

TDDC03 Project, Spring 2004

Biometri med fingeravtryck

Hans Hazelius
hanha320@student.liu.se

Karl Larsson
karla350@student.liu.se

Kristin Anderson

Supervisors:

Fredrik Claesson

Biometri med fingeravtryck

Hans Hazelius
hanha320@student.liu.se

Karl Larsson
karla350@student.liu.se

Linköpings tekniska högskola, Sverige

10 maj 2004

Sammanfattning

Denna rapport behandlar fingeravtrycksbaserad biometri. Den beskriver tekniken som används för att avläsa, behandla och jämföra ett fingeravtryck. Dessutom redogör rapporten för några av de problem som finns med denna teknik samt vilka attacker som fingeravtrycksbaserade biometrisystem kan utsättas för. Utöver detta beskrivs några praktiskfall som använder sig av fingeravtryck för t.ex. gränskonroll. Fingeravtrycksbaserad biometri har, enligt oss, fortfarande vissa brister och vi pekar på att en kombination av olika tekniker, som t.ex. fingeravtrycksbaserad biometri och ansiktsbaserad biometri, är att föredra.

1. Introduktion

För fördjupning i ämnet biometri med fingeravtryck har vi fått i uppgift att analysera området och sammanställa en rapport. Denna rapport är en del av examinationen i kursen TDDC03: Informationssäkerhet, på Linköpings universitet.

1.1 Frågeställning

- Hur fungerar biometriska system som använder sig av fingeravtryck som identifierare?
- Vilka problem finns det inom området?
- Vilka sorts attacker kan göras på system som använder sig av fingeravtrycksbaserad biometri?
- Vilka exempel finns det där fingeravtrycksbaserad biometri har använts i praktiken och hur har det fungerat?

1.2 Metod

Vi har valt att göra en kvalitativ litteraturstudie som tar upp ämnet fingeravtrycksbaserad biometri. Vi har sökt litteratur på Internet samt på Linköpings universitetsbibliotek. Framförallt har vi letat efter vetenskapliga publikationer. En kortare intervju med en examensarbetare, som arbetar inom ämnet, har även utförts.

Arbetet har varit uppdelat mellan rapportskrivarna. Under arbetets gång har diskussioner hållits för att kunna bibehålla enhetlighet mellan rapportens delar samt för att bibehålla vår gemensamma syn på arbetet. Analys och diskussion samt slutsats har genomförts gemensamt.

2 Teori

Detta avsnitt innehåller en överblick över biometriska tekniker, framförallt området som berör avläsning av fingeravtryck. Vi beskriver här olika metoder för inläsning och jämförande av fingeravtryck. Vi visar även på diverse problem och attacker som denna teknik kan medföra. Slutligen tar vi upp några användningsområden som existerar idag.

2.1 Biometriska tekniker

Biometriska system delas upp i två huvudgrupper, verifierarsystem och identifierarsystem. Det är metoden för att ta fram en persons identitet som skiljer grupperna åt. I verifierarsystem gäller det att bestämma om personen i fråga är den han säger sig vara och i identifierarsystem gäller det att fastställa personens identitet. För verifierarsystem så är det svaret på frågan "Är den jag säger att jag är" som söks. Med den här modellen räcker det att jämföra personens avtryck med det kända avtrycket som finns lagrat i en databas för att få svar på frågan. Ett exempel på denna modell är inloggning på en dator, användaren skriver in sitt användarnamn och lösenord. Om indata matchar med det som finns lagrat i datorn så får användaren tillgång till systemet. För identifierarsystem är det svaret på frågan "Vem är jag?" som söks. Här måste hela databasen med fingeravtryck sökas igenom för att få svar på frågan. Ett exempel på användning av den här metoden är kriminaltekniker som har hittat ett fingeravtryck på en brottsplats och vill veta vems det är.[1]

Biometriska tekniker baseras på fysiska eller beteendekaraktäristiska drag. Fysiskt biometriskt igenkännande använder sig till exempel av ansikte, ögon, fingeravtryck, handavtryck eller termiska bilder medan biometriskt igen-

kännande, som baseras på beteende, använder sig av exempelvis rösten eller skrivsätt på tangentbord som identifieringskälla. Teknologin har potential för att användas i flera olika tillämpningsområden. Biometrisk teknik kan bland annat användas för att hindra oauktorerad åtkomst till bankomater, mobiltelefoner, smarta kort, bärbara datorer, arbetsstationer och nätverk.[2]

2.2 Fingeravtrycksidentifikation

Fingeravtrycksidentifikation är den mest förekommande och kända formen av biometrisk teknik. Man har länge använt sig av fingeravtryck. Skillnaden är att man idag läser in fingeravtrycket till en dator med olika tekniker istället för att som förr i tiden registrera fingeravtryck genom att applicera bläck på fingret och sedan pressa detta mot ett papper.[2] Verifikationsprocessen går i korta ordalag till så att personen ifråga får sitt fingeravtryck läst med en avläsare. Bilden med fingeravtrycket som kommer ut av avläsningen behandlas för att förbättra kvalitén på bilden. Sedan extraheras punkter eller mönster med exempelvis en minutiaeanalys (se 2.5). Dessa data lagras som en mall eller används för att verifiera en person mot en redan lagrad mall.[3]

2.3 Olika skannertekniker

Det finns flera skannertekniker som används för att läsa av fingeravtryck. De flesta biometriska läsare läser av och analyserar mönster på avtrycket. Med mönster menas de åsar (upphöjningar i huden) och dalar (nedsänkningar i huden) som återfinns på fingrets yta.

