

Utredning av ansiktsgenkänning som autentiseringsmetod för klinik med narkotikaklassade preparat

Hanna Andersson Per Nielsen

Email: hanan106@student.liu.se, perni404@student.liu.se

Handledare: Viiveke Fåk, viiveke@isy.liu.se

TDDD17 Informationssäkerhet

Linköpings Universitet

Sammanfattning

I denna rapport har en utredning utförts om huruvida en ansiktsscanner skulle vara lämplig för en svensk rehabiliteringsklinik för drogmissbrukare. Vid bedömning om biometrimetoder och dess säkerhet är avvägningen som får göras systemets bekvämlighet. Ett system med en hög säkerhetsnivå har en högre nivå av felaktiga avvisanden och på samma sätt accepterar ett system med en låg säkerhetsnivå en större andel ej autentiserade personer. Biometrimetoder som kan användas är identifiering och verifiering. Identifiering innebär att svaret på frågan ”vem är jag?” ges och för verifiering ges svaret på frågan ”är jag den jag utger mig för att vara?”. Verifiering kan uppnås med exempelvis ett passerkort, något som idag redan tillämpas på kliniken. Då teorin för ansiktsgenkänningsteknik hade behandlats undersöktes det befintliga produktutbudet på marknaden. Resultatet av undersökningen är att kliniken bör behålla sina passerkort och komplettera dem med en ansiktsscanner. Då mängden användare kommer att vara begränsad kan säkerheten prioriteras något lägre för att göra systemet mer bekvämt och enkelt att använda. Viktigt för att kunna implementera ansiktsscannern i den dagliga verksamheten är att personalen utbildas i hur den kommer att användas samt får tillgång till direktiv om exempelvis glasögon kan användas vid verifieringstillfället. Produktutbudet av ansiktsscannrar är idag stort och det är svårt att ge direkta indikationer om vilken produkt som lämpar sig bäst för klinikens behov. Detta eftersom information om respektive produkt är begränsad och subjektiv. Rekommendationen är således att kliniken bör specificera kraven på

ansiktsscannern och därefter kan produktutbudet analyseras vidare för att ett beslut ska kunna tas.

1. Introduktion

Detta kapitel avser presentera rapportens bakgrund, syfte samt metod.

1.1 Bakgrund

I dagsläget finns ett flertal olika biometriska metoder som används för autentisering inom både privat och offentlig sektor i Sverige. Kraven skiljer sig vida åt och kan röra sig om alltifrån inloggning på privata persondatorer till passersystem på hemliga anläggningar. I och med den ständiga teknikutvecklingen har efterfrågan för ansiktsgenkänning och kostnadseffektiva lösningar stigit signifikant de senaste åren. Detta har lett till att utbudet har ökat och att utvecklingen av nya tekniker har tagit fart (Securitysales, 2011).

1.2 Problembeskrivning

En rehabiliteringsklinik för drogmissbrukare i en mindre kommun i Sverige överväger att implementera ansiktsgenkänning vid ingången till deras medicinförråd. Kliniken har tidigare haft problem med att patienter brutit sig in i förrådet med hjälp av stulna passerkort från personalen. Kliniken är välkänd och har ett väldigt gott rykte, problemet med att patienter på avvänjning har kunnat komma åt medicinska preparat har försvårat patienternas rehabilitering till den grad att klinikchefen nu anser sig behöva vidta åtgärder.

1.3 Syfte

Denna rapport syftar till att undersöka, baserat på teorier och forskares uppfattningar, huruvida ett

ansiktsgenkänningsystem kan ersätta alternativt komplettera ett befintligt passerkortssystem hos en rehabiliteringsklinik i Sverige. Följande frågeställningar kommer att besvaras för att kunna svara på syftet:

- Hur hög säkerhet kan det nya systemet erbjuda?
- Hur kan det implementeras för att effektivt fungera i den dagliga verksamheten?
- Vilka kostnader innebär det nya systemet?
- Fördelar respektive nackdelar med systemet?

1.3 Metod

Då rapporten är av teoretisk karaktär kommer den viktigaste källan för information att vara vetenskapliga artiklar inom ämnesområdet. Då tekniken ständigt utvecklas och även anpassar sig efter marknadens efterfrågan har vi valt att utesluta artiklar som är daterade tidigare än år 2002. Information och teorier kommer att inhämtas genom analyser av dessa vetenskapliga artiklar och olika författares teorier kommer vägas mot varandra och diskuteras. Även en undersökning av det befintliga produktsortimentet för ansiktsgenkänning och dess kostnader kommer att genomföras. Övriga elektroniska källor såsom tidningsartiklar inom ämnet kommer också att användas och utvärderas efter relevans.

