Az e-kereskedelem elvárásai a biometriával szemben

Őszi Arnold

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

oszi.arnold@bgk.uni-obuda.hu

Absztrakt: A jelen cikk egy szempontrendszert mutat be, amely segítségével meghatározható, hogy mely biometrikus technológia milyen mértékben felel meg az e-kereskedelem elvárásainak. Az e-kereskedelem és a bankkártyák számának gyors növekedésével megnövekedett az ezekkel történő visszaélések száma is. Ezeket általában lopott, talált kártyákkal vagy felhasználói adatokkal követik el. Ezért vált szükséges az azonosítás hatékonyságának növelése. Elindult a kezdeményezés, mely szerint a biometrikus azonosítást vezetik be a területre azon célból, hogy a jogosulatlan használatok száma hatékonyan csökkenhessen. A biometrikus azonosítás folyamatosan egyre több helyen kerül bevezetésre. Szükség van rá, hogy a technológiát folyamatosan javítsuk, hiszen számos gyenge ponttal rendelkezik. Ugyan ez a helyzet az e-kereskedelemmel is. A jelenleg működő rendszereken folyamatosan találnak biztonsági hiányosságokat, amelyeket nem mindig és nem azonnal javítanak ki. Mivel nem objektív alapon döntünk, ezért nem tudjuk a megfelelő technológiát kiválasztani. Ezért szükség van egy olyan megközelítésre, amely valós paraméterek szerint adja meg a legmegfelelőbb technológiát. A jelen cikk összefoglalja, hogy a szóba jöhető biometrikus technológiák közül melyek mennyire felelnek meg a legjobban az e-kereskedelem feltételeinek. A cikk bemutatja az e-kereskedelem szempontjából fontos biometrikus azonosítási lehetőségeket, majd kitér azokra a szempontokra, amelyek szerint vizsgálni szükséges az egyes technológiákat. Végül fontosság és súlyozás figyelembevételével meghatározásra kerül, hogy mely technológia és milyen mértékben alkalmas az e-kereskedelem által elvárt követelményeket teljesíteni.

1 Bevezetés

A jelen cikk egy szempontrendszert mutat be, amely segítségével meghatározható, hogy mely biometrikus technológia milyen mértékben felel meg az e-kereskedelem elvárásainak.

Az e-kereskedelem és a bankkártyák számának gyors növekedésével megnövekedett az ezekkel történő visszaélések száma is. Ezeket általában lopott, talált kártyákkal vagy felhasználói adatokkal követik el. Ezért vált szükséges az azonosítás hatékonyságának növelése. Elindult a kezdeményezés, mely szerint a

biometrikus azonosítást vezetik be a területre azon célból, hogy a jogosulatlan használatok száma hatékonyan csökkenhessen.

A biometrikus azonosítás folyamatosan egyre több helyen kerül bevezetésre. Szükség van rá, hogy a technológiát folyamatosan javítsuk, hiszen számos gyenge ponttal rendelkezik. Ugyan ez a helyzet az e-kereskedelemmel is. A jelenleg működő rendszereken folyamatosan találnak biztonsági hiányosságokat, amelyeket nem mindig és nem azonnal javítanak ki.

Mivel nem objektív alapon döntünk, ezért nem tudjuk a megfelelő technológiát kiválasztani. Ezért szükség van egy olyan megközelítésre, amely valós paraméterek szerint adja meg a legmegfelelőbb technológiát. A jelen cikk összefoglalja, hogy a szóba jöhető biometrikus technológiák közül melyek mennyire felelnek meg a legjobban az e-kereskedelem feltételeinek.

A cikk bemutatja az e-kereskedelem szempontjából fontos biometrikus azonosítási lehetőségeket, majd kitér azokra a szempontokra, amelyek szerint vizsgálni szükséges az egyes technológiákat. Végül fontosság és súlyozás figyelembevételével meghatározásra kerül, hogy mely technológia és milyen mértékben alkalmas az e-kereskedelem által elvárt követelményeket teljesíteni.