Nedan beskrivs några av de tekniker som finns för att läsa av ett fingeravtryck.

2.3.1 Optiska sensorer

Dessa sensorer använder sig av ljus för att lysa upp en platta som fingret trycks emot. Fingret reflekterar sedan ljuset som leds genom prisma och linser för att slutligen nå en kamera som lagrar bilden för analys.[3]

2.3.2 Elektriska sensorer

Genom att mäta variationer i ett konduktivt lager under fingrets yta läser dessa sensorer av fingeravtryck. Det som orsakar dessa variationer är differenser i tjocklek mellan åsar och dalar i fingrets yta. Detta formar ett fingeravtryck som kan analyseras.[3]

2.3.3 Kapacitiva sensorer

Kapacitiva sensorer är väldigt lika elektriska sensorer vad gäller storlek och funktion. De använder sig dock av en serie

sensorer som mäter differensen i kapacitansen mellan åsar och dalar.[3]

2.3.4 Ultraljudssensorer

Dessa sensorer mäter differensen i den akustiska impedansen mellan åsar och dalar i fingrets yta. Sensorerna använder sig av frekvenser från 20kHz, vilket är strax över vad människan kan höra, upp till flera GHz. Detta är nödvändigt för att få en upplösning som är hög nog för att urskilja ett fingeravtryck.[3]

2.3.5 Temperatursensorer

Temperatursensorer använder sig av en serie av temperaturkänsliga element som mäter temperaturskillnader i fingrets yta. Närmare bestämt mäts skillnaden mellan åsarnas temperatur och temperaturen på luften i dalarna. I och med detta får sensorn fram ett mönster som går att analysera.[3]

2.3.6 Trycksensor

Trycksensorerna har en flexibel yta som trycks ner med fingret. I sensorn finns en serie av tryckkänsliga element som skiljer på åsar och dalar på fingrets yta. På detta sätt skapas en bild av avtrycket.[3]

2.3.7 Sweepingsensorer

Detta är egentligen ingen särskild teknik. Med "sweeping" menas att fingret dras över en sensor istället för att fingret trycks mot en platta. En sweepingsensor kan använda sig av flera av de ovanstående teknikerna för att läsa av fingeravtrycket som till exempel en temperatur-, kapacitiv eller elektrisk sensor. En av fördelarna med detta är att det inte lämnas kvar ett avtryck som går att återanvända.[4]

2.4 Bildbehandling

När en sensor har skapat en bild av ett fingeravtryck är den bilden väldigt otydlig. En dålig bild kan medföra en felaktig identifieringsprocess och därför behöver bilden förbättras. Detta kan göras genom att applicera ett antal filter på bilden. Filttering av en bild tar för det mesta lång tid och därför är det ofta en avvägning mellan kvalitet och tid.[5] Nedan beskrivs några filtreringsmetoder.

2.4.1 Normalisering

Normalisering är ett bra första steg för att förbättra bildkvalitet.[3] Att normalisera bilden betyder att man sprider ut bildens färgskala så att den fyller alla tillgängliga värden i gråskalespektrumet. För att normalisera bilden gäller det att först hitta hur mycket gråskalan varierar, det vill säga

största och minsta punkten, eller pixelvärdet, i bilden. När man hittat dem, kan gråskalan spridas ut. Fördelen med normalisering är att ljusa och mörka bilder får samma spridning och att det då blir lättare att bestämma kvalitén på bilden.[6]

2.4.2 Binarisering

Binarisering är en process som gör det lättare att hitta minutiae punkterna (se 2.5) i ett avtryck. Det fungerar så att en gråskalig bild av ett fingeravtryck omvandlas till en binär bild. De binära värdena 0 och 1 representeras här av färgerna svart och vit. När en bild ska omvandlas plockas ett tröskelvärde ut i gråskalan. Detta värde används sedan för att omvandla varje pixel i bilden till antingen svart eller vit beroende på vilken sida om tröskelvärdet pixeln befinner sig från början. Allting som har ett lägre värde än tröskelvärdet, d.v.s. mörkare färg, blir svart och allting som har ett högre värde än tröskelvärdet, d.v.s. ljusare färg, blir följaktligen vitt[7].

