Biometriska metoder för teknisk bevakning

Henrik Karlzén, Christian Valassi, Johan Bengtsson och Amund Gudmundson Hunstad

FOI-R--5110--SE

Januari 2021

FOI

Henrik Karlzén, Christian Valassi, Johan Bengtsson
och Amund Gudmundson Hunstad

Biometriska metoder för teknisk bevakning

Titel	Biometriska metoder för teknisk bevakning
Title	Biometric methods for technical surveillance
Rapportnr/Report no	FOI-R--5110--SE
Månad/Month	Januari
Utgivningsår/Year	2021
Antal sidor/Pages	47
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E728188
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: Pixabay: Gerd Altmann

Sammanfattning

Rapporten beskriver vilka biometriska metoder som kan vara användbara för teknisk bevakning i Försvarsmakten. Biometriska metoder utgår från mänskliga individers biologiska eller beteendebaserade kännetecken (exempelvis fingeravtryck eller gångstil) för att automatiskt känna igen individerna. Teknisk bevakning utgörs av teknik som används för övervakning och skydd i syfte att kontrollera egen personal och upptäcka antagonister.

Vilka biometriska metoder som är användbara för Försvarsmakten utvärderades på två olika sätt. Den ena utvärderingen baserades på olika källors beskrivningar av de biometriska metoderna och hur väl metoderna fungerar teoretiskt eller i generella praktiska situationer (labbmiljöer). Källornas sätt att studera problemet varierar. Framförallt beaktar få av dem användningsmiljön, de igenkändas personliga integritet eller den biometriska metodens motståndskraft mot angrepp såsom imitering.

Den andra utvärderingen bedömde hur väl metoderna fungerade i olika användningsfall som är representativa för Försvarsmakten och dess behov av teknisk bevakning. Det visade sig att de bästa och mest relevanta metoderna är igenkänning baserat på iris, fingeravtryck, ansikte respektive öron.

Även dessa utvärderingar är dock gjorda på en ganska övergripande nivå. För specifika situationer och produkter behöver Försvarsmakten utvärdera ytterligare, inte minst för att jämföra med icke-biometriska alternativ. Det finns också rena forskningsmässiga utmaningar, exempelvis med att ta fram säkrare biometriska metoder där individer inte kan imiteras utifrån läckta databaser över biometriska data.

Nyckelord: biometri, igenkänning, teknisk bevakning, kännetecken, etik, informationssäkerhet

Summary

The report describes which biometric methods that can be useful for technical surveillance in the Swedish Armed Forces. Biometric methods are based on human individuals' biological or behavioural characteristics (for example, fingerprints or gait) in order to automatically recognise individuals. The use of biometrics has increased substantially in the last decade. Technical surveillance consists of technology used for surveillance and protection in order to monitor personnel and detect antagonists.

Two evaluations were used to determine which biometric methods that are useful to the Swedish Armed Forces. The first evaluation was based on different sources' descriptions of the biometric methods, and how well the methods work theoretically or in general practical situations (lab environments). How these evaluations are conducted differs, and there are no complete evaluations. Above all, there are few evaluations that take into account the usage environment, the privacy of the recognisees, or the biometric method's resistance to attacks such as impersonation.

Subsequently, an assessment was made of how well the methods worked in different use cases that are representative for the Swedish Armed Forces and its need for technical monitoring. It turned out that the best and most relevant methods are recognition based on either iris, fingerprint, face, or ear.

However, these evaluations have also been made at a fairly general level. For specific situations and products, the Swedish Armed Forces need to evaluate further, not least to compare with the use of non-biometric alternatives. There are also research challenges, for example in developing more secure biometric methods where individuals cannot be impersonated based on leaked databases of biometric data.

Keywords: biometrics, recognition, technical surveillance, characteristics, ethics, information security

Innehållsförteckning

1 Inledning

Denna rapport beskriver vilka biometriska metoder som kan vara användbara för teknisk bevakning inom Försvarsmakten. Begreppen *biometriska metoder* respektive *teknisk bevakning* innebär följande:

- Biometriska metoder utgår från mänskliga individers biologiska eller beteendebaserade kännetecken (exempelvis fingeravtryck eller gångstil) för att automatiskt känna igen individerna.
- Teknisk bevakning utgörs av teknik som används för övervakning och skydd i syfte att kontrollera egen personal och upptäcka antagonister.

Biometriska metoder används redan idag för många typer av teknisk bevakning i samhället. Exempelvis används biometri när användare låser upp mobiltelefoner, när resenärer går igenom automatiska passkontroller samt när människor övervakas automatiskt. Dessutom har det senaste decenniets förbättrade AI-algoritmer gjort biometriska metoder allt bättre (se exempelvis NIST (2019d)). Det finns alltså goda anledningar till att tro att biometriska metoder också kan användas i teknisk bevakning inom Försvarsmakten.

Rapporten togs på uppdrag av Försvarsmakten fram i ett projekt om teknisk bevakning vid FOI under hösten 2020. Parallellt med denna rapport tog projektet också fram en liknande rapport om videoanalys för teknisk bevakning.

1.1 Metod

Datainsamlingen för denna rapport grundar sig i en mindre litteraturstudie. Litteraturen utgjordes i huvudsak av akademiska forskningsartiklar men också av rapporter från standardiseringsorgan, nyhetsartiklar, tillverkares produktbeskrivningar med mera. Litteraturen identifierades utifrån sökningar i forskningsdatabaser och allmänt på webben. Dessutom identifierades litteratur utifrån referenser i tidigare FOI-rapporter.

De biometriska metoder som beskrivs i rapporten valdes ut baserat på deras mognadsgrad, exempelvis i vilken utsträckning de implementerats i kommersiella produkter. Metoderna som inkluderas utvärderades sedan utifrån grundläggande och etablerade krav på biometriska metoder.

De biometriska metoderna utvärderades också utifrån hur väl de fungerar i olika användningsfall. Användningsfallen togs fram utifrån de grundläggande kraven i kombination med projektgruppens övergripande kunskap om Försvarsmakten och dess behov av teknisk bevakning. Användningsfallen är avsedd att täcka in en betydande majoritet av de situationer som kan tänkas uppstå.

1.2 Avgränsningar

De användningsfall som beskrivs i rapporten täcker inte alla tänkbara situationer med bevakningsbehov som kan uppstå i Försvarsmakten. Etiska och juridiska aspekter beaktas i användningsfallen, men det ligger utanför ramen för rapporten att avgöra de exakta etiska och juridiska ramarna.

Rapporten omfattar inga egna tekniska analyser, exempelvis av algoritmer, eller praktiska tester av produkter, exempelvis i form av att införskaffa produkter för att testa dem i olika miljöer.

1.3 Läsanvisning

Kapitel 2 ger en bakgrund till biometri, typer av biometrisk igenkänning samt grundläggande krav på biometriska system. Dessutom beskrivs grunderna för teknisk bevakning i Försvarsmakten.

Kapitel 3 beskriver etiska och legala aspekter av biometri.

Kapitel 4 tar upp olika möjliga angrepp mot biometriska system.

Kapitel 5 redogör för vilka typer av användningsfall som finns och beskriver mer om några av dessa som är särskilt relevanta för Försvarsmakten.

Kapitel 6 beskriver olika biometriska metoder, hur de fungerar och ger exempel på olika användningsområden.

Kapitel 7 ger en koncis jämförelse mellan de olika biometriska metoderna.

Kapitel 8 beskriver vilka biometriska metoder som passar i vilka av användningsfallen.

Kapitel 9 presenterar en diskussion om det som framkommit i rapporten.

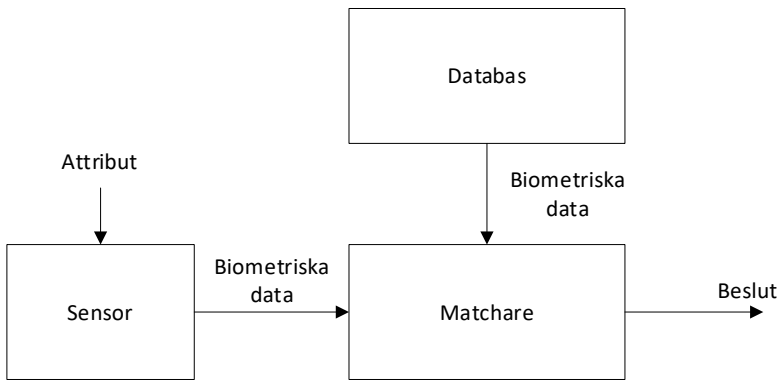
2 Bakgrund

Detta kapitel beskriver vad biometri innebär, vilka typer av biometrisk igenkänning som finns, grundläggande krav på biometriska system samt etiska och legala aspekter av biometri. Dessutom beskrivs vad teknisk bevakning innebär.

2.1 Introduktion till biometri

Biometri definieras som automatiserad igenkänning av individer (människor) baserat på deras biologiska eller beteendebaserade kännetecken[1] (ISO/IEC, 2017). Det finns många typer av biometriska kännetecken, som exempelvis strukturen av åsarna på fingertopparna, strukturen hos ögats iris, samt en handskriven underskrifts utformning. Strukturen kan beskrivas av detaljpunkter (eng. minutiae[2]).

Ett typiskt biometriskt system illustreras av Figur 1.



Figur 1 – ett typiskt biometriskt system (illustration baserad på Karlzén m.fl., 2020). I systemet ingår också nödvändig IT-utrustning (syns bara delvis i figuren).

I ett biometriskt system används en sensor för att läsa av en viss typ av detaljpunkter för ett kännetecken (avläsning), varefter insamlade data bearbetas. Därefter tas ett beslut om vilken individ som igenkänts (matchats) eller i övrigt hur individen ska klassificeras. Individen som ska kännas igen har först

[1] På engelska är termen *characteristics.* Kännetecken är synonymt med karaktäristik och betyder utmärkande drag.

[2] Ofta beskrivs processen mer komplicerat som att 1) det inhämtas *sampel* (eng. sample), 2) samplet digitaliseras och det utvinns *egenskaper* (eng. features) vilka exempelvis kan vara i form av *detaljpunkter* (eng. minutiae). I rapporten finns inget behov av termen sampel. Termen detaljpunkter föredras framför egenskaper eftersom egenskaper (som är ett vanligt svenskt ord) lätt blandas samman med annat.

registrerats på något sätt (vilket lagrats i en databas) och vid igenkänningen kan avlästa data då jämföras med registrerade data (eng. template). I ett biometriskt system ingår en eller flera biometriska metoder[3] (sensor och bearbetning för ett visst kännetecken), registrerade data samt nödvändig IT-utrustning. I system med multibiometriska metoder kombineras flera metoder i en, exempelvis genom att fingeravtrycksavläsning kombineras med irisavläsning.

