Handelshögskolan
VID GÖTEBORGS UNIVERSITET
Institutionen för informatik
2003-06-09

Digital autenticering - en del av e-demokrati

Abstrakt

Dagens samhälle går allt mer mot att vara ett informationssamhälle. Inga viktiga beslut sker idag utan att man först införskaffat tillräckligt med information; den har blivit en hårdvaluta och kritisk resurs. För att våga lita på informationen måste man veta att källan är pålitlig och att informationen är oförvanskad. Ett ökande medium för informationsspridning idag är olika former av digitala dokument. Digitaliseringen av samhället har dock lett till många nya sätt att manipulera informationen i dessa. Syftet med denna uppsats var att utreda vilka tekniker som finns för att autenticera digitala dokument. Frågan vi ställde oss var ”Hur kan man fastställa att ett digitalt dokument är ett original?” För att undersöka detta genomförde vi två skilda litteraturstudier; en inom området e-demokrati, vilken bidrog till en ökad förståelse för problemområdet och en teknisk studie. Den tekniska studien visade på tre tekniker; digitala signaturer, steganografi och digital vattenmärkning, vilka samtliga lämpar sig väl för fastställande av dokumentens autencitet. Vi fann dock att det inte finns någon optimal lösning på problemet, då samtliga lösningar har svagheter. Ytterligare utveckling inom området kommer att krävas.

Nyckelord: e-demokrati, digitala dokument, autenticering, digitala signaturer, steganografi, digital vattenmärkning

Författare: Cecilia Axelsson, Johan Fihn och Christoffer Rosenqvist
Handledare: Urban Nuldén
Magisteruppsats, 20 poäng

1 Inledning

Vårt samhälle har blivit ett informationssamhälle där information ses som en vara bland andra varor (SOU, 1999:12). Inga viktiga beslut fattas idag utan att man först skaffat all väsentlig information; den har blivit hårdvaluta och kritisk resurs. För att våga lita på den information som erhålles måste man veta att källan är pålitlig och att informationen är oförvanskad (Lindkvist, 2001b).

Det främsta mediet för informationsspridning idag är olika former av dokument. Vi sätter stor tilltro till dokument och förlitar oss på att det som står i dessa dokument är sant. De har blivit artefakter som vi kan samlas runt och enas om. Alla stora beslut förseglas i olika typer av dokument, protokoll och liknande, som sedan skall bevittnas av flera personer. Personer sätter sin namnteckning på pappret för att visa att de godkänt dokumentets innehåll och för att andra ska kunna lita på detta. Dokument är ofta det som bevisar vår legitimitet i olika frågor. Idag använder vi körkort för att visa att vi får köra bil och passerkort för att få vara på olika platser. Betyg visar din kompetens och diplom bevisar att du gått kurser. Allt detta hamnar på olika papper, som man sedan visar upp. Det finns en allmän uppfattning om att det som finns på papper är sant.

I och med att vårt samhälle allt mer förlitar sig på digital teknik för kommunikation blir även informationen i större utsträckning digitaliserad. Det skapas digitala dokument som kan utbytas över datornätverk. I många fall finns det inga förlagor till dessa digitala dokument vilket ställer oss inför många nya problem. När den analoga förlagan försvinner finns det inte längre något sätt att verifiera att informationen i dokumentet överensstämmer med det material som avsändaren inledningsvis avsåg. Ett digitalt dokument som manipuleras kan i alla avseenden vara likadant som sin förlaga förutom just det faktum att informationen det förmedlar inte är den samma. Detta gör att det kan vara omöjligt att skilja originalet från förvanskningen.

Digitalisering leder till många nya sätt att manipulera informationen i ett dokument. Ett signerat och bevittnat dokument på papper är svårt att ändra informationen i utan att pappret eller bläcket på något sätt uppvisar åverkan av förändringen. Likadant är ett gammaldags foto resultatet av en kemisk process och därmed svårt att förändra. Den digitala motsvarigheten uppvisar dock ingen åverkan när man förändrar dess innehåll. Idag är det nästan en omöjlighet att avslöja en förfalskning som är gjord av en kompetent person (Alling-Ode & Tubin, 1993).

Digitala dokument har blivit allt mer vanliga i takt med att den politiska processen flyttar ut på Internet. Det finns en stor förhoppning på informationsteknologin (IT), att den skall hjälpa till att förbättra den politiska kommunikationen mellan medborgare, politiker och myndigheter (Westholm, 2002). I och med ny teknik, såsom snabbare datorer och Internet, möjliggörs nya former av informationsutbyte och interaktion. Ett sådant exempel är e-demokrati[1]; en form av elektroniskt samarbete där myndigheter och medborgare har ett utbyte via IT. Att öka myndigheternas IT-användning stärker infrastrukturen och bidrar till teknisk utveckling, vilket i sin tur leder till att konkurrenskraften som IT-land ökar (Statskontoret 2000:21). Tanken med e-demokrati är att engagera medborgarna i beslutsprocessen och att ge mer insyn i myndigheternas arbete. En annan aspekt av e-demokrati är att den förväntas minska pappersmängden hos myndigheterna och även lätta på deras arbetsbörda på så sätt att man lägger ut delar av arbetet på medborgarna. Exempelvis kan en tillståndssökande fylla i de nödvändiga blanketterna online och därmed förbigå de första stegen i ansökningsprocessen. Ett annat exempel är inkomstdeklaration på nätet. När medborgarna kan deklarera på nätet minskar den mängd papper som måste skickas in. Även det manuella arbete som krävs för att överföra dessa deklarationsblanketter till databaser minskar.

[1] Med e-demokrati avser vi det IT-stödda samarbetet mellan myndigheter och medborgare, men även användandet av IT inom förvaltningar. I begreppet innefattar vi även medborgarndeltagandet i den demokratiska beslutsprocessen som kommer av detta samarbete i kombination med det ökande användandet av IT i samhället.

En tredje aspekt är att förenkla hanterandet av olika myndighetstjänster, där medborgarna ska kunna anmäla enklare brott eller rapportera sjukdom över Internet. Sådana tjänster gör det lättare både för myndigheter som privatpersoner, samtidigt som det underlättar hanteringen av ärendena. Man blir sin egen handläggare och kontrollant över sitt ärende och ansvaret ligger i ens egna händer.

I och med att medborgarna förväntas deklarera inkomst, anmäla brott och rapportera sjukdom med hjälp av Internet, blir förtroendet för myndigheternas tjänster en förutsättning för att medborgarna ska använda dem. När känslig information utbyts över nätet måste sändaren kunna lita på att information både hanteras konfidentiellt och att den inte förändras efter överföring. Detta förtroende måste vara ömsesidigt. Även myndigheterna måste kunna lita på medborgarna för att e-tjänsterna ska bli användbara.

Ett digitalt samhälle är på många sätt ett effektivt samhälle, men det blir också lätt opersonligt. I en e-demokrati behöver man ofta inte möta någon ansikte mot ansikte när man gör sin sjuk- eller stöldanmälan, vilket gör det lättare att bete sig på ett otillbörligt sätt. I och med Internets utbredning har antalet förfalskningar och bedrägerier ökat (IFCC, 2003), dels på grund av lättheten att förfalska och dels på grund av en viss avståndskänsla mellan bedragaren och den drabbade. När den personliga kontakten försvinner, försvinner även en del av känslan att det man gör är fel, samtidigt som det inger en falsk känsla av säkerhet att sitta på avstånd via Internet.

För att behålla de digitala dokumentens pålitlighet måste man utveckla och använda teknologier för att säkerställa att informationen är oförändrad och på så sätt skapa möjligheter att verifiera informationen i dokumenten. Det finns idag många sätt att hindra olaglig kopiering och distribuering av digitala dokument. Detta gäller framförallt lösningar för att spåra den ursprungliga ägaren till ett dokument som spridits illegalt. Lösningar för att förhindra modifiering eller för att spåra sådan är däremot mer ovanliga (Lindkvist, 2001b).

Vår uppsats syftar till att redogöra för möjliga lösningar för att verifiera innehåll i digitala dokument. Vi kommer att titta på olika tekniska lösningar och därefter utvärdera dessa efter en rad kriterier vi ställt upp. Man skulle kunna se vår uppsats som en sammanställning av en mängd tekniker, som avslutas med en diskussion om hur dessa skulle kunna användas i en e-demokrati.

1.1 Problem

Problemet idag är att det inte går att se om ett digitalt dokument är förfalskat eller ej. Förfalskade dokument kan leda till många felaktiga beslut beroende på inom vilket område man befinner sig. Ibland märker man dem eller så går de omärkt förbi. På senare tid har det uppkommit flera diskussioner vad gäller bevisning i bild/ljud eller video. Kravallerna i Göteborg sommaren 2001 är något som kommit på tal en hel del under de senaste åren. Diskussionen har handlat mycket om huruvida de videoband vilka använts som utredningsmaterial har manipulerats eller ej. Det finns flera olika versioner av samma händelse men med olika ljud. Det är uppenbart att någon eller några har ändrat på ljudsekvenserna. Frågan är då bara vilket av banden som är originalet. Ytterligare exempel där diskussionen kommit upp är de bilder och ljudupptagningar som USA tagit fram i sitt krig mot Irak. Är det någon annan som pratar på banden? Är det förfalskade bilder? Oklara och suddiga bilder har även dykt upp som s.k. bevis på att amerikanska soldater, vilka togs till fånga under Vietnamkriget, fortfarande hålls som fångar i vietnamesiska fängelser. Dessa bilder har dock endast rört sig om förfalskningar (Alling-Ode & Tubin, 1993). Det finns ett flertal exempel på problemet, men detta är några av dem.