2 Alapfogalmak

FAR: Az angol „False Acceptance Rate” kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a nem jogosult felhasználót jogosultként.

FRR: Az angol „False Rejection Rate” kifejezés kezdőbetűiből származik. Megadja, hogy milyen arányban azonosítja a rendszer a jogosult felhasználót nem jogosultként.

EER: Az angol „Equal Error Rate” kifejezés kezdőbetűiből származik. Azt a pontot adja, ahol a FAR és az FRR értékei egyenlőek egymással.

3 Biometrikus technológiák

Biometrikus azonosítás esetén a felhasználók először regisztrálják magukat, pontosabban a biometrikus mintájukat egy adatbázisban. Ezután történhet az azonosítás, amely során meghatározásra kerül, hogy az azonosítást végző személy biometrikus mintája szerepel-e az adatbázisban, és ha igen akkor melyik az. Ezt nevezzük 1:n-hez típusú azonosításnak. A másik lehetőség, hogy az azonosítást

végző személy biometrikus mintája nem a teljes adatbázissal, hanem csak egyetlen mintával kerül összehasonlításra. Ez utóbbi az 1:1-hez típusú azonosítás.

A következő biometrikus technológiák kizárhatóak az e-kereskedelemben történő alkalmazásból:

A járás felismerés, mert nagy teret igényel a megbízhatósága is vitatott.

A fül geometria, fül hőtérkép, arc hőtérkép, mert csak kis létszámban lett tesztelve, nem kiforrott technológia, jelenleg nem képes stabilan megbízható eredményt produkálni.

Az aláírás felismerést jelenleg nem használják azonosításra, csak hitelesítésre.

A továbbiakban a feladatra alkalmas azonosítási típusok jellemzőit vizsgálja a cikk.

3.1 Írisz

A legnagyíobb pontosságot biztosító technológiák egyike. Az írisz mintázata a biometrikus azonosítás szempontjából az egyik legnagyobb változatosságot biztosítja, ezért a legtöbb esetben az azonosítandó személy íriszét nem egy mintával (1:1 azonosítás), hanem az összes tárolt mintával össze lehet hasonlítani (1:n azonosítás). A felvételt az íriszről az esetek döntő többségében infra tartományban készítik. Az élőminta felismerése a pupillareflexek detektálásával történik.

Az azonosítás hibáinak leggyakoribb oka, hogy az írisz mintázatát takarja a szemhéj, valamint az írisz megvilágítását biztosító fényforrás tükröződést okoz az íriszen. Szemüveg viselése esetén a szemüvegen megjelenő reflexiók nehezítik meg a felismerést. [1] [2]

3.2 Erezet

A legújabbnak mondható technológia. A korábbi megoldások a kézháton elhelyezkedő erek mintázatát azonosította, a korszerűbb eszközök azonban a tenyér és az ujj érhálózatának mintázatát használják az azonosításhoz.

Az erezetről a felvételt általában 740 és 1000nm hullámhossz közötti infravörös tartományban készül, mivel a deoxidált hemoglobin a vérben elnyeli az infravörös sugárzást, így az erek sötétebb vonalak formájában detektálhatók. Ezen a vonalak alapján történik meg az azonosítás.

Az érhálózat mintázata egyedi minden embernél, még az egypetéjű ikrek esetében is, ezért jól használható biometrikus azonosításhoz. A többi biometrikus azonosítási módszerrel összehasonlítva pontosabban állapítja meg a személy azonosságát. Előnye, hogy belső biometrikus jellemzőt használ, az erek kevésbé sérülékenyek mint más biometrikus jellemzők (például ujjnyomat, hang). Ezen

kívül a hamis minta előállítása is nehezebb feladat, ugyanis az erek teljes mintázata az ember szem számára nem látható. A tapasztalatok szerint a gyakorlatban jól kizárja a megvilágítottság, hőmérséklet és a napfény zavaró jeleit bizonyos határokon belül. [3]

3.3 Ujjnyomat

Jelenleg a legelterjedtebb azonosítási forma és egyben a legrégebbi is, hiszen számítógép segítségével több mint 25 éve hasonlítanak össze ujjnyomatokat.