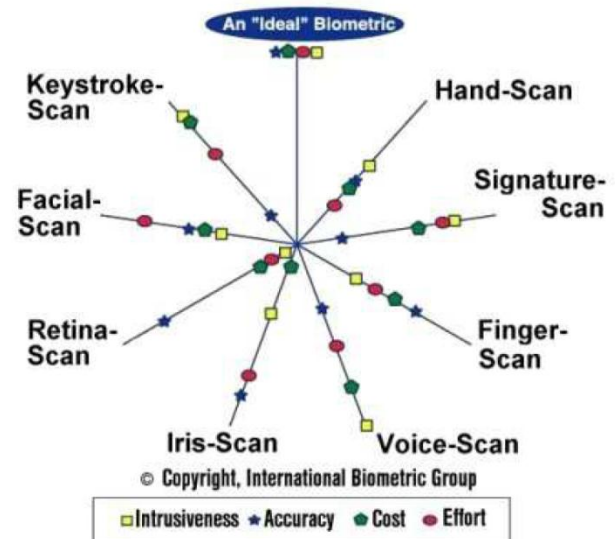
2. Teoretisk referensram

I detta avsnitt redovisas olika tekniker inom ansiktsgenkänning med syfte att ge förståelse för grundläggande tekniker och hur de kan implementeras.

2.1 Process

Med hjälp av en scanner speciellt utvecklad för ansiktsgenkänning har denna biometrimetod ökat i popularitet. Olika metoder inom biometri är lämpade för olika ändamål beroende på deras

kostnad, intrång, prestation och exakthet (se figur 1).



Figur 1 - Biometrimetoder och deras egenskaper

2.1.1 Metoder

Ansiktsgenkänning kan delas in i tre olika kategorier beroende på hur information och särdrag från ansiktet inhämtas. Den första kategorin behandlar de metoder som innebär identifiering utifrån hela ansiktet. Detta innebär att alla ansiktsdrag bevaras på ett detaljerat sätt vilket ger stora fördelar senare när olika ansiktsprofiler ska skiljas åt. När man tar hänsyn till hela ansiktet får man även in en global profil av ansiktet och ser inte endast till specifika ansiktsdrag. Dessa två fördelar följs direkt av en nackdel då det ställer höga krav på bilddatat som ska extraheras från ett ansikte. Denna nackdel kan åtgärdas genom att använda ett system där man försöker inhämta så mycket information som möjligt från en enda ansiktsbild.

Lokala metoder går under den andra kategorin i ansiktsgenkänning, där en persons lokala ansiktsdrag används. Det är den grupp av metoder som har använts längst och har en lång historia bakom sig. Jämfört med metoder från den första kategorin där information från hela ansiktet inhämtas, lämpar sig lokala metoder bättre för de

fall där man endast använder sig av en mall för var person som ska identifieras. Lokala metoder är mer flexibla då varje ansiktsdrag kan matchas mot en delmall samt ger en större diversifiering genom att man ser till de olika ansiktsdragen och inte endast till helheten. Svårigheten med lokala metoder uppstår då de olika ansiktsdragen ska infogas för att även kunna ge en helhetsbild av ansiktet.

Den tredje och sista kategorin inom ansiktsigenkänning är den så kallade hybrida. Namnet kommer ifrån att metoderna som används för ansiktsigenkänning i denna kategori är en blandning av globala och lokala metoder, från kategori ett och två. När man använder sig av hybrida metoder kan man välja när det är bättre att använda sig av igenkänning av lokala delar och när globala är att föredra. I viss utsträckning kan även metoder från kategori två anses utgöra en del av denna kategori tre, då de som tidigare nämnts ofta försöker återskapa en helhetsbild från de lokala delarna. Nedan visas i tabell 1 känsligheterna med respektive metod som identifierar lokala respektive globala ansiktsdrag.