Säkerhet har mycket att göra med att information inte ska kunna manipuleras. Förhoppningsvis leder inte bara den tekniska utvecklingen till att man har större möjlighet att utföra förfalskningar, utan även att man kan få kontroll över manipulationerna så att säkerheten kan bibehållas. Att informationen är korrekt spelar en viktig roll för framtida beslut och åtgärder vad gäller polismyndighetens och domstolarnas arbete. Inkorrekt information kan leda till

allvarliga konsekvenser både för den enskilda individen och för allmänheten i övrigt. Till exempel kan oskyldiga bli dömda eller skyldiga frikända. Att informationen är korrekt och fullständig är något som inte är angeläget bara för polisen utan även för andra myndigheter och företag som handhåller känslig information. Fel i sjukhusens journaler kan leda till att patienter får fel vård och i värsta fall kan människor dö eller få men för livet. Företag kan fatta fel beslut i viktiga förhandlingar vad gäller dess framtid, om dokumenten beslutsprocessen bygger på har manipulerats. Företagshemligheter kan bli stulna. Detta kan leda till att företaget går i konkurs, vilket ofta leder till att samhället även påverkas i form av att anställda avskedas. Det faktum att alla påverkas på ett eller annat sätt innebär att alla är problemägare.

Trots att dessa säkerhetsproblem har existerat lika länge som digitala dokument har funnits har det ännu inte, efter flera decennier, framtagits någon slutgiltig lösning på problemen. Flera lösningar har tagits fram under årens gång, men inget som man med säkerhet har kunnat kalla perfekt, vilket gör att dessa heller inte implementerats i någon större utsträckning. Det är en pågående kapplöpning mellan säkerhetsexperter och illvilliga hackers. Utifrån dessa problem har vi kommit fram till följande frågeställning:

Hur kan man fastställa att ett digitalt dokument är ett original?

Vi har även en sekundär frågeställning:

Finns det ett behov av tekniker för detta?

Med detta vill vi försöka belysa de möjliga tekniker som finns att tillgå på dagens marknad och om behovet för dessa finns inom e-demokratin.

1.2 Avgränsningar

Vi har i denna uppsats valt att se generellt på alla typer av digitala dokument eftersom bearbetningen av de olika typerna av dokument sker på ungefär

samma sätt. Däremot har vi valt att i våra exempel använda bilder, då man tydligt kan visa skillnader mellan en manipulerad bild och ett original. Vi har heller inte för avsikt att undersöka hur man tagit en bild, då man redan vid tagning kan styra motivet åt det håll man vill, genom att ändra ljussättning och placering av rekvisita o.s.v. Vi kommer endast att forska i hur man kan fastställa att ett dokument inte blivit manipulerat från det ögonblick informationen lagras på någon typ av digitalt medium.

Det finns flera olika infallsvinklar med vilka man skulle kunna angripa de problem som beskrivs ovan. Man skulle kunna tänka sig en psykologisk vinkel på studien med människan och dess behov och orsaker till otillbörligt beteende i centrum. Vi kommer dock främst inrikta oss på att beskriva tekniska lösningar på problemet. Många av de tekniska lösningar som utvecklas faller dock inom ämnet kryptografi. Då vi anser att detta inte innefattas i ämnet informatik, har vi valt att bortse från de lösningar som är rent kryptografiska. Vi har även valt att utesluta alla matematiska beräkningar, vilka skulle lägga uppsatsen på en alltför teknisk nivå.

1.3 Disposition

Det upplägg vi valt på vår uppsats är som följer. I kapitel 2 - Informationssamhället - redogör vi för hur dagens samhälle och myndigheter använder sig av IT och digitala dokument för att underlätta kommunikationen. I kapitel 3 - Digitala dokument - går vi mer noggrant in på dokumentens betydelse i vårt samhälle och vilka risker som finns med den ökade spridningen av dessa dokument. Utöver detta stipulerar vi här vilka kriterier som vi anser en teknik för autenticering av digitala dokument måste klara av. Kapitel 4 - Metod - ger en beskrivning, samt kritik, på hur vår studie har genomförts och vilken filosofisk infallsvinkel vi använt oss av. I kapitel 5 - Tekniska lösningar - redogör vi för de tekniker vi funnit under vår studie. Dessa diskuteras sedan, tillsammans med myndigheternas och medborgarnas användningsområden, samt olika moraliska aspekter i kapitel 6 - Diskussion. I kapitel 7 - Slutsats -

svarar vi på den uppställda frågan utifrån de diskussioner vi fört i tidigare kapitel.

För att få en bättre förståelse av uppsatsen, har vi i bilaga 1, definierat de svårare orden och begreppen som vi använder oss av genom uppsatsen.

2 Informationssamhället

Vi lever idag i ett informationssamhälle. Utvecklingen av detta samhälle har gått betydligt fortare än vi kunde förutse för bara fem år sedan. Samhället har utvecklats till att bli mer tekniskt styrt och datorer är mer och mer förekommande. De tekniska förutsättningarna för samhället förändras i en allt högre takt och kraven på effektivisering har ökat. Denna utveckling har även skapat möjlighet för nya samarbetsformer både mellan individer och mellan organisationer. Utvecklingen och utbredningen av Internet ger nya möjligheter till service och informationsutbyte mellan myndigheter, privatpersoner och företag. Det finns stor efterfrågan att använda Internet för kommunikation mellan myndigheter och allmänhet (Statskontoret, 2000:7). Det ökande Internetanvändandet har bidragit till att samhället i grunden förändrats. Detta gäller framförallt den offentliga förvaltningen. Myndigheternas webbplatser används i allt större grad av både medborgare och företag. I april 2002 besöktes de statliga myndigheternas webbsidor av 2,3 miljoner unika besökare, vilket är 45% av alla svenskar som var ute på Internet (Statskontoret, 2002:108).

2.1 E-demokrati

Det demokratiska samhället flyttar allt mer ut sin verksamhet på Internet och bildar vad vi idag kallar e-demokrati. Istället för att samlas i stadshuset möts människor nu på en elektronisk samlingsplats, där tid och rum inte längre spelar någon större roll. Målsättningen med e-demokrati är att medborgarna ska få större och starkare politiskt inflytande och att makten förflyttas från parlamentet till medborgarna. Sverige har länge legat på efterkälken vad gäller elektronisk demokrati, men nu har kraven börjat komma och utvecklingen av en 24-timmarsmyndighet har tagit fart (SOU, 1999:12), där Riksskatteverket (RSV) och tullmyndigheten kommit längst i utvecklingen. Informations-

mängden har ökat så kraftigt att en hantering av denna inte skulle vara möjlig utan att ta hjälp av IT[2].

Viktigt att tänka på är att alla generationer och samhällsklasser ska ha en rimlig chans att kunna delta. Ojämlikheter är ett av problemen inom en demokrati. Människor med mer kontakter och mer pengar kan oftast påverka mer. E-demokratin är inte någon lösning på detta problem och inte heller underlättar tekniken om inte alla kan ta del av de av tjänster som utvecklas. För att öka deltagandet i den demokratiska processen måste nätet därför göras tillgängligt och användbart för alla medborgare. Det får inte vara för dyrt för den enskilda individen. Det krävs även att myndigheterna gör sina beslut och de fullständiga beslutsunderlagen tillgängliga för allmänheten över nätet. Mycket av denna information finns redan tillgänglig i elektronisk form men väldigt lite av den är tillgänglig för medborgaren (SOU, 1999:12).

E-demokrati är en produkt av behovet av kommunikation och tillgången till Internet. Hilmar Westholm ställer i sin artikel *e-Democracy goes ahead* upp sex punkter han anser är de viktigaste fördelarna med e-demokrati (Westholm, 2002):

- E-demokrati möjliggör asynkron kommunikation: deltagare i virtuella diskussioner har mer tid att tänka igenom de politiska motståndarnas argument innan de reagerar.
- Diskussioner blir mer rationella än emotionella.
- Internetbaserade metoder är mer flexibla med hänsyn till tid och plats: användare måste inte deltaga i kvällsmöten eller besöka myndigheter under kontorstid.
- Planering kan lättare visualiseras.

[2] Tullverket, personlig kommunikation, 13 maj, 2003

- Medborgare kan bättre förbereda sig själva innan de besöker en myndighet, då de kan inhämta information via Internet. Kommunikation kan ske på en kvalitativt högre nivå.
- Anonymiteten på Internet lockar folk att deltaga som normalt inte skulle gjort detta och får till stånd diskussion bland medborgare som normalt inte har några politiska kontakter.

För att den demokratiska processen ska kunna flytta ut på Internet krävs det att de elektroniska dokumenten får samma funktion som de fysiska. Beslut som tas av myndigheter och andra elektroniska dokument måste också kunna säkerställas (SOU, 1999:12). Finns det inga metoder för att garantera ett dokuments äkthet kan de heller inte få den betydelse fysiska dokument har. Detta kan göra att papper ändå måste skickas fram och tillbaka då många av myndigheternas beslut bygger på information i olika typer av dokument. Mycket av e-demokratin handlar också om effektivisering, att få bort alla papper och manuella rutiner för att automatisera så mycket som möjligt. Deklarering via Internet är ett exempel på denna automatisering. Lyckas man hitta bra och användbara metoder för autenticering av elektroniska dokument skulle även politiska val kunna ske elektroniskt i framtiden.