Problemet med binarisering ligger i att hitta ett lämpligt tröskelvärde eftersom det är omöjligt att hitta ett globalt gemensamt tröskelvärde för en bild. Det har tagits fram många algoritmer som hanterar val av tröskelvärde. Många av dessa använder sig av global tröskelsättning vilket innebär att ett värde sätts för hela bilden[3]. Ett exempel på en sådan algoritm är Otsusmetoden[8]. Idag används dock lokal tröskelsättning mest. Det innebär att bilden delas upp i flera delar och att ett tröskelvärde beräknas för varje del. Detta kräver dock fler beräkningar och tar längre tid men det ger också ett mycket bättre resultat än global tröskelsättning.[3]

2.4.3 Lågpasfiltrering

Lågpasfiltrering fungerar så att en bildpunkt i taget bearbetas med avseende på de omkringliggande punkterna. Med detta menas att man ger den aktuella punkten en färg som beräknas fram genom att ta medelvärdet av omkringliggande punkter. Genom att göra detta avviker ingen punkt extremt mycket från sina grannar vilket annars skulle kunna ge felaktigheter vid en minutiaeanalys (se 2.5).[3]

2.4.4 Kvalitetsmärkning och segmentering

Kvaliteten vid en fingeravtrycksavläsning kan variera kraftigt. Det kan vara att personen som avger avtrycket har bråttom och inte trycker ner fingret ordentligt mot avläsaren eller att personen i fråga trycker för hårt. Bilden av avtrycket har då en dålig kvalitet och innehåller därför mycket data som är oanvändbar. Kvalitetsmärkning och segmentering är två metoder för att urskilja de data som är dåliga och onödiga och ta bort dessa från bilden. Annars kan dessa dåliga partier ge upphov till att flera falska punkter hittas vid en minutiaeanalys (se 2.5).[9]

När ett fingeravtryck avläses av en sensor så innehåller bilden även en bakgrund. Segmentering innebär att fingeravtrycket avskiljs från bakgrunden. Precis som vid binarisering beräknas ett tröskelvärde eftersom bakgrunden ofta är ljusare än själva fingeravtrycket. På det sättet kan de ljusare partierna, som tillhör bakgrunden, avlägsnas. Metoden är enkel men dock väldigt känslig för störningar i bakgrunden vilket kan leda till att dessa partier i bakgrunden räknas som en del av fingeravtrycket.[9]

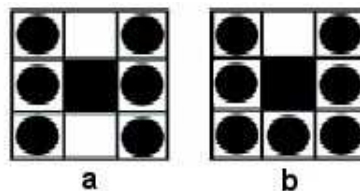
Kvalitetsmärkning går ut på att lokalisera dåliga delar i en bild och märka dem. Detta är dock inte lätt eftersom färgskalan på de dåliga partierna är i det närmaste de samma som den färgskala som återfinns i de bra partierna. Ett sätt för att skilja ut de dåliga partierna är att använda sig av s.k. fältriktninganalys. Tanken är att ta bort alla de partier där det inte finns något enhetligt mönster som det finns i de delar av bilden som innehåller åsar och dalar.[3]

2.5 Minutiaeanalys

En minutiaeanalys är en väldigt vanlig metod för att utvärdera ett fingeravtryck. Analysen fokuserar på områden där åsar klyvs, där åsar slutar, vinklar i avtrycket, samt avståndet mellan vissa nyckelpunkter i fingeravtrycket. Dessa nyckelpunkter kallas för "minutiae".[10]

2.5.1 Konnektivitetsnummer

Detta är en enkel process för att ta reda på antalet objekt som en pixel har i sin omgivning. Meningen med det här är att ta bort oönskade och oanvändbara data. För att kunna utföra detta ska bilden ha gått igenom en binariseringsprocess så att pixelvärdena endast representeras av svart och vitt. En centumpixel kan ha 8 stycken angränsande pixlar. De möjliga konnektivitetsnumren är 0,1,2,3 och 4 som räknas fram genom att ta det minimala antalet angränsande pixlar med färg av antingen svart eller vit. Den totala summan kommer alltid upp i 8. 0 innebär 0 eller 8 angränsande pixlar, 1 innebär 1 eller 7 angränsande pixlar o.s.v..[3]



I figuren ovan har 'a' ett konnektivitetsnummer på 2. I det här fallet kan centumpunkten inte tas bort eftersom den binder ihop objekten på höger och vänster sida om centumpunkten. 'b', som har konnektivitetsnummer 1, kan centumpunkten tas bort eftersom höger- och vänsterobjektet fortfarande hänger ihop vilket gör centumpunkten överflödig.

2.5.2 Tunning

Metoden går ut på att omvandla alla linjer i en binariserad bild så att de bara blir en pixel breda utan att förstöra mönstret i den ursprungliga bilden. Metoden kallas även för skelettbildning eftersom den efterlämnar en typ av skelettbild av den ursprungliga bilden. Metoden ger goda förutsättningar för att en minutiaeanalys ska få ett lyckat resultat.[3] En av de algoritmer som används för att utföra en tuning är Zhang-Suen algoritmen[11].