2.2 Typer av biometrisk igenkänning

För biometriska system finns det två övergripande typer av igenkänning. I den mest grundläggande typen ska systemet känna igen en individ enbart baserat på de data som inhämtas via sensorn och jämföra dessa med vad som sedan tidigare finns registrerat om alla individer i systemet. Igenkänning av denna typ går under benämningen *identifiering.* I den andra typen finns även data tillgängliga från en annan kanal, exempelvis i form av ett nummer på en identitetshandling. Denna typ kallas *verifiering.* Det är normalt enklare att söka fram ett identitetsnummer eller liknande i en databas och sedan göra en matchning mellan sensordata och en relevant uppsättning lagrade biometriska data än vad det är att söka fram biometriska data från grunden. Detta gör att verifiering är snabbare än identifiering, vilket kräver att alla individers lagrade data måste sökas igenom efter en matchning. Identifiering kan ses som *N* försök till verifieringar, där *N* är antalet individer i den biometriska databasen.

Ett annat sätt att dela in olika former av igenkänning på är beroende på om individen som ska kännas igen vill bli igenkänd eller inte. Om individen vill bli igenkänd (exempelvis vid en inloggning) samarbetar individen gärna med systemet. Om individen inte vill bli igenkänd (exempelvis vid brott) handlar det istället om att systemet används för att övervaka individen eller i efterhand spåra individen (med forensiska metoder).

Förutom att använda biometriska system för att känna igen individer, kan liknande system användas för att göra en mer grov bedömning av om ett objekt är en människa och i så fall vilken typ av människa enligt en kategorisering. Mänskliga kännetecken som är alltför generella för att känna igen en viss individ men som kan användas för kategorisering (såsom hårfärg, hårlängd eller förekomsten av en viss tatuering), går under benämningen mjuk biometri[4] (Jain m.fl., 2004a). Mjuk biometri kan användas på egen hand för kategorisering, eller i kombination med vanlig biometri för att snabba på igenkänning av en individ. Användningen av mjuk biometri liknar hur polisen använder signalement. På

[3] Eng. method används i rapportens engelska sammanfattning (summary). Men i litteraturen används ofta *mode*, eller *modality.*

[4] Mjuk biometri (eng. soft biometrics) är snarlikt vad som studeras inom forskningsfältet attribute recognition (sv. attributionsigenkänning).

liknande sätt som individer kan kategoriseras utifrån sina biologiska kännetecken, kan individerna kategoriseras utifrån deras beteende. En individ kan till exempel kategoriseras utifrån sitt beteende att dröja kvar vid en plats en viss tid, lämna kvar något vid en viss plats, förstöra något, återkommande visa sig vid en plats, förekomma vid flera platser, vara på samma plats som många andra individer, eller göra något (annat) avvikande.

2.3 Grundläggande krav på biometriska system

Enligt Jain m.fl. (2004b)[5] kan alla fysiologiska eller beteendemässiga egenskaper hos människan användas som biometriska kännetecken om de uppfyller följande krav:

- **Universalitet** – Varje individ måste inneha kännetecknet i fråga.
- **Unikhet** – Varje individ måste vara tillräckligt olik varje annan individ gällande kännetecknet.
- **Oföränderlighet** – Kännetecknet måste vara tillräckligt bestående över tid.
- **Insamlingsförmåga** – Kännetecknet måste kunna mätas kvantitativt.

Vid utvärdering av biometriska system motsvaras dessa fyra krav i grova drag av huruvida systemet felaktigt tror sig känna igen en individ (**falsk positiv**, FP) eller felaktigt tror sig *inte* känna igen en individ (**falsk negativ**, FN) (Karlzén m.fl., 2020). I forskningslitteraturen, tillverkares dokumentation och andra källor finns många olika definitioner av falska positiva respektive falska negativa. För att räknas som falska positiva ingår det ibland inte att angripare lurat systemet, utan systemet måste ha råkat blanda ihop en individ med en annan. Ibland ses systemets problem med att läsa av en individs kännetecken som något väsensskilt, i andra fall ingår det som en del i systemets förmåga att känna igen (eller inte känna igen) individen.[6] Förutom mått som falska positiva och falska negativa, innehåller litteraturen ofta mått på **träffsäkerhet** (eng. accuracy). Träffsäkerheten avser i vilken utsträckning det inte blir falska positiva eller falska negativa, dvs. andelen individer som kännas igen korrekt.

Vilka nivåer av falska positiva respektive falska negativa som är bra nog beror på det specifika systemet och dess användningsområde. Det är också relevant att jämföra systemets nivåer med vad som uppnås av alternativet till systemet.

[5] Den mest citerade forskningsartikeln om biometri i databasen Scopus.

[6] I engelskspråkig litteratur motsvaras falska positiva i olika mån av bland annat *false accept rate* (FAR), *false match rate* (FMR) och *false-positive identification-error rate* (FPIR). För falska negativa används begrepp som *false non-match rate* (FNMR), *false reject rate* (FRR) och *false-negative identification-error rate* (FNIR). (ISO/IEC, 2006).

Dessutom säger antalet falska positiva och falska negativa inget om hur snabbt systemet är, eller om de tänkta användarna accepterar systemet. En annan begränsning med att (enbart) förlita sig på falska positiva och falska negativa är att de enbart talar om sannolikheten för fel, inte konsekvenserna av felen. I exempelvis inloggning i sjukhusmiljö kan det vara mycket allvarligt att sjukvårdspersonal inte känns igen av systemet, medan det vid bankinloggning kan vara allvarligare att en utomstående felaktigt känns igen som kontoinnehavare. Det finns alltså ytterligare aspekter som biometriska system måste ta hänsyn till (Jain m.fl., 2004b):

- **Möjlig systemprestanda**.
  Systemprestanda avser hur väl systemet klarar av att korrekt känna igen individer och hur snabbt detta kan genomföras. Här inkluderas även aspekter relaterat till den miljö[7] som systemet ska verka i och hur dessa påverkar prestandan hos systemet.
- **Användarnas acceptans av användningen av kännetecknet.**
  Acceptansen avser till vilken grad som användare är villiga att nyttja systemet. Detta påverkas bland annat av hur inkräktande systemet är på användarnas personliga integritet samt hur tidskrävande systemet är. (Se även kapitel 3).
- **Resistensen mot antagonisters möjligheter att kringgå systemet.**
  Möjligheter att kringgå systemet avser hur lätt det är för individer att undvika att kännas igen av systemet samt hur individer kan lura systemet att ta felaktiga beslut. (Se även kapitel 4).

Den internationella standarden 19795-1 (ISO/IEC, 2006) beskriver teknisk utvärdering av biometriska system. Utvärderingen sker delvis på ett sätt som inkluderar de krav som beskrivits i detta avsnitt. Standardens fokus är på att bedöma antalet falska positiva och falska negativa. Separata parametrar finns för problem med att användare inte kan registreras inför användningen av systemet (exempelvis på grund av funktionsvariation) samt för problem med att användare vid användningen inte längre kan nyttja systemet (exempelvis på grund av skada). Utvärderingen sker också med avseende på hur många individer som systemet kan användas för per tidsenhet. Standarden nämner vidare att ytterligare faktorer bör beaktas vid utvärderingen, såsom systemmiljön (och därför effekter av exempelvis väder). Däremot inkluderar standardens typ av utvärdering inte någon bedömning som rör kraven på systemets säkerhet (med angripare) eller användarnas acceptans för systemet.

[7] I Försvarsmaktens handbok för fysisk säkerhet (Försvarsmakten, 2015) nämns exempelvis väder, buller och störningar från djur.

2.4 Teknisk bevakning

Teknisk bevakning utgörs av teknik som används för övervakning och skydd i syfte att kontrollera egen personal och upptäcka antagonister. Enligt Försvarsmaktens definition av teknisk bevakning, sker övervakning och skydd av både fasta och rörliga objekt (och verksamheter) (Försvarsmakten, u.å.). Försvarsmakten beskriver också på vilka sätt övervakningen och skyddet kan uppnås. I denna rapport ligger fokus på följande två av dessa sex sätt som bäst fungerar i samband med biometri:

- Inhämta, distribuera, lagra, bearbeta och presentera strukturerad bevakningsinformation bestående av exempelvis text, ljud och/eller bild.
- Tillhandahålla behörighetsstyrd passerkontroll för tillträde till objekt och verksamheter.

De fyra övriga sätten gäller insatsstyrkor, reaktiva och proaktiva skyddsåtgärder samt hotbildsanalyser.

Försvarsmakten beskriver i en handbok (Försvarsmakten, 2015) hur fysisk säkerhet kan uppnås. Kortfattat utgörs detta av:

- Bemannad bevakning.
- Passerkontroller.
- Larm och övervakning.
- Lås och murar.
- Tillträdesförbud.

I vissa fall kan ett av sätten vara tillräckligt, i andra krävs en kombination. Biometriska metoder passar in på både *övervakning* och *passerkontroller*. De biometriska metoderna kan sedan använda *larm* för att informera den som *bemannat bevakar*. I undantagsfall kan larmen istället för att informera personal, ha som uppgift att skrämma bort gärningspersoner, eller att påkalla omgivningens uppmärksamhet (Försvarsmakten, 2015). De mer statiska skydden (*lås och murar* samt *tillträdesförbud*) ligger längre utanför ramen för biometriska metoder, men kan utgöra ett kompletterande skydd.

3 Etiska och legala aspekter av biometri

Biometriska system har sina brister. Sådana brister beskrivs ofta på en övergripande statistisk nivå, utan att ta hänsyn till vilka individer som drabbas av bristerna.

I själva verket finns vissa individer som oftare än andra har svårt att bli igenkända av systemet. Det finns också individer som lättare än andra kan imiteras och som därför oftare än andra individer utnyttjas av angripare. I båda fallen kan det röra sig om individer som systemet inte utvecklats ordentligt för, och det finns en etisk problematik i att dessa individer drabbas av en orättvist stor del av systemets brister.

På befolkningsgruppsnivå finns exempel på hur biometriska system utvecklats undermåligt och därför grundlöst diskriminerat mot vissa grupper av individer. Exempelvis införde brittiska inrikesdepartementet en app för att ta och ladda upp passfoton inför passansökningar, trots att de kände till att appen fungerade dåligt för vissa etniska grupper (Vaughan, 2019). I en undersökning av olika varianter av ansiktsigenkänning kom amerikanska standardiseringsorganet NIST fram till att ansiktsigenkänning fungerade bättre för östasiater när algoritmerna tagits fram i Kina än i länder med annan demografi (Grother m.fl., 2019). NIST kom också fram till att det mellan olika demografiska grupper ofta skilde en faktor 10–100 i hur lätt individer blandades samman (i form av falska positiva), medan variationerna var betydligt lägre för situationer där individer inte känns igen (falska negativa).

För att människor ska ha mer tilltro till ett biometriskt system kan möjligheterna att kontrollera att systemet tar rätt beslut behöva ökas. Exempelvis finns det behov av att människor kan förstå hur systemet fungerar. Mjuk biometri kan då vara en fördel eftersom individer där kategoriseras mer övergripande än med annan (vanlig) biometri. En svårighet är dessutom att människor behöver förstå de komplicerade algoritmer som systemen använder och rentav den typ av algoritmer som anpassas efterhand algoritmerna lär sig. En möjlig lösning är att använda så kallad *förklarande artificiell intelligens*, vilken beskrivs mer i Svenmarck m.fl. (2018) samt Luotsinen m.fl. (2019).

