gyakrabban tároltak rajtuk személyes adatokat, képeket, videókat, dokumentumokat, vagy éppen jelszavakat. Mivel ezek egy számítógéphez, vagy akár egy laphoz képest is nagyon kis méretű eszközök, így könnyen elhagyhatja őket a gazdája, vagy egy másik fél jogtalanul tulajdoníthatja el azt. Ennek köszönhető az, hogy a felhasználók biztonsága és védelme az illetéktelen személyekkel szemben egy igen komoly, és nagy problémává vált az utóbbi időkben. Ezt a fejlődést meglovagolták a bankok is, és integrálták a saját alkalmazásukba a telefongyártó cégek által nyújtott lehetőségeket. Lehetővé tették a felhasználók számára azt, hogy néhány banki tranzakciójuk során az ujjlenyomatukkal, vagy az arcukkal azonosítsák magukat mobilkészülékeik segítségével. A meglévő csalás elleni megelőzéseikkel kombinálva, a lehető legbiztonságosabb felhasználói élményt próbálják meg nyújtani a felhasználóiknak. Ez a fajta módszer egy kiemelkedő védelmet nyújt azokkal a csalókkal szemben, akik megpróbálják olyan módon ellopni a felhasználók adatait, hogy ellesik, megszerzik azok felhasználónevét és jelszavát. (Stankevičiūtė, 2023)

### **3.2. Új ügyfelek fogadása**

Az új ügyfelek felvételénél az első lépés az ügyfél azonosítás. Erre a folyamatra azért van szükség, hogy a bankok biztosra mehessenek oly téren, hogy törvényes személlyel szerződnek. Ezzel a későbbi bűneseteket szűrik ki, illetve redukálják azokat. Az első lépést a biometrikus azonosítás előtt mindig személyesen kellett megtenni, be kellett menni az ügyfélnek a bankba, annak érdekében, hogy ellenőrizni tudják a személyazonosságát. Emellett olyan szempontból is fontos a lépés, miszerint a bankoknak be kell tartani a KYC(Know-Your-Customer), és a AML(Anti-Money Laundering) előírásokat, amik szintúgy azonosítást igényelnek. Az új folyamat megjelenésével a bankok általában arra kérik leendő ügyfeleiket, hogy szkenneljenek be egy képes igazolványt, ami lehet jogosítvány, útlevelel vagy személyi igazolvány. Ezt követően mobilkészülékük segítségével arcfelismerést hajtanak végre. A bank szoftvere elemzi a két képen látható arcot, és ha egyezést talált akkor megtörténik az azonosítás.

### **3.3. Újra azonosítás**

Nem csak akkor van szükség azonosításra, amikor új ügyfél érkezik az adott bankhoz. Ezek a pénzügyi szervezetek rendszeresen ismétlik ezeket a folyamatokat, ha a helyzet megkívánja azt. Általában erre a következő esetekben van szükség:

- Ha az ügyfél feltűnően nagy összegben szeretne végrehajtani tranzakciót a számláján, vagy olyan gyanús helyre szeretne utalni ahová eddig nem tette pl.: külföldre,
- Ha az ügyfél szeretné megváltoztatni valamely bizalmas adatát. Ilyen lehet a jelszó, telefonszám, e-mail cím, személyes adatok és a többi,
- Ha az ügyfél szeretné befagyasztani, esetlegesen akár törölni is a számláját,
- Ha eddig még nem használt eszközről, vagy ismeretlen böngészőből szeretne bejelentkezni.

### **3.4. Hagyományos banki tevékenység során**

Itt azokról a banki tevékenység sorairól beszélünk amikor az ügyfél bemegy személyesen a bankba, és itt intézi az ügyeit. Ahhoz, hogy ezt megtehesék az ügyfelek, régebben általában PIN-kódra volt szükség, vagy valamilyen személyes irat felmutatására. Napjainkban már többen nyújtanak olyan szolgáltatásokat, hogy szimplán beszkenne a munkatárs az ujjlenyomatunkat, vagy felismertetik az arcunkat a rendszerrel, és be is azonosítottak minket. Az arcfelismerő algoritmus már azelőtt segítheti ügyintézésünket, mielőtt helyet foglalnák a pultnál. Adott bankfiókokba lépésünkkor a szobába telepített kamera rendszer azonosíthat minket, és ez alapján az azonosítás alapján előkészítheti aktáinkat, számunkra releváns adatokkal állhat elő.

## **4. EMPIRIKUS KUTATÁS**

A kutatásom során egy online kérdőívet hoztam létre. A dolgozatom következő fejezetében ezt elemzem, és szeretnék minél több hasznos adatot kinyerni belőle. A kérdéssor létrehozásának fő célja az volt, hogy nem csak elméleti háttérrel rendelkezzen a kutatott téma terén, hanem releváns adatokkal tudjak szolgálni a kitöltők aktuális, mindennapi véleményei, és szokásai alapján az általam boncolt témában.

#### 4.1. A kutatásban részt vett személyek eloszlása

Az első táblázatban azt szeretném szemléltetni, hogy az ország mely részéről hányan töltötték ki a kérdőívemet.

<b>Ország</b>	<b>Vármegye</b>	<b>Kitöltők száma</b>
<b>Magyarország</b>	Veszprém	71
	Vas	2
	Pest	8
	Győr-Moson-Sopron	11
	Fejér	1
	Borsod-Abaúj-Zemplén	2
	Bács-Kiskun	5
	Budapest (Főváros)	4
	Zala	2
	Hajdú-Bihar	1
<b>Összes kitöltők száma:</b>		107

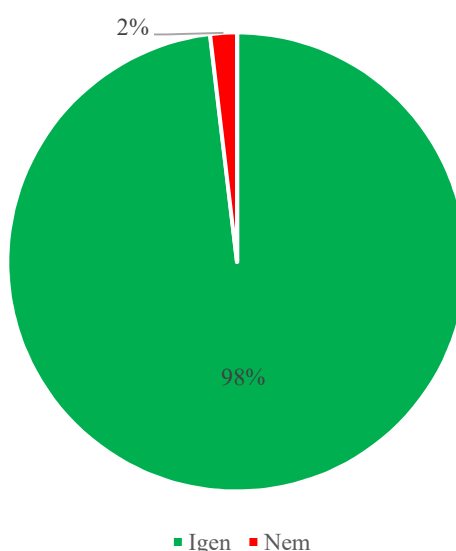
1. Táblázat. A kitöltők eloszlása vármegyék szerint

#### 4.2. A kutatásban részt vett személyek válaszai

Kutatásom során fontosnak találtam megkérdezni az alapvető kérdéseket, mivel ezekkel a kitöltő is könnyebben azonosul a témával, illetve én is fel tudtam tenni olyan kérdéseket, amelyekkel meg tudtam szűrni esetlegesen a kérdőív kitöltésére alkalmatlan személyeket.

#### 4.2.1. A válaszadók alkalmasságának vizsgálata

Alapvető kérdésnek találtam kutatásom során, hogy a kérdőívet kitöltők rendelkeznek-e egyáltalán bankszámlával, hiszen enélkül egyenesen lehetetlen lenne releváns válaszokat adni a kérdésemre. Szerencsémre ahogyan az a hatodik ábrán is látszik, az összes kitöltő közül csupán két ember nem rendelkezett számlával, a maradék százöt pedig igen. Ez 98,1 %-ban igenleges válasz az általam feltett kérdésre, ami egy erős egyhangúság. Ha azonban tovább elemezzük a kérdéseket látható az is, hogy csak egy olyan válaszadó volt, aki azt a választ adta a hatodik kérdésre, hogy egyáltalán nem hajt végre tranzakciót. Ebből következtethető az, hogy feltehetőleg hibásan választotta a nem választási lehetőséget ezen kérdés esetében.

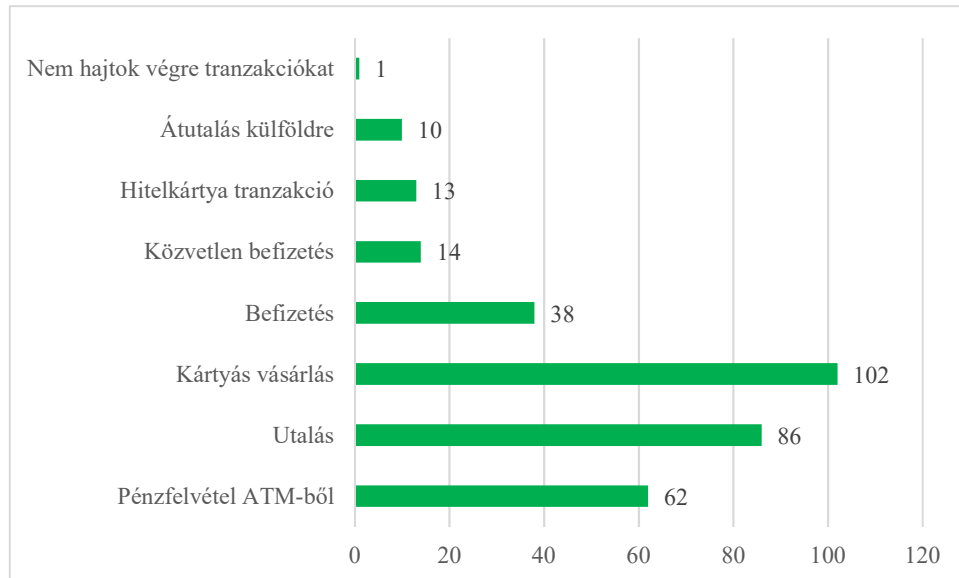


6. Ábra. Rendelkezik ön bankszámlával? (n=107)

A második, ilyen alapszintű kérdés a kilencedik kérdés volt. Ebben arra voltam kíváncsi, hogy a megkérdezett emberek mekkora része ismeri egyáltalán a biometrikus azonosítás fogalmát. Az eredmény számomra meglepő volt, hiszen a válaszadók kevesebb mint kétharmada adott csak igenleges választ. Ez szám szerint 67 embert takar. Annak ellenére, hogy ez egy viszonylag alacsony érték nem kell rossz értéknek felfogni, hiszen a kutatás célja az, hogy a folyamatban lévő lehetőségeket megvizsgáljuk, feltárjuk. Ha nem ismerik az emberek a biometrikus azonosítást, az számomra azt jelenti, hogy nem elég népszerű, így több kiaknázatlan területe van, mint azt elsőkézből gondolhatnánk.