Tabell 1 - Känsligheten för variationer i olika metoder

Faktorer till Variation	Lokala ansiktsdrag	Globala ansiktsdrag
Små variationer	Ej känslig	Känslig
Stora variationer	Känslig	Väldigt känslig
Belysning	Väldigt känslig	Känslig
Uttryck	Ej känslig	Känslig
Posering	Känslig	Väldigt känslig

Lokala ansiktsdrag har skilda känsligheter mot variationer som inte globala har. Exempelvis uppvisar lokala ingen känslighet för variationer i ansiktsuttryck vilket däremot klassas som en känslighet vid användandet av en global metod. (Tan, Chen, Zhou, Zang, 2005). Detta beror på att vid globala metoder representeras bilden på ett direkt sätt, exempelvis i en array med

pixelintensiteter från den ursprungliga bilden. Vid lokala metoder skapas ett brett spektrum av tänkbara ansiktsdrag vid extrahering av en bild. Dessa kan sedan kombineras på olika sätt och därmed är denna metod mindre känslig för variationer än den globala metoden (Li, Jain 2004) .

Typiska hybridmetoder är oftast inte lämpliga vid ansiktsigenkänning med endast en mall (Tan, Chen, Zhou, Zang, 2005).

2.1.2 Styrkor för ansiktsigenkänning

Fördelar med ansiktsigenkänning finner man främst vid olika former av övervakningssystem. Metoden kan tillhandahålla en första översiktlig scan från ett stort område med mycket information för att därefter kunna separera mängd från innehåll. Därför är ansiktsigenkänning väldigt populärt vid stora event, exempelvis Superbowl, där det behövs någon form av identifiering om något hot mot säkerheten skulle uppstå. Då ansiktet är något vi människor ofta visar öppet är det också väldigt svårt för någon att inte vara samarbetsvillig vilket underlättar inhämtning av data. En annan fördel är att det är en metod för igenkänning som är lätt att distribuera, en mjukvara kan införskaffas för att senare använda på exempelvis en webbkamera. Det finns således inget krav på att både hårdvara och mjukvara måste levereras i samma system eller en specifik teknisk utrustning för att metoden ska kunna användas fullt ut (Iridiantech, 2010).

2.1.3 Svagheter med ansiktsigenkänning

Då ansiktet är en kroppsdel som förändras med åldern försvårar det matchningen mot en mall, som då bör uppdateras regelbundet. Ansiktet är även en kroppsdel som är enkel att täcka över med exempelvis glasögon, något som även försvårar inhämtningen av en korrekt bild. En annan svaghet med ansiktsigenkänning är att en inhämtad bild från ett stort område ofta behöver processas en gång till för att uppvisa en någorlunda exakt bild som kan matchas mot en mall. Detta är nödvändigt att ha i åtanke vid användning av ansiktsigenkänning med större populationer inom samma område.

Som med många andra biometimetoder kan det uppstå en viss motvilja från en användare att behöva

existera i en databas. Detta då en del tycker att det påverkar deras integritet att de blir avsökta för att matchas mot en befintlig mall i en databas, alternativt att deras data läggs till i en databas för att senare kunna användas som mall (Iridiantech, 2010).

2.2 Verifiering och identifiering

Ansiktsgenkänning delas, som all biometri, upp i två former, verifiering och identifiering, beroende på hur det ska tillämpas. I verifiering ges svaret på frågan "är jag den jag utger mig för att vara" och systemet försöker matcha en mall som sedan tidigare finns lagrad i systemet med en bild som inhämtas vid verifieringstillfället (Gollmann, 2006).

Vid identifiering ges svaret på frågan "vem är jag?" vilket är en en- till många process där den bild som tas vid identifieringstillfället ska matchas mot en av många andra som finns lagrade i systemet. Detta görs genom att alla bilder i systemet genomsöks fram tills det att en matchning har uppstått eller tills allt har genomsökts (Gollman, 2006).

2.2.1 Positiv och negativ igenkänning

Inom biometri kan två synsätt användas för igenkänning, positiv och negativ. Detta görs genom att avgöra om:

1. Personen finns i databasen
2. Personen inte finns i databasen.

Ett positivt system har som främsta uppgift att avgöra om personen i fråga är den han utger sig för att vara. Positiva system används främst när man vill tilldela olika tillstånd till olika personer. Om en person vid ett verifieringstillfälle inte anses av systemet vara den han utgör sig för att vara blir han automatiskt nekad. På motsatt vis gäller att om systemet däremot anser att personen i fråga är den han utger sig för att vara, blir han istället från systemets sida accepterad. Positiva system förhindrar att flera personer använder sig av samma identitet (Maltoni 2003).