Az ujjnyomat az ujj felületén található völgyek és fodorszálak mintázata. Ezek azonosításhoz használt pontjai a minutiák. Az azonosítás a legtöbb esetben a minutiák egymáshoz viszonyított helyzete alapján történik. Az emberi kéz ujjnyomatai általában a magzat hét hónapos korában kialakulnak és nem változnak az ember élete folyamán, leszámítva az ujjat érintő baleseteket. [4]

A bűnüldözésben nagy hatékonysággal alkalmazták az akkor aktuális tintás módszert, azonban a túl nagy adatbázis miatt szükségessé vált az összehasonlítások géppel történő elvégzése. Napjainkban már a rendőrség is tinta nélküli szkennerekkel rögzíti az ujjnyomatok képeit.

Jelenleg az optikai, azon belül a prizmás technológia a legelterjedtebb. A legkorszerűbbnek a multispektrális képalkotó technológia mondható, amely a korábbi technológiák hiányosságait jó hatásfokkal küszöböli ki. Ezek a hiányosságok például a száraz vagy nedves ujj, az ujj erős nyomása miatt bekövetkező torzítás és az élőminta felismerése. [5] [6]

3.4 Arc

Jelenleg az arcfelismerés hatékonyságának javítására fordítják a legtöbb energiát. A tapasztalatok azt mutatják, hogy még mindig kihívás az élőben készített arcképet összehasonlítani az adatbázisban szereplővel. Amennyiben a rendszer nagy adatbázissal dolgozik, ezek a zavaró hatások még erősebben rontják az azonosítás sikerességét, ezért érdemes lenne 1:n helyett 1:1 típusú azonosítást alkalmazni.

A leggyakoribb zavaró hatások a megvilágítás, a kamera nézőpontja, az arc elfordulása, arckifejezés, öregedés, smink és a szemüveg. A 3D arcfelismerés a 2D zavaró hatásait jó hatásfokkal zárja ki, azonban a 3D csak relatív közelről alkalmazható és a felhasználó nagyobb fokú együttműködését igényli. [7]

3.5 Kéz geometria

A kézről felvételt készítenek általában infra tartományban. Az így kapott képről megállapítható a kéz geometriája. Egyes eszközök esetén különböző szögből is készítenek képeket, így a kézről kvázi 3D képet lehet kapni, amely növeli az

azonosítás hatékonyságát. A torzítás minimalizálása érdekében a kamerát minimum fél méterre érdemes elhelyezni a kéztől. Az eszköz méretét úgy csökkentik, hogy tükrös rendszert építenek a készülékbe, azonban még így is relatív nagy méretű marad az olvasó.

Méretei miatt kevésbé elterjedt technológia. Előnye, hogy a kéz tisztaságának mértéke nincs hatással az azonosításra. Hátránya, hogy az azonosítás pontossága kicsi, így általában csak 1:1-hez típusú azonosításhoz alkalmazzák. A módszer általában az ujjak hosszát, szélességét, a területet, az ízületeknél lévő szögeket, valamint ezek arányait vizsgálja. Az azonosítást megnehezíti, vagy lehetetlenné teszik a kéz deformációs megbetegedései, elváltozásai, a bandázs, a kesztyű vagy nagyobb gyűrű viselése. [8]

3.6 Retina

Az azonosítás során általában infravörös spektrumú fénnyel világítják meg a retinát, amelyről egy, közvetlenül a szemlencse előtt elhelyezkedő kamera készít felvételt. Az így készített képen jól kirajzolódik a szemfenék érhálózata.

