

Biometri som Underhållning

Martin Fagerfjäll
marfa233@student.liu.se

Handledare: Kristin Anderson

Sammanfattning

Biometrisk identifiering är en teknik som utvecklats mycket de senaste åren. Det finns flera företag som säljer biometriska säkerhetssystem, men det riktiga genomslaget för dessa produkter har ännu inte skett. Inom nöjesbranschen används dock biometrin i betydligt större utsträckning sedan flera år. Denna rapport utvärderar hur biometrin används i ett urval av stora filmproduktioner. Det visar sig att den biometriska tekniken avbildas förhållandevis korrekt ur teknisk synvinkel medan den ofta är dåligt implementerad ur säkerhetssynpunkt. Mest tydligt är detta då system med dålig liveness-detection används i säkerhetskritiska installationer, vilket ofta inbjuder till problem.

Inledning

Biometri är ett mycket brett ämne som i grund och botten går ut på att kunna identifiera en person på elektronisk väg. Det som gör ämnet brett är de myriader av olika tekniker som finns att tillgå för att utföra identifieringen. Dessa tekniker sträcker sig från system för att mäta karaktäristiska egenskaper hos kroppen som fingeravtryck och ansiktsform till mätning av dynamik skapad av kroppen såsom tal, gång och handstil.

Trots de stora framsteg som gjorts inom biometrin verkar det breda allmänna genomslaget för biometrisk identifiering fortfarande låta vänta på sig, förutom inom ett område; underhållningsbranschen. Här passar tekniken perfekt eftersom den både är spektakulär och ger en rad nya problem att spinna berättelser kring. Biometri är därför bland stora delar av allmänheten främst känd via filmer och andra typer av underhållning såsom dataspel och TV-serier, medan själva tekniken i sig fortfarande är relativt okänd för de flesta. Även om det på senare tid har börjat skrivas mer om denna teknik i dagspress är tekniken fortfarande nära förknippad med Hollywoodproduktioner.

Som bekant finns det ingen garanti för att något som avbildas på vita duken faktiskt finns i verkligheten, men denna företeelse börjar dyka upp i många olika filmer kanske det kan finnas anledning att tro att det ligger något i vad som visas? Som ett exempel på detta fenomen kan tas det ständigt lika aktuella påståendet om att människor påverkas av underhållningsvåld i filmer. Få människor har upplevt den typ av våld som brukar finnas med i actionfilmer, men de tycker sig ändå ha en uppfattning av vad som händer när en knytnäve träffar någons pannben, när en pistolkula träffar en person i magen eller när en handgranat briserar. Om man kan ha en uppfattning om en handgranat som man bara har sett på film, kan man då inte ha bildat sig en uppfattning även om andra företeelser?

Jag anser att det inte är ett allt för djärvt påstående att säga att människors förhållande till biometri idag i mycket stor utsträckning påverkas av hur den används i filmer. Detta grundar jag på att tekniken används flitigt inom filmbranschen samtidigt som den används klart mindre flitigt ute i den riktiga världen. Detta gör det i sin tur intressant att undersöka huruvida biometrin faktiskt används på ett realistiskt sätt i dagens filmproduktioner, eller om det handlar om ren science fiction. Förutom den rent tekniska aspekten på problemet är det dessutom intressant att undersöka hur biometrin tillämpas säkerhetsmässigt i dessa filmer.

1.1. Frågeställningar

Återspeglar den biometriska tekniken i dagens filmer verkligheten ur ett tekniskt perspektiv?

Hur är de biometriska systemen i filmerna implementerade säkerhetsmässigt?

2. Metod

För att kunna besvara frågeställningarna har jag valt att studera användandet av biometrisk teknik i ett antal filmer. Studien kommer att genomföras som en kvalitativ undersökning, då det data som avses studeras inte kan kvantifieras på ett meningsfullt sätt.