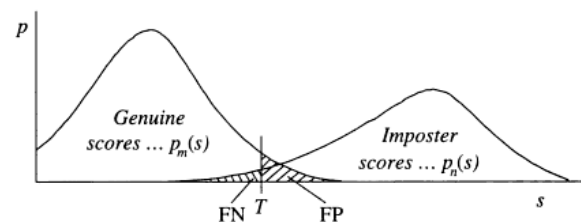
Ett negativt synsätt används i system där man vill säkerställa att en person inte redan är en del av en mängd, exempelvis i sociala system så som försäkringskassan för att säkerställa att personen i

fråga inte har sjukpenning. I ett negativt system avgör man således om personen i fråga är den han nekar sig till att vara och dess syfte är att förhindra att en person använder sig av flera identiteter (Maltoni, 2003). Generellt sett är negativa system de mest förekommande när det gäller autentisering i stora skalor (Hossein Bidgoli, 2004).

2.2.2 Utvärderingsmått

För ett ansiktsgenkänningsystem kan två olika fel uppstå. Det första är att systemet felaktigt inte kan hitta en matchning vilket innebär att en person blir felaktigt avvisad. Det andra är att det uppstår en felaktig matchning mellan en mall och den inhämtade datan. Detta kan uppstå då en person utger sig för att vara någon han inte är i ett positivt system, eller att någon oregistrerad misstas för att vara en redan registrerad i ett negativt system, och systemet upptäcker inte detta. Det första felet benämns som falskt negativ (FN) och det senare som falskt positiv (FP). För att se med vilken frekvens de båda felen uppstår används False Negative Rate (FNR) samt False Positive Rate (FPR). I ett positivt system används False Match (FM) och False Non Match (FNM) för att beskriva de två fel som kan uppstå. FM är det fel som uppstår när systemet felaktigt matchar användaren och det senare, FNM, beskriver felet som uppstår när systemet borde ha sagt ja till användaren och uppvisat match, men inte gjorde det (John D. Woodward, 2003).

Skillnaden mellan ett negativt och ett positivt synsätt är att en felaktig matchning i ett negativt system resulterar som falskt negativt och i ett positivt system enbart som false reject (FR). Därför, om säkerhet anses vara ett problem, sätts gränsen T (se figur 2) generellt sett lägre i ett negativt system än i ett positivt system för att minimera de falskt negativa felen.



Figur 2 - Minimering av FNR

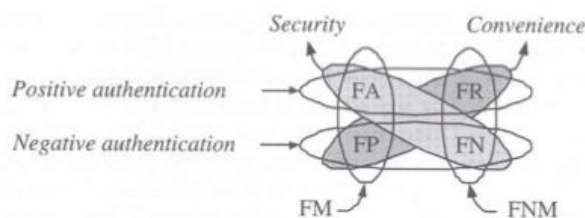
Två olika typer av fel kan få olika typer av konsekvenser då vikten av säkerhet skiljer sig från fall till fall. Ett falskt accpeterande i ett säkerhetssystem innebär att en obehörig har lyckats ta sig in och därmed finns det brister i säkerheten. Ett falskt avvisande visar att en auktoriserad person har blivit nekad tillgång, vilket inte är en brist i säkerheten men däremot obehändigt och kan orsaka vidare besvär och problem beroende på situationen. Avvägningen man således får göra mellan falskt accepterande och falskt avvisande har att göra med säkerhet och behändighet (Ruud Bolle, 2003). Sambandet och avvägningen man får göra är följande:

$$\text{Bekvämlighet} = 1 - \text{FRR}$$

$$\text{Säkerhet} = 1 - \text{FAR}$$

Tabell 2 - Konsekvenser

Positiv Autentisering	Negativ Autentisering
FA = FM → Säkerhetsproblem	FN = FNM → Säkerhetsproblem
FR = FNM → Bekvämlighetsproblem	FP = FM → Bekvämlighetsproblem



Figur 3 - Relationer

I tabell 2 och i figur 3 visas vilka fel som leder till respektive problem. Dessa varierar beroende på om systemet är negativt eller positivt. Då de påverkar varandra är en avvägning om säkerhet respektive bekvämlighet således nödvändigt.

2.3 Marknad

Efterfrågan på avancerade säkerhetssystem är större nu än någonsin då kraven på säkerhet ständigt ökar. De ökade säkerhetskraven beror till stor del på de terrorattentat som utförts det senaste decenniet och därför tvingas länder världen över skärpa säkerheten. (Frost and Sullivan, 2006)

Ansiktsgenkänning är en teknik som passar dessa ökade säkerhetskrav mycket väl och därför ser marknaden för ansiktsgenkänning mycket ljus ut. Frost & Sullivan (2006) spår att marknaden för ansiktsgenkänning kommer öka med 27,5% per år mellan 2005-2012. International Biometric Group spår att marknaden för ansiktsgenkänning kommer att överstiga 1 miljard dollar i årliga intäkter för år 2012 och framåt.