2.5.3 Punktidentifiering

Nu har vi kommit till den delen i minutiaeanalysen som innebär identifiering av minutieapunkter. Som sagts tidigare är det här en fördel om fingeravtrycksbilden genomgått en tunningsprocedur. Problematiken här ligger i att veta hur skelettbilden har tagits fram. Närmare bestämt hur en pixel är kopplad till andra pixlar i bilden. Är pixeln kopplad till alla åtta omgivande pixlar eller bara de fyra som har direkt kontakt med den aktuella pixeln? Som exempel kan vi ta Zhang-Suen algoritmen[11] som togs upp som exempel i tidigare avsnitt. Denna algoritm resulterar i en skelettbild där varje pixel är kopplad till alla omgivande pixlar. Det normala sättet att leta efter minutieapunkter i det här fallet är att välja en förgrundspixel och sedan kontrollera vilka av de omgivande pixlarna som är förgrundspixlar. Blir summan 1 så är den valda förgrundspixeln en ändpunkt. Är summan 2 ligger den valda förgrundspixeln på en ås och är summan 3 eller mer ligger den valda förgrundspixeln i en förgrening.[3]

2.6 Matchning

Matchning kallas den process då två fingeravtryck ska jämföras med varandra. Normalt sett brukar fingeravtrycket jämföras mot en mall som tidigare registrerats med hjälp av ett fingeravtryck och minutiaeanalys. Om dessa två fingeravtryck överensstämmer med varandra till en viss grad eller tröskelvärde kallas det att avtrycken matchar varandra. Det finns mycket problematik länkat med den här processen. Även om exakt samma minutieapunkter återfinns i två olika fingeravtryck så finns chansen att matchningen inte blir positiv. Detta beror på att positionen och vinkeln på fingret vid de båda avläsningarna skiljer sig från varandra vilket får minutieapunkternas placering att bli olika. För att komma runt det här problemet brukas en metod som innebär att en centrumpunkt placeras ut på fingeravtrycket som fungerar som en referenspunkt för ett koordinatsystem. Normalt försöker matchningsalgoritmen att rotera runt centrumpunkten och jämför minutieapunkter i olika vinklar inom ett visst intervall. För att begränsa antalet beräkningar brukar ett intervall av ± 10 grader användas. På

detta sätt kan fel som bygger på förflyttningen av ett finger begränsas.[10]

2.7 Problem

De problem som kan uppstå med fingerigenkänning kan delas upp i två huvudproblem. Dels är det de tekniska aspekterna som t.ex. problem vid inläsning, men det finns även problem med den personliga integriteten.

2.7.1 Tekniska aspekter

En läsare kan bli skadad, t.ex. en optisk läsare måste ha en transparent lins vilken kan bli repig och på så sätt försämrar inläsningen. Vissa sensorer analyserar endast bilden av fingeravtrycket och tar inte hänsyn till om det är ett levande finger bakom. När ett fingeravtryck ska läsas in så finns det flera faktorer som spelar in om hur bra avtrycket blir, vissa scannertekniker är mer känsliga än andra. Faktorerna är bland annat: temperaturen på ett finger, om fingret är fett eller uttorkat, hur luftfuktigheten är vid scannern, med vilken vinkel som fingeravtrycket lämnas, med hur hårt tryck avtrycket lämnats, positionen på scannern (om fingret är centrerat på sensorn eller inte), sår på fingret eller andra märken som kan komma via tex trädgårdsarbete. Ett fingers struktur ändras även med åldern.[10]

Optiska sensorer är den typ som har används längst tid och är även den typen som är billigast och det kan vara en orsak att använda den. Dock är denna sorters sensor mycket känslig för ytliga förändringar på fingret såsom sår och temporära missfärgningar. Tekniken som används i optiska sensorer gör att sensorn även blir ganska stor jämfört med andra sorts sensorer.

Sensorer som använder sig av ultraljudsteknik läser av fingeravtrycket på en nivå längre in i fingret än ytan och är därför inte känslig för missfärgningar som t.ex. oljefläckar. En stor nackdel med ultraljudssensorer är priset. Detta gör att användning av den här typen av sensor vid stora projekt som t.ex. flygplatser ökar kostnaderna markant.

På grund av tekniken som tyckkänsliga sensorer är uppbyggd på så har de inte så hög känslighet. Därför blir inte fingeravtryck från en sådan sensor bra.[10]

Temperatursensorer använder temperaturskillnader som måtelement och är således mycket känslig för temperaturändringar i fingret. För att uppväga det så brukar sensorerna värmas till en viss arbetstemperatur. Kapacitansbaserade sensorer är känsliga för förändringar i kapacitansen som kan uppstå t.ex när fingret är vått.

Ett annat problem är statisk elektricitet som kan uppstå. Därför är det mycket viktigt att jorda sensorn på ett bra sätt.[10] Ett annat problem som kan uppstå: Vad händer om sensorn som har läst in referensavtrycket går sönder och måste bytas ut? Olika sensorer kan använda olika meto-

der att lagra avtrycket i en databas.[12] I värsta fall så måste nya referensavtryck läsas in, vilket kan vara en besvärlig process.