2.1. Urval

Jag har valt att avgränsa studien till filmer och kommer således inte att analysera tv-serier och spel. Anledningen till detta är främst att filmerna har den största tillgängligheten för allmänheten. Tv-serier och spel brukar ha en betydligt smalare kundbas och lägre tillgänglighet än de ofta mycket påkostade spelfilmerna. En storfilm brukar kunna ses av i stort sett alla människor i den industrialiserade världen på bio eller DVD/VHS, medan en tv-serie kräver ett avtal med den station som äger rättigheterna till serien. Datorspel och tv-spel kräver i sin tur tillgång till särskild hårdvara, vilket begränsar kundkretsen. Det är därmed inte ointressant att studera även denna typ av underhållning, men det ligger utanför studiens fokus.

Det potentiella urvalet filmer för denna studie är alla filmer där biometri förekommer på något sätt, ett mycket stort antal filmer med andra ord. Den första begränsningen på urvalet är således att bara använda filmer som är relativt kända för en publik i västvärlden. Någon närmare definition av vilka kriterier som konstituerar en känd film kommer jag inte att gå in på, men analogt brukar det juridiska kravet för att ett varumärke skall vara inarbetat (känt) vara att minst 30 % av populationen (filmbesökarna) skall känna till det. Någon statistisk undersökning kommer dock inte utföras inom ramarna för denna uppsats.

Bland de filmer som uppfyller ovanstående kriterier har jag valt ett antal intressanta exemplar från de senaste årens utbud, eftersom det främst är bland filmer från de senaste åren som den biometriska tekniken har någon möjlighet att kunna presenteras på ett korrekt sätt då det är en relativt ny teknologi.

2.2. Studiens omfattning

I de studerade filmerna har jag valt att fokusera på den biometri som används i filmen för att kunna utvärdera den ur säkerhetssynpunkt med utgångspunkt i dagens teknik. För att avgöra vilken teknik som finns idag har jag använt mig både av vetenskapliga artiklar och av företag som verkar inom branschen. Artiklarna ger en god överblick över den forskning som bedrivs inom området, medan företagshemsidor och produktkataloger ger en bild av den biometriska teknik som finns tillgänglig som kommersiella produkter.

2.3. Metodkritik

Först och främst är problemet med denna typ av studie att få ett bra urval av filmer att jobba med, som uppfyller studiens kriterier. Den största svårigheten i detta avseende har varit att sammanställa ett grundurval av filmer som är intressanta ur biometrisynpunkt. Detta urval har gjorts dels genom att besöka Internetsidor för filmentusiaster och dels genom att använda mina egna och andras förkunskaper inom ämnet. Studien kan därför bli lidande av att urvalet inte är representativt för filmbranschen i alla avseenden. Jag anser dock att detta inte påverkar studiens giltighet i någon större utsträckning, då varje urval som görs av filmer eller konstnärliga skapelser kan angripas på liknande sätt.

Eftersom främst elektroniska källor används och vissa av dem är knutna till företag eller intresseorganisationer inom biometris område finns det en risk att de framhäver fördelarna med tekniken och döljer nackdelarna. Exempelvis finns det detaljerade data om olika fingeravtrycksläsares tekniska prestanda, såsom andel felaktig avvisning och accept, att tillgå på tillverkarnas hemsidor, medan det inte går att hitta information om hur enkelt det är att lura läsarna med exempelvis gummifingrar. Det är förvisso inte underligt att denna information inte presenteras, då den är mycket svår att kvantifiera och inte bidrar till att höja marknadsvärdet på utrustningen, men det är ändå något som bör uppmärksammas. Den data som faktiskt presenteras från tillverkarnas sida har jag dock ingen anledning att ifrågasätta, då de valda företagen är seriösa aktörer inom säkerhetsbranschen som inte har något att vinna på lögner i det långa loppet.

3. Filmer

I detta kapitel beskrivs de studerade filmerna med fokus på de biometriska system som förekommer.

3.1. Face/Off (1997)

Face/Off handlar om hur John Travolta, filmens hjälte, byter ansikte med den känslokalle men underhållande skurken Nicolas Cage för att kunna infiltrera dennes terrororganisation och desarmera en bomb som hotar förstöra statlig egendom i USA.