Nordamerika är den största geografiska marknaden för ansiktsgenkänning, men bland annat Europa spås snart komma ifatt den amerikanska marknaden. Västeuropa antas bli en viktig marknad som kommer att stå för en stor del av intäkterna. Östra Asien identifieras också som en nyckelmarknad för implementering av ansiktsgenkänning. (Frost & Sullivan, 2006)

Den ökade efterfrågan och teknikens ständiga utveckling antas resultera i något minskade priser som kan ge tekniken möjlighet att penetrera på nya marknader. Ansiktsgenkänning väntas kunna utmana andra biometriska tekniker vad gäller både prisnivå och prestanda inom de kommande åren. (Frost & Sullivan, 2006)

2.3.1 Användningsområden

De branscher som ansiktsgenkänning anses vara applicerbara på är följande:

- Brottsbekämpande myndigheter
- Finansbranschen
- Sjukvårdsbranschen
- Transport och resebranschen

Frost och Sullivan (2006) identifierar myndigheter som det största användningsområdet. Exempelvis har brottsbekämpande myndigheter ett stort behov av att kontrollera individers identiteter på sårbara platser såsom flygplatser och tunnelbanor. Inom finans- och sjukvårdsbranschen kan ansiktsgenkänning istället användas för passerkontroll samt tids- och närvarorapporter.

2.3.2 Produkter och leverantörer

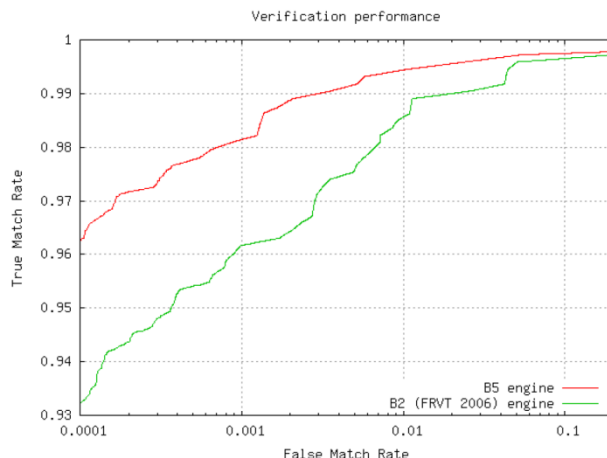
På marknaden finns det ett flertal leverantörer av ansiktsgenkänningsteknik. Vissa företag fokuserar bara på att sälja mjukvara medan andra säljer ansiktsscannrar som en hel produkt. Några exempel på aktörer på marknaden är följande:

FaceVACS – SDK av Cognitec

Cognitec är ett globalt företag med huvudkontor i Tyskland. De har bland annat blivit tilldelade Frost & Sullivans Best Practics Award 2008 för deras ansiktsgigenkänningsmjukvara och dess strategi för denna. Cognitech riktar in sig på att sälja mjukvara som är kompatibel med kundens nuvarande datorer och kameror och på så sätt kunna tillämpa både passerkontroll och tids- och närvaroredovisning med hjälp av ansiktsgigenkänning. Den produkt som är aktuell i detta fall är deras FaceVACS - SDK. Den senaste versionen är 8.4 vilken släpptes i december 2010.

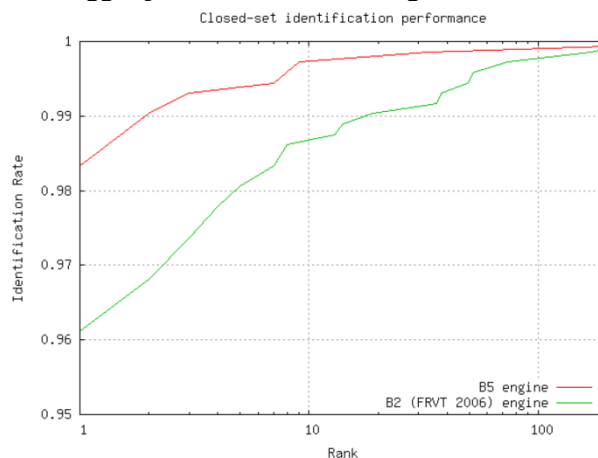
Denna programvara stöder inregistrering, verifiering och identifieringsprocesser och är implementerbar på både 2D och 3D data. Det finns även en kvalitetsbedömning av ansiktstillbilden integrerad i programvaran. Programvaran ska även kunna hantera typiska minändringar, positionsavvikelser med +/- 15 grader (utifrån kort tagna rakt framifrån), hantera glasögon, skägg- och frisyrförändringar samt ljusförändringar. Programvaran kan hantera både bilder och videoströmmar och de filformat som stöds för bilder är bland annat JPG, PNG och BMP. Kvalitetskraven på bilderna som används är att bilderna är skarpa, att avståndet mellan pupillerna är minst 32 pixlar (dock är minst 60 pixlar rekommenderat) samt att det är minst 64 gråskalor i ansiktsregionen på bilden.