2.7.2 Personlig integritet

System som hanterar fingeravtryck måste lagra informationen om fingeravtrycket någonstans. Eftersom fingeravtryck har biologiskt ursprung så kan annan information extraheras från fingeravtrycket. Ett exempel på det är att det är känt att en speciell fingerform är starkt bunden till en viss genetisk defekt. I framtiden kanske forskare kommer fram till andra samband mellan fingeravtryck och sjukdomar. Att kunna extrahera sådan information från ett fingeravtryck påverkar den personliga integriteten stort. Många sensorer kräver att man pressar sitt finger mot själva sensorn för att det ska bli ett så bra resultat som möjligt, nackdelen med det är att det även blir ett bra avtryck kvar på sensorn som senare kan extraheras med diverse metoder. Sweepingsensorer har den fördelen att när personen läser in sitt fingeravtryck så rengör han samtidigt sensorn från sitt fingeravtryck så inget användbart avtryck sparas.[10]

Eftersom fingeravtryck har använts länge inom kriminalteknik för att spåra brottslingar kan det vara risk att människor förknippar att lämna ett fingeravtryck med något negativt. För att minska risken att användarna uppfattar tekniken som negativ så är det bästa alternativet att informera användaren om hur tekniken fungerar. Fördelen med fingeravtrycksbaserad biometri jämfört med andra biometriska tekniker är att normalt sett så har en människa 10 st fingrar att lämna fingeravtryck med, så man kan använda olika fingrar till olika system.[13]

2.8 Attacker

Exempel på attacker som kan göras på system för fingeravtrycksigenkänning är bland annat s.k. denial of service attack, dvs att systemet skadas så att användare som egentligen skulle komma in i systemet nekas tillgång.

- Tvång: En användare tvingas att identifiera sig mot systemet av en icke legitim användare.
- Intrång: En illvillig användare använder sig av metoder för att få tillgång till systemet.

I den här rapporten kommer vi endast att ta upp det senaste alternativet.

Eftersom ett system som identifierar användaren m.h.a. fingeravtryck består av flera delsystem som t.ex. själva avtrycksavläsaren, en databas och alla led mellan de två, så finns det flera ställen där attacker kan utföras. Här kommer vi bara att ta upp attacker mot själva avtrycksläsaren då det är den delen av systemet som är lättast åtkomlig för en attackerare.[10]

2.8.1 Artificiella fingrar

Ett sätt utföra en attack på fingerscannern är att skapa ett artificiellt finger som imiterar det riktiga fingret som har tillgång till systemet. För att skapa ett artificiellt fingret kan man göra en avgjutning av silikon eller gelatin. Metoden för att framställa ett sådant finger är att först ha tillgång till det avtryck som man vill kopiera, antagligen en bild på ett avtryck från en person som har legitimt tillträde till systemet. Det kan också vara ett avtryck som är genererat av en dator. En människas fingertoppar har många små fett och svettporer som gör att när en person tar på någon yta så lämnas det kvar ett tunt fingeravtryck av fett på ytan som berördes. Detta avtryck kan senare tas vara på genom att t.ex. strö kolpulver över det och sedan överföra avtrycket till ett papper m.h.a. en tejpbit. Därefter kan man förbättra bilden i en dator för att sedan skapa en gjutform till avtrycket. Trots att det är en relativt enkel procedur att skapa en tredimensionell kopia från ett fingeravtryck så är det mycket svårt att få tillgång till ett fingeravtryck som duger till att skapa kopian. Först och främst så måste man veta var ett fingeravtryck från den person, vars fingeravtryck som ska förfälskas, finns. Sen är det inte säkert att fingeravtrycket är komplett vilket t.ex. kan inträffa om ytan som fingeravtrycket hämtats ifrån inte är helt plan eller glatt.[10]

För att försvåra attacker med artificiella fingrar är en möjlighet att testa om fingret som används verkligen är från en person, d.v.s. att testa att fingret är levande. Det gäller alltså att kunna skilja mellan ett riktigt finger och ett som är framställt på syntetisk väg. Det kan göras genom att testa olika egenskaper för den mänskliga huden, exempel på sådana är fingrets värme, hur väl fingret leder ström, eller fingrets optiska egenskaper. Andra mänskliga egenskaper är t.ex. puls, blodtryck och svettutsöndring.[10]

Ett levande finger brukar vara några grader varmare än omgivande temperatur medan ett artificiellt finger i regel brukar vara lite kallare. Skillnaden vid rumstemperatur mellan ett levande finger och ett gjort av silikon är runt 2 grader Celsius.[10] Denna skillnad skulle kunnas användas för att skilja ett levande finger från ett artificiellt. Dock kan temperaturen på ett levande finger variera ganska mycket, t.ex. p.g.a. luftkonditionering eller om användaren har haft något kallt i handen innan han lämnar sitt fingeravtryck. Detta tillsammans med att det inte är så svårt att värma upp ett artificiellt finger lite, gör att metoden att kontrollera om fingret är levande m.h.a. värme är ganska otillförlitlig.[10]

Människans huds konduktivitet skiljer sig från konduktiviteten i gelatin eller silikon. Därför vore ett sätt att upptäcka ett artificiellt finger att testa konduktiviteten. Nackdelen med det här är att konduktiviteten ändras beroende på luftfuktigheten eller om fingret är fuktigt. Om man t.ex. fuktar ett finger av gelatin med lite alkohol så får det en konduktivitet som är väldigt snarlik konduktiviteten hos ett riktigt finger.[10]