Ett annat etiskt problem är att biometri är nära knutet till individen. Samtidigt som det ur ett säkerhetsperspektiv är bra att det finns stark anknytning till (betrodda) individer, eftersom det gör det svårare för angripare, kan det ses som omänskligt att funktionellt reducera människor till data (Brey, 2004). Det kan också ses som att individerna förlorar kontrollen över sin kropp i och med att biometriska data om den ägs av andra (Brey, 2004).

Ett annat problem med biometriska system är att de förutom vad Försvarsmakten ser som godartad användning, också kan användas till att kränka mänskliga rättigheter. Exempelvis har kinesiska myndigheter anklagats för att använda ansiktsigenkänning för att spåra och kontrollera uigurer (Mozur, 2019). Flera stora amerikanska IT-företag har nyligen tillkännagivit att de inte kommer låta sina biometriska system användas för massövervakning (Hern, 2019 samt IBM, 2020) och de ser ett behov av mer lagstiftning på området (Amazon, 2020 samt IBM, 2020).

De legala krav som ställs vid användningen av biometriska metoder i Sverige och övriga EU utgörs bland annat av dataskyddsförordningen (GDPR). Enligt GDPR räknas biometriska data som *särskilda kategorier av personuppgifter* (även benämnda *känsliga uppgifter*), vilka kräver särskilt goda anledningar för att få behandlas (insamlas, struktureras, bearbetas, spridas, raderas, med mera) (Dataskyddsförordningen, 2016). Exempelvis var olovlig användning av biometrisk ansiktsigenkänning i en gymnasieskola upphovet till att Datainspektionen för första gången utfärdade en sanktionsavgift för att en aktör brutit mot GDPR (Datainspektionen, 2019). Sanktionsavgiften motiverades med att ansiktsigenkänningen övervakat eleverna i deras vardagliga miljö, varit ett intrång i deras integritet, samtidigt som övervakningens syfte (närvarokontroll) kunde uppfyllts på andra sätt som svar mindre integritetskränkande (Datainspektionen, 2019).

Datainspektionen nämner också att skyddskraven ökar i takt med riskerna, vilka i sin tur är större ju känsligare personuppgifterna är (Datainspektionen, 2020a). Det kan också behövas ytterligare skyddsåtgärder när personuppgifter förs över till länder utanför EU (Datainspektionen, 2020b). Vad gäller restriktiva lagar utanför EU har flera större städer i USA helt förbjudit offentliga myndigheter att använda biometrisk ansiktsigenkänning (Haskins, 2019). I Storbritannien förbjöds nyligen en polismyndighets användning av ansiktsigenkänning (Rees, 2020). Polisen hade i flera år använt ansiktsigenkänning vid bland annat större sportevenemang och konserter, men domstolen ansåg inte att riskerna för de övervakades personliga integritet utretts ordentligt.

Förutom GDPR finns också andra relevanta lagar. Ett exempel är kamerabevakningslagen (SFS 2018:1200). Försvarsmakten behöver dock inte ”tillstånd för övervakning som sker för att skydda en byggnad, en annan anläggning eller ett område som förklarats som skyddsobjekt enligt 5 §. 1-5 Skyddslagen, om övervakningen endast omfattar skyddsobjektet eller ett område i dess omedelbara närhet.” (Försvarsmakten, 2015)

4 Angrepp mot biometriska system

Det är vanligt att utvärdering av biometriska system görs utan att beakta antagonisters möjliga angrepp mot systemen. Exempelvis dröjde det till 2019 innan den första genomgången (eng. review) av forskningsartiklar på ämnet angrepp mot fingeravtrycksigenkänning kom (Yang m.fl., 2019). Det tyder på att forskningen dittills fokuserat på annat eller inte hunnit bli specialiserat nog att göra sådan genomgång. Vidare ingår ingen utvärdering av angreppsmöjligheter i den internationella standarden för teknisk utvärdering av biometriska system (ISO/IEC, 2006). Biometriska system är dock, precis som alla system, möjliga att angripa. Angreppen kan ha två generella syften: att hindra legitim användning eller att få systemet att acceptera illegitim användning. Ett biometriskt system måste därför skyddas mot angripare, så att följande två krav uppfylls:

1. Systemet känner inom rimlig tid igen de individer som ska kännas igen i olika situationer.
2. Systemet känner inte igen individer som inte ska kännas igen.

Dessa krav motsvarar i huvudsak de som beskrevs i avsnitt 2.3. Där fanns dock också krav på att användarna skulle acceptera systemet. Det ligger delvis utanför ämnet angrepp, men det kan noteras att om angrepp särskilt drabbar användare av systemet (snarare än systemet) kommer användarna förmodligen bli mindre benägna att vilja delta i systemet (om de har något val). Dessutom kan systemen oavsiktligt samla in data som användarna vill hålla hemliga. Exempelvis kanske ett system som baseras på ansiktsigenkänning råkar samla in vad som står skrivet i ett hemligt dokument en person håller i. Sådana risker beskrivs dock inte vidare i denna rapport.

I de följande avsnitten beskrivs mer om de två kraven, hur angrepp påverkar dem och hur kraven kan upprätthållas trots angreppen.

4.1 Hindrande av legitim igenkänning

Det finns två skäl för en angripare att hindra ett biometriskt systems användning. Det första skälet är att hindra individer från att kännas igen varpå individerna går miste om en resurs som systemet bevakar. Det andra skälet är att hindra systemet från att upptäcka individer som systemet är tänkt att upptäcka. Oavsett skäl kan angriparen använda många olika tekniker för att sabotera. Ibland vill angripare sabotera så mycket som möjligt. I andra fall vill angriparen bara påverka viss användning och angriparen använder då mer riktade sabotageförsök. Exempelvis kanske angriparen använder någon form av maskering för att dölja sina kännetecken och därmed hindrar systemet.

Försök att sabotera biometriska system kan ske genom direkt fysisk påverkan eller genom logisk påverkan i form av sådant som överbelastningsangrepp mot

IT-komponenter (DoS). Förutom olika maskeringsmöjligheter, är problemen med angripare som hindrar det biometriska systemets legitima användning i huvudsak desamma som (en delmängd av) de problem som alla IT-system står inför. Detta märks också av forskningslitteraturen om biometri som enbart i undantagsfall tar upp hindrande av legitim igenkänning. Någon utförlig analys av problemen görs därför inte här.

En sammanfattning av lösningarna på problemen är att det behöver finnas rutiner för vad som ska ske om systemet slutar fungera samt förståelse för i vilken mån reservalternativen skiljer mot det huvudsakliga systemet och hur de kan utnyttjas av angripare.

4.2 Införande av illegitim igenkänning

I de följande avsnitten beskrivs hur angripare kan införa illegitim igenkänning.

4.2.1 Manipulation vid registrering

För att minska möjligheterna för angripare att påverka registreringsprocessen och därmed systemets databas behöver det finnas kontroll över processen. Exempelvis måste det beaktas att även de individer som ska registreras kan utgöra angripare. Den som är ansvarig för systemet måste därför kontrollera att dessa individer inte för in otillåtna data i samband med registreringen. Brister vad gäller sådan kontroll beskrivs i Kalvet m.fl. (2018).

4.2.2 Utnyttjande av undermålig granskning

Vid testning av system läggs det ofta in olika typer av testdata som förenklar testarnas arbete och gör att de i vissa situationer inte behöver gå igenom hela de normala (skarpa) processerna. Exempelvis vid testning av IT-system läggs det ofta in enkla lösenord och sådana lösenord måste tas bort före skarp användning. På liknande sätt kan det vid test av biometriska system läggas in genvägar som sedan måste tas bort före skarp användning.

Snarlikt detta varnar Jain m.fl. (2008) för att de biometriska systemens algoritmer kan innehålla sårbarheter som gör det möjligt för angripare att bli accepterade av systemet om de matar in vissa ovanliga indata (som aldrig förekommer vid legitim användning). Att granska algoritmer efter sårbarheter är svårt och särskilt svårt är det om algoritmerna delvis konstrueras av egna lärdomar utifrån testdata (maskininlärningsalgoritmer, vilka beskrivs i Svenmarck m.fl. (2018)).

4.2.3 Uppspelning av legitimt beteende

Ett möjligt problem är angripare som kan spela in legitim igenkänning och sedan spela upp den för systemet för att på så vis få systemet att tro att det känner igen något som inte längre är aktuellt. Sådan uppspelning kan stoppas genom att igenkänningen görs lite olika varje gång. Exempelvis kan tiden för igenkänningen inkluderas som en variabel i processen, eller så kan något annat specifikt och nytt förväntas (Jain m.fl., 2008).

4.2.4 Imitation av legitimt beteende

Ett annat möjligt problem är angripare som kan använda imitation[8] (eng. spoofing) för att efterlikna de kännetecken som tillhör en annan individ. Exempelvis kan angripa försöka imitera någon annans gångstil, eller med olika tekniker försöka få sina fingeravtryck att se ut och kännas igen som någon annans. Ett exempel på hur angripare lyckats imitera rörde röstigenkänning. Angriparna använde algoritmer baserade på artificiell intelligens för att lära en dator att härma en viss individs röst. Sedan lät de datorn med imiterad röst instruera en kollega till den härmade individen att föra över pengar till angriparna (Stupp, 2019). Detta var dock inte ett angrepp mot ett biometriskt system utan mot mänsklig igenkänning.

Det är inte klarlagt hur lätt det är att imitera individer på ett sätt som kan lura biometriska system. Biometriska system testas i huvudsak utan att analysera om realistiska angripare skulle kunna lura systemet. I forskningslitteraturen studeras dock olika imitationsmöjligheter och hur de kan stoppas. Exempelvis har metoder baserad på ytlig kontroll av fingeravtryck kompletterats med kontroll av att fingret svettas. (Parthasaradhi m.fl., 2005). Sådana kontroller kallas ibland *liveness detection* och de förs allteftersom in i skarpa biometriska system.

Angripare som vill lära sig att imitera en individ i ett system kan försöka tolka hur individen känns igen genom att studera de data som lagras om individen i systemets databas (om angriparen lyckas få tillgång till databasen). Om angriparens försök lyckas och det upptäcks, vore det lämpligt att reagera genom att individen registrerades på nytt i systemet och framöver känns igen på ett annat sätt. På så vis skulle angriparens inhämtade kunskap bli förlegad och fortsatt imitation stoppas. Det är dock svårt för individen att ändra sin grundläggande biologi eller sitt beteende (kännetecknen). Systemen bör därför baseras på säregna varianter av kännetecknen (exempelvis *upphävningsbar biometri*, efter eng. cancelable biometrics) (Patel m.fl., 2015). Om det upptäckts att information om varianten av kännetecknet läckt ut, kan variationen som används i systemet ändras utan att individens kännetecken måste ändras. Om

[8] I den engelskspråkiga litteraturen om biometri används ofta ordet *spoofing*. Det används också inom IT-säkerhet men då främst när det talas om förfalskningar i nätverkstrafik (logisk spoofing) snarare än den imitation som avses här vilken kan vara både logisk och fysisk.

variationen är systemspecifik gör detta också att lagrade data som används i ett annat biometriskt system inte kan användas för att ta sig in i detta biometriska system. Variationerna kan liknas vid att kombinera olika biometriska metoder, men tillåter att icke-biometriska data används i kombinationen, varför det finns större möjligheter att skapa unika varianter (Karlzén m.fl., 2020). Det är svårt att ta fram varianter som är säkra mot försök att, utifrån varianten av kännetecknet, dra slutsatser om själva kännetecknet. Inspiration kan dock dras till hur lösenord lagras med envägsfunktioner (hashfunktioner). Med sådana funktioner ges helt olika utdata om indata skiljer det allra minsta. För biometri är visserligen sådana stora förändringar ett problem eftersom exempelvis miljön vid avläsning av biometriska kännetecken varierar, men detta är trots allt en lösning som ofta används (Patel m.fl., 2015). För fingeravtrycksigenkänning har lösningarna visat sig ge tiofaldigt högre falska positiva och falska negativa (Yang m.fl., 2019).