FaceVACS prestanda har mätts med FMR och True Match Rate (TMR). Nedan visas två ROC-diagram för verifiering och identifiering.



Figur 4 - Prestanda vid verifiering

Beroende på vilka inställningar som används erhålls följande kurvor. Av diagrammet ovan framgår att FaceVACS uppnår en TMR på strax över 98 % då FMR ligger på 0,1 % för verifiering.



Figur 5 - Prestanda vid identifiering

För identifiering erhålls ROC-kurvan ovan. Av den framgår att identifieringsandelen då rank¹=1 är strax över 98 %. (Cognitec)

Cognitec kontaktades för att erhålla prisuppgifter, dock ville företaget ej bistå med detta.

¹ "The identification rate at rank k is the fraction of probes that have rank k or lower. Plotting identification performance against rank on a cumulative match characteristic (CMC) allows us to assess whether the correct match is in the top k matches rather than just the first. Most applications are based on performance at lower ranks." (Roli & Vitulano, 2005)

3D FastPass Face Reader av L-1 Identity Solutions

L-1 Identity Solutions är ett globalt företag med huvudkontor i USA. De säljer flera former av biometriteknik, såsom ansiktsgenkänning och fingeravtrycksläsare. För ansiktsgenkänning säljer de både programvara och kompletta produkter. Deras produkt 3D FastPass Face Reader används för passerkontroll och har flera kundreferenser där produkten används idag.



Figur 6 - 3D FastPass Face Reader

Denna produkt klarar av att autentisera användare på mindre än en sekund. Den ska även kunna skilja på enäggstvillingar då tre tekniker används (Wire mesh, Semantic Analysis, Real-Time 3D Mode) och 40 000 datapunkter jämförs. Det går även att komplettera ansiktsgenkänningen med exempelvis passerkort och PIN-koder. Registreringsprocessen av nya användare kan denna läsare också hantera, den fotomall som görs vid registreringsprocessen tar omkring 6-8 sekunder att generera.

Priset för 3D FastPass Face Reader var 2008 \$6 145 inklusive ett års garanti, dock är det oklart vad som ingick i detta priset. L-1 Identity Solutions kontaktades för uppgifter angående prestanda och pris, dock gavs inga svar.

FR1000 av Jiangxi Pineworld Biometrics Technology

Jiangxi Pineworld Biometrics Technology, tidigare Pineworld, är ett kinesiskt företag baserat i Jiangxi. De har varit aktiva på marknaden sedan 1992 och innehar flera patent inom biometriteknik. De säljer flera typer av biometrisk produkter, såsom fingeravtryckscannrar och

ansiktsscannrar. En av deras produkter benämns FR1000 och är en ansiktsscanner som kan användas för passerkontroll.



Figur 7 - FR1000

FR1000 har kapacitet att hantera olika ljusskillnader och ska kunna användas i allt från mörka rum till utomhus i solen. Den kan även hantera användares åldrande. Produkten har enligt deras produktblad en imponerande FAR på 0,01% och en FRR på 99,8%. Tiden för identifiering för FR1000 är mindre än 2 sekunder och det tar upp till 20 sekunder att registrera en ny användare manuellt. Produkten använder 3D-data och kan hantera ansiktsvinklar på +/- 15 grader.

Priset för FR1000 är \$225 per enhet.

iFace301 av APEC Tech

APEC Tech är ett kinesiskt företag baserat i Hong Kong som startades 2001. De är aktiva inom biometriteknikbranschen och säljer både fingeravtrycks- och ansiktsscannrar men de säljer även exempelvis RFID-teknik för passerkontroll. Den av deras produkter som är av intresse för detta projekt är iFace301 som är en ansiktsscanner som är kompatibel med RFID passerkort.



Figur 8 - iFace301

Det är begränsad information som ges om denna produkt, men det framgår att verifieringstiden är mindre än 2 sekunder. Priset för iFace301 är \$280 per enhet.