Biometrikus azonosítók esetén ritkán használt technológia, mert túl nagy méretű az eszköz és használata kényelmetlen. Ezen technológiával relatív nagy pontossággal meghatározható az egyén személyazonossága.

3.7 Hang

A hang az egyik legkönnyebben elérhető és a legolcsóbban vizsgálható biometrikus jellemző. Egyre kevésbé használt technológia, szerepét más biometrikus módszerek veszik át. Létezik szövegfüggő és szövegfüggetlen beszéd-felismerés. Az ember hangja gyakran megváltozhat, ez okozza a technológia pontatlanságát. A módszer hiányossága, hogy a hangképzés igen komplex folyamat, a hangszínt nem csak az anatómiai adottságok, de az érzelmi állapot, a beszélt nyelv sajátosságai, az aktuális hangulat valamint a betegségek is befolyásolják. Ezért még ma is kihívás egy stabilan nagy hatásfokkal működő beszéd-felismerő rendszert létrehozni. [9]

3.8 DNS

Nagy azonosítási pontosságot tesz lehetővé, azonban lassú és drága technológia. A DNS-minta szinte bárhonnan elérhető, ebben rejlik a hátránya is, hiszen egy nem jelenlévő személy DNS mintáját is képes azonosítani. Napjainkban már nagyságrendekkel csökkent az azonosítási idő és az azonosítás ára is, azonban ez még mindig nagyságrendekkel több az elfogadhatónál.

4 Szempontok

Az egyes biometrikus azonosító eljárásokat különböző szempontok szerint szükséges vizsgálni.

Néhány szempont triviális, így ezek szükséges feltételek. Ilyen például, hogy azonos eredménnyel reprodukálható legyen az azonosítás eltérő helyszíneken, napszaktól függetlenül, megvilágítástól függetlenül és a hőmérsékleti viszonyoktól függetlenül. [5]

Más szempontok technológiától függően változhatnak. Ezek a szempontok a következők:

4.1 Mindenkinél alkalmazható

A biometrikus minta az emberi test geometriai vagy viselkedéstani jellemzőiből származik. Vannak emberek, akiknek hiányzik néhány biometrikus adata, például a némáknál a beszédfelismerés. Fontos, hogy a módszer minden embernél legyen alkalmazható, a lehető legtöbb emberre lehessen elvégezni az azonosításhoz szükséges minta megfelelő minőségű beolvasását. [5] [10]

4.2 Egyediség

A biometrikus minta egyedisége biztosítja azt, hogy minden ember a világon megkülönböztethető az adott biometrikus minta alapján. Ennek jó tesztje az egypetéjű ikrek vizsgálata. Szintén vizsgálható a biometrikus minta egyedisége, amennyiben nagy elemszámú adatbázist adatait hasonlítjuk össze egymással. Az ilyen nagy számú biometrikus mintát tartalmazó adatbázisban az egyes biometrikus mintáknak nem szabad hasonlóknak lennie. [10]

4.3 Eszköz mérete

Mivel az e-kereskedelem nagyrészt mobil eszközökben használja a biometrikus eszközöket, ezért fontos, hogy az eszköz geometriai méretei ne legyenek túl nagyok. Az alkalmazott eszközöknek el kell férniük egy íróasztalon, esetleg olyan technológiát kell alkalmaznia, ami a közeljövőben mobiltelefonokba is integrálható lesz. Ezért nagy mérete miatt kizárható például a kézgeometria azonosító.

4.4 Megbízhatóság

Amennyiben sok mintát tárolunk egy adatbázisban, és összehasonlítjuk a mintákat, akkor azoknak különbözőeknek kell lenniük. Ezen kívül az azonosításkor beolvasott mintának nagyon hasonlítania kell a már eltárolt biometrikus mintára. Amennyiben ezek a kritériumok fennállnak, akkor lehet nagy

biztonsággal azonosítani a személyt, tehát biztosan nem keveri össze mással az algoritmus, valamint biztosan kiválasztja, amennyiben regisztrálva van.