4.2.5 Tvingande av individer

Förutom att imitera andra individer kan angripare tvinga individer att delta i igenkänning. Czajka och Bowyer (2018) beskrev denna angreppsmetod, men noterade också att det saknas forskning på området, med den angivna anledningen att det vore svårt att utföra sådan forskning på ett etiskt och samtidigt verklighetstroget sätt. För att undvika att angripare släpps in och att personal skadas, vore det bra om individer som tvingas kan visa upp ett alternativt kännetecken som accepteras av systemet på vanligt vis, samtidigt som ett tyst larm går om tvånget. Försvarsmakten använder liknande överfallslarm idag i vissa situationer.

5 Användningsfall

I detta kapitel beskrivs några generella situationer (användningsfall) där Försvarsmakten har behov av teknisk bevakning vilka kan mötas med biometriska metoder. Denna rapports författare gör bedömningen att dessa användningsfall är mer sannolika i praktiken, än andra användningsfall. Användningsfallen är dock inte tänkta att täcka alla relevanta situationer, utan fokuserar på ett urval av situationer som bedömts vara mest relevanta.

Användningsfallen förutsätter att när ett biometriskt system införts, finns det också något sätt att avgöra om det är läge att använda systemet. Det förutsätts därmed att det biometriska systemet kan utgå från en upptäckt människa, snarare än från ett objekt som först måste kategoriseras som människa. Det förutsätts också att det identifierats ett behov av att känna igen individen, exempelvis i form av att individen är på ett visst ställe, håller i en viss typ av föremål, är på plats tillsammans med många andra individer, eller setts agera på något visst sätt.[9]

Varje användningsfall beskrivs utifrån följande parametrar[10]:

- Bevakningsobjekt (exempelvis förråd, sensor, transmissionsutrustning, kontorsbyggnad eller transport).
- Oönskad händelse (vad igenkänningen ska larma om, ex. förstörelse, stöld, hindrande, kartläggning eller våld).
    - Händelsens potentiella allvarlighet.
    - Händelsens sannolikhet.
- Miljö (exempelvis glesbygd eller tätort).
- Deltagande (exempelvis om individerna som ska igenkännas poserar för kameran eller om de maskerar sig).
- Individer (vilka som ska kännas igen; ex. vitlistad personal, svartlistade terrorister eller grålistade som tidigare känts igen vid samma eller annan plats).

Nedan beskrivs användningsfallen.

[9] Igenkänning av visst agerande kallas på engelskt fackspråk för *action recognition*. Det kan till exempel handla om att känna igen en rörelse av viss hastighet eller att ett objekt läggs vid en plats.

[10] Användningsfall beskrivs bara för ett urval av alla möjliga värden på varje parameter och kombinationer av dessa.

5.1 Kartläggning av avlägset förråd

Bevakningsobjekt: Förråd.

Oönskad händelse: Kartläggning på plats.

- Allvarlighet: Medel, kartläggningen leder inte till några direkta konsekvenser, men antagonisten har förmodligen god kunskap om ytterligare förråd varför kartläggningen kan bli omfattande och kan därför utnyttjas för att vid krig slå ut Försvarsmaktens förmåga.
- Sannolikhet: Hög, antagonister har visat klar intention att kartlägga på detta sätt.

Miljö: Skog, 1 timme från närmaste vakt, polis och tekniker.

Deltagande: Nej, de som kartlägger kommer inte underlätta igenkänningen. Möjligen maskerar de sig till och med eller på annat sätt försvårar igenkänningen.

Individer: Grålistade individer som observerats vid liknande platser tidigare och som då kan ha brutit mot avbildnings- och beskrivningsförbudet.

5.2 Stöld ur avlägset förråd

Bevakningsobjekt: Förråd.

Oönskad händelse: Stöld.

- Allvarlighet: Hög, förrådets funktion upphör och antagonisten kommer över potentiellt farlig materiel.
- Sannolikhet: Medel, att ta reda på var förråden finns är visserligen görbart, men tjuvarna har ingen möjlighet att veta vad där finns och de flesta liknande antagonister vill hellre ge sig på mål som inte skyddas av Försvarsmakten.

Miljö: Skog, 1 timme från närmaste vakt, polis och tekniker.

Deltagande: Nej, tjuvarna kommer inte underlätta igenkänningen. Men de är förmodligen inte kompetenta nog att maskera sig.

Individer: Svartlistade individer som är efterlysta av polisen.

5.3 Förstörelse av avlägsen radiomast

Bevakningsobjekt: Radiomast.

Oönskad händelse: Förstörelse genom att masten välts.

- Allvarlighet: Hög, förstörelsen leder till omfattande skador som tar lång tid att reparera.
- Sannolikhet: Medel, dessa individer har genomfört liknande aktioner och bryr sig inte om risken för upptäckt.

Miljö: Skog, 30 minuter från närmaste vakt, polis och tekniker.

Deltagande: Delvis, de som förstör vill ha uppmärksamhet och förväntar sig att bli gripna vid platsen.

Individer: Svartlistade individer som är efterlysta av polisen.

5.4 Kartläggning av kontorsbyggnad i tätort

Bevakningsobjekt: Kontorsbyggnad och personal.

Oönskad händelse: Kartläggning genom fotografering med mindre kamera.

- Allvarlighet: Medel, kartläggningen av personal kan användas för värvningsförsök, medan kartläggningen av byggnaden kan underlätta intrång i viss grad.
- Sannolikhet: Hög, stora mängder individer passerar utanför byggnaden varje dag och många av dem har nyfiket noterat byggnaden och dess personal och är vana vid att de normalt får fotografera det de är nyfikna på. De är också vana vid att lägga ut bilder i sociala medier vilka kan övervakas av terrorister.

Miljö: Tätort, 1–5 minuter från närmaste vakt och tekniker; 15 minuter från polis.

Deltagande: Nej, men de som fotograferar gör inte heller något försvårande eftersom de inte vet att vad de gör är förbjudet.

Individer: Grålistade individer som förekommer på andra kameror i närheten, exempelvis vid parkeringshus eller ombord kollektivtrafik. Övriga kan inte kännas igen.

5.5 Obehörig inpassering till mindre förläggning i glesbygd

Bevakningsobjekt: Mindre förläggning.

Oönskad händelse: Antagonister passerar in för att stjäla materiel, sabotera eller bruka våld mot personal.

- Allvarlighet: Hög.

- Sannolikhet: Låg, personalen är alert och beväpnad. Få antagonister vill ge sig på en förläggning i fredstid.

Miljö: Glesbygd, 1–5 minuter från närmaste vakt; 1 timme från polis och tekniker.

Deltagande: Delvis, personalen saktar ner fordon för att bli igenkända, men har inte möjlighet att helt stanna eller ta av sig mundering. (Antagonister är inte deltagande, men kan överhuvudtaget inte kännas igen eftersom de inte finns registrerade på förhand).

Individer: Vitlistade individer i form av personal och besökare. Övriga kan ej kännas igen.

5.6 Stöld och sabotage i serverrum i kontorsbyggnad i tätort

Bevakningsobjekt: Serverrum i kontorsbyggnad.

Oönskad händelse: Antagonister passerar in och stjäl materiel eller saboterar.

- Allvarlighet: Hög, stöld leder till att stora mängder skyddsvärd information läcker ut, sabotage leder till att en avsevärd del av verksamhet inte kan utföras.
- Sannolikhet: Låg, vakter och yttre skalskydd gör att enbart egen personal och ledsagade besökare kan utgöra antagonister.

Miljö: Tätort, 1 minuter från närmaste vakt och tekniker; 15 minuter från polis. Inomhus.

Deltagande: Delvis, särskilt auktoriserad personal följer reglerna för igenkänning, medan insiders kommer försöka undgå upptäckt.

Individer: Vitlistad auktoriserad personal samt grålistade individer i form av övrig personal och besökare.

5.7 Stöld och sabotage i kontorsbyggnad i tätort

Bevakningsobjekt: Kontorsbyggnad och personal.

Oönskad händelse: Antagonister passerar in och stjäl materiel eller saboterar.

- Allvarlighet: Medel, mycket materiel finns att stjäla eller sabotera, men det mest skyddsvärda är inte åtkomligt utan att passera ytterligare barriärer.

- Sannolikhet: Medel, stora mängder individer passerar utanför byggnaden varje dag och vissa kan få för sig att ge sig på byggnaden; samtidigt har de vetskap om att objektet är mer välbevakat än de flesta.

Miljö: Tätort, 1–5 minuter från närmaste vakt och tekniker; 15 minuter från polis.

Deltagande: Delvis, personal och besökare följer reglerna för igenkänning, medan övriga kommer försöka undgå upptäckt.

Individer: Vitlistade individer i form av personal och besökare samt grålistade individer som förekommer på andra kameror i närheten, exempelvis vid parkeringshus eller ombord kollektivtrafik.

6 Biometriska metoder

De följande avsnitten presenterar ett urval av biometriska metoder. Avsnitten inkluderar inte alla biometriska metoder som existerar. De metoder som inte nämns är de vars utveckling är i ett tidigt stadium samt de som har användningsområden som inte stämmer överens med rapportens fokus.

Varje metod beskrivs mot bakgrund av kraven i avsnitt 2.3. Vad som beskrivs per metod framgår av Tabell 1.[11] I vissa fall har ingen information hittats om hur en metod uppfyller ett visst krav, cellen i tabellen är då tom.

Tabell 1: Vad som beskrivs (markerat med symbolen ●) om de biometriska metoderna, utifrån kraven.

Metod	Unik.	Oför.	Insaml.	Träff.	Prest.	Anv.-acc.	Resist.
Finger	●		●	●	●		●
Iris	●	●	●	●	●		●
Ansikte			●	●	●	●	●
Öra	●	●	●	●			
Blodåder	●	●	●	●		●	●
Röst	●		●	●			●
Hand	●	●	●	●	●	●	
DNA	●		●	●	●		

Unik. = Unikhet; Oför. = Oföränderlighet; Insaml. = Insamlingsförmåga; Träff. = träffsäkerheten i form av att det inte ges falska positiva och falska negativa; Prest. = Systemprestanda; Anv.acc. = Användarnas acceptans av användningen av kännetecknet; Resist. = Resistens mot antagonisters möjligheter att kringgå systemet.