Än så länge kan man generellt säga att IT har bidragit till att den fysiska pappersmängden inom myndigheter har ökat och inte tvärtom. Viktiga dokument skrivs fortfarande först ut för att noggrant gås igenom innan de skickas iväg och dokument skrivs ut för att läsas där det inte finns tillgång till dator[3]. Arkiveringsbestämmelser gör även att dokumentmängden ökar, då dessa måste lagras fysiskt under ett visst antal år[4]. E-tjänster inom Tullverket och RSV, där deklarationer kan göras elektroniskt har däremot gjort att den fysiska pappersmängden minskat inom dessa områden[5]. Även Migrationsverket, vilka

[3] RSV, personlig kommunikation, 14 maj, 2003

[4] Polisen i Göteborg, personlig kommunikation, 11 maj, 2003

[5] RSV, personlig kommunikation, 14 maj, 2003 & Polisen i Göteborg, personlig kommunikation, 11 maj, 2003

under 2003 genomför ett försöksprojekt för ansökningar över Internet, ser en minskning av den fysiska pappersmängden om deras projekt visar sig framgångsrikt. De menar då att antalet mellanled där fysiska dokument används minskar [6].

2.2 24-timmarsmyndigheten

Stora ansträngningar görs för att skapa en så kallad 24-timmarsmyndighet där allmänhetens tillgång till myndigheterna är oberoende av dag eller tid. För att skapa en 24-timmarsmyndighet har regeringen gett statskontoret och RSV i uppdrag att tillsammans stödja och stimulera denna utveckling (Statskontoret, 2002:108). Statskontoret definierar begreppet 24-timmarsmyndighet som: ”*en vision om att den offentliga förvaltning [sic] skall kunna uppfattas som en utåt sammanhållen enhet, en nätverksförvaltning, som samverkar för att fullgöra sina uppdrag med Brukarna, dvs. medborgare och företag, i centrum”* (Östberg, 2003). En ”virtuell” myndighet tar mer och mer form där den allmänna administrationen inte ses som en mängd oberoende organisationer, utan som ett kollektiv, till vilket kontakt kan ske genom en och samma portal. Detta gör myndigheterna mer genomskinliga för utomstående och kan liknas vid ”one stop government” (Lenk & Traunmüller, 2002). Ur medborgarnas perspektiv är det ointressant om informationen härstammar från den privata eller den offentliga sektorn; medborgaren är intresserad av en tjänst som kan hjälpa i en specifik situation samtidigt som den är snabb att använda och är säker (van Rossum, et al., 2002). E-demokrati är ett sätt för myndigheterna att använda de nya teknologierna för att förse folk med enklare tillgång till myndighetsinformation och service, för att förbättra kvaliteten på tjänsterna och för att ge större möjlighet att delta i våra demokratiska institutioner och processer (Grönlund, 2001). Utmaningen myndigheterna nu står inför ligger i att involvera medborgarna i de områden där IT tillåter användningen av flexibla och lättillgängliga medel – inte bara för politiska val (Westholm, 2002). I takt med att 24-timmarsmyndigheten utvecklas och allt fler traditionella tjänster utvecklas till e-tjänster kommer det

[6] Migrationsverket, personlig kommunikation, 13 maj, 2003

bli naturligare att även myndigheter i framtiden använder Internet i sin dialog med medborgarna (Statskontoret, 2002:108).

2.3 E-tjänster

E-demokrati handlar framförallt om att ge information om och insyn i verksamheten och en möjlighet till att medverka i verksamheten, men det innefattar även e-tjänster. E-tjänster syftar till att tillhandahålla interaktiva tjänster på olika nivåer till medborgare och andra myndigheter. Regeringens mål är att all information och alla tjänster som kostnadseffektivt kan tillhandahållas elektroniskt skall tillhandahållas elektroniskt (Statskontoret, 2002:30).

Målet för utvecklingen av e-tjänster är bl.a. att företag och medborgare enklare och snabbare ska kunna anmäla sig, skicka in ansökningar, betala avgifter och ansöka om bidrag direkt via Internet. Man ska inte heller behöva vända sig till flera olika myndigheter för att få uträttat sina ärenden, utan det ska räcka med en. Därefter ska myndigheterna själva skicka den information som behövs mellan sig. Bättre kvalitet är också något myndigheterna strävar efter. De interaktiva tjänsterna över Internet hos både myndigheter och förvaltningar ska ge en hög och likvärdig kvalitet över hela landet. Detta gäller även de tjänster där en tjänsteman behöver göra individualiserande bedömningar. Medborgare och företag ska kunna följa och kommunicera med myndigheter i egna ärenden, där all information om ärendet ska finnas tillgänglig liksom all den information som finns lagrad hos myndigheterna om företaget eller medborgaren.

Tyvärr är det än så länge inte en självklarhet att företag och medborgare kan skriva ut blanketter direkt via webbplatser. Än mindre är det en självklarhet att man kan utföra tjänster elektroniskt. Avsaknaden av gemensamma etablerade lösningar har hämmat utvecklingen av nya tjänster för samverkan mellan myndigheter. Utvecklingstakten har därvidlag bromsats då detta är ett problem som måste lösas innan utvecklingen åter kan ta fart och nya tillämpningsområden kan bli aktuella (Statskontoret, 2002:30). Efter intervjuer

med ett flertal myndigheter har det visat sig att det inte bara beror på säkerhetsbrister att de inte har infört fler e-tjänster. Även Sveriges lag har bidragit till att utvecklingen stannat upp, då denna i vissa fall kräver att det finns en namnunderskrift på ett fysiskt dokumentet[7].

Myndigheterna har själva börjat titta på lösningar för sina e-tjänster, men dessa har inte implementerats i någon större utsträckning. Bankerna är de som kommit längst med sina digitala signaturer. Myndigheterna har däremot kommit på efterkälken. Tullmyndigheten, RSV och Rikspolisstyrelsen (RPS) är några av de myndigheter som har börjat implementera e-tjänster på sina hemsidor. För att deklarera över Internet kunde du i år (2003) gå in på RSV:s hemsida och identifiera dig själv med hjälp av de säkerhetskoder som fanns på den hemskickade deklarationen. Skulle du däremot göra tillägg var du tvungen att använda dig av en elektronisk ID-handling. Denna ID-handling kunde du bara få om du redan tidigare var kund hos någon av de parter RSV tecknat avtal med. För att erhålla denna ID-handling hänvisades du till t.ex. någon banks hemsida för att få vidare information.

Tullmyndigheten har flyttat ut flertalet av sina tjänster på Internet och har fler under utveckling. Polisen i Uppsala har startat ett projekt under namnet ”Kontaktcenter”. Syftet med projektet är att förbättra polismyndighetens service och tillgänglighet för allmänheten genom att införa en nationell kontaktcenterlösning för tillhandahållande av upplysningar, tipsmottagning samt mottagning av enklare förlust- och brottsanmälningar[8]. RPS i Stockholm har dock bestämt att projektet ska läggas på is, då brandväggarna inte har den säkerhet som krävs för elektronisk överföring, vilket polisen i Uppsala inte kan se som ett problem då det har fungerat utmärkt de senaste åren[9].

[7] RSV, Tullverket och PRV personlig kommunikation, 13 maj, 2003

[8] RPS, personlig kommunikation, 22 april, 2003

[9] Polisen i Uppsala, personlig kommunikation, 13 maj, 2003

2.4 Förtroende

Användning av Internet medför inte bara fördelar utan även risker som upplevs som större än vid traditionella metoder. Statliga myndigheter använder sedan tidigare datamedier för överföring av information. Detta sker dock genom slutna system, då man bedömer att riskerna med att använda Internet är för stora. Den statliga förvaltningen kan inte som privata företag ägna sig åt risktagning. ”Statsförvaltningen förvaltar folkets förtroende.” ”Det kan inte accepteras att den enskilde utsätts för risker ledande till ekonomiska eller rättsliga förluster” (Statskontoret, 2000:7, s.23).

Förtroende är en viktig del av den statliga förvaltningen och en central aspekt av många ekonomiska och sociala interaktioner. Warkentin et al. (2002) definierar förtroende som: *Tilltron att motparten uppför sig på ett socialt ansvarsfullt sätt och genom detta uppfyller den tilltroende partens förväntningar.*

För en myndighet som vill utöva kommunikation över Internet med allmänheten är det av yttersta vikt att de har förtroende från densamma. Förtroende är därför en av grundpelarna för att den eftertraktade 24-timmarsmyndigheten ska kunna bli den succé den förväntas bli. För att förtroende ska kunna uppnås och bevaras även när elektroniska tjänster erbjuds måste myndigheterna ställa stora krav på säkerhet. Statskontoret ställer följande grundläggande krav för att tillfredsställande säkerhet ska kunna uppnås (Statskontoret, 2000:7):

- Säker identifiering
- Oavvislighet
- Insynsskydd
- Förvanskningsskydd
- Tillgänglighet och tillförlitlighet
- Begriplighet

Av dessa krav är förvanskningsskydd kanske det minst utforskade området. Samtidigt är det ett av de viktigaste. Vi vill gärna tro att det vi ser i ett dokument är sanningsenligt. Kan inte detta garanteras faller hela konceptet med en e-demokrati. En liten grupp människor med ont uppsåt kan orsaka stor skada genom förfalskningar och förändring av befintliga dokument. ”Det är ett problemområde där vi inte ser någon lösning för tillfället”, säger Carl Wessbrant vid Statskontoret[10].