Tanken bakom filmen är att man kan maskera en person så att alla hans biometriska data matchar någon annan persons och därigenom kunna bereda sig tillgång till den andre personens bekantskapskrets. Möjligheten att i verkligheten utföra de kirurgiska ingrepp som görs i filmen ligger utanför denna uppsats fokus, jag har istället valt att föra diskussionen kring det säkerhetsfängelse där vår huvudperson hamnar när han försöker infiltrera den undre världen.

3.1.1. Fingeravtryck

På det säkerhetsfängelse dit huvudpersonen kommer efter sin förvandling finns det en stor och bastant säkerhetsdörr som öppnas med en obehörig fingeravtrycksläsare. Det bör ur fängelsets säkerhetssynpunkt vara synnerligen ofördelaktigt om dörren genom felaktig accept öppnas för obehöriga personer. I dagens läge finns kommersiellt tillgängliga läsare som klarar en falsk accept per 100 000 försök för ett rimligt litet antal registrerade fingeravtryck, vanligen omkring ett hundratal [10,11]. Huruvida denna andel felaktiga accepter är acceptabla för en säkerhetskritisk applikation som ett fängelse är en öppen fråga, men det finns dock ett annat problem med biometriska lås i fängelsemiljö; ett fängelse bör inte ha några dörrar ut till friheten som kan öppnas inifrån, all in- och utpassering bör ske via vakter på utsidan. Att som i filmen ha en säkerhetsdörr som i teorin kan öppnas automatiskt genom att kidnappa en vakt och trycka hans tumme mot en läsare måste ses som synnerligen bristfälligt. För att biometri skall kunna användas för att automatisera utpasseringen från ett fängelse krävs bättre motmedel mot tvång av olika former. Systemet måste kunna skilja på biometriska data från en frivillig person och från en person under tvång, och vi har inte den tekniken ännu. Dessutom måste låset klara av att avvisa förfälskade fingeravtryck, till exempel gummifingrar eller avklippta fingrar, genom någon form av liveness-kontroll. Även detta är ett område som inte är särskilt väl utvecklat ännu. Ser vi till de olika tillverkarna finns det bland de tekniska data som presenteras ingen information om fingeravtrycksläsarnas möjligheter att skilja på äkta och falska fingrar.

En annan aspekt av biometriska lås som aktualiseras när en av fångarna skjuter låset i småbitar är låsets felmodell. Om låset slås sönder måste dess beteende vara deterministiskt, inte slumpmässigt. För en enkel dörr av trä är detta kanske

inte lika viktigt eftersom dörrens hållfasthet ändå är begränsad, men en två tons bepansrad ståldörr bör inte fastna i läget "10 % öppen" som i filmen bara för att någon använder ett finkalibrigt vapen mot låsmekanismen. En dylik dörr uppfyller inte sitt syfte och skulle inte accepteras i ett fängelse.

3.2. Enemy of the state (1998)

Filmen handlar om hur en advokat spelad av Will Smith av misstag får tag på bevis om ett politiskt mord och sedan blir jagad av NSA med alla till buds stående medel. Dessa medel inkluderar satelliter, telefonavlyssning och allsköns annan teknik. Den teknik som används i filmen som närmast är relaterad till biometri är fingeravtrycksläsare, ansiktsavläsning och röstigenkänning.

3.2.1. Fingeravtryck

Användandet av fingeravtryck i filmen är begränsat till NSA:s byggnad, där dessa används som identifiering för att få tillträde till den hemliga del av byggnaden där de stygga personerna sitter och konspirerar. Något annat säkerhetssystem visas aldrig på filmen, men det kan antas att någon typ av bemannad säkerhetskontroll måste passeras för att få tillträde till en av regeringens mest sekretessbelagda byggnader. Med utgångspunkt i detta kan man anta att de personer som kan nå fingeravtrycksläsaren har rätt att befinna sig i byggnaden. Av filmen att döma är dock läsaren oöverbaskad, men detta är förmodligen ett mindre problem eftersom de enda personer som har möjlighet att komma i kontakt med läsaren är "säkra". Eftersom ett flertal personer arbetar i den hemliga delen av byggnaden är troligen ett större problem att flera personer kan slinka igenom på ett fingeravtryck. Hur denna problematik är löst framgår inte i filmen, men det är en given sårbarhet för "social engineering"-attacker.