En metod för att upptäcka artificiella fingrar är att undersöka de optiska egenskaperna hos fingret, till exempel hur ljus med olika våglängder beter sig i fingret. Dock är det inte så svårt att tillverka ett artificiellt finger med liknande optiska egenskaper som ett mänskligt finger. Fingrar som är gjorda av gelatin har optiska egenskaper som liknar ett mänskligt finger väldigt mycket. Ett annat sätt att upptäcka falska fingrar är att använda sig av mycket hög upplösning när man läser in fingeravtrycket så att man får med små detaljer i fingeravtrycket som t.ex. svettkörtlar. Ett finger som saknar sådana detaljer är med hög säkerhet inget mänskligt finger och kan därför nekas tillträde.[10]

Ett vanligt sätt att undersöka om en människa lever är att känna efter dess puls. Denna metod kan även användas för att identifiera ett levande finger, men eftersom det kan dröja några sekunder mellan varje pulsslag så måste själva insamlingen av fingeravtrycket pågå ett tag vilket kan tänkas vara en nackdel. Om man använder ett mycket tunt fingeravtryck av t.ex. gelatin och fäster det på ett riktigt finger så kommer sensorn att känna pulsen från det riktiga fingret samt läsa av det falska fingeravtrycket och på så sätt kan systemet kringgås.[10]

2.9 Användning i praktiken

Biometrisk teknik har varit aktuellt under en längre tid för att ersätta kort och nycklar för att kontrollera tillträde till olika anläggningar eller avdelningar. Detta är framför allt märkbart i USA där nya lagar och regler kräver en större användning av biometrisk teknik. Som exempel kan nämnas att hälften av kärnkraftverken i USA använder sig av handgeometri för att kontrollera tillträde till olika avdelningar. Ett annat exempel på användningsområdet för biometri är USA:s försvars-, energi- och justitiedepartement som använder tekniken för att kontrollera åtkomst till konfidentiella filer och dokument. De nya lagarna i USA har även krävt en större användning av biometri inom gränsövervakning.[14]

2.9.1 Gränsbevakning

Det senaste och mest kända fallet där bland annat fingeravtryck används är det system som USA officiellt har infört sedan den 5 januari 2004. Det handlar om gränsbevakning och systemet kallas för US-VISIT och finns nu installerat på 115 internationella flygplatser och 15 stora båthamnar. Innan slutet av år 2004 ska även 50 stycken av de gränsövergångar som finns i USA ha ett liknande system.[15]

Systemet fungerar så att man kombinerar de två biometriskerna fingeravtrycksavläsning och igenkänning av ansiktsdrag. Varje individ som besöker USA med visum får båda sina pekfingrar avlästa samtidigt som en bild av ansiktsdragen tas. Dessa data lagras sedan i en gigantisk databas. Denna databas används för att kunna identifiera varje

person på ett enkelt sätt men också för att kunna jämföra dessa data med andra register över t.ex. kända terrorister eller förbrytare.[15]

Tidiga tester som utförts på Atlanta International Airport var framgångsrika. Av 20 000 testpersoner lyckades man finna 21 personer som återfanns på FBI:s lista för eftersökta personer.[16]

Vetskapen om att dagens biometrisk teknologi inte är 100% tillförlitlig fanns redan innan projektet startades men tanken med systemet var inte att ersätta andra säkerhetsdetaljer utan att biometrisk teknik ska bli ytterligare en del i säkerhetskontrollen. Samtidigt ska biometrisk kontrollen fungera som avskräckande medel.[17]

På Cebitmässan i Tyskland var det gränsövervakning som stod högst upp på dagordningen när det gällde biometrisk produkter. Ett antal företag visade upp sina system för detta ändamål.[4]

2.9.2 Matvaruhandel

Kruger Co är en av USA:s största matvarukedjor. Matvarujätten har testat ett system där kunden betalar med sitt fingeravtryck. Det hela fungerar så att kunden registrerar sig i systemet och lämnar pekfingrets fingeravtryck. Kunden behöver alltså inget kreditkort eller pengar utan debiteras allt eftersom han/hon köper något. Systemet är dock bara på försöksstadiet och det återstår att se om det införs i matvarukedjans butiker. Matvarujätten menar dock att tidiga tester har varit framgångsrika. Dessa uppgifter är dock två år gamla och nya uppgifter om huruvida systemet används i större skala idag har inte erhållits.[18]

2.9.3 Bärbara produkter

Idag blir bärbara elektroniska produkter mer vanliga såsom fickminne och bärbara datorer. I och med att man numera tar med sig sin digitala information har kraven på säkerhet ökat även på dessa produkter. Tidigare fanns bara lösenordsskydd på fickminnen men det har nu kommit minnen med inbyggd fingeravtrycksläsare. Funktionen varierar väldigt mycket mellan olika minnen där vissa kombinerar lösenord och fingeravtryck medan andra enbart förlitar sig på fingeravtrycksläsaren.[19] Likadant är det med bärbara datorer, där det i vissa fall krävs fingeravtryck för att starta den bärbara datorn.[20]

3 Analys och diskussion

3.1 Biometrisk teknik

Det finns många olika tekniker för att läsa in fingeravtryck. De tekniker som den här rapporten berör är: optiska sensorer, elektriska sensorer, kapacitiva sensorer, ultraljudssen-

sorer, temperatursensorer, trycksensorer och sweepingsensorer. Alla har sina styrkor och svagheter. Optiska sensorer är de som har använts längst i praktiken och är därför väldigt vanliga, men andra tekniker som sweepingsensorer är på stark frammarsch. Mycket beroende på att dessa sensorer kan produceras i mindre storlek samt att de löser många fysiska problem som sår och att det lämnas kvar fingeravtryck på avläsaren.