Néhány biometrikus rendszer FAR mutatója nagyságrendileg:

- hang azonosítás: 500 : 1;
- arc azonosítás (2D): 2.000 : 1;
- ujjnyomat azonosítás: 1.000.000 : 1;
- írisz azonosítás: 10.000.000 : 1;
- retina azonosítás: 10.000.000 : 1. [11]

Az EER két jellemzőből származtatható. Ezek a FAR és az FRR. Az utóbbiakat egy küszöb beállításával eszközönként lehet állítani, ezért javasolt alapul venni az EER mutatót, amely független a kizárási küszöb beállításától. Az EER mutató adja meg egy eszköz megbízhatóságát a fent leírt kritériumok szerint. [10] [12]

4.5 Változatlanság

Sok biometrikus jellemző változik az évek múlásával, ilyen például a hang vagy az arc. Az írisz és az ujjnyomat ebből a szempontból stabilitást mutat. A hosszú távon jól működő biometrikus azonosítás feltétele, hogy olyan jellemzőt válasszunk, amely évek után is változatlan marad. A változatlanság a biometrikus adat hosszú távú stabilitásának is tekinthető. [10]

4.6 Elérhetőség

Nem minden biometrikus jellemző érhető el egyszerűen. Például retina azonosítás esetén közelről kell erős fénnyel a szembe világítani és közben képet készíteni a retináról. Ehhez képest például az arcfelismerés esetén a biometrikus minta elérhetősége jobb, hiszen ebben az esetben egy megszokott környezetben készül fénykép az arcról.[10]

4.7 Elfogadottság

Néhány eszköz némi érzelmi ellenállást válthat ki a használó személyek felől. Ilyen például az retina azonosítás, ahol nagyon közel kell a szemet helyezni az eszközhöz, amely egy erős fénnyel világítja meg a szemfeneket. [10]

4.8 Belső biometrikus jellemzőt használ

A belső biometrikus jellemzők kevésbé sérülékenyek, mint a külső biometrikus jellemzők. A test felületén lévő biometrikus jellemzők könnyen leolvashatatlanná válhatnak külső fizikai vagy kémiai behatások által. Ez rontja a biometrikus minta rendelkezésre állását. Ezen kívül a belső biometrikus jellemzőkről nehezebb másolatot készíteni. [5]

4.9 A technológia kiforrottsága

Néhány biometrikus technológia fejlődő fázisban van, ezért még nem készültek olyan eszközök, amelyek nagy létszámban bizonyították a technológia sikerességét. A kevésbé kiforrott technológiákat még nem tesztelték nagy sokaság által, így előfordulhat, hogy olyan hiányosságai vannak az aktuális verziónak, amelyek miatt az aktuális megoldás nem működik megfelelő hatékonysággal. Egy kiforrott technológia, ezzel ellentétben, nagy létszámban ki lett próbálva, tehát a hiányosságai is felfedezésre, majd javításra kerültek.

4.10 Élőminta felismerés

A legtöbb biometrikus minta lemásolható. Fontos az, hogy a másolatokkal ne lehessen elérni sikeres azonosítást, ezért valamilyen egyei módszerrel meg kell győződni arról, hogy a biometrikus minta élő emberé és nem egy másolat. [10] [12]

4.11 Érintés nélküli

A biometrikus eszközök megérintése sok emberből rossz érzést vált ki. Ezért előny, ha az eszköz úgy képes az azonosításra, hogy a felhasználónak nem kell hozzáérni. Higiéniai szempontok miatt érdekes a szempont, hiszen a hiedelmek szerint a biometrikus eszközök a betegségek átadásában szerepet játszhatnak. [5]

4.12 Azonosítási idő

Az azonosítási időnek nem szabad túlzottan hosszúnak lennie. Az azonosítási idő a technológiától függően változhat, azonban a DNS azonosítást leszámítva ezen időtartamok a célnak megfelelőek. [5]

5 A szempontok kiértékelése

A szempontok, melyek az előző fejezetben meghatározásra kerültek, az 1. táblázatban összegezve olvashatóak.