3.2.2. Ansiktsavläsning

Ansiktsavläsningen är i filmen mycket avancerad för att vara 1998. I filmen identifieras Gene Hackman med hjälp av en bild tagen av en lågupplöst övervakningskamera i en butik under ganska dåliga ljusförhållanden. Han kan därmed kopplas till en tjugo år gammal bild och identifieras som en f.d. spion för NSA. Det är ingen enkel procedur att genomföra denna typ av identifiering med de något bristfälliga indata som presenteras i filmen, men det är inte orimligt att detta kan göras eller åtminstone kommer att kunna göras inom några år.

3.2.3. Röstigenkänning

Den tredje biometriska tekniken som används i filmen är röstigenkänning, som används för att identifiera Will Smith när han ringer ett telefonsamtal. Tanken är att NSA

avlyssnar all telefontrafik i hela USA och med röstigenkänning och igenkänning av vissa speciella ord kan avgöra om trafiken hotar rikets säkerhet. Dessutom hävdas det att denna teknik har funnits i tjugo år, alltså från 1978.

Den del av tekniken som hör till det biometriska området är röstigenkänning. Taligenkänning, alltså identifikation av ord och fraser, brukar inte räknas till biometrin och jag kommer inte att närmare analysera filmens användande av detta. Röstigenkänning är fortfarande en relativt omogen teknik, och att som i filmen låta datorer analysera all telekommunikation i Amerika för att kunna identifiera vem som säger vad är fortfarande science-fiction, om man jämför med de kommersiella tjänster som finns i dagsläget [7,8,9].

De stora problemen i dessa fall är dels det stora urvalet röster (Amerikas befolkning) och dels den dåliga kvaliteten på en generell telefonledning. Dessutom brukar röstigenkänning fungera genom att jämföra en röstinspelning med en tidigare inspelning, vilket blir mycket komplicerat att göra i löpande tal där en likadan tidigare inspelning inte finns att tillgå. Tekniken för att kunna analysera löpande tal har dock utvecklats mycket under senare år, men att påstå att Amerikas regering har haft möjlighet att analysera all telefontrafik sedan slutet av 70-talet är aningen magstarkt.

3.3. The 6th day (2000)

Filmen utspelar sig i en inte allt för avlägsen framtid och berör problematik kring kloning av människor, samt biljakter, skottlosning, sprängning och avlivning av skurkar. Arnold Schwarzenegger spelar rollen som helikopterpiloten som av misstag blir klonad och sedan får kämpa för sitt liv när misstaget uppdagas och problemet skall rättas till.

3.3.1. Fingeravtryck

I denna film spelar fingeravtryck en stor roll, eftersom de används till i stort sett alla identifieringsärenden. Arnold Schwarzenegger använder i filmen sitt fingeravtryck till att betala taxin, komma in på jobbet och identifiera sig hos polisen. Han använder även andras fingeravtryck till lite mer illegala saker; dessa inkluderar bilstöld och ett antal fall av inbrott samt datorintrång.

Att betalning skall kunna ske enbart med hjälp av ett fingeravtryck, som det gör i filmen, är i princip ingen dum idé förutsatt att systemen är tillräckligt säkra. Det som gör filmens system svårt att implementera i dagens läge är att identifikationen och betalningen sker med ett enda fingeravtryck. Detta innebär att en fingeravläsning skall

identifiera en person bland ett urval av större delen av den industrialiserade världens befolkning, och dessutom debitera personens konto. En felaktig identifiering innebär alltså att någon slumpmässig person får stå för hela kalaset. En hyggligt bra läsare i dagens läge ger felaktig accept en gång på 100 000 försök, och då med bara ett antal hundra registrerade fingeravtryck [10,11]. För att ett system skall kunna fungera som i The 6th day med kanske två miljarder registrerade användare och i snitt fem miljarder transaktioner per dag krävs att andelen felaktiga accepter är mycket låg. Om vi antar att en felaktig accept per miljard försök är okej med två miljarder användare, kan vi jämföra det med dagens kommersiella system och inse att fingeravtryckstekniken troligen aldrig kommer att uppnå den pris-prestanda nivå som krävs för ett globalt banksystem baserat på ett fingeravtryck.