När en bild skapas i fingeravtrycksläsare har bilden ofta en dålig kvalitet. Därför appliceras ett antal olika filter på bilden för att förbättra kvaliteten för att bilden ska kunna användas för en matchning eller som underlag till en mall. Exempel på sådana filter som tas upp i den här rapporten är normalisering, binarisering, lågpasfiltrering, kvalitetsmärkning och segmentering. Alla filtreringsmetoder har sina problem och resultatet av filtreringen hänger mycket på vilken typ av algoritm som används under vare filtrering. Dessutom måste tidsaspekten för varje filtrering vägas in för att verifieringsprocessen inte ska ta för lång tid. Till detta kan andra processer som konnektivitetsnummer och tuning läggas till för att förenkla nästa steg som innefattar en minutiaeanalys. Denna analys går ut på att få fram ett par nyckelpunkter från ett fingeravtryck, s.k. minutieapunkter. Dessa används sedan för att skapa underlag för en mall som lagras i en databas eller underlag för att utföra en matchning mellan ett fingeravtryck och en tidigare registrerad mall.

3.2 Problem

Fingeravtrycksbaserad biometri är inte helt utan problem. De tekniska problem som kan uppstå är många då det är komplicerat att känna igen fingeravtryck. Det gäller att garantera att den personen som vill logga in verkligen är den han säger sig vara. Men marknaden vill även ha små och smidiga sensorer som lätt kan integreras i befintliga system. Lösningar på problemet som innebär att biometri kan vara ett hot mot den personliga integriteten är nödvändiga för att användarna ska känna sig säkra att använda systemet. Att använda decentraliserade system där användaren har ett smart kort och en sensor som jämför datan på det smarta kortet med fingeravtrycket som lämnas kan vara ett steg mot ett biometrianvändning där användarna inte känner sig övervakade.

3.3 Attacker

Att förhindra fysiska attacker mot sensorerna, som syftar till att sabotera själva sensorn, är näst intill omöjligt då sensorerna är uppbyggda av känslig elektronik. Ett exempel är att använda en slägga och slå på sensorn tills den går sönder. Men för en attackerare som vill få tillgång till systemet är inte detta något primärt mål. För att få illegal tillgång till systemet finns två vägar, antingen kan man hota eller lura

den riktiga användaren att logga in, eller så kan man använda sig av artificiella fingrar. Utvecklarna av sensorer har satsat på att försvåra användandet av artificiella fingrar så att sensorn ska känna skillnad mellan det riktiga fingret och det artificiella, t.ex. genom att undersöka om fingret lever, d.v.s. kommer från en riktig människa.

3.4 Användning i praktiken

Användningen av biometri i praktiken har pågått under en längre tid. Det som har drivit på utvecklingen är viljan att slippa passerkort och nycklar samtidigt som nya lagar, framförallt i USA, har fungerat som drivmedel för ny biometriteknik. Användningsfallen varierar från åtkomst och passerkontroller till betalningsmedel. Det system som fått mest uppmärksamhet den senaste tiden är USA:s gränskontrollsystem US-VISIT. Det har fått mycket kritik för att det kränker den personliga integriteten. Eftersom detta system togs i bruk i januari 2004 finns det i skrivande stund ingen tillförlitlig information om hur bra detta system egentligen fungerar. Vi har dock spekulerat kring detta och kommit fram till att det faktum att systemet använder sig av flera olika biometritekniker för identifiering borgar för en säkrare verifieringsprocess. Vad gäller användningen av fingeravtryck som betalningsmedel måste vi ställa oss mer skeptiska. Denna tvekan baserar vi på de problem och attacker som relateras till fingeravtrycksbaserad biometri och som återfinns i den här rapporten. Vi ser en stor risk för fusk och feldebitering om bara fingeravtryck används som verifieringsmetod vid betalning.

4 Slutsats

Vid fingeravtrycksbaserad biometri fokuserar man på de åsar och dalar som återfinns på fingrets yta. Filtrering av fingeravtrycksbilder är ett måste för att verifieringsprocessen ska kunna bli säker. Dock måste insikten finnas att filtrering av en bild kan ta lång tid och därför är det viktigt att man gör en avvägning mellan kvalitet och tid. Genom att inrikta sig på vissa punkter på fingrets yta, s.k. minutieapunkter, kan man skapa underlag för en mall som lagras i en databas eller underlag för att utföra en matchning mellan ett fingeravtryck och en tidigare registrerad mall. Det finns olika tekniker som används för att läsa av ett fingeravtryck som t.ex. optik, ultraljud, temperatur och tryck.