Myndigheterna måste vinna användarnas förtroende för att 24-timmarsmyndigheten ska kunna bli verklighet, men de måste även kunna lita på att användaren beter sig på ett tillbörligt sätt. I en e-demokrati kommer mycket förtroende att ligga hos användaren och så måste även vara fallet. Idag förlitar vi oss på att den som t.ex. anmäler sig sjuk är det. Detta måste vi även fortsättningsvis kunna göra i framtiden. Problemet med internet-kommunikation är anonymiteten. Anonymitet kan lätt få den konsekvensen att en människa beter sig på ett helt annat sätt än den skulle ha gjort om den inte var anonym. Internet har också det problemet att allt sker med hjälp av knapptryckningar. En normal datoranvändare är van vid att klicka på länkar och knappar hundratals gånger per dag. Att då signera viktiga överenskommelser med en knapptryckning kan kännas oseriöst. Det vi idag menar med signering innefattar mer än att man bara sätter sin namnteckning på ett papper; det finns en underförstådd betydelse i underskriften som säger att man står för det man undertecknat på heder och samvete. Det finns en viss vikt av att t.ex. lämna in sin deklaration fysiskt vid skattemyndigheten. Det känns som om det väger tyngre och inger en högre säkerhetskänsla än en knapptryckning på en hemsida. I det fallet blir namnteckningen något känslomässigt engagerat. Den som ska signera tänker till en gång extra innan han eller hon sätter sitt namn på något man inte står för. Samma typ av ”ceremoni” behöver införas vid signering på datorn för att en användare ska inse att det är ”på heder och samvete” man signerar[11].

[10] Wessbrant, C. Statskontoret, personlig kommunikation, 2003.

[11] Klang, M. Viktoriainstitutet, personlig kommunikation, 24 april, 2003.

3 Digitala dokument

Tendensen i vårt samhälle med en digitalisering i allt större omfattning har medfört att de dokument som förr enbart fanns i pappersform, nu allt som oftast även eller endast finns i digital form. Den elektroniska bildlagringen är t.ex. på väg att helt slå ut de traditionella fotoarkiven. Vi går mot ett papperslöst samhälle där digitala dokument tillhör en del av vardagen. Medier som tidigare var representerade i analogt format, t.ex. musik på kassettband, har konkurrerats ut av kvalitets- och prestandamässigt bättre lösningar i digitalt format. Bl.a. lade TV 4 redan för över tio år sedan över hela sitt bildarkiv på digitalt medium (Alling-Ode & Tubin, 1993).

I takt med den ökande användningen och spridningen av digitala dokument ökar även riskerna med att information sprids till personer utan rättigheter att inneha, se eller ändra i dessa dokument. Den tekniska utvecklingen har lett till större möjligheter för personer med stora kunskaper inom området och tvivelaktiga avsikter, att på ett illegalt sätt, med hjälp av dataintrång, komma åt dokument som tidigare varit omöjliga för dem att nå. Detta kan medföra stor skada då känslig information, företagshemligheter, säkerhetsklassad information och dylikt hamnar i fel händer. Det kan även innebära brister i den enskildes integritet då sjukjournaler och polisrapporter även de lagras i digitalt format. Många säkerhetssystem klarar inte ens av att motstå väldigt små attacker på grund av att de som designat dem inte tagit hänsyn till grundläggande kryptografiska principer (Katzenbeisser & Petitcolas, 2000).

De ökade risker digitaliseringen har inneburit för samhället medför även ett krav på ökade möjligheter att skydda sin information från oönskade attacker. ”Med något års mellanrum måste IT-säkerheten återuppfinna sig självt. Nya teknologier och nya applikationer bär med sig nya hot och tvingar oss att uppfinna nya säkerhetsmekanismer” (Katzenbeisser & Petitcolas, 2000). Nya metoder för att hindra skadliga angrepp på informationen framtas ständigt i takt med att nya riskområden upptäcks och hamnar i blickfånget. Nya användningsområden för digital information upptäcks och nya tekniker krävs

för att skydda denna. Utvecklingen av säkerhetstänkandet är en ständigt pågående process.

Införandet av digitala dokument i samhället har varit en stor förändring från tidigare sätt att administrera information. Den nya tekniken har inneburit att man med större lätthet kan behandla och bearbeta stora mängder information. Det är enklare att komma åt information man behöver, arbeta eller ändra i denna oberoende av geografiskt avstånd eller tidpunkt på dygnet. Internet medför en stor möjlighet för ett företag att bli mer globalt, då medarbetarna inte måste vara knutna till en speciell geografisk punkt. Digitala dokument är även lättare att arkivera och lagra, då de inte tar upp samma fysiska utrymme som pappersdokument. Dessa egenskaper gör att man även börjat digitalisera sina gamla pappersdokument (Alling-Ode & Tubin, 1993), då information i dataformat inte heller tar samma skada som papper och fotografier gör, vilket leder till att dokumentens livslängd förlängs. Texter och bilder bleknar med tiden och har större risk att gå sönder då pappret bli allt skörare av t.ex. syraangrepp. Den tekniska utvecklingen har inneburit att digitalisering av t.ex. pappersdokument eller vanliga fotografier, blivit mycket lättare. Numera kan gemene man genomföra detta med hjälp av en vanlig scanner. Även analoga videosignaler kan lätt omvandlas till digitala bara man har de rätta verktygen. När väl dokumentet är inne i en dator kan man med hjälp av de flesta nyare bild- och textbehandlingsprogram ändra, lägga till eller ta bort information i dokumenten.

Generellt är även kvaliteten på digitala dokument högre. Möjligheten att få tillgång till bättre och noggrannare material är för många företag, t.ex. inom forskning och teknologi, viktig. Här bidrar den digitala kvaliteten till att bistå forskare med material med väldigt hög precision och tydlighet. Men möjligheten till manipulation av materialet, framförallt vad gäller bilder, har sedan början av 90-talet tagits upp till debatt i både svenska och utländska facktidskrifter. I tv-programmet *Tro inte dina ögon* vilket sändes för några år sedan, avslutade producenten Rolf Olson sin diskussion om datorer och förfalskade bilder med att påstå att ”manipulationen ökar beroende på att den

nya tekniken finns" (Alling-Ode & Tubin, 1993). Fred Ritchin säger i sin bok *Bildens förändrade värld* något som syftar på ungefär samma sak, "Vi har hittat anden som kan göra var och en av oss till den vackra prinsessan eller den ståtlige prinsen och andra till fula ankungar". Ritchin påstår vidare att de som har tillgång till datorns elektroniska retuschering för första gången har det yttersta vapnet i sin hand. Detta gör skaparen av dokumentet maktlös och möjligheten till att se hur informationen egentligen skulle ha sett ut blir i värsta fall till en omöjlighet (Ritchin, 1991). Hittills har speciellt fotografier ansetts ha en hög trovärdighet, då dessa avbildar något vi kan se med våra egna ögon och förväxlar dem därför lätt med verkligheten, men denna trovärdighet minskar i takt med att tekniken utvecklas. Man kan säga att vi befinner oss i en bildrevolution där man kan skapa trovärdighet med hjälp av tekniken och allt som vår mänskliga fantasi kan tänka ut (Alling-Ode & Tubin, 1993).

Manipulering kan både ha en positiv och negativ betydelse. Den kan även ha olika betydelse för olika människor. Men när får man egentligen manipulera? Manipuleringar förkommer nästan överallt i t.ex. reklam, konst, tidningar, filmer och musik m.m. Det man måste studera är innebörden av ändringen eller ändringarna. Att med datorns hjälp förbättra skärpan eller färgerna i ett suddigt dokument kan inte räknas som något negativt så länge man inte riktar in sig på speciella delar för att ge dokumentet en annan betydelse. Inte heller kan man se det som negativt då man med datorns hjälp ändrar utseendet på en försvunnen person för att på något vis få en aning om hur denna kan se ut i dag (Alling-Ode & Tubin, 1993).

Denna debatt om hur enkelt det är att manipulera digitala dokument har lett till en diskussion om digitala dokuments bevisvärde och om huruvida det finns principiella och generella skillnader i bevisvärde mellan digitala dokument och traditionella pappersdokument. I stort har folk ett lägre förtroende för digitala dokument, just på grund av vetskapen om hur lätt det är att manipulera dessa. Under ett seminarium anordnat av IT-rättsliga observatoriet om just detta ämne, dominerades dock diskussionen av uppfattningen att det inte generellt går att säga att digitala dokument skulle ha ett lägre bevisvärde än

pappersdokument. En slutsats som seminariet kom fram till var att digitala dokuments äkthet i sig inte behöver bevisas på annat sätt än traditionella dokumenttyper. Bevistemat, både när det gäller digitala och traditionella dokument, skall inte vara dokumentets äkthet utan det som dokumentet handlar om (IT-rättsliga observatoriet, 2001:11).

Den ökande spridningen av dokument ökar riskerna för att informationen kommer i orätta händer. Detta är en prioriteringsfråga man får ta vid övergång till digitala system. Stora organisationer med omfattande administration kan dock tjäna mycket på att byta, då fördelarna ofta överväger nackdelarna.

För e-demokratins vidare utveckling är det ur medborgarnas perspektiv och övriga instansers perspektiv av vitalt intresse hur myndigheter och liknande hanterar de digitala dokumenten. De dokument som skapas genom olika typer av e-tjänster innehåller oftast information om avsändaren som inte får komma i orätta händer (Nydén, 2000). Därför är myndigheternas sätt att lagra informationen väsentlig för medborgarnas förtroende för de e-tjänster som tillhandahålls.

För att hanteringen av de digitala dokumenten skall kunna ske på ett säkert och tillitsfullt sätt, är det nödvändigt att det finns tekniker som kan garantera ett dokuments autencitet. Kan inga garantier för ett dokuments äkthet ges, så kan aldrig en fullgod tillit erhållas.

3.1 Kriterier för användbarhet

Ett av syftena med den här uppsatsen är att utreda vilka av de tekniker, som finns för autenticering av digitala dokument som är mest tillämpbara. För att kunna jämföra olika lösningar behövs en gemensam referensram att utgå ifrån. Vi har därför valt att diskutera de olika teknikerna utifrån ett antal kriterier, som vi anser måste uppfyllas för att lösningen skall kunna anses vara tillräcklig för att kunna säkerställa att ett digitalt dokument är ett original. Vi har utgått från en lista av kriterier som ställts upp av Jessica Fridrich (Fridrich, 2002). Denna

lista är ursprungligen en kravlista för design av ett skört vattenmärke. Då den är specifik för sköra vattenmärken (se kap. 5.3.4) och inte lämpad till andra tekniker, har vi studerat och modifierat den för att passa alla typer av tekniker.