Ett system som skall identifiera ett fingeravtryck i en databas av två miljarder avtryck kommer oavsett inläsningstekniken även att kräva en databehandling som inte är av denna världen. Ross et. al hävdar att fingeravtrycksidentifiering med deras teknik, med en beräkningskraft motsvarande en 800 MHz P-III processor i en databas av max 1000 avtryck, tar ungefär 0.2 sekunder per avtryck att matcha för identifiering [1]. Om vi antar att databasen kan skalas till två miljarder avtryck med linjär söktid innebär detta att identifieringen kommer att ta nästan 13 år att genomföra. Detta är naturligtvis inget realistiskt scenario, men det visar vilka datamängder och beräkningar vi talar om för biometrisk identifiering.

Om man däremot måste hävda sin identitet först och sedan verifiera den med ett fingeravtryck är urvalsrymden betydligt mindre och ett fingeravtryckssystem likt dagens bör kunna fungera. Med en 800 MHz P-III processor tar denna 1:1 identifiering cirka 1.4 sekunder att utföra [1].

Resonemanget kring polisens identifieringsteknik är analogt med resonemanget i föregående stycke kring bankverksamhet med fingeravtryck. Antalet identifieringar polisen utför per dag bör dock vara betydligt färre än för det globala banksystemet, och konsekvenserna vid en felaktig identifiering bör vara mindre allvarliga, åtminstone vid en av polisen bemannad läsare. Om läsaren identifierar fel person får identifieringsprocessen göras om. Givetvis gäller även här att identifiering är betydligt svårare att genomföra än verifiering.

I denna framtida värld finns dock en synnerligen oroande svaghet som utnyttjas av hjälten vid både bilstöld och olaga intrång i onda företag; avklippta fingrar. Efter en eldstrid lyckas huvudpersonen komma över ett av skurkarnas fingrar som ligger och skräpar och kan därmed få tillträde både till skurkens bil och till skurkens högkvarter på ett

ganska enkelt sätt. I ett samhälle som baserar sig så mycket på fingeravtryck som detta, bör det finnas någon typ av liveness-test som avgör om det som trycks mot läsaren faktiskt är ett levande finger med blodflöde och nervimpulser eller om någon varit framme med sekatoren. Liveness-test är dock inget som är helt enkelt att genomföra. Idag kan många fingeravtrycksläsare luras av falska fingeravtryck [3], något som skrupelfria gangsters från Indonesien bevisade när de stal en ny bil med fingeravtryckslås på ett osmakligt sätt [6]. Ett samhälle som förlitar sig på biometri i den utsträckning som visas i filmen är skyldig sina medborgare att på något sätt säkra dem mot denna typ av brott, för glädjen att slippa ha nycklar som kan bli stulna grusas om fingrar och händer börjar stjälas istället.

Fingeravtrycksläsare måste bli betydligt mer resistent mot förfälskningar om samhället som avbildas i denna film skall kunna fungera, eftersom vinsten med att kunna lura systemet potentiellt sett är mycket stor. Detta kommer med all säkerhet att driva på utvecklingen av förfälskningstekniker. Om fingeravtrycksläsare i framtiden accepterar avklippta fingrar på det sätt som de gör i filmen förutsäger jag att bankväsendet inte kommer att grunda sina transaktioner på denna teknik.

3.4. Ocean's Eleven (2001)

Filmen handlar om en välplanerad stöt mot ett kasino i Las Vegas. Det centrala i filmen är det synnerligen välbevakade kassavalvet 60 meter under marken där filmens huvudpersoner planerar att ta sig in för att göra ett större uttag. De biometriska system som används i filmen är båda kopplade till säkerheten kring valvet och inkluderar fingeravtrycksläsare och röstidentifiering.