Även om man har gjort framsteg inom området identifiering med biometri, framförallt fingeravtryck, så finns fortfarande funderingar på den personliga integriteten. En lösning kan vara att använda ett decentraliserat system med smarta kort istället för att lägga all data på ett ställe. I och med detta får användarna kontroll över sina uppgifter och samtidigt förhindrar man att system, såsom nationella register, blir för stora för att söka i och därmed långsamma.

En attack mot biometrisystem, som använder sig av fingeravtryck, är att skapa en kopia av ett fingeravtryck som har tillgång till systemet. Detta kan göras på flera olika sätt. Sensorerna använder sig dock av olika metoder för att fastställa äktheten i fingret som avläses, vilket försvårar användandet av artificiella fingrar. Vi har kommit fram till att användningen av biometri, i det här fallet fingeravtrycksbaserad biometri, blir allt mer vanligt. Användningsfallen varierar från åtkomst och passerkontroller till betalningsmedel. Vi menar, med utgångspunkt från de problem och attacker som vi beskriver i rapporten, att en kombination av olika tekniker är att föredra. Exempel på detta är gränskontrollsystemet US-VISIT där kombinationen ansiktsbaserad biometri och fingeravtrycksbaserad biometri används.

Referenser

- [1] Biometricsinfo.org, "Biometrics." <http://www.biometricsinfo.org/biometrics.htm> (Maj 2004).
- [2] L. Dong-hun, "Biometrics as a new technology," 1999. http://maincc.hufs.ac.kr/~argus/o343/t_c2.htm (Apr. 2004).
- [3] J. Blommé, "Evaluation of biometric security systems against artificial fingers," Master's thesis, Linköpings universitet, 2003.
- [4] Intervju med Marie Sandström, Examensarbetare på ISY Linköpings Tekniska högskola, Apr. 2004.
- [5] L. Hong, "Automatic personal identification using fingerprints," Tech. Rep. MSU-CPS-98-24, Department of Computer Science, Michigan State University, East Lansing, Michigan, June 1998.
- [6] D. Simon-Zorita, J. Ortega-Garcia, S. Cruz-Llanas, and J. Gonzalez-Rodriguez, "Minutiae extraction scheme for fingerprint recognition systems," tech. rep., Dpt. Ingenieria Audiovisual y Comunicaciones - Speech and Signal Processing Group (ATVS) EUIT Telecomunicacion, Universidad Politecnica de Madrid, Spain, 2002.
- [7] S. Greenberg, M. Aladjem, D. Kogan, and I. Dimitrov, "Fingerprint image enhancement using filtering techniques," tech. rep., Electrical and Computer Engineering Department, Ben-Gurion University of the Negev, Beer-Sheva, Israel, 2000.
- [8] N. Otsu, "A threshold selection method from gray level histograms," *IEEE Trans. Systems, Man and Cybernetics*, vol. 9, pp. 62–66, Mar. 1979. minimize inter class variance.
- [9] R. Qun, T. Jie, and Z. Xiaopeng, "Automatic segmentation of fingerprint images," tech. rep., AILAB, Institute of Automation, C.A. S., Beijing, China, 2002.
- [10] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2003.
- [11] T. Y. Zhang and C. Y. Suen, "A fast parallel algorithm for thinning digital patterns," *Commun. ACM*, vol. 27, no. 3, pp. 239–242, 1984.
- [12] A. Ross and A. Jain, "Biometric sensor interoperability: A case study in fingerprints," tech. rep., West Virginia University and Michigan State University, 2004.
- [13] "Privacy risks of biometrics: Bioprivacy risk ratings." http://www.biometricgroup.com/reports/public/reports/privacy_technology.html (Apr. 2004).
- [14] K. A. Rhodes, "Challenges in using biometrics," tech. rep., United States General Accounting Office, 2003. <http://www.gao.gov/new.items/d031137t.pdf> (Apr. 2004).
- [15] "Biometric border control system launched in us airports and seaports," 2004. <http://europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=1958&parent=chapter&preChapterID=0-140-194-329-348> (Apr. 2004).
- [16] "U.s. department of homeland security press release." http://www.ilw.com/lawyers/immigdaily/doj_news/2004,0106-hutchinson.shtm (Apr. 2004).
- [17] D. Carlton, "Biometric and the border management challenge," tech. rep., International Biometric Group, 2004. <http://www.biometricgroup.com/US-VISIT.html> (Apr. 2004).
- [18] M. Brink, "Shoppa med fingeravtryck," 2002. http://pcforall.idg.se/ArticlePages/200212/25/20021225140501_PFA527/20021225140501_PFA527.dbp.asp (Apr. 2004).
- [19] Sony. <http://www.sony.net/Products/Media/Microvault/> (Apr. 2004).
- [20] D. C. Sharma, "Gateway adds fingerprint sensor to notebook," 2004. <http://news.com.com/2100-1044-5178842.html> (Apr. 2004).