Utöver kraven beskrivs också metoderna utifrån deras historik eller popularitet (först i varje avsnitt).

6.1 Fingeravtrycksigenkänning

Fingeravtryck har använts för igenkänning i över ett århundrade, men automatiseringen av metoden dröjde till mitten av 1970-talet (Moses m.fl., 2011). Fingeravtryck tros vara unika, både mellan människor och mellan en viss individs fingrar (Maltoni m.fl., 2009).

Avläsningen av fingeravtryck kan ske med flera typer av sensorer, exempelvis optiska, ultraljudbaserade eller kapacitiva (som på en smartphone) (Al Shehri

[11] Ingen information hittades om *universaliteten* (att alla individer innehar kännetecknet) för de kännetecken som ligger till grund för metoderna. Detta krav utelämnas därför från tabellen, men framgår till viss del av hur oföränderlig metoden är, eftersom oföränderligheten handlar om huruvida kännetecknet innehas vid varje tidpunkt av individerna.

m.fl. 2018; Levalle, 2020). Avläsningen görs av en delmängd av de över hundra detaljpunkter som kan nyttjas för igenkänning. I de allra flesta fall räcker det att jämföra 12–15 detaljpunkter (Maltoni m.fl., 2009).

NIST (2004) visade att fingeravtryckssystem generellt ger låga andelar falska positiva och falska negativa. Det bästa systemet i utvärderingen fick ner andelen falska negativa till 0,014 % när bara ett finger användes och till 0,001 % för fyra eller fler fingrar[12]. Dessa resultat stod sig tio år senare, men fler olika algoritmer uppnådde samma goda nivå (NIST, 2014). NIST (2014) såg dessutom att de snabbaste algoritmerna fick högre andel falska negativa. NIST (2020a) genomförde en analys av både kontaktlösa och kontaktberoende fingeravtrycksläsare och fann att kontaktberoende avläsare fick lägre andel falska negativa och falska positiva än de kontaktlösa fick. För de kontaktlösa var siffrorna extremt höga när bara ett finger användes, men nere på 0,005 % när flera fingrar användes.

Grosz m.fl. (2020) fann att avläsningen av fingeravtryck påverkades mer av mänskliga faktorer som trycket på sensorn, eller fingrets värme och svettning, snarare än miljömässiga faktorer såsom temperatur eller luftfuktighet. Detta styrks även av resultaten från Stewart m.fl. (2009) som skriver att fingeravtryckssystem generellt inte påverkas av temperatur (-30°C till +20°C i studien).

Angrepp mot fingeravtrycksigenkänning kan exempelvis ske genom att använda gelatinavgjutningar av fingeravtryck, digitalt utskrivna fingeravtryck eller till och med att blåsa på en sensor för att återanvända latenta fingeravtryck (Maro och Kovalchuk, 2018; Levalle, 2020). Det finns dock metoder att tillgå för att minska riskerna för att systemet blir lurat, exempelvis mätning av puls, värme eller svettning.

6.2 Irisigenkänning

Igenkänning baserat på iris används i stor utsträckning, såsom i ett nationellt indiskt system där mer än en miljard individers irisar registrerats (Anderson, 2020). Människors irisar är unika för varje individ[13] (Daugman och Downing, 2001) och det gäller även när identiska tvillingar jämförs (Anderson, 2020).

Irisar förändras inte mycket med tiden (Daugman och Downing, 2001). Irisskanning har visat sig kunna känna igen individer även om de har relativt vanligt förekommande sjukdomar eller skador som exempelvis hornhinneödem eller bindhinneinflammation. Däremot påverkades resultaten hos individer med

[12] Givet ett FP-värde av 0,01 %.

[13] Sannolikheten för att två irisar är lika till minst 70 % är 1 på 7 miljarder.

akut druvhinneinflammation, vilket dock är en sjukdom som förekommer i mindre utsträckning (Aslam m.fl., 2009).

Vid irisigenkänning avläses irisen med antingen synligt ljus eller nära-infrarött ljus. För mörka irisar är det svårt att se detaljer med enbart synligt ljus, vilket gör att det då behövs nära-infrarött ljus (NIST 2019c).

Metoden är generellt bra på att känna igen individer (Daugman, 2009; NIST 2018). NIST (2018) testade olika algoritmer och den bästa algoritmen hade mindre än 1 % falska negativa.[14]

Irisigenkänning är väldigt snabb. För en databas med 160 000 individer lyckades de produkter som inkluderades i NIST (2018) klara verifiering på under en millisekund och identifiering på elva millisekunder (i median). Vid kontrollerade ljusförhållanden kan irisigenkänning även användas för att känna igen individer på avstånd (Matey m.fl., 2006).

Angrepp mot irisigenkänning kan exempelvis ske genom att en angripare håller upp ett högupplöst fotografi av en iris (Czajka, 2016). Detta kan motverkas av exempelvis mätning av pupillens storleksförändring under belysning.

6.3 Ansiktsigenkänning

Ansiktsigenkänning är en vanligt förekommande metod som exempelvis används flitigt för att känna igen individer när de vill ha åtkomst till sina mobiltelefoner.

Ansiktsigenkänning utgår från mätning av olika delar av ansiktet, som bland annat avståndet mellan ögonen, näsans bredd, käklinjens längd och formen på kindbenen (Paderes 2015). Ansiktsigenkänning delas upp beroende på om avläsningen sker tvådimensionellt (2D) eller tredimensionellt (3D). 2D-ansiktsigenkänning använder en vanlig kamera som sensor (Zhou och Xiao, 2018). 3D-ansiktsigenkänning utgår från insamling via 3D-skannrar eller från flera bilder från 2D-kameror där vinklarna varieras.

Ansiktsigenkänning har tack vare införandet av AI-algoritmer förbättrats kraftigt det senaste decenniet (NIST, 2019b). Idag finns flera algoritmer som ger falska positiva och falska negativa under 1 % (NIST, 2019b; NIST, 2020b).[15] De automatiska metoderna är dessutom bättre på att känna igen ansikten än vad de bästa mänskliga forensiska experterna är (Phillips m.fl., 2018).

I början av pandemin med Covid-19 gjorde amerikanska standardiseringsorganet NIST (2020c) en undersökning av om gängse algoritmer för ansiktsigenkänning

[14] Givet ett FP-värde på 0,001% för identifiering och 0,00001 % (1 av 100 000) för verifiering.

[15] Under ideella förhållanden, exempelvis passfoton där bilden är av bra kvalitet och ansiktet syns tydligt rakt framifrån.

fungerade även när individerna som ska kännas igen bär ansiktsmasker som skydd mot viruset. En slutsats var att ansiktsigenkänningen fungerade relativt väl trots ansiktsmaskerna. Senare under pandemin gjorde NIST (2020d) ett nytt test och det visade att algoritmer som tagits fram senare fick ännu bättre resultat, vilket tyder på att tillverkarna börjat anpassa sig för ansiktsmaskerna. 2D-ansiktsigenkänning påverkas av sådant som omgivningens ljus, rörelser av huvudet och rörelser av ansiktet (Zhou och Xiao, 2018). 3D-ansiktsigenkänning påverkas inte i lika stor utsträckning som 2D ansiktsigenkänning av detta, varför mer forskning börjat inriktas på 3D-varianten (Zhou och Xiao, 2018).

Eftersom ansiktsigenkänning kan utföras på relativt långa avstånd och inte kräver någon särskild interaktion med användaren är metoden inte särskilt inkräktande för individen. Däremot kan möjligheterna för igenkänning på avstånd möjliggöra att metoden används utan att individerna får avgöra om de ska delta eller ej. (Zhou och Xiao, 2018)

Möjligheten att avläsa på avstånd gör det relativt lätt för angripare att samla in kunskap om en individs ansikte vilket kan nyttjas för att imitera individen (Zhou och Xiao, 2018).

6.4 Öronigenkänning

Metoden är vanlig bland rättsväsendet i andra länder. Exempelvis använder den tyska polisen visuellt avläst öronigenkänning i kombination med andra utseendebaserade kännetecken för att känna igen misstänkta på bilder från övervakningskameror (Pflug och Busch, 2012).

Huruvida öron är unika är inte klarlagt. Burge och Burger (2006) kom visserligen fram till att alla öron är unika, men Pflug och Busch (2012) påstår att det inte fanns tillräcklig evidens för att säga att öron verkligen är unika.

Örat utgör ett stabilt kännetecken som endast ändras något i storlek över tid (Pflug och Busch, 2012). Vidare finns två sätt att mäta öron: antingen visuell mätning av örats form, eller genom att med akustiska signaler mäta hörselgångens form.

Tidigare lösningsförslag som nyttjat akustiska signaler för att mäta hörselgångens form gav relativt höga falska positiva och falska negativa (0,8 till 18,0 %). Det senaste decenniets tekniska utveckling har dock förbättrat situationen (Mahto m.fl., 2018). Arakawa m.fl. (2016) föreslog en lösning som skickar en ljudsignal från en hörlursenhet in i hörselgången och mäter sedan det eko som spelas tillbaka. Med denna lösning nåddes falska positiva och falska negativa på under 1 %.

6.5 Blodådersigenkänning

Mokroß m.fl. (2020) beskriver att det finns många system för blodådersigenkänning som kan känna igen individer, men att många av systemen nyttjar långsamma algoritmer.

Blodådrorna i handen anses av forskare utgöra ett någorlunda unikt biometriskt kännetecken (Yüksel m.fl., 2010; Shinzaki, 2020). Blodådrorna i handen utgör dessutom en relativt stabil datapunkt som sällan förändras över tid, förutom i storlek. Delvis beror detta på att blodådror ligger skyddade inne i kroppen och därför inte påverkas av externa slitningar eller skador. (Shinzaki, 2020)

Igenkänning baserat på blodådror utförs vanligen genom att fotografera och analysera blodådersmönstret i ena sidan av handen eller i fingrarna. I Shinzaki (2020) beskrevs ett test som visat på att andelen falska positiva är under 0,0001 % och andelen falska negativa är på 0,01 %. Testet utgick dock från att sensorn avläste individernas händer flera gånger på rad.

Igenkänningen sker ofta kontaktlöst och är då hygienisk (Shinzaki, 2020). Shinzaki (2020) beskriver också att eftersom blodådror är inne i kroppen är det svårare för angripare att stjäla eller kopiera information om dem.

6.6 Röstigenkänning

Röstigenkänning, även kallad talarigenkänning, är en biometrisk metod som känner igen individer baserat på deras röster[16]. Det senaste decenniet har röstigenkänning blivit tillräckligt bra för att kommersialiseras (Wu m.fl., 2015).

Röster (och tal) är ganska unika vilket beror på både fysiologiska och beteendebaserade skillnader mellan individer (Wu m.fl., 2015).

Röstigenkänning kan primärt utföras på två olika sätt: *frasoberoende* eller *frasberoende*. I frasoberoende igenkänning utförs jämförelser på tal som inte innehåller specifika fraser eller ord. I den frasberoende metoden, som primärt används för verifiering, nyttjas en specifik fras som individen talat in när den först registrerades i systemet. För den frasoberoende metoden däremot lägger forskning större vikt vid identifiering snarare än verifiering (Wu m.fl., 2015). Samma källa beskriver att röstigenkänningssystem förbättrades under 2010–2015 med hjälp av nya tekniker inom så kallad kanal- och ljudkompensation.