3.4.1. Fingeravtryck

Hissen som länkar det underjordiska valvet till ytan kräver identifiering med fingeravtryck. För att nå denna hiss måste man dock passera en säkerhetsdörr med en vakt, där det dessutom krävs ett speciellt nyckelkort för att få passera. Detta system används bara en gång i filmen, och då av en vakt som har tillträde till hissen. I planeringsstadiet till kuppen nämns systemet också, då det pekas ut som omöjligt att knäcka.

Säkerhetsmässigt är det ingen dum idé att använda fingeravtrycksavläsning på det sätt som det används i filmen, förutsatt att läsaren är bra nog. Genom att ha den biometriska läsaren "skyddad" bakom ett mer traditionellt säkerhetssystem kan ökad säkerhet uppnås vid valda platser, då flera olika system kan samverka för identifiering.

3.4.2. Röstigenkänning

I filmen presenteras röstigenkänning också som en del av valvets säkerhet. Av allt att döma krävs röstidentifiering både från personen som skall ner i valvet och från vakten nedanför hissen. Eftersom röstigenkänning är en något mindre mogen teknik än fingeravtryck finns det en rad potentiella problem med att implementera det i kombination med fingeravtryck. Om vi antar att båda systemen är helt robusta och aldrig gör fel kommer en säkrare identifiering av användarna att fås, men om det ena eller båda systemen har en tendens att ofta ge felaktig avvisning (false reject) kommer tillgängligheten för systemet som helhet att minska. Fingeravtryckstekniken brukar i dagsläget anses ge mindre än 1 % felaktig avvisning för high-end läsare [10,11] vid identifiering, men för röstigenkänning är det betydligt svårare att göra en bedömning av hur stor den felaktiga avvisningen är. Tillverkarna påstår att deras teknik är säker [7,8,9] medan andra menar att tekniken inte är mogen ännu [4].

3.4.3. Är systemet omöjligt att knäcka?

Påståendet att systemet är omöjligt att knäcka är lite förvånande för att komma från en grupp gangsters med synnerligen goda resurser både avseende pengar och teknisk kompetens. Den lösning man skulle kunna tänka sig som ett alternativ för att knäcka systemet i fråga är att huvudpersonen får tag på en av vakternas fingeravtryck, till exempel genom att bjuda honom på en drink och sedan "lyfta" fingeravtrycket från det använda glaset. Med denna information kan sedan ett falskt fingeravtryck tillverkas som kan användas för att lura fingeravtrycksläsaren. Med den teknik som finns tillgänglig idag finns det anledning att anta att en dylik manöver faktiskt skulle kunna lyckas. Att sedan lura röstidentifikatorn bör vara så enkelt som att spela in vaktens röst och antingen använda den direkt för att lura systemet eller gå bakvägen och skapa en syntetisk röst som passerar kontrollen. Det senare förutsätter att du har tillgång till de algoritmer som röstidentifieringen bygger på, men detta bör vara ett mindre problem för gangsters med både charm, pengar och flinka fingrar.

Med detta i bagaget behöver du dock fortfarande komma förbi vakterna, men med lite fantasi, smink och stulna passerkort borde det kunna lösas. Givetvis måste du även ha en plan när du väl kommit ner i valvet, men här tänker jag inte utveckla mitt resonemang vidare. Det jag vill poängtera är att de flesta av dagens system för biometrisk identifiering går att lura, särskilt om du har kunskap om hur den bakomliggande tekniken fungerar. I filmen är dock säkerheten implementerad på ett i mina ögon korrekt sätt eftersom de biometriska läsarna på alla ställen är bevakade.

3.5. The Bourne Identity (2002)

Jason Bourne (Matt Damon) hittas medvetslös i Medelhavet med två kulor i ryggen. Han minns ingenting av sitt tidigare liv, men snart upptäcker han att han har en naturlig fallenhet för att misshandla folk på ett effektivt sätt. Jason finner sig på grund av sitt något plumpa agerande tidigt i filmen snart vara jagad, både av polisen och av osympatiska män med automatvapen.

3.5.1. Handavtryck

När Bourne ska checka ut sin agentutrustning från en bank i Zürich tillfrågas han först om sitt kontonummer. När han har uppgivit detta får han åka hiss ner i bankvalvet för att där lägga sin hand på vad som ser ut som en 15" TFT-skärm som läser av Bourne's högerhand och identifierar honom som innehavare till kontot.