Följande kriterier anser vi bör uppfyllas, för var och en av teknikerna, för att dessa ska anses vara användbara vid autenticeringen av ett digitalt dokument.

- **Säkerhet** - Tekniken skall vara säker och klara av de attacker som idag finns kända.
- **Funktionalitet -** Tekniken skall kunna förhindra att manipulation av ett digitalt dokument kan ske, alternativt lokalisera var i dokumentet en manipulation har skett.
- **Överförbarhet -** Tekniken skall vara överförbar på flera former av digitala dokument.
- **Implementerbarhet -** Tekniken skall vara snabb och enkel att använda.

En teknik som uppfyller dessa kriterier skulle, om någon sådan är framtagbar, enligt oss vara en tänkbar lösning och även lämplig att använda som en standard för säkerställande av digitala dokuments äkthet.

3.1.1 Säkerhet

För att ett digitalt dokument skall kunna verifieras, måste det kunna motstå alla kända modifieringsattacker. Bland dessa kan nämnas otillåten manipulation, men även informationsförlorande handlingar som byte av filtyp med medföljande kompression, t.ex. från bitmap till jpeg. Som diskuterats i inledningen av kapitlet finns det både positiva och negativa attacker mot dokumenten. Vi menar att om ett dokument definitivt ska kunna garanteras vara ett original och tekniken ska kunna anses vara säker, så måste även de positiva manipulationerna förhindras. Detta skulle annars kunna bli alltför osäkert, då bedömningen av vad som är en positiv manipulation och vad som är en negativ skulle bli alltför subjektiv.

Även tekniken som ska verifiera dokumentets innehåll måste kunna anses vara säker och kunna motstå alla de kända attacker som den kan utsättas för. En teknik som digitala signaturer (se kap. 5.1) måste t.ex. kunna garantera att signaturen alltid finns i samband med dokumentet och att ingen kan avlägsna densamma. Inte heller ska det finnas möjlighet för någon att använda ens egen signatur. Därför bär också individen ett ansvar gentemot teknikens säkerhet, då denne inte bör föra lösenord och krypteringsalgoritmer vidare till obehöriga personer. Ingen teknik kan anses vara säker om det finns motsvarande tekniker för att bryta ner eller avlägsna den. Givetvis är inga tekniker helt felsäkra. Det kan aldrig lämnas garantier att en teknik aldrig kommer att bli offer för en framgångsrik attack. Det bör dock kunna ges garantier för att tekniken ska kunna motstå de attacker som är kända idag. Viktigt är att de möjliga lösningarna inte stannar upp i utvecklingen. För att behålla en hög säkerhetsnivå måste utvecklarna till teknikerna konstant informera sig om nya möjliga attacker, för att snabbt kunna införa åtgärder för att stoppa dessa.

3.1.2 Funktionalitet

Det finns ett flertal olika tekniker för att förhindra manipulation av digitala dokument. Några av dem skiljer sig ganska grundligt från varandra. Vilken teknik man ska välja beror på vilken typ av dokument det är som ska skyddas och vilken funktion detta dokument ska fylla i organisationen. Förutom detta beror även teknikvalet på vilken nivå av säkerhet man vill uppnå. Ska man få lov att kopiera, göra geometriska förändringar så som förstoringar och rotationer, eller ska man kanske få lov att göra ändringar så länge möjligheten finns att kunna se hur originalet såg ut? Man måste med andra ord även bestämma sig för hur olika förändringar av dokumenten ska kunna spåras. Som vi ser det finns det framförallt två huvudfunktioner; vilken man använder beror lite på vad dokumentet innehåller och vilken funktion det ska tjäna. Antingen låser man dokumentet så att användaren endast har behörighet att läsa och möjligtvis kopiera valda delar av dokumentet, eller så lägger man in en funktion som kan spåra alla de förändringar som gjorts. Om vi tar en bild som exempel, så skulle alla försök att ändra något i en låst bild kunna leda till att hela bilden

förstörs eller att, om man använder vattenmärkning (se kap. 5.3) som teknik, bara själva vattenmärket förstörs/ändras. Vattenmärket skulle i sin tur kunna påvisa att bilden blivit förändrad eller peka ut var i bilden förändringar gjorts.

3.1.3 Överförbarhet

Digitala dokument kan vara av flera olika slag. Det vanligaste är att de är text, bild eller ljud, sparade i olika format. Även kombinationer kan förekomma som t.ex. film, som är en kombination av en stor mängd bilder och ljud. En aspekt på effektivitet hos en teknik är hur mångsidig den är. Om en teknik kan användas till fler än en typ av dokument är den kanske att föredra framför en teknik som är specifik för en typ av dokument. Vid valet av teknik är det viktigt att man väger in säkerhetsaspekten. Oftast kan en teknik vara mer säker på en typ av dokument än vad den är på ett annat. Det vore dock en stor fördel om en och samma teknik gick att använda på alla sorters digitala dokument samtidigt som den uppfyllde säkerhetskraven.

3.1.4 Implementerbarhet

Några av de viktiga funktionerna för en användare är att en mjukvara är snabb, lätt att använda och har en låg inlärningströskel. Om programmet saknar detta kommer användarna att välja något annat. Historien har visat att program som är för svåra att förstå eller använda, aldrig får någon större grupp användare. För att en lösning ska vara praktisk måste den vara lättanvänd. Med lättanvänd menas i det här fallet att det måste finnas en applikation som abstraherar bort de algoritmer som används för att skydda dokumentet och för användaren presenterar ett intuitivt gränssnitt med tillräcklig hjälpfunktion för att lätt förstå sig på programmet. Som användare vill man förstå vad som händer och hur, men man behöver inte förstå allt det bakomliggande.

Samma sak gäller för snabbhet vid användandet av tekniken. En algoritm får inte uteslutande vara bra på att skydda digitala dokument, den måste även

kunna utföra arbetet på relativt kort tid. Det duger inte för en användare att sitta och vänta långa stunder för att en algoritm ska bli klar. Liksom på många andra områden är tidsfaktorn viktig även här. Anta till exempel att algoritmen ska användas i realtid för autenticering av bilder direkt vid tagning i en digitalkamera. Fotografen vill inte vänta på att algoritmen blir klar mellan varje bildtagning, utan vill fortsätta att ta fler bilder med en gång. Användaren bör inte märka av någon tidsfördröjning, utan autenticeringen bör ske utan att vara märkbar.

4 Metod

Under forskningsarbetet använder sig forskaren av en eller flera metoder på ett eller annat sätt. Dessa metoder är filosofiskt influerade med att antal idéer och beroende på hur metoderna används kan de anses vara kvalitativa eller kvantitativa o.s.v. Nedan kommer vi kortfattat att beskriva två av vetenskapsteorierna och några av de termer som kretsar kring en forskningsmetod samt hur vi använt oss av dessa under vårt arbete.

4.1 Positivism och fenomenologi

Enligt Easterby-Smith et al. (1991) har det länge funnits en diskussion om hur man filosofiskt bör positionera sig vid utformningen av ett forskningsarbete. De menar att det finns två huvudkategorier att välja mellan; positivism och fenomenologi. Den positivistiska idén är att den sociala världen existerar externt och att man i sin forskning bör använda sig av objektiva metoder där forskaren genom sin subjektiva bedömning inte kan påverka resultatet. Positivisterna menar att teorier byggs på faktiska iakttagelser av verkligheten och strävar därför efter den absoluta kunskapen, där förklaringen är viktigare än själva förståelsen. De använder sig mycket av statistiska metoder och anser att det bara finns två sätt att skaffa sig kunskap; antingen genom våra sinnen eller med hjälp av logiska slutledningar. Här anser positivisterna att logiken är att föredra då våra sinnen har en förmåga att lura oss[12].

Fenomenologi sägs vara läran om det som visar sig och genomsyrar mer eller mindre alla kvalitativa forskningsansatser. Idén är att samhället är socialt konstruerat och till skillnad från positivisterna så vill man inom fenomenologin försöka förklara och förstå istället för att bara titta på rent objektiva fakta (Easterby-Smith et al., 1991). Målet är att utan förvrängning kunna återge upplevelsen av ett fenomen utan några förutfattade meningar. Man är inte

[12] http://www.edu.kristianstad.se/soderport/so/vetenskap/beg.html

intresserad av något dolt budskap och försöker därför inte göra några medvetna tolkningar utan man vill beskriva världen i stort sådan den visar sig, inte bara för blotta ögat utan också för den rena tanken. Det finns olika sätt att se världen, därför bör vi vara medvetna om vårt eget sätt på vilket vi tänker och bygger upp världen. Man bör därför vara kritisk i sitt tänkande och ompröva föreställningarna innan man kan säga att man vet något säkert. Fenomenologi kan i princip vara vad som helt som blivit föremål för betraktande och sedan för eftertanke (Bjurwill, 1995).

4.2 Kvalitativa och kvantitativa metoder

Forskningsmetoder kan delas upp i *kvalitativa och kvantitativa.* Skillnaderna mellan dessa två typer är inte alltid klara. Vissa metoder kan ses både som kvantitativa eller kvalitativa beroende på hur de används. Syftet med studien styr vilka metoder man använder och hur man använder dem. Andra viktiga saker att tänka på vid val av metod är kostnader, tillgänglighet till information, tidsåtgång och vad forskaren känner sig komfortabel med (Easterby-Smith et al., 1991). Kvantitativa metoder kan ses som statistiska metoder och fokuserar på att samla in stora mängder data som sedan analyseras. Sammanställningen av kvantitativa data sker ofta på ett statistiskt sätt med hjälp av datorer. Kvalitativa metoder är en teknik där forskaren försöker beskriva, tolka och översätta. Forskaren söker efter meningar snarare än frekvenser (Easterby-Smith et al., 1991).