#### 4.2.2. A megkérdezettek mindennapi banki szokásai

Mivel kutatásom során szeretnék legalább egy új lehetőségre fényt deríteni, illetve igazolást, vagy ellentmondást találni a hipotéziseimre, ezért megkérdeztem a kitöltőket a mindennapi szokásaikról a banki tranzakciók területén. Elsőnek azt derítettem ki, hogy az emberek milyen szolgáltatásaikat veszik igénybe a bankoknak. A hetedik ábrán erre a kérdésre kapott válasz van megjelenítve.



7. Ábra. Mindennapjai során milyen banki tranzakciókat hajts végre? (n=107)

Jól látható, hogy a megkérdezettek nagyrésze (majd 96%-a) hajt végre bankkártyás fizetéseket a mindennapjaik során. Ezt követi a sorban az átutalás belföldre, majd a dobogó harmadik helyén a pénzfelvétel végzett. Értelmszerűen, mivel ezek a leginkább használt módszerek, első sorban ezeknek a használata során lenne érdemes biometrikus azonosítást alkalmazni, hiszen ezzel tudnánk a legtöbbet gyorsítani, egyszerűsíteni a banki tranzakciók során.

A szolgáltatás mikéntje mellett, azt is szükséges tudni, hogy ezeket milyen rendszerességgel hajtják végre a bankok ügyfelei. Mivel konkrét számokat, értékeket értelmetlen lett volna megkérdezni, ezért a válaszadási lehetőségeket időintervallumokra bontottam. Erre a kérdésre az alábbi válaszok születtek eredményként.

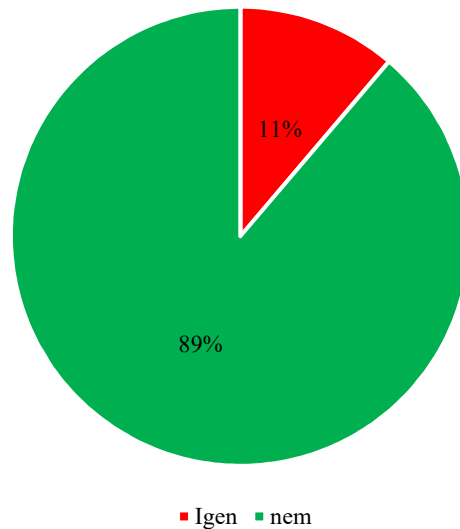
Ahogy a kettes számú táblázat is mutatja, az emberek több mint fele az első két gyakorisági változóra szavazott. Ami emellett a mutató mellett még meggyőző lehet az az, hogy igen kicsi az a százalék a válaszadók között, aki ritkábban hajt végre tranzakciókat heti 1-2 alkalomnál. Személyes véleményem szerint, ami 3-4 naponta történik, az már erős szokásnak mondható, így bizalommal jelenthetem ki, hogy az emberek szokásai közé tartozik a banki tranzakciók végrehajtása. Ha ilyen rendszerességi szinten hajtják végre az emberek ezeket a tranzakciókat, akkor sok időt tudnának spórolni a mindennapjaikban egy gyorsabb módszer használatával.

<b>Végrehajtás gyakorisága</b>	<b>Opciót választottak száma</b>	<b>Az összeshez viszonyított arány (%)</b>
Napi rendszerességgel	41	38,3
Hetente 3-5 alkalommal	35	33,6
Hetente 1-2 alkalommal	17	15,9
1-2 hetente	5	4,7
Havonta 2-3 alkalommal	7	6,5
Ritkábban	1	0,9
Összesen:	107	100

2. Táblázat. Milyen gyakran hajt végre banki tranzakciókat?

#### 4.2.3. Azonosítási módszerek biztonsága

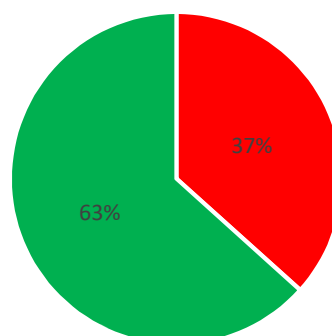
Az azonosítás során az elsődleges szempont mindenkinek az, hogy minél biztonságosabb legyen. Ezután következik csak a gyorsaság és a praktikum. Ezért is foglalkoztam kutatásom során több kérdésen keresztül a jelenlegi, illetve a biometrikus azonosítási módszerek megbízhatóságával, védelmi képességeivel. Annak az érdekében, hogy ezt a témát tovább fejtegethessem, illetve a téma által felvetett kérdésre választ kaphassak először arra voltam kíváncsi, hogy a megkérdezettek mekkora része volt már banki visszaélés áldozata. Ez a szám az én esetemben 11% volt, ami jól látszik az alábbi, nyolcadik ábrán.



8. Ábra. Volt-e már banki visszaélés áldozata? (n=107)

Mivel ez az adat magában nem mérvadó, ezért a következő kérdésem arra irányult, hogy a szerencsétlen esetben, mégis milyen módon sikerült kijátszani harmadik félnek a megkérdezett biztonságát. Erre a kérdésemre meglehetősen egyértelmű válasz született, hiszen a tizenhárom megkárosított közül a visszaélés idején mindannyian valamilyen hagyományos védelmet használtak.

Ugyan valószínűsíthetjük, hogy a megkérdezettek nagyrésze nem banki szakember, azonban ennek ellenére személyes véleményem szerint erős meglátásuk lehet arra, hogy a károkozás megelőzhető lett volna, ha biometrikus azonosítást használnak a hagyományos helyett. Ennek a feltételezésemnek eleget téve fogalmaztam meg a következő kérdésemet, aminek eredményét az alábbi ábra prezentálja[9].



9.Ábra. Mit gondol, megelőzhető lett volna az eset, ha biometrikus adattal védi magát? (n=107)

Ahogy jól látható, a károsított felek 63%-a szerint megelőzhető lett volna a káreset, ha más technológiát alkalmaznak. Ebből az a következtetés vonható le, hogy több esetben is a biometrikus azonosítás nagyobb biztonságot nyújt, mint hagyományos társai. Legalább is az esetek kétharmadában nagyobb biztonságot nyújthatott volna a megkérdezettek elmondása, személyes véleménye szerint.

A közvetetten a témára vonatkozó kérdések mellett, egy közvetlen kérdést is feltettem, ami azt célozta kideríteni, hogy a közvélemény szerint mennyire is biztonságos a biometrikus azonosítás. Mivel a kérdés, illetve a válaszadási lehetőségek sem voltak alrendszeres leosztásban vizsgálva, ezért csak egy távolabbi átfogó képet kapunk a módszerekről összefoglalva (gondolok itt az ujjlenyomat szkennelés, arcfelismerés, retina szkennelés stb. módszerekre). Ezeket az adatokat az alábbi táblázatban[3] láthatjuk a biztonság mértéke szerint növekvő sorrendbe rendezve. Az egyes a semennyire sem biztonságos, az ötös a nagyon biztonságos.