2.4 Förutsättningar

Utöver de tekniska krav som finns för att enheten ska vara kompatibel med det befintliga passersystemet måste personalens åsikter tas hänsyn till. Att behöva scanna sitt ansikte varje gång en anställd ska gå in i medicinförrådet kan uppfattas som integritetskränkande. De kan även uppfatta de nya säkerhetsåtgärderna som jobbiga och onödiga. För att kunna implementera en ansiktsscanner effektivt i verksamheten måste idén förankras hos personalen först för att säkerställa att denna lösning godtas.

Då personalen på kliniken inte är av teknisk inriktning kommer även support att behövas under en inledande fas, särskilt under installationen och registreringen av användare.

Det kan uppkomma akuta situationer på kliniken och då får inte ansiktsscannern neka en behörig anställd tillträde till medicinförrådet. För att minimera risken att detta inträffar är det ett krav att det finns en alternativ öppningsprocedur, exempelvis genom att det finns en huvudnyckel som alltid kan öppna medicinförrådet. Detta är även viktigt vid eventuella strömavbrott eller andra störningar så att man fortfarande kan ha tillträde till medicinförrådet.

3. Analys och implementering

Nedan redovisas analysen av produkterna och dess tekniker utifrån syftet och frågeställningarna för rapporten.

3.1 Säkerhet

Samtliga produkter som undersökts anses kunna ha tillräcklig säkerhet för att användas av kliniken. Dock kommer en avvägning mellan säkerhet och tillgänglighet att behöva göras. Exempelvis FR1000 kan ha en imponerande låg FAR, dock har den då en mycket hög FRR vilket avsevärt minskar tillgängligheten och bekvämligheten. Detta gäller samtliga produkter. Det är vitalt att hitta en bra avvägning mellan säkerhet och tillgänglighet för att effektivt kunna utnyttja produkten.

För att minska risken för FAR och även minska autentiseringstiden anser vi att kliniken ska använda

en produkt som går att kombinera med deras nuvarande passerkortssystem och på så sätt använda en verifieringsmetod vid autentisering.

Detta baseras även på den grundläggande teorin i datasäkerhet om att kombinera olika säkerhetsmetoder för att uppnå en ännu högre säkerhet, i detta fall "Something you carry" och "Something you are" (Gollman, 2006).

Det ska noteras att de tekniska specifikationerna som givits för de olika produkterna kommer från produkternas försäljningsblad och därför bör de analyseras kritiskt. De flesta företagen verkar vara villiga att skicka provexemplar eller testlicenser för att kunna testa produkterna, vilket anses vara ett bra tillvägagångssätt för att testa prestandan för produkterna i miljön där de ska användas.

3.2 Implementerbarhet

De produkter som undersökts skulle alla vara implementerbara på kliniken. Dock är vissa mer eller mindre lämpliga beroende på dels kapacitet och dels utrustning. 3D FastPass Face Reader är avsedd för större användningsområden än att enbart öppna en dörr. Det finns exempelvis flera framgångsrika implementationer där produkten använder identifiering för inpassering i byggnader, alltså att samtliga anställda passerar ansiktsscannarna för att ges tillträde till byggnaden. Jämför med passerkontrollerna i Stockholms tunnelbana, fast med ansiktsgenkänning istället för biljettkontroll. 3D FastPass Face Reader är dock möjligt att implementera på kliniken, men vi anser att systemet har en överkapacitet för uppgiften.

De mindre kinesiska produkterna verkar vara mer lämpliga kapacitetsmässigt för uppgiften och inga stora system behöver installeras.

Cognitecs programvara är också enkel att implementera, förutsatt att det finns tillgängliga datorer och kameror med tillräcklig prestanda.

För att kunna implementera tekniken är det också viktigt att det ges en hög nivå av support, särskilt i inledningsfasen. Kliniken har ingen teknisk personal och därför kan support- och servicenivån som erbjuds helt avgöra vilken produkt som bör väljas.

3.3 Kostnad

Kostnaderna för de olika systemen skiljer sig mycket åt. Det kan ifrågasättas varför 3D FastPass Face Reader är mer än 20 gånger så dyr som de kinesiska alternativen. Då denna produkt är så mycket dyrare än alternativen, och har en högre kapacitet än vad som är nödvändigt, kommer inte denna produkt att rekommenderas till kliniken. Ett pris för Cognitecs programvara har inte kunnat erhållas och kan därför inte analyseras utifrån ett prisperspektiv. Kostnaden för FR1000 och iFace301 är relativt låga och författarna förvånades över det låga priset. Priserna kommer direkt från företagen men det bör undersökas närmare vad som ingår i de priserna.