Handavläsning är en teknik som finns på marknaden idag och fungerar ungefär som för fingeravtrycksläsning. Det som kan påpekas är att det även finns teknik som läser av handens geometri i tre dimensioner, men denna teknik används uppenbarligen inte i filmen. De system som finns tillgängliga är dock genomgående betydligt dyrare än motsvarande fingeravtrycksläsare [12,13], vilket till stor del beror på att sensorns inläsningsyta är större och dyrare, samt att en större mängd data samlas in vid varje sampel vilket kräver mer beräkningskapacitet hos läsaren. För en schweizisk bank bör dock denna prisskillnad vara tämligen ointressant om säkerheten kan förbättras.

4. Diskussion

4.1. Tekniken

Användandet av biometri i det studerade urvalet filmer är ur en rent teknisk synvinkel inte orimlig om vi ser till den teknik som finns i dagsläget. Idag finns till exempel kommersiella fingeravtrycksläsare som fungerar ungefär som de system som visas i filmerna, både på gott och på ont. I filmen *The 6th day* behövs ett registrerat fingeravtryck för att kunna starta bilen och denna teknik finns i dagsläget i tillräckligt utvecklad form för att vara användbar. I filmen kan dock bilen startas genom användandet av ett avklippt finger och detta verkar dessvärre också vara en svaghet hos dagens biometriska system. De läsare som finns idag är bra på att skilja olika fingeravtryck åt men de är mindre bra på att skilja mellan äkta och falska versioner av samma fingeravtryck.

Den vanligaste orsaken till att filmers biometriska system inte är implementerbara ur teknisk synvinkel är annars att ingen åtskillnad görs mellan identifikation och verifikation av en användares identitet. I filmen *The Bourne identity*

används fingeravtryck för att verifiera huvudpersonens identitet, vilket är möjligt att göra i dagens läge. I filmerna *Face/Off* och *The 6th day* används istället den biometriska tekniken för att fastställa identiteter vilket är betydligt svårare att göra, särskilt om användarens identitet skall matchas mot en stor databas med biometriska data.

4.2. Säkerhetstänkandet

Ett annat område där det finns saker att anmärka på filmernas hantering av biometri är ur det säkerhetsmässiga perspektivet. Det verkar finnas en överdriven tilltro till biometrisk identifiering som gör att denna teknik likställs med total säkerhet, även i de filmer där tekniken betvingas. Detta har givetvis ofta en dramaturgisk bakgrund eftersom filmen berättar en historia, men vissa frågor bör ändå ställas om säkerheten i dessa system.

I filmen *The 6th day* kan huvudpersonen ta sig in på ett hemligt område genom att använda ett avklippt finger som enda identitetshandling. De som ansvarar för säkerheten måste rimligen veta om att systemet har denna brist och det är därmed mycket underligt att en biometrisk läsare med denna uppenbara brist kan användas som enda identitetskontroll vid ett objekt med hög säkerhetsklass. Den identifieringssäkerhet som ett dylikt system ger bör inte anses vara bättre än den säkerhet som ges genom användandet av en vanlig nyckel, då den kontroll som genomförs enbart verifierar att personen är i besittning av ett visst objekt, oavsett om objektet är en nyckel, ett magnetkort eller ett finger. För att ett biometriskt system skall fungera som avsett krävs att systemet faktiskt mäter någon del av en människa för att därigenom kunna identifiera eller verifiera människan. Ett system som gör avkall på detta och inte kontrollerar att det som mäts faktiskt fysiskt tillhör den person som det antas tillhöra är att jämföra med ett vanligt nyckelsystem. Det är svårare för gemene man med dagens teknik att förfalska ett finger än en nyckel, och det är betydligt obehagligare att stjäla ett finger än att stjäla en nyckel eller ett smartkort, men om biometrin inte kan avgöra vad som är en kroppsdel och vad som inte är en kroppsdel kommer säkerheten enbart att bestå i att identitetshandlingarna i dagens läge är svårörfalskade och svåra/obehagliga att stjäla. Dessutom skall vi inte glömma bort att vi ständigt lämnar fingeravtryck i vår omgivning, till exempel på muggar och dörrhandtag.