<b>Mennyire tartja biztonságosnak a biometrikus azonosítást?</b>	<b>A válaszadók százalékos eloszlása:</b>
1	3,7 %
2	1,9 %
3	21,5 %
4	36,4 %
5	35,5 %

3. Táblázat. Mennyire tartja biztonságosnak a biometrikus azonosítást? (n=107)

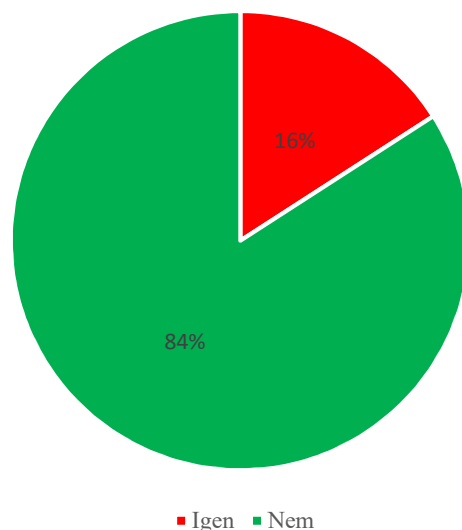
Mint leolvasható a válaszok legnagyobb hányada a felső 40%-ba esik. Ez a százalék kiteszi az összes válasz 71,9%-át. Ezt követi sorban a hármas számú választás, ami a közepesen biztonságos, kicsit annak is tartom, de nem is választ hivatott képviseltetni. Erre a válaszadók 21,5%-a szavazott. A semennyire sem biztonságos, illetve a kicsit biztonságos opciók mérhetően elmaradtak az eddigiektől, e kettőre összesen az emberek 5,6%-a voksolt. A sokaság módusza a négyes opció volt, ami azt jelenti, hogy ezt az értéket választották a leggyakrabban. A medián, azaz a középső is ugyanaz a válaszárték

lett. Így statisztikailag is igazolást nyert az állítás, hogy az emberek biztonságosnak tartják a biometrikus azonosítást. Kutatásom során az első hipotézisem az alábbi volt: „Feltételezhető, hogy a biometrikus azonosítási módszerek hatékonyabbak a banki tranzakciók során alkalmazott "hagyományos" azonosítási módszerekkel szemben.” Ez az alfejezet kapcsolódik ehhez a hipotézisemhez, hiszen a hatékonyság nagy részét teszi ki az azonosítás során a biztonsági faktor. Mivel a 0. fejezetben alátámasztottam, hogy a kutatott módszerek biztonságosabbnak tekinthetők, mind hagyományos társak, ezért a hipotézis erről a végről megerősítést nyert.

#### 4.2.4. Azonosítási módszerek megbízhatósága

Amellett, hogy megvédenek minket a nemkívánatos belépésektől, azonosításoktól, az is egy fontos szempont egy ilyen folyamat során, hogy megbízható legyen. Mivel az ember is része ennek a bizonyos folyamatnak, ezért az ő mulasztását, hibáját is figyelembe kell vennünk, ha ilyen tényezőt szeretnénk megvizsgálni. Kutatásom során mind a hagyományos, mind a biometrikus azonosítással kapcsolatban tettem fel olyan kérdéseket, amik a módszer hatékonyságára utalnak. A válaszok statisztikáit kielemezve egy egész jó képet kaphatunk arról, hogy egymáshoz viszonyítva miként is áll a két módszer.

Elsőnek a biometrikus rendszert vizsgáltam meg, amelynek az eredménye az alábbi ábrán jelenik meg [10].



10. Ábra. Előfordult már Önnel, hogy a tranzakciója a biometrikus rendszer működési hibája miatt nem valósult meg? (n=107)

Mint látható, összesen a válaszadók 16% tapasztalt már tranzakciói során olyat, hogy nem tudott fizetni a biometrikai rendszer hibája miatt. Ha ezt összevetjük azzal, hogy a kitöltők több mint 88% hetente több alkalommal végez tranzakciókat, akkor ez egy meglehetősen jó aránynak mondható. Ezzel szemben kiválasztottam egyet a hagyományos módszerek közül is, mégpedig a PIN-kóddal történő azonosítást. Itt már az kitöltők 49,5%-a adott igenleges választ arra a kérdésre, hogy már felejtette-e el a kódját, és emiatt hiúsult meg már tranzakciója. Ez 38,3%-ban magasabb arányt azoknál, akik biometrikus azonosítást használnak. Ezek alapján a számok alapján biztosan kijelenthető, hogy a biometrikus azonosítási rendszerek a mindennapok során a felmérésemre alapozva megbízhatóbbak, mint hagyományos társaik. A negyedik számú táblázattal is ezt a kijelentésemet kívánom alátámasztani.

Az azonosítási módszer:	Folyamat közbeni hibák:
PIN-kódos azonosítás	53
Biometrikus azonosítás	17

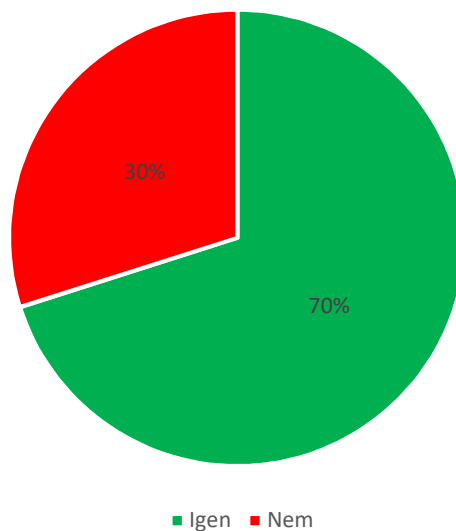
4. Táblázat. Azonosítási hibák mennyiségének összehasonlítása.

Az előző alfejezetben már egy oldalról alátámasztottam az egyes számú hipotézisemet. A hatékonyság másik felét a biztonság mellett a megbízhatóság teszi ki. A tényt, hogy a biometrikus azonosítási módszerek hatékonyabbak, mint hagyományos társaik, a mostani alfejezetben igazoltam. Ezzel az általam első számmal jelölt hipotézist sikeresen igazoltam az empirikus kutatásom során.

#### 4.2.5. Biometrikus módszerek praktikuma a hétköznapiakban

Amellett, hogy egy rendszernek megvizsgáltuk a biztonsági tényezőit, majd a megbízhatósági tényezőit is, ügyfél szempontból nézve mindenképpen fontos azt is megtekinteni, hogy mennyire praktikus az adott módszer. Kutatásom során erre a kérdésre is szerettem volna választ kapni, így ilyen irányú megcélzó kérdéseket is tettem fel.

Ahogy az a tizenegyes számú ábrán is remekül látható, a kitöltők hetven százaléka úgy gondolkodik, hogy a mindennapok során praktikusabb lenne biometrikus azonosítást használni, mint a jelenleg is életben lévő, hagyományos módszereket. Ennek több oka is lehet, csak hogy néhányat említsek: gyorsaság, biztonság, kényelem.

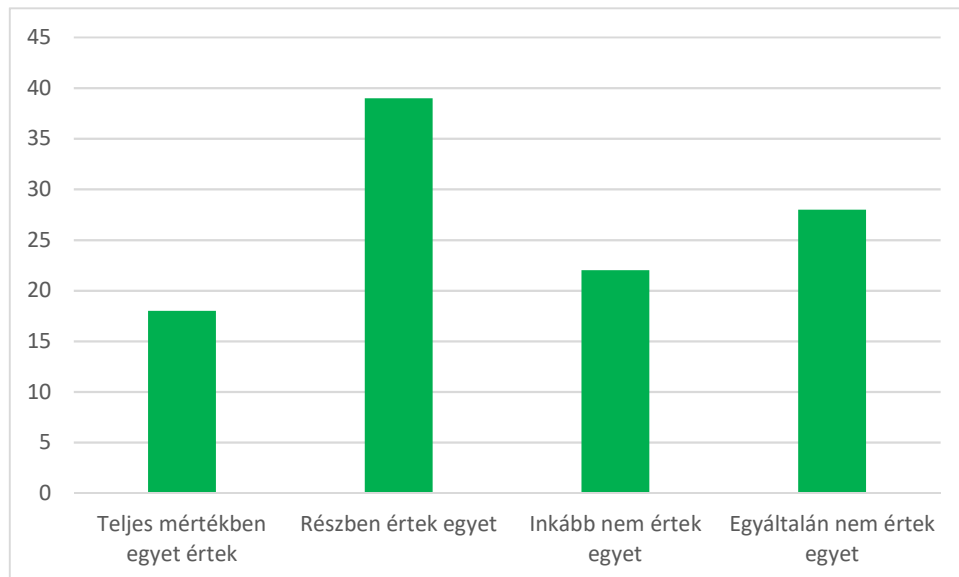


11. Ábra. Ön szerint a hétköznapiakban praktikusabb lenne biometrikus azonosítást használni, mint hagyományosat? (n=107)

#### 4.2.6. Emberek bizalma a hitelintézetek felé

Egy újfajta módszer bevezetésénél nem elegendő az, ha maga a módszer kiemelkedően működik. Szükséges elnyerni az ügyfelek bizalmát is ahhoz, hogy az profitábilis lehessen hosszú távon mind a bankok, mind a felhasználók számára. Kutatásom egyik kérdésében így arra voltam kíváncsi, ha a megszokott módszereket kivezetnék az azonosítási folyamatok közül, és újak lépnének a helyükbe, vajon meginogna-e a bizalom az intézetek felé.

Ahogy a tizenkettedik ábra is mutatja, a kitöltők 36%-a részben ért egyet, míg 17% teljesen egyet ért azzal a ténnyel, hogy a kérdésben felvetett esetben csökkenne a bizalmuk a bankok felé. Ugyan a maradék 47%-részben, vagy nem ért egyet, és feltételezhető, hogy részükről lenne nyitottság és bizalom az új módszerek felé, azonban még ha nem is sokkal, de a negatív irányba billen a mérleg nyelve ez esetben. A hármas számú hipotézisem is erre a témára épült. Mint korábban említettem az emberek egy része válaszaival alátámasztaná a hipotézist, ám sajnos ez a szám egyelőre alacsonyabb, mint az a rész, akik a felvetés ellen adták le válaszaikat. Így a hármas számú hipotézis megcáfolásra került a kutatásom során.