4.3 Validitet och reliabilitet

Vid utformning av forskningsarbeten bör man alltid sträva efter att hitta en metod som skapar en hög validitet och en hög reliabilitet [13]. För positivisterna är validitet en fråga om hur säkra vi kan vara på att en metod verkligen mäter det den avser att mäta. Fenomenologerna anser däremot att graden av validitet

[13] http://www.infovoice.se/fou/bok/10000035.htm

beror på om forskaren i sin undersökning tagit del av all befintlig kunskap och om han förstått betydelsen av material som undersökts. Validitet innebär även att arbetet ska skapa en hög tillförlitlighet.

Reliabilitet handlar om att informationen ska vara pålitlig. För positivisterna är det därför viktigt att måtten ger samma resultat vid olika tillfällen. Resultatet får inte på något sätt vara format av forskarens egna åsikter. Enligt fenomenologerna ska därför samma resultat kunna uppnås med hjälp av liknande observationer gjorda av olika forskare vid olika tillfällen för att skapa en hög reliabilitet (Easterby-Smith et al., 1991). Sambandet mellan dessa två är att låg reliabilitet alltid medför låg validitet och för att skapa en hög validitet förutsätter det att man även har en hög reliabilitet. Har man däremot en hög reliabilitet kan man inte dra slutsatsen att man även har en hög validitet[14].

4.4 Induktion och deduktion

Det finns två olika sätt att med hjälp av teorin förklara den verklighet som studerats; induktivt eller deduktivt. Ett deduktivt arbete vill försöka bevisa något och handlar om att man utifrån allmänna principer och existerande teorier drar slutsatser om enskilda fall. Den befintliga teorin man använder sig av kan här bestämma vilken information som samlas in och även hur man kopplar sitt resultat till teorin (Patel & Davidsson, 1991).

Motsatsen till deduktion är induktion och går ut på att forskaren börjar sin undersökning utan att först förankra den i en befintlig teori. Teorin tas sedan fram utifrån resultatet av den samlade empirin (Patel & Davidsson, 1991). Forskaren försöker att utifrån ett antal observationer försöker hitta ett gemensamt mönster som han sedan drar en generell slutsats ifrån. Målet är att med hjälp av ett antal enskilda fall hitta vad som gäller för det allmänna, däremot behöver inte det allmänna gälla för varje enskilt fall[15].

[14] http://www.edu.kristianstad.se/soderport/so/vetenskap/beg.html

[15] http://www.ne.se/

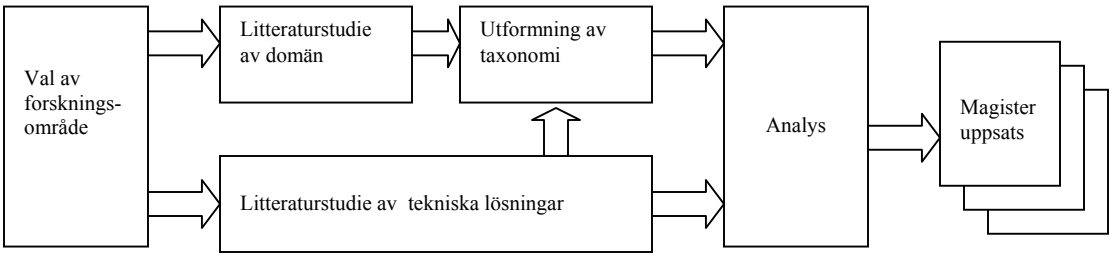
4.5 Tillvägagångssätt

Den metod vi använt oss av i denna uppsats består uteslutande av en kvalitativ litteraturstudie. Denna ansats har legat till grund för en omfattande analys av det läge vi befinner oss i idag vad gäller olika metoder för att autenticera dokument. Däremot kan vi inte säga att vi enbart utgått från en positivistisk eller en fenomenologisk synvinkel, utan arbetet har bestått av en blandning beroende på var i vårt forskningsarbete vi befunnit oss. Målet var att vi skulle hålla oss så objektiva som möjligt och se det digitala dokumentet som ett objekt och försöka förklara de tekniker som finns. Detta blev dock svårare än vi från början trodde. Målet blev därför istället att vi själva skulle förstå och på ett förståeligt och enkelt sätt förklara vårt resultat för läsaren utan att på något vis förvränga verkligheten. Konsekvensen av detta blev då att vi mer och mer gled in på den fenomenologiska banan i vårt forskningsarbete.

Ur ett fenomenologiskt perspektiv har vårt arbete en hög grad av både validitet och reliabilitet. Vi har läst igenom stora mängder informationsmaterial under vår litteraturstudie och anser därför att vi tagit del av mycket av den befintliga kunskapen inom området. Efter ett flertal diskussioner med varandra och detaljerade genomarbetade artiklar har vi fått den förståelse som behövs för att kunna genomföra en mer informatisk studie. Samma resultat bör även kunna uppnås med hjälp av liknande observationer av andra forskare då vi inte gjort några medvetna egna tolkningar och eftersom vår empiri nästan enbart bygger på litteraturstudier. Vi har använt oss av ett induktivt angreppssätt där vi bildat oss en uppfattning om hur man kan autenticera ett digitalt dokument. Utifrån detta material har vi sammanställt en taxonomi. Med hjälp av ett antal artiklar om varje teknik har vi försökt hitta ett gemensamt mönster för varje område, vilket vårt resultat bygger på. Diskussionen utgår sedan bl.a. från vår taxonomi för att förklara vad som krävs för att fastställa att ett digitalt dokument är omanipulerat.

Man kan säga att vi använt oss av två helt skilda litteraturstudier, en för domänen och en för befintliga tekniker. Vi startade båda litteraturstudierna

samtidigt. Studien av domän avslutades däremot tidigare för att gå över i utformningen av vår taxonomi vilken bygger på båda litteraturstudierna.



Figur 4.1: En översiktsbild över vår arbetsgång från val av forskningsområde till färdig magisteruppsats.

Under vår litteraturstudie använde vi oss av olika sökmotorer på Internet som t.ex. Google[16] och Altavista[17]. De sökord vi använt oss av finnes i bilaga 2. För att hitta en passande domän och information för att kunna sätta in problemet i ett sammanhang sökte vi nästan uteslutande i olika biblioteksdatabaser som t.ex. Gunda och Libris[18]. Dessa databaser innehöll dock inte mycket om lösningarna på vårt problem, antagligen beroende på att ämnet inte är så välutforskat, utan vi fick istället vända oss till artikeldatabaser, vilka var mer inriktade på olika datatekniker. CiteSeer[19] och ScienceDirect[20] är två av dem vi fick mest information ifrån, men vi har även sökt bland flertalet av de förslag som finns under det digitala biblioteket i Gunda där artiklar visas i fulltext.

[16] http://www.google.com
[17] http://www.altavista.com
[18] http://www.ub.gu.se/Ge/
[19] http://citeseer.nj.nec.com/
[20] http://www.sciencedirect.com

Utöver dessa delar har vi även genomfört kortare intervjuer per telefon eller e-mail med tekniska experter. Personerna har antingen varit anställda vid någon myndighet eller varit forskare inom några av de tekniker vi funnit. Orsaken att vi inte valt att göra några djupare intervjuer beror på att många av personerna med expertis inom området befinner sig väldigt spridda runt om i världen och chansen att få tag på dem och kunna genomföra en längre bra intervju per telefon ansåg vi var liten. Istället fick det bli enklare e-mail med frågor om tips på artiklar och liknande. Ytterligare en orsak till att vi inte valt att göra fler intervjuer beror på att vi fick svar på de frågorna vi hade med hjälp av de böcker och artiklar vi använt oss av. Chansen att myndigheter och liknande mer i detalj skulle tala om hur de hanterar sina elektroniska dokument såg vi som liten och bestämde oss därför för att bara ringa och ställa mer övergripande frågor.

4.5.1 Litteraturstudie

Litteraturstudier är en viktig och grundläggande del av forskningen. Forskaren är alltid skyldig att ta reda på vilken kunskap som redan finns i det område som utforskas. Litteraturstudier är något som alla forskare som börjar forska inom ett nytt ämne bör ägna tid åt. Urban Nuldén nämner några viktiga orsaker till att genomföra en litteraturstudie[21].

1) Skilja på vad som är gjort och på vad som behöver göras.
2) Identifiera centrala variabler.
3) Syntetisera och se nya perspektiv.
4) Få en tydlig begreppsapparat. Vara noga med att använda samma namn hela tiden och inte variera sig för varierandets skull, så att läsare av uppsatsen kan förstå och inte får problem att följa med i resonemanget.
5) Förstå strukturen på området.
6) Identifiera hur andra forskat på området.
7) Vilken forskning är state-of-the-art?

[21] U.Nuldén, Ph. D. Viktoriainstitutet, personlig kommunikation, 21 november 2002

Vi har till den allra största delen valt att fokusera vår litteraturstudie till böcker och vetenskapliga artiklar. Utöver detta har vi använt oss av diverse andra publikationer såsom statens offentliga utredningar. De områden vi har valt att begränsa denna litteraturstudie till och som vi anser är relevanta för vår frågeställning har varit e-demokrati, digitala signaturer, steganografi och digital vattenmärkning.