Om en person lyckas få tag på ditt fingeravtryck och gör en förfalskning som är godtagbar för de fingeravtrycksläsare som finns tillgängliga är det svårt att möta detta problem på ett bra sätt. Ett nyckelkort som kommer ur din besittning kan spärras, en borttappad nyckel kan hanteras genom att

låsmechanismen byts ut, men ett borttappat fingeravtryck går inte att byta ut. Om inte läsarna i detta fall kan uppgraderas för att upptäcka förfalskningen måste ditt fingeravtryck spärras, vilket resulterar i att du kommer att behöva identifiera dig på något annat sätt. Detta kan bli ett mycket obekvämt problem för användare, samtidigt som det är en realitet för alla typer av biometriska system. Om en näthinna eller en persons röst kan förfalskas resulterar detta i samma typ av problem. Om biometrin någonsin skall kunna slå igenom på bred front måste det finnas en beredskap för att hantera dessa problem, annars kommer biometriska säkerhetssystem att vara dömda till en tillvaro i säkerhetens utkanter.

5. Slutsats

Nedan besvaras de frågeställningar som presenterades i uppsatsens inledande kapitel.

Återspeglar den biometriska tekniken i dagens filmer verkligheten ur ett tekniskt perspektiv?

Denna fråga anser jag har två svar; ja och nej. Biometrin i de studerade filmerna avspeglar den teknik som idag finns tillgänglig, till exempel inom fingeravtrycksområdet. Det går utmärkt att läsa av ett finger i en läsare och matcha inläsningen mot en person. I filmerna finns dock en tendens att inte skilja på identifiering och verifiering av identiteter. Det är i dagsläget svårt att utföra identifiering mot stora urvalsgrupper på ett snabbt och säkert sätt. Ur denna synvinkel avspeglar filmernas biometri inte alltid verklighetens biometri.

Hur är de biometriska systemen i filmerna implementerade säkerhetsmässigt?

Säkerhetsmässigt är biometrin ibland mycket dåligt implementerad i filmerna. De främsta problemen härrör till obefintlig liveness-detektering eller underlig placering av biometriska läsare, till exempel på insidan av fängelser.

6. Referenser

[1] A Ross, A Jain, J Reisman (2003), *A Hybrid Fingerprint Matcher*, Pattern Recognition Journal, Vol. 36, No.7, pp. 1661-1673

[2] BioEnable, *The biometric white paper*, <http://bioenabletech.com/biometrics/whitepaper4.htm>

[3] Biometrics Info, *Liveness detection in biometric systems*, <http://www.biometricsinfo.org/whitepaper1.htm>

[4] Fran Howarth, Bloor research 17/02/2005, *Technological barriers to the take up of biometrics*, www.it-director.com

[5] Fran Howarth, Bloor research 15/02/2005, *Social barriers to the take up of biometrics*, www.it-director.com

[6] Jonathan Kent, BBC News 31/03/2005, *Malaysia car thieves steal finger*, <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>

Röstigenkänningsteknik - företag

[7] Voice Security Systems, <http://www.voice-security.com/>

[8] VoiceVault, <http://www.voicevault.com>

[9] PerSay, <http://persay.com>

Fingeravtryck - företag

[10] Arrow Vision, <http://www.arrowvision.us>

[11] Hongda Group, <http://www.cchongda.com.cn>

[12] Acroprint, <http://www.acroprintstore.com>

[13] Cross Match. <http://www.crossmatch.com/pdf/id2500.pdf>

Filmer

Face/Off (1997), <http://www.imdb.com/title/tt0119094>

Enemy of the State (1998), <http://www.imdb.com/title/tt0120660>

The 6th day (2000), <http://www.imdb.com/title/tt0216216>

Ocean's Eleven (2001), <http://www.imdb.com/title/tt0240772>

The Bourne identity (2002), <http://www.imdb.com/title/tt0258463>