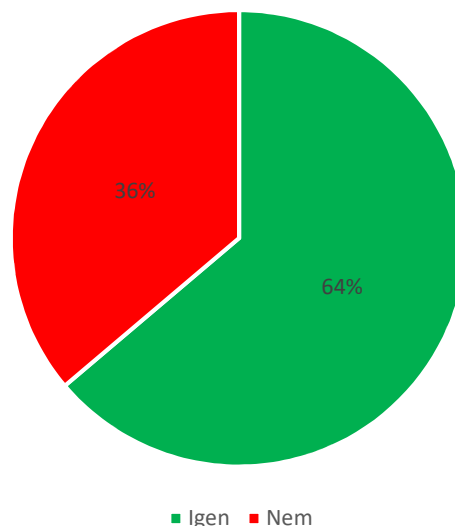
12. Ábra. Ha a bankja kivezetné a hagyományos azonosítási módszereket, és biometrikusra cserélné azokat, Önnek csökkenne a bizalma feléjük?(n=107)

## 5. KIAKNÁZATLAN LEHETŐSÉGEK

Bár úgy gondolom egyre nagyobb és nagyobb térnyerése van ennek az új technológiának, de további hatalmas terek állnak rendelkezésre, amit be tudna tölteni sikerei növeléséhez. Ebben a fejezetben ezeket a lehetőségeket szeretném bemutatni, illetve egy megoldási tervvel előállni egyes esetekben.

### 5.1. Népszerűsítés

Elsőre furán hangozhat ez a megközelítés, mivel nem egy adott módszert építünk be egy új folyamatba, vagy esetlegesen gondolunk tovább, hanem a már meglévő módszereket kívánjuk népszerűsíteni. Ezt a gondolatot a[4.] fejezetben boncolgatott empirikus kutatásaim eredményére alapozom. Jól látható az alábbi ábrán[13], hogy az emberek egy része nem is ismeri a biometrikus azonosítási módszereket.



13. Ábra. Ön ismeri a biometrikus azonosítást?(n=107)

Ahogy a kördiagrammunk is prezentálja, a válaszadók 36%-a nem ismeri ezeket a módszereket. Ha ezeket az embereket is el tudnák érni a bankok, azzal további felhasználókat tudnának megmozgatni, amivel mind a felhasználók biztonságát, mind az általuk tapasztalt felhasználói élményt javítani tudnák. Egy további kérdés során arra voltam kíváncsi, hogy akik ismerik a biometrikus azonosítási módszereket, ők melyeket

ismerik, használják a mindennapok során. Az alábbi ötödik táblázatban azt foglalom össze, hogy miként is mutatkozik meg az emberek ismerete az előbb említett területeken.

<b>Módszer megnevezése:</b>	<b>Ennyien ismerik:</b>
Ujjlenyomat szkennelés	102
Arcfelismerés	78
Retina szkennelés	23
Szemírisz szkennelés	5
Kézírás-analízis	15
Vénás felismerés	5
Hangfelismerés	22

5. Táblázat. Az alábbi azonosítási módszerek közül melyikkel találkozott már?

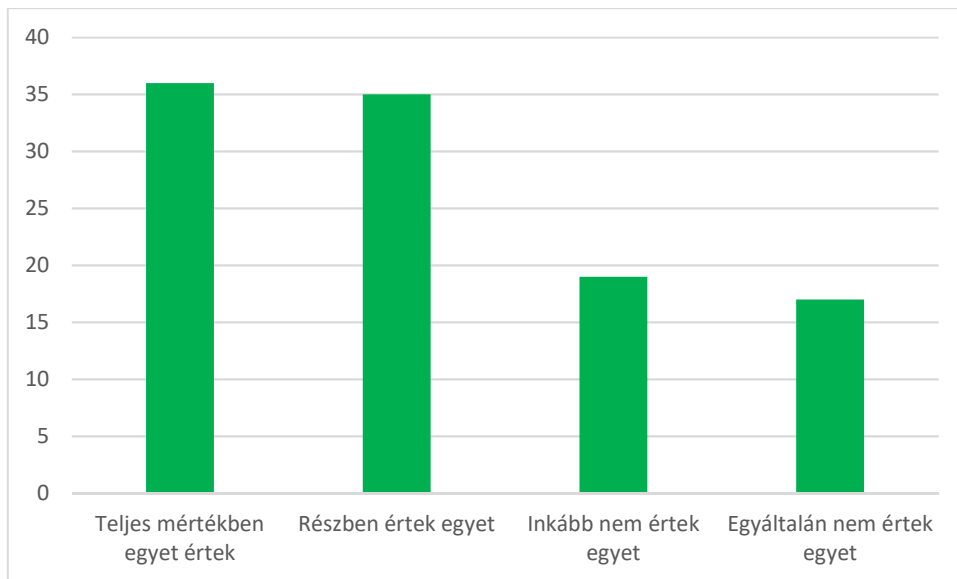
Mint az látható, magasan vezet az ujjlenyomat szkennelés, amivel a válaszadók 95,3%-a találkozott már. Ezt követi sorrendben az arcfelismerés, majd a retina szkennelés. A többi módszert, mint például a vénás felismerés vagy a kézírás analízis alig párán ismerték. Ezekből az értékekből több dologra is tudunk következtetni:

1. Az emberek tudása felszínes ilyen téren. Ezt a megállapításomat arra alapozom, hogy a tizedik ábrán jól látható, a megkérdezettek 36%-vallotta azt, hogy nem ismeri a biometrikus azonosítást. Ezzel szemben az ötös táblázat jól mutatja, hogy több mint 95% találkozott már ujjlenyomat olvasással, ami beletartozik a biometrikus azonosítás módszerei közé. Ha a bankok ismertetnék ezeket a megoldásokat ügyfeleikkel, valamiféle tájékoztatást nyújtanának róluk, akkor talán javulásnak indulna ez a mérőszám is.
2. Amellett, hogy magát a módszerek összességét és tudatos használatát is népszerűsíteni kellene az ezeket nem ismerők körében, a létező azonosítási módok tárházát is tudatosítani lehetne mind az előző, mind az egyes módszereket már aktívan használók körében. Erre azért lenne szükség, mivel az ötödik táblázatban

megfigyelhető, egy igen nagy eltérés a különböző technológiák ismeretsége között.

A kettes pontja a felsorolásnak azon felül, hogy feltárja a tényt, miszerint nagy a szórás a módszerek között, az általam kettes számúként megjelölt hipotézist is sikeresen megerősíti. A megerősített hipotézis a következőt mondja ki: „Feltételezhető, hogy Magyarországon az alkalmazott biometrikus azonosítási lehetőségek közül legelterjedtebb az ujjlenyomattal történő azonosítás.” A felsorolás adott pontján felül az ötödik táblázat is segítséget nyújt az említett hipotézis bebizonyításában. Míg az ujjlenyomatfelismerést a kitöltők 95,3%-a ismerte, addig a második helyen álló arcfelismerés módszert csak 72,9%. Ahogy azt a kettes számú táblázat is mutatja, az összes kitöltő Magyarország területén él, így a hipotézis ezen része is alá lett támasztva a kutatásom során.

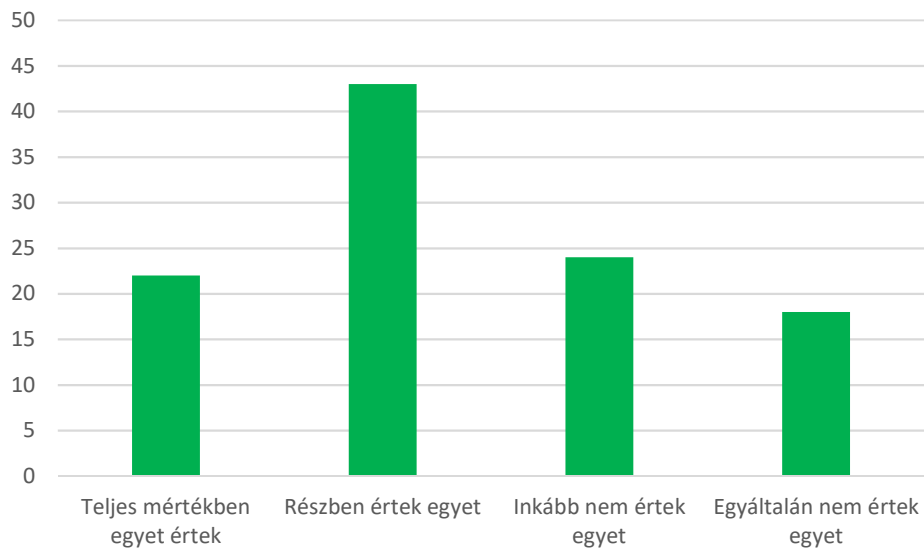
A tudatlanság mellett, az emberek hozzáállását is lehetne javítani, hiszen olyan személyek is vannak, akik ugyan tudnak ezekről a lehetőségekről, de bizalmi vagy egyéb okok miatt nem szívesen élnek a használatukkal. Ennek a kérdésnek a megválaszolására, kibontására kutatásomban egy skálázható válaszokkal rendelkező kérdéscrát hoztam létre. A kérdéssor első kérdése arra irányult, hogy szívesen adják-e meg az ügyfelek a bankjaik számára a biometrikus adataikat. Erre a kérdésre a válaszok az alábbi, tizennégyes ábrán látható módon oszlottak el.