4.6 Metodkritik

Vi anser själva att vi genomfört en tillräckligt omfattande litteraturstudie för att få den kunskap som behövdes för vårt problemområde och de lösningar vi funnit. Vi kan däremot inte säga att vi hittat de mest lämpade teknikerna då vi bara gjort en teoretisk studie över tänkbara lösningar och aldrig testat dem praktiskt. Det hade varit intressant om vi i vår undersökning kunnat utvärdera varje teknik mer ingående för att styrka vår teoretiska ståndpunkt. Tyvärr blev detta en omöjlighet då programvaror för alla tänkbara lösningar inte finns tillgängliga på marknaden.

Det hade även varit intressant om vi genomfört muntliga intervjuer med forskare inom området, för att få fram deras syn på det hela. Intervjuer hade även kunnat öka förståelsen, från första början, för de artiklar vi varit tvungna att läsa om och om igen.

5 Tekniska lösningar

Utvecklingen av tekniker för autenticering är en ständigt pågående process som antagligen kommer att fortgå så länge det finns någon som klarar av att besegra de tekniker som finns ute på marknaden. Vi kommer nedan att redovisa de tre lösningar vi funnit, som i nuläget är tillämpbara för autenticering av digitala dokument. Lösningarna är: digitala signaturer, steganografi och digitala vattenmärken.

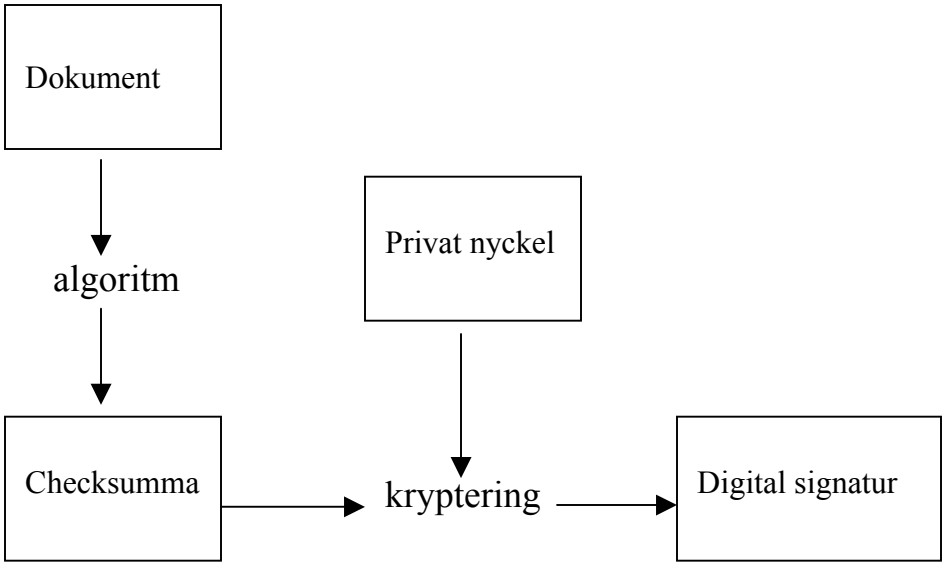
5.1 Digitala signaturer

Digitala signaturer är en teknik som är baserad på asymmetrisk kryptering. Asymmetrisk kryptering bygger på ett unikt nyckelpar bestående av en publik nyckel och en privat där både den publika nyckeln och den privata nyckeln kan användas till kryptering och dekryptering. Ordet asymmetrisk kommer av att man bara kan dekryptera det krypterade meddelandet med krypteringsnyckelns motpart, d.v.s. om man krypterade med den publika nyckeln kan man bara dekryptera med den privata och vice versa. Detta betyder att skaparen av ett digitalt dokument krypterar detta med sin privata nyckel, varefter det krypterade dokumentet endast kan dekrypteras av skaparens publika nyckel. Detta är den omvända ordningen mot hur man brukar använda publika och privata nycklar i asymmetrisk kryptering där syftet oftast är att säkerställa att bara den specificerade mottagaren ska kunna läsa meddelandet, varför man använder dennes publika nyckel för kryptering (European Commission, 2000).

Tanken med att använda asymmetrisk kryptering för autenticering är att man kan bekräfta avsändarens identitet med hjälp av den privata nyckeln. Avsändaren krypterar dokumentet eller delar av det med sin privata nyckel, varpå mottagaren kan kontrollera avsändarens identitet genom att dekryptera dokumentet med den antydda avsändarens publika nyckel. Om dekrypteringen misslyckas är inte avsändaren den han utger sig för att vara (European Commission, 2000).

Digitala signaturer är en vidareutveckling av asymmetrisk kryptering, eller kanske snarare en tillämpning. För att digitalt signera ett dokument går man till väga som följer (European Commission, 2000):

- Det första steget är att skapa det dokument som ska signeras.
- Det andra steget är att skapa ett *hashvärde*, eller checksumma, för dokumentet. Om dokumentet förändras kommer inte längre checksumman stämma överens med den som dokumentet genererar
- Som tredje steg krypterar avsändaren checksumman med sin privata nyckel. Resultatet – den digitala signaturen – kommer att vara unikt, både för dokumentet och för nyckeln som krypterade det, och måste skickas med dokumentet.



Figur 5.1: Schematisk bild över skapandet av en digital signatur

I och med att den digitala signaturen består av både en checksumma för dokumentet och en privat nyckel, så kan den användas till två saker: autenticering av dokumentets innehåll och verifiering av avsändaren. För att verifiera avsändaren använder man, liksom i asymmetrisk kryptering, den

antydda avsändarens publika nyckel för att dekryptera signaturen. Om dekrypteringen lyckas är avsändaren den han utger sig för att vara och resultatet blir checksumman för dokumentet. Checksumman kan man sedan använda för att autenticera dokumentets innehåll genom att på nytt räkna ut dokumentets checksumma med samma algoritm som tidigare och jämföra resultatet med den bifogade checksumman. Stämmer de överens är dokumentet oförvanskat, men är bara en bokstav eller en pixel i dokumentet förändrad kommer inte längre checksummorna stämma överens och dokumentets innehåll är inte längre autentiskt (European Commission, 2000).

Digitala signaturer är idag den teknik som myndigheter och företag tittar mest på som ett alternativ för elektronisk identifiering. Tanken med myndigheternas arbete på detta område är att kunna ersätta handskrivna signaturer med digitala eller likställa dem ur ett juridiskt perspektiv. EU utfärdade 1999 det s.k. EG-direktivet som innehåller ett ramverk för elektroniska signaturer. I direktivet anges att under vissa förutsättningar ska en elektronisk signatur kunna jämställas med en underskrift (Statskontoret 2000:7).

Myndigheternas arbete idag går mycket ut på att ta fram lösningar för elektronisk identifiering av personer, s.k. EID. Dessa baserar sig oftast på asymmetrisk kryptering och något som kallas PKI, Public Key Infrastructure. Detta är benämningen på de standarder och rutiner som krävs för att på ett säkert sätt hantera nycklar, t.ex. i ett elektroniskt ID-kort. Skillnaden mellan fysiska och elektroniska ID-handlingar är sättet att verifiera innehavaren, d.v.s. att kortinnehavaren verkligen är den som ID-handlingen är utfärdad för. Fysiska, visuella ID-kort verifieras genom att innehavaren har ett utseende som överensstämmer med ID-handlingen och kan skriva en korrekt namnteckning. För certifikatet gäller att innehavaren kan visa att han är i besittning av den privata nyckeln som hör ihop med den publika nyckeln i ett nyckelpar. Den privata nyckeln finns endast på det elektroniska ID-kortet. Det är alltså certifikatet som är den elektroniska ID-handlingen (Rikspolisstyrelsen, 2000).

En inriktning som myndigheterna har i sitt arbete med EID är att kombinera EID med personliga ID-kort. Det här skulle lösa problematiken med förtroende för signaturerna då man vet att nycklarna är lika säkra som utfärdade ID-kort då det finns en säker EID-utfärdare. Spridningen av digitala certifikat som detta skulle kunna bidra till acceptansen för digitala signaturer både juridiskt och i samhället i stort. Bl.a. i Finland har detta genomförts framgångsrikt (Rikspolisstyrelsen, 2000).

Fördelen med digitala signaturer framför andra tekniker för att skydda digitala dokument är att signaturer kan användas till alla typer av filer, då en checksumma kan räknas ut för vilken digital fil som helst. Detta i kombination med enkelheten i implementation gör digitala signaturer till ett bra val för dokumentverifiering.

Det finns dock en del nackdelar och betänkligheter när det gäller digitala signaturer och asymmetrisk kryptering som verifiering. Den första är att för att kunna vara säker på att ett dokument kommer från den man tror, måste man vara säker på att den publika nyckel man använder för att dekryptera meddelandet verkligen tillhör den man tror att den tillhör. Detta kan lösas genom att godkända certifikatutfärdare, s.k. Certification Authority – CA, som t.ex. staten, banker, posten etc., står för utfärdandet av publika nycklar och därmed går i god för att en nyckel verkligen tillhör den person som den uppges tillhöra (Rikspolisstyrelsen, 2000).

Ett annat problem är att signaturen alltid måste finnas tillgängliga i anknytning till det dokument det ska verifiera. Detta skulle kunna lösas med hjälp av någon form av elektroniska kuvert: en filtyp där dokumentet och signaturen sparas tillsammans i samma fil, med lätt tillgång till båda[22].

[22] Existerande exempel på elektroniska kuvert kan vara en zip-fil. Se http://www.winzip.com för exempel på implementering.