	Szempontok
1.	Mindenkinél alkalmazható
2.	Egyediség
3.	Eszköz mérete
4.	Megbízhatóság
5.	Változatlanság
6.	Elérhetőség
7.	Elfogadottság
8.	belső biometrikus jellemzőt használ
9.	A technológia kiforrottsága
10.	Élőminta felismerés
11.	Érintés nélküli
12.	Azonosítás idő

1. táblázat
A biometrikus technológiák hatékonyságát vizsgáló szempontok

A szempontok szerint minden biometrikus technológiát minősíteni lehet. A minősítés három lépcsőben került meghatározásra, ez a 2. táblázatban látható.

Válaszok:
Jó
Közepes
Rossz

2. táblázat
A minősítés lehetséges lépcsői

A szempontok szerint az adott biometrikus technológiák értékelését a 3. táblázat mutatja be.

	Technológia								
	Írisz	Erezet	Arc	Ujjnyomat	DNS	Aláírás	Hang	Retina	Kéz geometria
1	Jó	Közepes	Jó	Közepes	Jó	Közepes	Közepes	Közepes	Közepes
2	Jó	Jó	Közepes	Jó	Jó	Jó	Rossz	Jó	Rossz
3	Jó	Jó	Jó	Jó	Rossz	Közepes	Jó	Rossz	Rossz
4	Jó	Jó	Közepes	Közepes	Jó	Rossz	Rossz	Jó	Közepes
5	Jó	Jó	Közepes	Jó	Jó	Közepes	Közepes	Jó	Közepes
6	Jó	Jó	Jó	Jó	Jó	Jó	Jó	Rossz	Jó
7	Közepes	Közepes	Jó	Közepes	Közepes	Jó	Jó	Rossz	Jó
8	Jó	Jó	Rossz	Rossz	Közepes	Jó	Jó	Jó	Rossz
9	Jó	Jó	Jó	Jó	Rossz	Közepes	Rossz	Rossz	Jó
10	Jó	Jó	Jó	Közepes	Jó	Jó	Közepes	Jó	Közepes
11	Jó	Jó	Jó	Rossz	Rossz	Rossz	Jó	Rossz	Rossz
12	Jó	Jó	Jó	Jó	Rossz	Jó	Jó	Jó	Jó

3. táblázat
A biometrikus technológiák hatékonysága a szempontok szerint

5.1 Súlyozás

A 2. táblázatban látható, hogy az egyes mezők háromféle minősítést kaphatnak. Az egyes minősítések pontszámra konvertálhatóak, melyet a jelen cikk súlyozásnak nevez. A válaszok súlyozását a 4. táblázat mutatja be.

Válaszok súlyozása:	
Jó	3 pont
Közepes	1 pont
Rossz	0 pont

4. táblázat
A technológiák pontértéke a súlyozás után

Az egyes technológiákra adott válaszokat minden megadott szempontból numerikus értékké konvertálva, majd az így kapott értékeket összegezve megkapjuk az adott technológia jóságát.

A súlyozást alkalmazva az egyes technológiákra a következő eredményeit az 5. táblázat mutatja be.

Írisz	Erezet	Arc	Ujj-nyomat	DNS	Aláírás	Hang	Retina	Kéz geometria
34 pont	32 pont	27 pont	22 pont	20 pont	21 pont	21 pont	19 pont	16 pont

5. táblázat
A technológiák pontértéke a súlyozás után

5.2 Fontosság

Számtalan szempontot lehet felsorakoztatni, azonban vannak olyan szempontok, amelyek fontosabbak, még más szempontok kevésbé fontosak az e-kereskedelem szempontjából. A fontosság figyelembe vételével az egyes szempontoknak különböző szorzó konstanst állíthatunk be, így a végeredmény megmutatja, hogy melyik eszköz a legalkalmasabb a feladat ellátására. A fontosságot meghatározó paraméter a következőképpen került beállításra:

1	Mindenkinél alkalmazható	5
2	Egyediség	5
3	Eszköz mérete	5
4	Megbízhatóság	5
5	Változatlanság	5
6	Elérhetőség	4
7	Elfogadottság	4
8	belső biometrikus jellemzőt használ	4
9	A technológia kiforrottsága	4
10	Élőminta felismerés	4
11	Érintés nélküli	2
12	Azonosítás idő	2

6. táblázat
A technológiák pontértéke a súlyozás után

A korábban bemutatott súlyozás azzal egészül ki, hogy az adott szempont fontosságát meghatározó paraméter szorzótényezőként kerül a képletbe:

$$a_n = \sum_{k=1}^{12} s_k \cdot f_k$$

Írisz	Erezet	Arc	Ujj-nyomat	DNS	Aláírás	Hang	Retina	Kéz geometria
139 pont	129 pont	105 pont	93 pont	92 pont	88 pont	77 pont	80 pont	61 pont

7. táblázat
A technológiák pontértéke a Fontosság paraméterezése után

Az így kapott eredmény tekinthető valóságosnak, mely figyelembe veszi az adott szempont fontosságát is. A táblázat alapján meghatározható, hogy mely technológia a megfelelőbb a feladat ellátására.

6 Következtetések

A 7. táblázatból leolvasható, hogy mely technológiák milyen mértékben alkalmasak az e-kereskedelem által szabott elvárásoknak. A két legmegfelelőbb technológia az írisz és az erezet azonosítás. Az is látható, hogy a legkevésbé megfelelő technológiák a hang, retina és a kéz geometria azonosítás.

A bemutatott módszer jól alkalmazható a biometrikus azonosítási módszer kiválasztására nem csak az e-kereskedelem, de más cél szempontjaihoz, amennyiben a szempontokat és a súlyozást módosítjuk az adott feladathoz.

Irodalomjegyzék

[1] SUPLICZ Sándor - FŰZI Beatrix - HORVÁTH Sándor: Írisz felismerésen alapuló beléptető rendszer által keltett attitűdök és averzív reakciók vizsgálata, 6. Nemzetközi Mechatronikai és Biztonságtechnikai Szimpózium, Budapesti Műszaki Főiskola, 2006., ISBN 978-963-7154-59-1

[2] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 71-90

[3] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 253-270

[4] R. Cappelli, D. Maio, D. Maltoni, J.L. Wayman, and A.K. Jain. Performance evaluation of fingerprint verification systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(1):3–18, 2006.

[5] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, Balla József rendőr alezredes, A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- és közbiztonság alakulására, Doktori (PhD) értekezés, Budapest, 2013. p 80.

[6] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 23-28

[7] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 43-70

[8] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 91-107

[9] Springer kiadó: Anil K. Jain, Patrick Flynn, Arun A. Ross: Handbook of Biometrics, ISBN-13: 978-0-387-71040-2 év: 2008 p. 151-170

[10] David Zhang·GuangmingLu - 3D Biometrics - Systems and Applications - Springer kiadó, Hong Kong, Kína, ISBN 978-1-4614-7399-2, Kiadás éve: 2013, page: 6-7

[11] KOVÁCS Tibor: A biometrikus azonosítás alapjai, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Alkalmazott Biometria Intézet (Applied Biometrics Institute – ABI), Digitális jegyzet, Budapest 2014

[12] ComputationalIntelligence and Informatics (CINTI), 2011 IEEE 12th International Symposiumon - Theory of thebiometric-basedtechnologyinthefield of e-commerce, Arnold ŐSZI, Tibor KOVÁCS, ISBN: 978-1-4577-0044-6, Dátum: 2011. november 21-22, Budapest, p. 567-571

Vállalkozásfejlesztés a XXI. században
Budapest, 2014.