14. Ábra. Nem szívesen adom meg biometrikus adataimat a bankom számára. (n=107)

Ahogy az ábrán is reprezentálva van, a megkérdezett ügyfelek egyharmada, egyáltalán nem szívesen adná vagy adja meg biometrikus adatait. Enélkül a lépés nélkül pedig nyilvánvalóan nem lehet biometrikus azonosítást használni. További harminckét százalék részben nem ért egyet, vagyis ők sem adnák meg ezeket a bizalmas adatokat a bankjaik felé. Összesen tizenhat százalék volt az, akik szívesen adják meg ezeket az adatokat. Ez a szám meglehetősen alacsony. Annak, hogy ilyen bizalmatlanok az emberek, több oka is lehet. Megkérdezésem alapján az emberek bizonyos rétegéi tartanak attól, hogy ezeket az adataikat ellopják. A félelmük valamilyen szinten megalapozott lehet, hiszen a biometrikus adatok nagyon bizalmas dolgok. Ellopásuk esetén ugyanis a megkárosított fél nem tudja ezeket megváltoztatni, cserélni, vagy kitörölni. Innentől kezdve, ha például valakinek megszerzik az arcának szkennelt képét, és ezt tudják reprodukálni egy háromdimenziós modellben, a szkennerek egy része becsapható már ezzel a képpel. A bankok ezért is fordítanak kiemelt figyelmet ezekre a biztonsági kérdésekre.

Ebben az esetben is az figyelhető meg a tizenötödik ábrán, hogy a megkérdezettek több mint hatvan százaléka tart attól, hogy ellopják majd felhasználják számukra káros módon a bankjaik részére megadott biometrikus adatokat. Ha a bankok tudnának ezeken a mutatókon javítani, és megnyerni az emberek bizalmát a mindennapi dolgok során, akkor mindenféle technikai fejlesztés, vagy nagy újítás nélkül tudnának fejlődni. Ehhez a meglévő rendszerek is elegendők, és csak a rendszeres karbantartásukkal kellene foglalkozni.



15. Ábra. Tartok attól, hogy biometrikus adataimat ellopják és felhasználják ellenem. (n=107)

## 5.2. Viselkedés alapú azonosítás

Az eddigi kutatásom során vizsgált biometrikus adatok mindegyike valamilyen passzív azonosítási folyamatok voltak. Ezalatt az értendő, hogy az azonosítási folyamat során elég volt egyszer szkennelni valamely egyedi azonosítónkat, esetleg egy két lépcsős megoldást használatba venni, de minden esetben egy felvétel készült, amit később összevetettünk egy másik felvétellel, és egyezés esetén mondtuk sikeresnek az azonosítást. A viselkedés alapú azonosítás erőssége abból fakad, hogy az eddig felsorolt folyamatokkal ellentétben ez egy aktív, a háttérben futó azonosítási folyamat, amely folyamatosan gyűjti az adatokat, ezáltal lehetetlen lemásolni, vagy helyettesíteni a felhasználó egyedi azonosítási kódját. Tehát ez nem egy azonosítási esemény, hanem annál inkább egy hosszan tartó folyamat, ami a felhasználó bármiféle megzavarása nélkül végzi működését.

Hagyományos társaival, például a PIN-kóddal szemben egy hatalmas előny az, hogy ezt a fajta adatot nem tudjuk sem elfelejteni, sem elhagyni, illetve ellopni sem tudják tőlünk.

Hogy milyen adatokat is vizsgálunk a folyamat során? Az alábbi felsorolás választ adhat erre a kérdésünkre:

- Billentyűleütések dinamikáját,
- Az érintőképernyő használatának dinamikáját,
- A szem mozgását,
- A felhasználó járását,
- A felhasználó testének gesztusait,
- Egyéb tényezőket.

A billentyűzet használati szokások vizsgálatánál azonosítjuk, megfigyeljük az írás sebességét, a leütések hosszát, az eltelt időt a leütések között, esetlegesen ha az eszköz kompatibilis akkor a leütések erősségét is. Elsősorban amikor ez a módszer megjelent a fizikai billentyűzettel rendelkező készülékeken alkalmazták. Az érintőképernyő megjelenésével azonban új perspektívákkal bővült a látókör, ugyanis amikor írunk a telefonunkon a példának okáért, nem csak a képernyő érzékeli, hogy éppen melyik betűt érintjük meg a képernyőn, de a készülékben elhelyezett gyorsulásmérő, és giroszkóp is folyamatosan adatokat rögzítenek. A billentyűzet mellett az egér mozgását is naplózhatják ezek a szoftverek, így még szélesebb adatbázist állíthatnak fel a pontosság növelésének érdekében. A módszernek egy hátránya lehet, hogy a telefonok esetében különböző élethelyzetekben különböző módon használjuk a billentyűzetét az eszköznek. Gondolok itt arra, hogy máshogy írunk amikor fekszünk, máshogy amikor sétálás közben vagyunk, vagy szintén máshogy, ha mondjuk ülünk a metróban és az rázkódik velünk együtt. Ennek az elkerüléséhez olyan algoritmus szükséges, ami képes különbséget tenni több élethelyzet között, és ezeket a helyükön tudja kezelni. (Liang, Samtani, Guo, & Yu, 2019)

Az érintőképernyővel rendelkező eszközökön, legyen ez egy okostelefon vagy akár tablet, nem csak a billentyű leütéseket tudja naplózni, figyelni, hanem az interakció teljes ideje alatt képes adatokat gyűjteni ahhoz, hogy azonosítani tudja a felhasználót. Figyeli az érintés erősségét, az ujj húzásának gyorsaságát, illetve azt is, hogy milyen módon

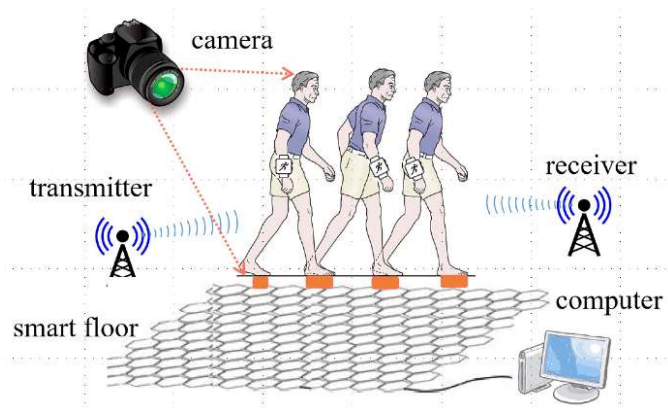
tartjuk kezünkben a telefont. Mivel ezek a műveletek eltérnek akkor, ha különböző alkalmazásokat használunk, ezért olyan algoritmust kell megalkotni, ami alkalmazásomként képes elkülöníteni a felhasználó viselkedési adatait. A folyamat akkor kezdődik meg amikor a felhasználó feloldja a telefonját, és akkor fejeződik be, amikor lezárja azt. A két interakció között a szoftver dolgozik a háttérben úgy, hogy közben a felhasználót nem zavarja a tevékenysége során. (Liang, Samtani, Guo, & Yu, 2019)

Az agy és a szemek mozgásáért felelős izmok kapcsolata minden ember esetében egyedi, így ezek alapján a mozgások alapján is lehetőség van azonosítani az egyént. Ilyen mozgás lehet például egy pislogás vagy éppen a tekintetünk vándorlása. Mivel ez a mozgás is velünk együtt fejlődött ki, ezért szinte lehetetlen lemásolni, így a biztonsága a módszernek igen magasnak mondható. Alapvetően az azonosítási folyamat két kategóriára bontható: vannak, amik a szem dinamikai mozgását figyelik, például az előbb említett pislogás vagy tekintet követés, és vannak, amik a szem statikus mozgásait figyelik. Ilyen mozgás lehet például a pupilla szűkülés különböző ingerekre. Annak ellenére, hogy a módszer nagyon biztonságos és praktikus, nem ez lehet a legjobb megoldás a mindennapokban. Ez pedig nem másnak tudható be, mint annak, hogy a szem ilyen mértékű vizsgálatához igen jó minőségű, nagy felbontású kamerára van szükség, amit általában a legtöbb okostelefon nem biztosít. A leggyakoribb esetekben, amikor ilyen technológiát alkalmaznak külső kamerát használnak, ami direkt erre a célra lett kifejlesztve. (Liang, Samtani, Guo, & Yu, 2019)

A mozgáskultúrán alapuló azonosítás egy olyan modern technológia, ami képes a felhasználót annak járása, és testének mozgáskultúrája alapján azonosítani. Az ilyen típusú azonosítást az alábbi eszközök segítségével lehet elvégezni: kamerák, padlóba épített szenzorok, és a testen viselt szenzorok. Ilyen szenzorként funkcionálhat akár egy okosóra is.