[16] Metoden ska dock inte blandas ihop med taligenkänning (eng. speech recognition), vilket är en teknik för tal-till-text-applikationer eller virtuella assistenter. Taligenkänning kan hantera verbalt språk, men kan inte identifiera en talares identitet, vilket biometrisk röstigenkänning kan.

Röstigenkänning fungerade länge ganska dåligt, med falska positiva och falska negativa på upp mot 10 % (Unar m.fl., 2014). Att metoden kommersialiserats nyligen gör dock att det finns anledning att tro att den kan ha blivit bättre.

Sriskandaraja m.fl. (2018) beskriver att ett problem med röstigenkänning är att det är svårt att automatiskt upptäcka angrepp där en angripare spelat in en individs röst och sedan spelar upp inspelning för systemet. Sådant angrepp kan dock motverkas genom att exempelvis jämföra nya åtkomstförsök med tidigare för att se om det nya är en exakt reproduktion.

6.7 Finger- och handgeometriigenkänning

Finger- och handgeometriigenkänning utgår från geometrin hos fingrar och händer. Igenkänning baserat på handgeometri har använts sedan 1970-talet (Štruc och Pavešić, 2015).[17] Metoden används bland annat för åtkomstkontroll och för tid- och närvaroövervakning.

Det är inte klarlagt hur unika händer och fingrar är, men det finns inte så stora skillnader mellan individer, vilket gör att metoden nästan uteslutande används för verifiering. Igenkänningen kan påverkas av viktförändring eller diverse medicinska åkommor, som exempelvis resulterar i svullnad eller skador på handen.

I metoden görs visuell avläsning av en individs hand och fingrar, exempelvis fingrarnas olika längd och bredd samt handens längd och bredd. Kommersiella system[18] använder en högpixelkamera i kombination med infrarött ljus och en spegel för att ta tredimensionella avbildningar av handen.

Graden av falska positiva (FP) och falska negativa (FN) ligger oftast mellan 0,1 % och 1 %.

En av metodens främsta fördelar är att den är enkel och snabb att använda. Metoden lämpar sig dessutom väl även för användning i mer utmanande klimat som extrem kyla, vilket många andra metoder inte klarar av.

Metoden beskrivs ha hög användaracceptans och i en undersökning 1991 föredrog många individer den framför andra biometriska metoder. Handgeometriska system är dock inte särskilt hygieniska då de kräver att alla användare berör samma kontaktyta.

[17] Hela avsnittet, utom en detalj från en annan källa, är extraherat från denna referens. För läsbarhetens skull nämns referensen därför inte igen.

[18] En skanner för att läsa av handgeometri kostar cirka 9 000–18 000 kronor (Štruc och Pavešić, 2015; Bayometric, 2018).

6.8 DNA-igenkänning

Igenkänning baserat på DNA har ett stort användningsområde i form av DNA-profilering, där exempelvis brottsmisstänkta individers DNA jämförs med bevis-DNA som hittats på en brottsplats. DNA-profilering har använts sedan 1986 men var från början inte automatiserad (Saad 2005).

Även om nästan allt DNA är identiskt för olika människor, räcker en liten återkommande skillnad för att unikt särskilja alla individer (Saad, 2005). För att inhämta DNA från en individ används vanligen blodprov, buckalsvabbning (svabbning av kindens insida) eller salivprov (Rethmeyer m.fl., 2013). Sannolikheten för fel vid DNA-igenkänning varierar, men är typiskt extremt låg, i storleksordningen 1 på 1000 miljarder (Butler, 2015).

DNA-profilering kunde tidigare ta veckor eller månader, men kan numera gå på mindre än en timme (Butler 2015).

7 Jämförelse mellan metoderna

Detta avsnitt jämför de biometriska metoderna utifrån deras beskrivningar i kapitel 6. Detta kompletteras med en analys av hur lik utvärderingen är jämfört med några andra liknande utvärderingar som gjorts av andra forskare.

Jämförelsen i det här kapitlet är inte fullständig, vilket har flera skäl. Dels är denna typ av bedömningar svåra att göra, dels skiljer det mycket i hur metoder beskrivits och utvärderats i litteraturen. Både metoder samt olika produkter och algoritmer som nyttjar olika metoder, utvärderas på olika sätt i litteraturen. Exempelvis används olika kriterier och det varierar vilken miljö och med vilka individer utvärderingarna sker. Det är därför svårt att konkret och korrekt utvärdera hur bra en metod är och jämförelsen ska tolkas med försiktighet.

Tabell 2 visar resultatet av jämförelsen. I vissa fall (celler i tabellen) finns inte bra data att tillgå och inte heller har någon bedömning kunnat göras. Då har bedömningen istället hämtats från Jain m.fl. (2004) som utgör en liknande utvärdering.

Tabell 2: Jämförelse av de biometriska metoderna. Skalan är Låg, Medel, Hög, där Hög betyder högst kravuppfyllnad.

Metod	**Univ.**	**Unik.**	**Oför.**	**Insaml.**	**Träff.**	**Prest.**	**Anv. -acc.**	**Resist.**
Finger	(M)	H	(H)	M	H	H	(M)	M
Iris	(H)	H	H	M	H	H	(L)	M
Ansikte	(H)	(L)	(M)	H	M	***H***	H	***L***
Öra	(M)	M	M	M	M	(M)	(H)	(M)
Blodåder	(M)	H	M	M	H	(M)	M	***H***
Röst	(M)	M	(L)	H	L	(L)	(H)	M
Hand	(M)	L	L	M	M	H	M	(M)
DNA	(H)	H	(H)	M	H	***L***	(L)	(L)

Metoderna har förkortats enligt vilket kännetecken de baseras på (för Finger- och handgeometriigenkänning står det för att spara plats enbart Hand). Bedömningarna är gjorda utifrån kraven: Univ. = Universalitet; Unik. = Unikhet; Oför. = Oföränderlighet; Insaml. = Insamlingsförmåga; Träff. = träffsäkerheten i form av att det inte ges falska positiva och falska negativa.; Prest. = Systemprestanda; Anv.acc. = Användarnas acceptans av användningen av kännetecknet; Resist. = Resistens mot antagonisters möjligheter att kringgå systemet. Kursiverade bedömningar avviker mycket mot bedömningar i andra utvärderingar. Bedömning i parentes är gjord av Jain m.fl. (2004).

De två metoder som i störst utsträckning uppfyller kraven är fingeravtrycksigenkänning och irisigenkänning. Blodådersigenkänning är nästan lika bra. De två metoder som i minst utsträckning uppfyller kraven är röstigenkänning samt finger- och handgeometriigenkänning.

De jämförelser som baseras på resultaten i kapitel 6 skiljer sig en del från andra liknande utvärderingar: Jain m.fl. (2004)[19], Oloyede och Hancke (2016) samt Dahia m.fl. (2020). De större skillnaderna, när det skiljer mer än ett steg mellan bedömningarna i denna rapport mot källorna, är värda att nämnas. Fyra sådana fall finns (markerade med fetstil och kursivering i tabellen):

- Systemprestandan för ansiktsigenkänning bedömdes som Hög här, men som Låg i Jain m.fl. (2004) och i Dahia m.fl. (2020). Anledningen till att bedömningen blev Hög här är att igenkänningen fungerade bra även när individerna använde ansiktsmasker (som skydd mot Covid-19). Detta är förmodligen inget som de två andra utvärderingarna beaktat.
- Systemprestandan för DNA bedömdes som Låg här, men som Hög i Jain m.fl. (2004). Anledningen till att bedömningen blev Låg här beror på att det tar åtminstone någon timme att få resultat från DNA-igenkänning. Varför Jain m.fl. (2004) gjorde en helt annan bedömning är oklart.
- Angreppsmotståndskraften för ansiktsigenkänning bedömdes som Låg här, men som Hög i Jain m.fl. (2004). Anledningen till att bedömningen blev Låg här beror på att det är lätt för angripare att observera individers ansikten och därmed skapa sig en grund för att imitera. Varför Jain m.fl. (2004) gjorde en helt annan bedömning är oklart.
- Angreppsmotståndskraften för blodådersigenkänning bedömdes som Hög här, men som Låg i Jain m.fl. (2004). Anledningen till att bedömningen blev Hög här beror på att det är svårt för angripare att observera blodådrorna och därmed skapa sig en grund för att imitera. Varför Jain m.fl. (2004) gjorde en helt annan bedömning är oklart.

[19] Jain m.fl. (2004) bedömde utifrån samma krav, men utan att bedöma de falska positiva och falska negativa. De två andra utvärderingarna bedömde med något annan terminologi, varför viss tolkning varit nödvändig för att jämföra dem med de resultat som fåtts här.

8 Användningsfall och biometriska metoder

Detta kapitel utgår från användningsfallen i kapitel 5 samt de biometriska metoderna som beskrivits och jämförts i kapitel 6 och 7. För varje användningsfall beskrivs vilka av de biometriska metoderna som kan vara lämpliga att använda.

8.1 Kartläggning av avlägset förråd

Vid kartläggningen kommer antagonisten i huvudsak hålla sig på avstånd från förrådet och kanske rentav maskera sig. Samtidigt är det förmodligen sällan tal om att antagonisten gör rejäla försök att dölja sin närvaro.

Lämpliga metoder

Ansiktsigenkänning fungerar bra på distans och har visat sig kunna känna igen individer ganska väl trots maskering.

Öronigenkänning är en metod som till viss del kan fungera bättre eftersom antagonisten nog inte är lika van vid att behöva maskera sina öron.

Röstigenkänning kan fungera om antagonisten kommunicerar med någon via tal (ex. för att få detaljerade instruktioner om vilken del av objektet att fokusera på). Förmodligen finns inga källor till buller i närheten som skulle kunna störa röstigenkänningen.

Irisigenkänning kan fungera på ganska långt avstånd och det är sannolikt att antagonisten inte maskerat sina ögon. Å andra sidan kan kameror och kikare vara i vägen.

DNA-igenkännning skulle möjligen kunna fungera i efterhand som forensisk metod, vilket kan ingå i en bred tolkning av teknisk bevakning eftersom antagonister ibland behövas ställas inför rätta. Men om spår enbart lämnats utomhus är det tveksamt om det finns tillräckligt kvarlämnat i efterhand för att igenkänning skulle vara möjlig.

8.2 Stöld ur avlägset förråd

Stölden kräver att antagonisten är i och vid förrådet. Förmodligen kommer antagonisten enbart kunna gissa om vad förrådet innehåller. Användningsfallet utgår också från att antagonisten inte kommer att maskera sig.

Lämpliga metoder

Samman metoder som används för att bekämpa kartläggning (8.1) kan även användas här. Ett förbehåll är dock att antagonisten här rör sig snabbare (snarare än rör sig långsamt eller är stilla), vilket gör att metoderna har svårare att känna igen antagonisten. Å andra sidan finns bättre möjligheter till igenkänning när antagonisten är närmare förrådet och tar på olika objekt. Någon form av f*ingeravtrycksigenkänning* kan därför vara lämpligt.