3.4 För- och nackdelar

Nackdelar med samtliga dessa system är att de kan inkräkta på den personliga integriteten. Om en ansiktsscanner installeras måste detta diskuteras med personalen så de får ge sin åsikt på lösningen. Ytterligare en nackdel är att systemet kan upplevas som omständigt och besvärligt av personalen, särskilt om tillgängligheten är låg.

Fördelar med systemen är att de kan uppnå en hög säkerhet, högre än i dagsläget. De går även att komplettera med passersystem och då höjs säkerheten ännu mer. Som nämnts tidigare, det är viktigt att systemet har en hög tillgänglighet och har en kort autentiseringstid. Om verifiering används och det hittas en lämplig avvägning mellan säkerhet och tillgänglighet antas detta kunna uppnås.

4. Slutsats och rekommendation

I detta avsnitt presenteras de slutsatser och rekommendationer som identifierats för att besvara syftet.

Vår rekommendation är att gå vidare och undersöka produktutbudet ytterligare. Vi anser att en ansiktsscanner som kombineras med nuvarande passerkortssystem vore en effektiv och säker lösning. Då kan en verifieringsmetod tillämpas vilket kan leverera säkra och snabba resultat.

Då kliniken är av mindre storlek och ansiktsscannern endast kommer att ha den berörda personalen som användare, kan bekvämlighet prioriteras något högre

och systemet kan tillåtas ha en lägre FRR. Om systemet däremot exempelvis skulle användas av en brottsbekämpande myndighet där kraven på säkerhet är höga, skulle prioriteringen bli annorlunda.

Den produkt kliniken väljer att använda sig av bör lämpligtvis använda sig av positiv verifiering. Detta då den inte kommer att ha många användare och ett positivt system skulle förhindra att flera personer använder sig av samma identitet. Idag har kliniken problem med att patienter utger sig för att vara någon i personalen för att få tillgång till medicinrummet och ett positivt system skulle förhindra detta. Ansiktsscannern som köps in bör även använda lokala metoder för verifiering. En avgörande faktor för vilken produkt som bör köpas, utöver tekniska specifikationer, är vilken support och service som erbjuds. Då kliniken saknar teknisk kompetens är detta viktigt för att kunna använda produkten effektivt. Det bör även tas fram riktlinjer för personalen angående hur ansiktsscannern ska användas, exempelvis att de vid registrering ej bär solglasögon eller andra plagg som täcker delar av ansiktet.

Det finns produkter som uppfyller klinikens syfte, dock ges begränsad information om dessa. Om kliniken bestämmer sig för att gå vidare måste produkterna analyseras ytterligare och framförallt testas eftersom den erhållna informationen är baserad på försäljningsinformation. Även priserna behöver undersökas ytterligare så att det framgår vad som ingår i varje pris avseende support, service och garantier.

Referenser

- [1] Securitysales, 2011, <http://www.securitysales.com/Blog/Under-Surveillance/Story/2011/01/Panasonic-President-Sees-Industry-Getting-a-Facial-Recognition-Lift.aspx> (hämtat 110322)
- [2] Xiaoyang Tana, Songcan Chen, Zhi-Hua Zhou, Fuyan Zhang, Face recognition from a single image per person: A survey, 2006, Pattern Recognition
- [3] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, 2003

http://bias.csr.unibo.it/maltoni/handbook/chapter_1.pdf

- [4] R. Bolle, Guide to Biometrics, Springer Professional Computing, 2003
- [5] Hossein Bidgoli, The Internet Encyclopedia Vol. 1, Wiley, 2004
- [6] John D. Woodward, Biometrics: Identity Assurance in the Information Age, 2003, http://web.law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2003_2004/burnham.pdf
- [7] Frost & Sullivan, World Face Recognition Biometrics Markets, 2006, <http://www.marketresearch.com/product/display.asp?productid=1397723&xs=r&SID=83630890-506715704-449824018&curr=USD&kw=&view=abs> (hämtat 110329)
- [8] Iridian Technologies, http://epic.org/privacy/surveillance/spotlight/1005/irid_guide.pdf (hämtat 20110406)
- [9] Stan Z. Li, Anil K. Jain, Handbook of face recognition, Springer, 2004
- [10] Dieter Gollman, Computer Security, Second Edition, Wiley, 2006
- [12] Fabio Roli, Setgio Vitulano, Image analysis and processing- ICIAP 2005, Springer Verlag, 2005