A folyamat alapvetően a kamerák által rögzített vizuális anyagra épít, ebből állít össze sablonokat a különböző járási mintákra. A többi eszköz kiegészítő feladatokat lát el, ezekkel javítják a folyamat pontosságát, illetve növelik annak biztonságát. A padlóba épített szenzorok ugyan nagy pontossággal tudnak dolgozni, és kiemelkedően érzékelik a nyomásváltozásokat, ezáltal alkotnak pontosabb képet, mint a kamera, de alkalmazásuk

nagyon költséges, és csak limitált terekben és nem utolsó sorban limitált számú embereken alkalmazható. Így például egy nagyobb bankfiókban valószínűsíthetőleg gyorsan megbukna ez a módszer. A testre szerelhető eszközök ugyan laboratóriumi körülmények között jól teljesítettek, azonban egy bankban ez nagyon nehezen kivitelezhető. Egy ügyfél sem szeretne karpereceket felvenni, mielőtt elintézné ügyeit, annak érdekében, hogy azonosítva lehessen. Az okosóra egy jó alternatíva lehetne, azonban egyrészt sokan nem rendelkeznek ilyen eszközzel, vagy szimplán csak nem engednék meg a bankoknak, hogy a helységbe lépéskor rácsatlakozzanak azokra. A sétálás mellett a testmozgásunk, a különböző gesztusaink is szolgálhatnak azonosításunk alapjaként. Ilyen gesztusok lehetnek például kézjeleink. Ezzel a probléma annyi, hogy ezeket a gesztusokat általában nem használjuk, szükség van valamire, ami kiváltja őket. Ilyen lehet akár egy párbeszéd, egy hirtelen történés, egy külső inger a környezetünktől vagy akár valamilyen zene, amit hallgatunk. Akármilyen jól működhetnek is ezekre a mozgásokra alapuló azonosítási módszerek, egy banki környezetben ilyen formában nem lehetne őket kivitelezni. Azonban egy másik gesztusunk, a kézmozgás gesztusa az írással egybekötve már egy fokkal közelebb áll ahhoz, hogy hatékony módszert alkosson a mindennapokban. Akár a levegőbe írva, akár egy digitális érzékelő padra vetve a nevünket, nem csak az írásképünk tér el egyénileg, hanem az is, hogy közben milyen gesztusokat végzünk kezeinkkel.



16. Ábra. A sétálás alapján való azonosítás folyamata.

Forrás: (Liang, Samtani, Guo, & Yu, 2019)

Vannak egészen fura és szürreális lehetőségek is arra, hogy azonosítsanak egy személyt. Ilyen metódus például valakinek az azonosítása az egyén rágása alapján. Ugyanis rágás során az állkapcsunkat mozgató izmok feszültsége máshogy változik. Ezen felül eltérő hangokat is adunk ki a rágás folyamata közben. A BiLock nevezetű prototípus rendszer a mobiltelefonokba épített mikrofont használta arra, hogy rögzítse az állkapcsunk hangjait, és ez alapján döntse el, hogy vajon a felhasználó jogosult-e a belépésre vagy sem. Előnye, hogy nem igényel bármilyen plusz eszközt a telefonunkon kívül. Sajnos a módszernek több hátránya van. Az egyik ilyen, hogy nagyon érzékeny a környezetre, mivel a rögzíteni kívánt hangok meglehetősen halkak, illetve minimális eltérések is lehetnek a két minta között. Ha a környezet megfelelő, még akkor is meglehetősen közel, 10-15 centire kell tartani a készüléket a hangok forrásától. Ezenkívül a légzést is felhasználják a felhasználó azonosításához, jellemzően a légzés által okozott finom rezgés leírásával. Például a BreathPrint mély tanulási modelleket alkalmaz a légzés által okozott akusztikai jellemzők hatékony megfigyeléséhez a felhasználó azonosítása érdekében az erőforrásokban korlátozott eszközökön. (Liang, Samtani, Guo, & Yu, 2019)

Ahogy a hatodik táblázatban is olvasható, megvan mindegyik folyamatnak a maga előnye és hátránya. Ami talán kiemelkedhet más biometrikus azonosítási módszerekkel szemben az az, hogy a háttérben történnek ezek a folyamatok, folyamatosan történnek, így ezáltal nem zavarják meg a felhasználót még egy kis időre sem. A technika hazánkban még közel sem kiforrott, de nagy potenciál lehet benne. A különböző módszerek ötvözésével akár a banki rendszerekbe is építhetők lennének, ami egy új szintre emelhetné a hétköznapi banki szokásainkat.

Kategória	Jel	Leírás	Sebezhetőség	Korlátozottság	Diszkréció	Magánszféra
Billentyű leütések	Gépelés	Írás megfigyelése az adott periférián	✓	✗	✗	✓
Érintési műveletek	Érintőképernyőn keresztül	Az ujj mozgását figyeljük a képernyőn	✓	✗	✗	✓
A szem mozgása	Biometrikus jel	Biometrikus jelek, a szem mozgása által generálva	✗	✗	✓	✓
	Időbeli változások	A szem mozgásának dinamikája	✓	✗	✓	✓
Sétálás analízálása	Kamera	Videó készítése a járás stílusáról	✓	✗	✗	✓
	Padlóba épített érzékelő	Mozgási minták, nyomás minták alapján	✗	✗	✗	✗
	Viselhető szenzorok	Mozgás minták lekövetése	✗	✗	✓	✓
Testjelek	Kar mozgása	Mozgási minták, amik a kar mozgatásával keletkeznek	✗	✗	✓	✓
	Fej mozgása	Mozgási minták, amik a fej mozgatásával keletkeznek	✗	✗	✗	✓
	Száj mozgása	Mozgási minták, amik a száj mozgatásával keletkeznek	✗	✗	✗	✓
	Kézírás	A kezünk írás közbeni mozgásának figyelése	✗	✓	✓	✓
Hangok elemzése	Rágás hangjai	A fogak, izmok egyedi hangjai	✓	✓	✓	✓
	Testünk hangjai	Egyedi hangok testünkben pl.: légzés, nevetés stb.	✗	✗	✓	✓

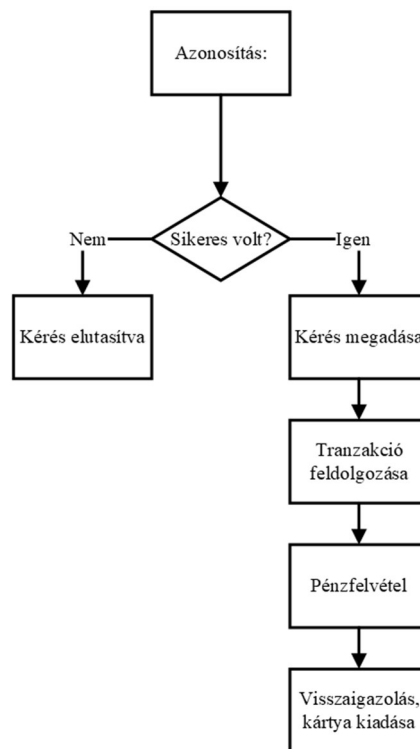
6.Táblázat. A viselkedés alapú azonosítás összefoglalása

## 6. PROBLÉMA FELVETÉSE

Mint az empirikus kutatásom során is kiderült, az emberek három leggyakrabban végzett banki tevékenységei között van a készpénzes pénzfelvétel banki ATM-ből. Ebbe a csoportba jómagam is beletartozom, ezért saját tapasztalás alapján is tudok nyilatkozni a témában. Ezen alapgondolatok alapján vettem fel az első problémát dolgozatomban: Készpénzfelvételi lehetőségek határai hazánkban, az ATM-ek használata során.

### 6.1. Jelenlegi helyzet a probléma területén

Magyarországon jelenleg közel ötezer darab készpénzfelvételre képes ATM működik. Ezek legnagyobb százaléka mind ugyanazon az elven hajt végre tranzakciókat. Az alábbi tizenhetedik számú ábra egy átlagos készpénzfelvételi folyamatot hivatott bemutatni.



17. Ábra. ATM-ből történő készpénzfelvétel folyamata.

Az első lépés, mint jól látható itt is az azonosítás. Ennek két lépcsője van ebben az esetben. Elsőként az ügyfél behelyezi bankkártyáját az automata nyílásába. Ezután a gép kéri a kártyához tartozó négy számjegyből álló PIN-kódot. Probléma felvetésében ez az a lépés, amit részletesebben szeretnék kielemezni, és egy modernebb, gyorsabb, és

biztonságosabb módszerrel helyettesíteni azt. Az azonosításnak két kimenetele lehet, vagy elutasítja a kérést a rendszer rossz PIN-kód esetén, vagy elfogadja azt, és ezen esetben folytatódhat a tranzakció. Ezt követően megadja az ügyfél, hogy mekkora összegben szeretne készpénzt felvenni a gépből. Miután elküldi a kérelmet a rendszer feldolgozza azt, majd kiadja a kért összeget. Kivéve az összeget, véget vetünk a tranzakciónak, a gép a folyamat végeztével nyomtat egy bizonylatot, majd visszaadja a kártyánkat is.