8.3 Förstörelse av avlägsen radiomast

Förstörelsen handlar om att hindra Försvarsmaktens förmåga men också om att skapa uppmärksamhet kring Försvarsmaktens roll i samhället. Antagonisten har därför inget intresse av att dölja sin närvaro utan snarare vill bli uppmärksammad. Antagonisten maskerar sig därför inte och dröjer troligen kvar vid platsen.

Lämpliga metoder

Samma metoder som används för att bekämpa kartläggning (8.1) kan även användas här. Ett förbehåll är dock att antagonisten här rör sig snabbare (snarare än rör sig långsamt eller är stilla), vilket gör att metoderna har svårare att känna igen antagonisten. Å andra sidan finns bättre möjligheter till igenkänning när antagonisten är närmare radiomasten. Men om radiomasten förstörs kommer kommunikationsmöjligheterna minska vilket gör att de biometriska metoderna helst bör ge ett resultat före det.

8.4 Kartläggning av kontorsbyggnad i tätort

Kartläggningen sker i huvudsak öppet och till del är den utan någon avsikt att skada. Därför sker inga maskeringsförsök. Buller och andra störande signaler försvårar dock igenkänning.

Lämpliga metoder

Ansiktsigenkänning fungerar bra på distans och har visat sig kunna känna igen individer ganska väl trots maskering.

Öronigenkänning är en metod som till viss del kan fungera bättre eftersom antagonisten nog inte är lika van vid att behöva maskera sina öron.

Irisigenkänning kan fungera på ganska långt avstånd och det är sannolikt att antagonisten inte maskerat sina ögon. Å andra sidan kan kameror vara i vägen.

8.5 Obehörig inpassering till mindre förläggning i glesbygd

Antagonisten kan utnyttja inpasseringen för att ta sig in i förläggningen och stjäla, sabotera eller bruka våld. Antagonisten kan ha tagit över legitimt fordon och utger sig för att vara en del av personalen. Legitim personal stödjer gärna säkerhetsåtgärderna för inpassering men kan av säkerhetsskäl inte helt stanna upp med sina fordon eller ta av sig sin mundering. Snabbhet samt motståndskraft mot buller och maskering är därför viktig hos de biometriska metoderna.

Lämpliga metoder

Ansiktsigenkänning fungerar bra på distans och har visat sig kunna känna igen individer ganska väl trots maskering. Maskeringen som testats har dock inte inkluderat att ögonen täcks vilket kan vara fallet vid inpassering som sker i mörker (pga. glasögon för mörkerseende).

Öronigenkänning är en metod som till viss del kan fungera bättre eftersom skyddsmasker, mörkersikt och liknande inte alltid täcker öronen.

8.6 Stöld och sabotage i serverrum i kontorsbyggnad i tätort

Inpasseringen till serverrummet sker inne i en kontorsbyggnad vilket betyder att det är inomhus. Det gör också att vakter kan vara på plats väldigt snabbt. Samtidigt kan kort tid räcka för att åstadkomma stor skada med tanke på de stora möjligheter som finns i ett serverrum.

Lämpliga metoder

Alla metoder som inte tar alltför lång tid kan fungera vid denna inpassering, dvs. alla utom DNA-igenkänning. Röstigenkänning exkluderas dock också eftersom det är mindre önskvärt att den som passerar i närheten kan snappa upp delar av proceduren för inpassering.

8.7 Stöld och sabotage i kontorsbyggnad i tätort

Inpassering till kontorsbyggnaden sker tämligen öppet och i närheten av vakter. Antagonister som försöker ta sig in tar ganska stora risker. Vid generell inpassering krävs snabbhet för att personalstyrkan och besökare ska kunna komma in, vilket ställer krav på snabbheten för stödjande biometriska metoder.

Lämpliga metoder

Fingeravtrycksigenkänning fungerar generellt bra för inpassering, men kräver att individerna tar av sig handskar på vintern, vilket gör processen långsammare.

Ansiktsigenkänning fungerar också generellt bra för inpassering, men ställer krav på individens fokus, snarare än att individen kanske samtidigt som inpasseringen skriver på mejl på sin telefon eller pratar i telefonen och har svårare att fokusera blicken.

Finger- och handgeometriigenkänning kan fungera med liknande restriktioner som fingeravtrycksigenkänning.

9 Diskussion

Användningen av biometriska metoder har ökat kraftigt det senaste decenniet. Delvis kan detta förklaras av att de underliggande algoritmerna förbättrats i takt med framsteg inom forskningsfältet artificiell intelligens. Rapportens fokus har varit att ta reda vilka biometriska metoder som kan vara användbara för teknisk bevakning inom Försvarsmakten. Arbetet har utgått från en litteraturstudie och generella användningsfall för biometriska system i Försvarsmakten.

De två biometriska metoder som uppvisat störst grundläggande kravuppfyllnad är *irisigenkänning* och *fingeravtrycksigenkänning*. Irisigenkänningen passar också väl in i användningsfallen, medan fingeravtrycksigenkänningen passar in något sämre. Blodådersigenkänning hade nästan lika hög kravuppfyllnad, men passar nästan inte alls in i användningsfallen. Två metoder med medelgod kravuppfyllnad (*ansiktsigenkänning* samt *öronigenkänning*) passar bäst in i användningsfallen.

Det finns dock begränsningar med den typ av utvärderingar som gjorts i rapporten. Sådana begränsningar beskrivs närmare i nästa avsnitt (9.1). Därefter kommer ett avsnitt (9.2) som beskriver vilka ytterligare utvärderingar som Försvarsmakten behöver se till utförs. Kapitlet avslutas med ett avsnitt (9.3) om framtida utmaningar med användningen av biometriska metoder.

9.1 Utvärderingarnas begränsning

Utvärderingar av biometriska metoder sker oftast i labbmiljö eller i form av teoretiska resonemang. I utvärderingarna görs typiskt bedömningar av olika kvalitetsparametrars värden, vilket även är fallet i denna rapports utvärderingar. Sådana utvärderingar måste tolkas med försiktighet. Detta beror på flera saker:

- Utvärderingarna skiljer sig åt metodmässigt och tar var och en bara upp en delmängd av alla kvalitetsparametrar.
- Utvärderingarna inkluderar sällan bedömningar av hur miljömässiga faktorer påverkar, ex. störningar av väder eller falsklarm av djur.
- Utvärderingarna ignorerar ofta problematiken kring etik, eller nämner bara sådana aspekter i förbifarten. Exempelvis undersöks fel i medeltal utan att beakta att systematiska fel för grupper av individer (ex. minoriteter) kan ge stora konsekvenser för individerna.
- Utvärderingarna görs sällan utifrån vad realistiska angripare skulle kunna uppnå i angrepp mot systemen, såsom imitation av legitima individer. Skydd mot angrepp har med dagens teknik visat sig i vissa fall försvåra igenkänning av legitima individer med mer än tio gånger. Det är möjligt att mindre försämringar skulle uppnås om säkerheten infördes från början snarare än klistrades på i efterhand.

- Utvärderingarna görs ofta på generella grunder snarare än med specifika användningsfall och när det är mer specifikt så avviker det samtidigt från de situationer Försvarsmakten agerar i. Det är därför troligt att Försvarsmakten inte kan använda biometriska system i deras grundutförande varför det krävs att systemen anpassas, vilket kan vara svårt att få till.

9.2 Kompletterande utvärderingar som behövs

Rapportens teoretiska resonemang och urval av andvändningsfall behöver kompletteras med olika praktiska utvärderingar. Sådana utvärderingar kommer Försvarsmakten behöva göra själva i sina egna miljöer och komplettera med bedömningar av hur mycket säkerhet som ges per krona. Det behöver också utvärderas vilka negativa effekter det kan få på säkerheten att införa biometriska system. Exempelvis har Försvarsmakten ibland behov av att dölja sig genom mörkläggning, eftersom hot (såsom flyganfall) kan rikta in sig på ljuskällor. Då är det olämpligt att använda en biometrisk metod vars sensor kräver rikligt med synligt ljust. En annan risk är att ett övertaget övervakningssystem används av motståndaren för att inhämta information om Försvarsmakten.

Samtidigt måste problemen med utvärdering av biometriska metoder ställas mot alternativen. Sådana alternativ har inte studerats i denna rapport, men framtida forskning skulle kunna besvara följande:

- Hur väl utvärderade är dagens bevakningssystem?
- Är de icke-biometriska system som används idag verkligen bättre, eller är deras brister bara inte lika enkla att beskriva?

9.3 Framtida utmaningar

Det senaste året har mer fokus hamnat på hur biometriska system ska kunna användas utan att ge alltför stora negativa konsekvenser för de individer som ska kännas igen. Bland annat har tolkningen av hur personuppgifter får användas i EU blivit mer begränsande vad gäller överförandet av personuppgifter till länder utanför EU. Sådana begränsningar kan påverka vilka produkter och tjänster som är lämpliga att använda. Som framgår av kapitel 3 har domstolar flera gånger bedömt övervakning med biometriska metoder som olaglig. Flera stora tillverkare har dessutom uttryckt oro för att deras produkter och tjänster ska användas för ändamål som kränker mänskliga rättigheter, exempelvis i form av diskriminering av etniska minoriteter. Tillverkarna har därför blivit försiktigare i sin försäljning till bland annat polisiära myndigheter. Det kan tänkas att Försvarsmakten som säkerhetsmyndighet kommer omfattas av liknande begränsningar. Det är också tänkbart att det i framtiden kommer mer

begränsningar i hur centraliserade databaser får användas för att samla in biometriska data.

Precis som att lösenordslistor kan läcka ut, kan biometriska systems registrerade kunskap om individer läcka ut. Samtidigt kan lösenord enkelt bytas, medan biometriska kännetecken är betydligt mer permanenta. Systemen behöver därför lagra specifika krypterade variationer av kunskapen om kännetecknen, varpå ett byte till en annan variation kan göras om läckage skulle ske. Att etablera sådana variationer är dock en utmaning i biometriska system, eftersom krypteringen gör systemet känsligare för miljömässig påverkan. Den forskning inom biometrifältet som fokuserar på skydd mot angrepp handlar till stor del om att hitta bättre krypterade variationer som kan användas av systemen för att lagra deras kunskap om biometriska kännetecken.

Referenser

Al Shehri, H., Hussain, M., Abo Al Samh, H., Al Zuair, M. 2018. A large-scale study of fingerprint matching systems for sensor interoperability problem. Sensors, vol. 18:4.

Amazon. 2020. We are implementing a one-year moratorium on police use of Rekognition. https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

Anderson, R. 2020. Security Engineering. A guide to building dependable distributed systems. Tredje upplagan. Chapter 17. Biometrics. *Wiley*.

Arakawa, T., Koshinaka, T., Yano, S., Irisawa, H., Miyahara, R., Imaoka, H. 2016. Fast and accurate personal authentication using ear acoustics. *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference*.

Aslam, T. M., Tan, S. Z., Dhillon, B. 2009. Iris recognition in the presence of ocular disease. *Journal of The Royal Society Interface*, vol. 6:34.