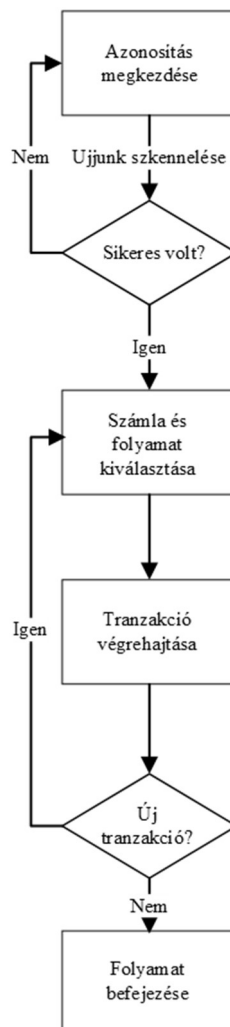
## **6.2. Biometrikus azonosítás bevezetése a készpénzfelvételi folyamatokba**

Saját javaslatom szerint, a kártyás azonosítás helyett, lehetne használni az emberek ujjlenyomatát is. Ezalatt nem csak a PIN-kód lecserélését tudnám javasolni a biometrikai adatokra, hanem magát a fizikai bankkártyát is elhagynám a képből. Ekkor annyiban változna az azonosítás folyamat, hogy az ügyfél adatának beolvasása egy folyamatban történne meg az azonosítással. Hogy ez hogyan lehetne kivitelezhető? A jelenlegi azonosítás során amikor behelyezzük a kártyánkat a gép az azon elhelyezett mágnescsíkot olvassa le. Ebben a mágnescsíkban vannak eltárolva az azonosítandó személy adatai. Ilyen adatok például a tulajdonos neve és bankszámlaszáma. Ezekon az adatokon felül tárolva van a kártyához tartozó négy vagy hatjegyű kód is. A gép ezt a kódot kéri el, és ha egyezés van a kettőben, akkor azonosítja a felhasználót.

Az általam javasolt folyamat során, a terminál egyetlen input adattal dolgozna, ez pedig az ujjlenyomatunk. Miután az beszkeneltük, a rendszer elkezdi keresni az adatbázisában. Ha egyezést talál, akkor az olyan személy esetében, aki több számlával is rendelkezik megkérdezi, hogy melyik számlán, milyen tranzakciót szeretne végre hajtani. A továbbiakban, ahogyan ez a tizennyolcadik ábrán is látható, a folyamat megegyezik a napjainkban is használt folyamattal, azzal az apró eltéréssel, hogy utolsó lépésként nem szükséges kivenni a kártyát, hiszen annak már elhagytuk a használatát. Ez amellet, hogy gyorsítja is a folyamatot, még egy kockázati tényezőt is kiküszöböl. Ezalatt a tényező alatt a bankkártya gépben ragadását értem.

Egy másik megoldás lehet, ha nem csak egy biometrikus módszert vonunk be a folyamatba, hanem kettőt is. Ebben a gondolatmentetben az első azonosítási lépés lenne az ujjlenyomat, ahogyan az a tizennyolcadik ábrán is látható volt. Azonban miután

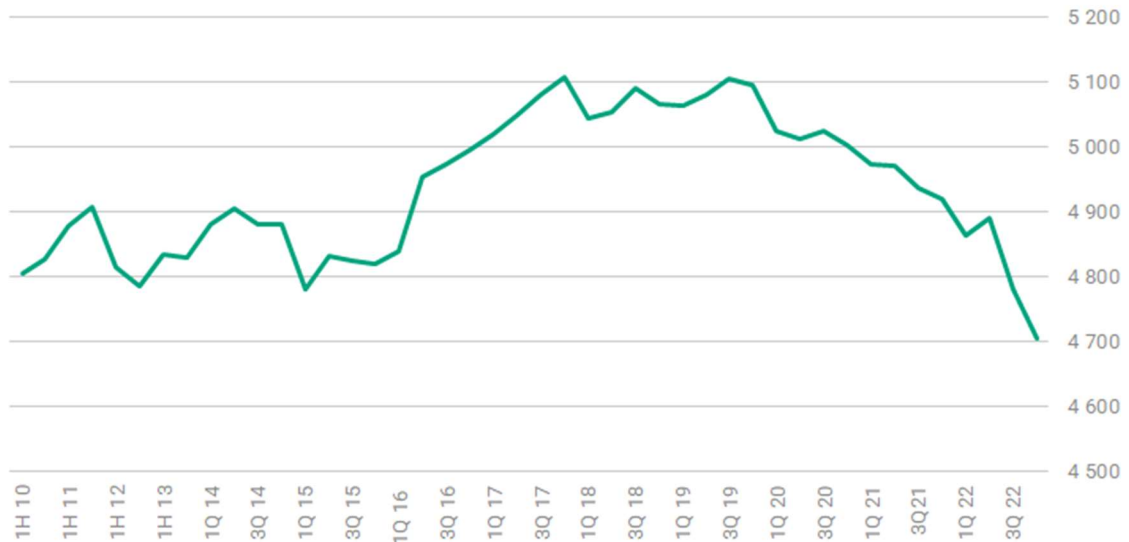
leolvasták az ujjlenyomatunkat, és a rendszer pozitívan jelzett vissza számlánk meglétéről, még szükség lenne egy második lépcsős azonosításra is. Ez az azonosítás pedig az arcunk beolvasásával történne meg. Így ugyan az első megoldási javaslattal szemben lassulna a folyamat, de a biztonság mértékét még magasabb szintre lehetne emelni ezzel. Ezt az állításmat az „Empirikus Kutatás” című fejezettel támasztom alá, ahol is már bizonyosságot kaptunk arról, hogy a banki visszaélések sokkal nagyobb részben történtek meg az emberekkel akkor, ha PIN-kódót használtak, mint akkor amikor biometrikus adattal azonosították magukat. Az ATM-ek egyébként is gyakran adnak helyszínt a banki adatok ellopásának, hiszen csak pár óvatlan pillanat, és a hátunk mögött álló személy már el is tudta lesni az általunk beírt kódot. A biometrikus adatokkal történő azonosítás során ilyen bűncselekmény nem történhet meg.



18. Ábra. Az általam javasolt folyamat ábrája.

### 6.3. Javaslatok kivitelezési tervezete

Mivel az új módszerek nem csak szoftveres frissítéseket igényelnek, ezért az automatákon fizikai, hardveres átalakításokat is kell végezni. Hazánkban annak ellenére, hogy a COVID-19 járvány idejében jelentősen csökkent az ATM-ek száma, így is több, mint 4000 üzemelő pénzkidó automata található, ahogyan az a tizenkilencedik ábrán is látható.



19. Ábra. Üzemelő ATM-ek Magyarországon.

Forrás: (Portfolio.hu, 2023)

Ezt a számot a Magyar Nemzeti Bank a járvány előtti időkre akarja visszatornászni, így a hazai hitelintézetek kötelesek létesíteni új, készpénzkidásra képes egységeket. Ez a kötelesség, akár meglepően jó lehetőség is lehet, hiszen új gépek létesítésénél nem szükséges a meglévőket átalakítani, hanem helyettük lehetséges lenne az új konstrukció beüzemelése. Mivel a lakosság a felmérésem alapján nem tudatos a biometrikai azonosítási folyamatok kapcsán, így akár ez egy jó ugródeszka is lehetne, mivel a pénzfelvétel után megtapasztalhatnák az emberek, hogy az új módszer mennyivel gyorsabb és kényelmesebb lett, mint a régi PIN-kódos társa. A pénzük pedig ugyanolyan biztonságba hozzájuk kerül a számlájukról. Ezt követően az intézetek az új pénzkidókról készült statisztikákkal tudnák népszerűsíteni a lakosság körében őket, és ha a

későbbiekben lenne rá igény, akkor elkezdhetnék a már telepített, régi módszer alapján hitelesítő gépek átkonvertálását is biometrikai ATM-é.

#### 6.4. Hátrányok

Mint minden más módszernél, itt is vannak hátrányok, és olyan tényezők, amik gátolnák a kivitelezést vagy a módszer sikerességét, profitáló képességét. A Magyar Nemzeti Bank becslése szerint a bankoknak több, mint egymilliárd forintjába kerülne a hagyományos ATM-ek telepítése is. Ha ehhez még hozzávesszük a fejlesztésnek a költségét, illetve a modernebb, újabb gépek beszerelésének, üzembehelyezésének, és karbantartásának a költségeit, ennél egy jóval jelentősebb összeggel számolhatunk. Ez köszönhető annak, hogy az ujjlenyomat olvasó mellett szükséges lenne egy jobbfelbontású kamera beszerelése is az ATM-be, hogy az ügyfél arca is felismerhető legyen.

### 7. A DOLGOZAT HIPOTÉZISEI

Munkám során három hipotézist vettem fel, amiket a kutatásommal szerettem volna igazolni, vagy elvetni. A felvetések eredményeit az alábbi, hetes számú táblázatban szeretném összefoglalni.

Hipotézis leírása	A kutatás során keletkezett eredmény
Feltételezhető, hogy a biometrikus azonosítási módszerek hatékonyabbak a banki tranzakciók során alkalmazott "hagyományos" azonosítási módszerekkel szemben.	A hipotézist megerősítettem, mivel kutatásom során eredményül azt kaptam, hogy ezeknél a módszereknél kisebb számban hiúsultak meg azonosítások.
Feltételezhető, hogy Magyarországon az alkalmazott biometrikus azonosítási lehetőségek közül legelterjedtebb az ujjlenyomattal történő azonosítás.	A hipotézist megerősítettem, mivel kutatásom során eredményül azt kaptam, hogy az ujjlenyomattal történő azonosítást 102-en, míg a második helyen álló arcfelismerést csak 78-an ismerik.
Feltételezhető, hogy a banki felhasználók körében igény lenne újfajta azonosítási módszerek bevezetésére és a bizalmuk sem csökkenne a bank irányába a mostani azonosítási rendszer leváltása esetén.	A hipotézist megcáfoltam, mivel kutatásom során eredményül azt kaptam, hogy a felhasználók nagyobb részének csökkenne a bizalma újfajta módszer bevezetése során

7. Táblázat. A hipotézisek összefoglalása.

## 8. ÖSSZEFOGLALÁS

Dolgozatom során több kérdésre és feltevésre sikerült választ kapni, illetve a feladatként meghatározott négy pontot is teljesítettem. Elméleti kutatást végeztem a napjainkban használt biometrikus azonosítási módszerek területén. A kutatásom során feltártam három módszert, amiket részletesen ismertettem. Ezek a következők voltak: ujjlenyomat szkennelés, arcfelismerés, illetve retinaszkennelés alapú azonosítás. Az elsőnek említett metódus esetében bemutattam három különböző típust: Az optikai, a kapacitív és az ultraszónikus szkennelést. A fejezetben foglalkoztam még, egy hazánkban nem ismert folyamattal is: ujjlenyomat mint bankkártya. Kiemelkedően magas biztonsággal rendelkezik, két dolognak köszönhetően. A hagyományos plasztikkártya helyett ezen módszer a biometrikus adatunkat használj, illetve különleges titkosítási folyamattal rendelkezik. A szekunder kutatás további eredményeként az arcfelismerés alapú hitelesítést, és annak a fejlődéstörténetét mutattam be. Ezen felül kitértem szerepére a mindennapi használatban is. Ezen kutatás végén, a retinaszkennelést ismertettem. Bemutattam a működést a szem anatómiájának ismertetésén keresztül.

Primer kutatásom során bebizonyítottam, hogy Magyarországon a legelterjedtebb azonosítási módszer az ujjlenyomatszkenneléses azonosítás. Megerősítést adtam dolgozatomban arról a felvetésről is, hogy a biometrikus módszerek hatékonyabban működnek a banki tranzakciók során, mint hagyományos társaik ugyan ezen a területen. Kisebb százalékban hibásodnak meg, illetve az illetéktelen hozzáférések száma is jelentősen alacsonyabb. Harmadik hipotézisem megcáfolásra került, ugyanis a kvantitatív kutatásom megmutatta, hogy az emberek többségben nem táplálnak teljes bizalmat a hitelintézetek felé. A bizalom hiánya mellett az emberek a témában való járatlanságuk miatt sem használják gyakran a biometrikus azonosítást, derült ki a feldolgozott adatokból. Ezen eredmények segítségével alapoztam meg az egyik lehetséges fejlesztési javaslatomat. Az embereknek szükségük lenne edukációra a téma területén, a hitelintézetek felől. Ezzel mind a bankok, mind a felhasználóik előrelépést tennének a mindennapi banki tranzakció végrehajtások folyamatában.

Bemutattam a viselkedés alapú azonosítást, ami hazánkban jelenleg teljesen ismeretlen. A válaszadók közül senki sem ismerte ezt a módszert, illetve a hazai bankok sem használják a tranzakcióik védelmének biztosítására. Hat lehetséges kivitelezési módját prezentáltam, amik közül mindegyik más-más területen lehetne hasznos. A gépelési szokások monitorozásával a banki alkalmazások lennének biztonságosabbá tehetővé. A szem mozgása az ATM-ből történő pénzfelvétel során hozhatna újítást, míg a test gesztusainak vizsgálata a járás megfigyelésével összekapcsolva a fizikai bankfiókokban jelenthetne előrelépést a mostani helyzethez képest.

Felvettem egy problémát, miszerint a készpénzfelvételi folyamat lassú és támadható. A folyamat fejlesztésére javasoltam egy megoldást, amiben a bankkártya helyett a biometrikus adataink alapján azonosítanának bennünket. Ezzel nem csak a folyamat sebessége növekedne, de nagyban megnőne annak biztonsága is. Kutatásom számai alapján a megkérdezettek körében tizenkét százalékkal magasabb azon kitöltők száma, akik hagyományos azonosítási módszer hibája miatt károsultak meg, mint azok, akik biometrikus adatokat használtak. A módszer implementálására egy gazdasági folyamatban találtam lehetőséget, miszerint hazánkban a Magyar Nemzeti Bank kötelezi a hitelintézeteket arra, hogy megnöveljék a készpénzfelvételre képes aktív ATM-ek számát.

## IRODALOMJEGYZÉK

- Alsolami, F. (2019). BioPay: Your fingerprint is your credit card. *International Journal of Advanced Computer Science and Applications*, 10(1), 522-524.
- Brezitska, M. (2023. Március 29). *Biometrics in Banking: Which Biometric System Ensures 100% Security*. Forrás: binariks.com: <https://binariks.com/blog/biometric-security-online-banking/>
- Farzin, H., Abrishami-Moghaddam, H., & Mohammad-Shahram, M. (2008). A Novel Retinal Identification System. In *EURASIP Journal on Advances in Signal Processing 2008* (old.: 1-10).
- Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2019). A behavioral authentication method for mobile based on browsing behaviors. *IEEE/CAA Journal of Automatica Sinica*, 7(6), 1528-1541.
- MOHANAN, V. (2021. Május 11). Interfacing R307 Optical Fingerprint Scanner with Arduino Boards for Biometric Authentication.
- NEC. (2022. Május 12). A brief history of Facial Recognition. Letöltés dátuma: 2023. November 19, forrás: <https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/>
- Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*.
- Stankevičiūtė, G. (2023. Szeptember 25). *Top 5 Use Cases of Biometrics in Banking*. Forrás: iDenfy: <https://www.idenfy.com/blog/biometrics-in-banking/>
- Ujhegyi, P. (2023). A biometria elterjedésének elemzése. *Belügyi Szemle*, 71.(8), 1463-1491. Forrás: <https://doi.org/10.38146/BSZ.2023.8.7>

Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., & Lin, D. (2023). A Review of Fingerprint Sensors: Mechanism, Characteristics,. *Micromachines*, 14(6). Forrás: <https://www.mdpi.com/journal/micromachines>

### **Elektronikus hivatkozások**

Portfolio.hu. (2023. május 19.). *Portfolio.hu*. Forrás: <https://www.portfolio.hu/>

## **TARTALMI KIVONAT**

A dolgozat a biometrikus azonosításban rejlő lehetőségeket mutatja be, illetve kutatja különböző perspektívákból. Az első részben a jelenleg hazánkban is ismert, illetve használt azonosítási módokat gyűjti össze. Ezt követően egy online felmérés segítségével az emberek banki szokásait, illetve az ezekhez tartozó biometrikai azonosítási szokásokat részletezi a kutatás. Kitér a használt módszerekre, az emberek hozzáállására, illetve a kitöltők tapasztalataira a mindennapi életben ezek kapcsán. Vizsgálja a technikák biztonságát, megbízhatóságát, praktikusságát, illetve ezekben a kategóriákban össze is hasonlítja őket mind egymással, mind a hagyományos, napjainkban még gyakran használt nem biometrikus módszerekkel is. A kutatási eredmények felhasználásával megoldást javasol a módszerek hiányosságának javítására, illetve az emberek feléjük táplált bizalmának növelésére. Emellett egy itthon nem használt, és nem is ismert módszert mutat be, amiben nagy potenciál van a jövőre tekintve abban, hogy élenjáró lehessen a biometrikus technikák területén.

## **SUMMARY**

The dissertation is about the opportunities in the field of biometric authentication during banking transactions. In the first section the biometric technologies are collected, which are used frequently in our country during this time. They are analysed from different perspectives, and compared with each other. In the next section the daily banking routine of the fillers is checked, with the biometric authentication during these transactions. The different technologies have different benefits. They are compared in different sections for example which one is the safest, or the most practical one. They are also compared with some of the old methods. Using the data from the previous section, in the 5<sup>th</sup> it recommends a solution for the problems of biometric authentication, and also presents a method, called the behaviour-based authentication. It is a method which is not known and used in our country, but there is a big potential in it, to become a leading authentication type in the field of banking.