Bayometric. 2018. Hand Geometry Recognition Biometrics: All You Need To Know. https://www.bayometric.com/hand-geometry-recognition-biometrics/

Brey, P. 2004. Ethical aspects of facial recognition systems in public places. *Journal of Information, Communication and Ethics in Society*, vol. 2:2.

Burge, M., Burger, W. 2006. *Ear Biometrics*.

Butler, J. M. 2015. The future of forensic DNA analysis. *Philosophical transactions of the royal society B: biological sciences*, vol. 370:1674.

Czajka, A. 2016. Iris liveness detection by modelling dynamic pupil features. I *Handbook of Iris Recognition*. Springer.

Czajka, A. Bowyer, K. W. 2018. Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art. *ACM Computing Surveys*, vol. 51:4.

Dahia, G., Jesus, L., Pamplona Segundo, M. 2020. Continuous authentication using biometrics: An advanced review. *Data Mining and Knowledge Discovery*, vol. 10:4.

Datainspektionen. 2019. Sanktionsavgift för ansiktsigenkänning i skola. https://www.datainspektionen.se/nyheter/2019/sanktionsavgift-for-ansiktsigenkanning-i-skola/

Datainspektionen. 2020a. Dataskyddsförordningen (GDPR). Är det tillåtet att skicka känsliga personuppgifter med vanlig post eller måste vi skicka rekommenderat?. https://www.datainspektionen.se/fragor-och-svar/gdpr/

Datainspektionen. 2020b. Så här påverkar Schrems II-domen överföringar till tredje land. https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/sa-har-paverkar-schrems-ii-domen-overforingar-till-tredje-land/

Dataskyddsförordningen. 2016. Europaparlamentets och rådets förordning (EU) 2016/679.

Daugman, J., Downing, C. 2001. Epigenetic randomness, complexity and singularity of human iris patterns. *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 268:1477.

Daugman, J. (2009). How iris recognition works. In *The essential guide to image processing* (pp. 715-739). Academic Press.

Försvarsmakten. 2015. *Handbok säkerhetstjänst fysisk säkerhet 2015*. M2015-15165.1.

Försvarsmakten. u.å. (arbetsutgåva, 31 augusti 2020). SYMM TBG 3.0.

Grosz, S. A., Engelsma, J. J., Jain, A. K. 2020. White-Box Evaluation of Fingerprint Recognition Systems. *arXiv*.

Haskins, C. 2019. Oakland Becomes Third U.S. City to Ban Facial Recognition. Vice. https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz

Hern, A. 2019. Microsoft boss: tech firms must stop 'if it's legal, it's acceptable' approach. *The Guardian*.

IBM. 2020. IBM CEO’s Letter to Congress on Racial Justice Reform. https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

ISO/IEC. 2006. International Standard. Information technology — Biometric performance testing and reporting Part 1: Principles and framework. ISO/IEC 19795-1.

ISO/IEC. 2017. Information technology — Vocabulary — Part 37: Biometrics. ISO/IEC 2382-37.

Jain, A. K., Dass, S. C., Nandakumar, K. 2004a. Soft Biometric Traits for Personal Recognition Systems. *Proceedings of International Conference on Biometric Authentication.*

Jain, A. K., Ross, A., Prabhakar, S. 2004b. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14:1.

Jain, A. K., Nandakumar, K., Nagar, A. 2008. Biometric Template Security. *Journal on Advances in Signal Processing*.

Kalvet, T., Karlzén, H., Hunstad, A., Tiits, M. 2018. Live Enrolment for Identity Documents in Europe. I: Parycek, P. m.fl. (red.) Electronic Government. EGOV 2018. *Lecture Notes in Computer Science*, vol. 11020. Springer.

Karlzén, H., Gudmundson Hunstad, A., Hyllienmark, E., Rodhe, I. 2020. Beteendebaserad biometrisk autentisering. FOI-D--0991--SE. Totalförsvarets forskningsinstitut.

Levalle, Y. 2020. Bypassing biometric systems with 3D printing and 'enhanced' grease attacks. Dreamlab Technologies. https://dreamlab.net/media/img/news/WP_Biometrics_v5.pdf

Luotsinen, L., Oskarsson, D., Svenmarck, P., Wickenberg Bolin, U. 2019. Explainable Artificial Intelligence: Exploring XAI Techniques in Military Deep Learning Applications. FOI-R--4849--SE. Totalförsvarets forskningsinstitut.

Mahto, S., Arakawa, T., Koshinak, T. 2018. Ear acoustic biometrics using inaudible signals and its application to continuous user authentication. *26th European Signal Processing Conference (EUSIPCO)*.

Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. 2009. *Handbook of fingerprint recognition*. Springer Science & Business Media.

Maro, E., Kovalchuk, M. 2018. Bypass Biometric Lock Systems With Gelatin Artificial Fingerprint. *Proceedings of the 11th International Conference on Security of Information and Networks*.

Matey, J. M., Naroditsky, O., Hanna, K., Kolczynski, R., LoIacono, D. J., Mangru, S., Tinker, M., Zappia, T. M., Zhao, W. Y. 2006. Iris on the Move: Acquisition of Images for Iris recognition in Less Constrained Environments. Proc IEEE vol. 94:11.

Mokroß, B. A., Drozdowski, P., Rathgeb, C. Busch, C. 2020. Efficient identification in large-scale vein recognition systems using spectral minutiae representations. I Uhl, A., Busch, C., Marcel, S., Veldhuis, R. (red.) *Handbook of Vascular Biometrics*. Springer.

Moses, K. R., Higgins, P., McCabe, M., Prabhakar, S., Swann, S. 2011. Automated fingerprint identification system (AFIS). *Scientific Working Group on Friction Ridge Analysis Study and Technology and National institute of Justice*.

Mozur, P. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. 2019. *New York Times*. April. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

NIST. National Institute of Standards and Technology. 2004. NISTIR 7123 Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. 2004, juni.

NIST. National Institute of Standards and Technology. 2014. NISTIR 8034 Fingerprint Vendor Technology Evaluation. December.

NIST. National Institute of Standards and Technology. 2018. NISTIR 8207 IREX IX Part One: Performance of Iris Recognition Algorithms. April.

NIST. National Institute of Standards and Technology. 2019a. NISTIR 8280 Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects. December.

NIST. National Institute of Standards and Technology. 2019b. NISTIR Draft Face Recognition Vendor Test (FRVT). Part 1: Verification. April.

NIST. National Institute of Standards and Technology. 2019c. NISTIR 8252 IREX IX Part Two Multispectral Iris Recognition. Juni.

NIST. National Institute of Standards and Technology. 2019d. NISTIR 8271 Face Recognition Vendor Test (FRVT). Part 2: Identification. September.

NIST. National Institute of Standards and Technology. 2020a. NISTIR 8307 Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture. Maj.

NIST. National Institute of Standards and Technology. 2020b. NISTIR 8271 Draft Supplement Face Recognition Vendor Test (FRVT). Part 2: Identification. Februari.

NIST. National Institute of Standards and Technology. 2020c. NISTIR 8311 Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms. Juli.

NIST. National Institute of Standards and Technology. 2020d. NISTIR 8331 Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms. Novmeber.

Oloyede, M. O., Hancke, G. P. 2016. Unimodal and Multimodal Biometric Sensing Systems: A Review. *IEEE*, vol. 4.

Paderes, R. E. O. 2015. A comparative review of biometric security systems. *International Conference on Bio-Science and Bio-Technology*.

Parthasaradhi, S. T. V., Derakhshani, R., Hornak, L. A., Schuckers, S. A. C. 2005. Time-series detection of perspiration as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man and Cybernetics Part C*, vol. 35:3.

Patel, V. M., Ratha, N. K., Chellappa, R. 2015. Cancelable Biometrics: A Review. *IEEE Signal Processing Magazine*, vol. 32:5.

Pflug, A., Busch, C. 2012. Ear biometrics: a survey of detection, feature extraction and recognition methods. *IET biometrics*, vol. 1:2.

Phillips, P. J., Yates, A. N. Hu, Y., Hahn, C. A., Noyes, E., Jackson, K., Cavazos, J. G., Jeckeln, G., Ranjan, R., Sankaranarayanan, S., Chen, J. C., Castillo, C. D., Chellappa, R., White, D., O'Toole, A. J. 2018. Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. *PNAS*, vol. 115:24.

Ratha, N., Bolle, R. (red.) 2003. *Automatic fingerprint recognition systems*. Springer Science & Business Media.

Rees, J. 2020. Facial recognition use by South Wales Police ruled unlawful. *BBC*. https://www.bbc.com/news/uk-wales-53734716

Rethmeyer, J. A., Tan, X., Manzardo, A., Schroeder, S. R., Butler, M. G. 2013. Comparison of biological specimens and DNA collection methods for PCR amplification and microarray analysis. *Clinical Chemistry and Laboratory Medicine (CCLM)*, vol. 51:5.

Saad, R. 2005. Discovery, development, and current applications of DNA identity testing. *Baylor University Medical Center Proceedings*, vol. 18:2.

Seetharaman, K., Ragupathy, R. 2012. Iris recognition based image authentication. *International journal of computer applications*, vol. 44:7.

SFS 2018:1200. Kamerabevakningslag. Regeringskansliet. http://rkrattsbaser.gov.se/sfst?bet=2018:1200

Shinzaki, T. 2020. Use case of palm vein authentication. I Uhl, A., Busch, C., Marcel, S., Veldhuis, R. (red.) *Handbook of Vascular Biometrics*. Springer.

Sriskandaraja, K., Sethu, V., Ambikairajah, E. 2018. Deep Siamese Architecture Based Replay Detection for Secure Voice Biometric. *Interspeech*.

Stewart, R. F., Estevao, M., Adler, A. 2009. Fingerprint recognition performance in rugged outdoors and cold weather conditions. *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*.

Štruc, V., Pavešić, N. 2015. Hand-geometry device. I Li, S. Z., Jain, A. K. (red.) *Encyclopedia of Biometrics*. Second edition. Springer.

Stupp, C. 2019. Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case. *The Wall Street Journal*. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Svenmarck, P., Luotsinen, L., Nilsson, M., Schubert, J. 2018. Possibilities and Challenges for Artificial Intelligence in Military Applications. *NATO Big Data*

and Artificial Intelligence for Military Decision Making Specialists' Meeting. STO-MP-IST-160. FOI-S--5864--SE.

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern recognition, 47*(8), 2673-2688.

Vaughan, A. 2019. UK launched passport photo checker it knew would fail with dark skin. *New Scientist*. https://www.newscientist.com/article/2219284-uk-launched-passport-photo-checker-it-knew-would-fail-with-dark-skin

Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F., Li, H. 2015. Spoofing and countermeasures for speaker verification: A survey. *Speech communication*, vol. 66.

Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C. 2019. Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry*, vol. 11:141.

Yüksel, A., Akarun, L., Sankur, B. 2010. Biometric identification through hand vein patterns. *International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics*.

Zhou, S., Xiao, S. 2018. 3D face recognition: a survey. *Human-centric Computing and Information Sciences*, vol. 8:1.

FOI

ISSN 1650-1942

www.foi.se