5.2 Steganografi

Människan har under flera århundraden strävat efter att hitta ett säkert sätt att gömma information. De gamla grekerna försökte redan på sin tid gömma meddelanden på träskivor som sedan täcktes med vax för att de skulle se blanka och fina ut. En annan metod var att raka huvudet på en slav, tatuera in ett meddelande och låta håret växa ut igen innan slaven skickades iväg (Johnson & Jajodia, 1998). Strävan efter att gömma information har fortsatt och idag har man även utvecklat tekniker för att gömma information i digitala dokument, delvis beroende på att företag och privatpersoner allt mer väljer att utbyta information över osäkra medier så som Internet. Steganografi, vilket betyder ”dold text”, handlar framförallt om att gömma hemlig information inuti andra dokument. Hemlig information i en textfil kan t.ex. bäddas in i en digital bild eller en mp3-fil[23].

Kryptografi och steganografi är nära släkt med varandra. Kryptografi är den teknik som gör informationen svårläst eftersom meddelandet krypteras, medan steganografi gömmer information och gör den svår att hitta (Johnson & Jajodia, 1998). Dessa två tekniker används ofta tillsammans då de väger upp varandras svagheter. Kryptografi riktar mer in sig på överföring medan steganografi ser mer på förvaring[24].

Steganografi används vid kommunikation över sårbara kanaler och för att skydda upphovsrätten av digitala verk[25]. Förutom dessa två användningsområden kan företag och andra organisationer använda steganografi för att skydda sina digitala dokument. Antag att en anställd inom ett företag bifogar ett dokument i ett mail, vilket innehåller företagshemligheter. Med hjälp av ett meddelande till företagets mailserver, som är steganografiskt inbäddat i dokumentet, vilket anger att dokumentet inte får lämna företagets

[23] http://www.hanshusman.nu/smm/smmoktober.html#s1

[24] http://pgp.press.nu/index.php

[25] http://pgp.press.nu/index.php

interna system, skulle man kunna förhindra att detta dokument skickas vidare[26]. Meningen är att någon som försöker förvanska, kopiera eller skicka vidare ett dokument inte ska veta att där finns hemlig information gömd.

För att gömma data på steganografisk väg behövs två filer. Den som informationen ska gömmas i, *skyddsobjektet*, och en fil som innehåller meddelandet som ska gömmas. Meddelandet kan vara en enkel text, chiffer, bilder eller vad som helst som kan lagras i en bitsträng. Det kombinerande objektet av skyddsobjektet och meddelandet skapar ett s.k. *stego-objekt*, vilket ser exakt likadant ut som det ursprungliga objektet för det mänskliga ögat. Ju mindre skillnaderna mellan skyddsobjektet och stego-objektet är desto lättare är det att gömma informationen (Johnson & Jajodia, 1998). Ett flertal av experterna inom steganografi rekommenderar därför användning av gråskaliga bilder för att gömma information, då dessa inte förändras lika mycket som färgbilder. Skyddsobjektet ska helst innehålla meningsfull och till synes ofarlig information för att inte väcka misstankar. För att försvåra processen ytterligare används ofta nycklar, *stego-nycklar*, i samband med inbäddning och verifiering av meddelandet[27].

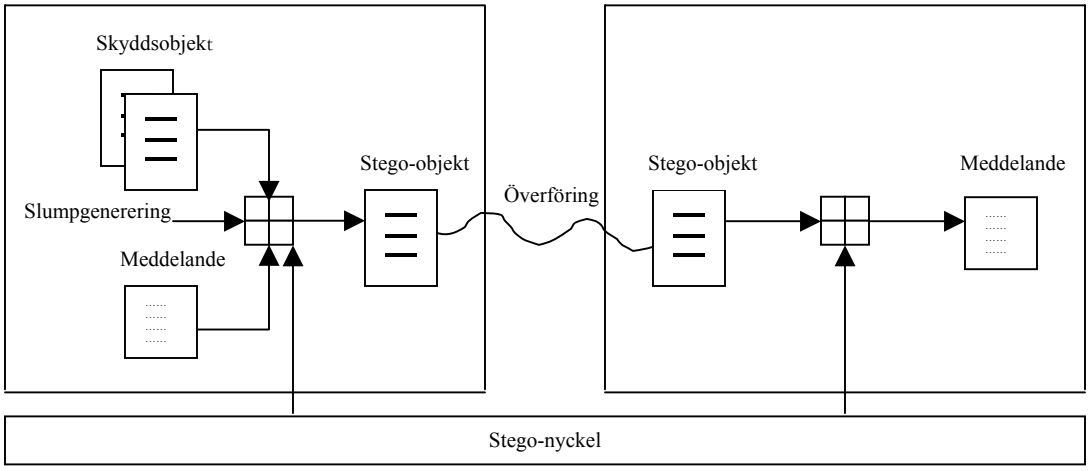
En säker steganografisk algoritm bör ha följande egenskaper (Katzenbeisser & Petitcolas, 2000):

- Meddelandet ska gömmas med hjälp av en publik algoritm och en privat nyckel. Den privata nyckeln måste identifiera avsändare, så att denne inte kan utge sig för att vara någon annan.
- Det är bara personen med korrekt nyckel som ska kunna hitta, plocka ut och bevisa existensen av ett gömt meddelande. Det får inte finnas några statistiska bevis för att meddelandet existerar.

[26] http://www.hanshusman.nu/smm/smmoktober.html#s1

[27] http://www.hanshusman.nu/smm/smmoktober.html#s1

- Om en utomstående person vet innehållet i ett gömt meddelande så ska han med hjälp av detta inte kunna spåra andra hemliga meddelanden.
- Meddelandet ska inte kunna avslöjas med hjälp av olika slags beräkningar.



Figur 5.2: Steganografi fungerar generellt enligt följande: Ett slumpmässingt skyddsobjekt väljs ut och bäddar in meddelandet med hjälp av stego-nyckeln, vilket skapar stego-objektet. Stego-objektet skickas till mottagaren som med hjälp av stego-nyckeln rekonstruerar meddelandet (Katzenbeisser & Petitcolas, 2000).

5.2.1 Tre olika typer av steganografi

Man kan säga att det finns tre olika typer av steganografi: ren steganografi, steganografi med privata nycklar och steganografi med publika nycklar (Katzenbeisser & Petitcolas, 2000).

Ren steganografi är ett system där det inte behöver utbytas någon hemlig information, såsom stego-nycklar för att starta en kommunikationsprocess. Säkerheten bygger i stället på att ingen ska få reda på den algoritm som används vid inbäddning och verifiering av meddelandet. Det som krävs är att skyddsobjektet är lika stort eller större än meddelandet som ska gömmas och att både sändaren och mottagaren vet vilken algoritm som ska användas.

För att få ett säkrare steganografiskt system kan man använda sig av en stego-nyckel. Utan denna nyckel ska ingen kunna utläsa vad som står skrivet i det hemliga meddelandet. Systemet fungerar enligt följande: processen startar med att sändare och mottagare måste göra ett utbyte av nycklar, sändaren väljer därefter ut ett dokument som används vid inbäddning av meddelandet. Med hjälp av den privata nyckeln kan mottagaren sedan vända på processen för att få ut det hemliga meddelandet.

Steganografi med publika nycklar kräver en användning av minst två nycklar, en publik och en privat, där den publika nyckeln är sparad i en publik databas. Den publika nyckeln används vid inbäddning och den privata för att rekonstruera meddelandet. Detta system kan liknas vid motsvarande system för kryptografi.

5.2.2 Robust eller säker steganografi

Steganografiska system är extremt känsliga mot t.ex. olika bild- och ljudbehandlingstekniker. En person med onda avsikter kan enkelt förstöra innehållet i det hemliga meddelandet genom att komprimera eller filtrera dokumentet, därför krävs det att steganografiska system är robusta (Katzenbeisser & Petitcolas, 2000).

Ett system kan kallas robust om den inbäddade informationen inte kan förstöras utan att man gör dramatiska förändringar i stego-objektet. Tyvärr måste man alltid göra en avvägning mellan att ha ett robust eller ett säkert system, då ett robust system blir mindre säkert. Det finns två generella sätt att göra ett steganografiskt system mer robust. För det första kan man göra detta genom att försöka förutse de möjliga modifieringar som någon kan vilja göra på skyddsobjektet. Inbäddningsprocessen kan då göras mer robust för att modifikationerna inte ska förstöra den hemliga informationen. En annan variant är att försöka vända på modifikationerna för att återskapa det ursprungliga stego-objektet (Katzenbeisser & Petitcolas, 2000).

För att kunna skapa ett säkert system för steganografi måste man alltid räkna med att det finns personer som vill orsaka skada på dokumentet och att dessa har obegränsad tillgång till datateknik, kunskap och vilja att göra det (Katzenbeisser & Petitcolas, 2000).

5.2.3 Autenticering med steganografi

Autenticering kan utföras både med hjälp av steganografi eller kryptografi. Dessa tekniker skiljer sig dock åt på vissa punkter även om man i princip är intresserad av samma sak d.v.s. att göra informationen svåråtkomlig. Kryptografisk autenticering riktar mer in sig på att skydda kommunikationskanalen för att se till att dokumentet som kommer fram är äkta och inte för att skydda dokumenten på hårddisken. Steganografi erbjuder däremot alternativ till de autenticeringsproblem som kryptografi saknar för kontroll av dokumentets integritet. Då informationen i en bild oftast är redundant medför detta att man till viss del kan modifiera bilden för att i ett senare skede kunna kontrollera om bilden på något vis blivit manipulerad och var detta i sådana fall skett. Informationen som behövs för att verifiera dokumentet bäddas med hjälp av steganografi in i dokumentet medan kryptografin i stället bifogar informationen (Fridrich, 1999).

Den ständiga kampen mot piratkopiering och möjligheten att på ett enkelt sätt manipulera dokument har gjort att det idag finns en stor mängd produkter vilka kan användas för steganografi. Oftast används inte produkterna för renodlad steganografi utan i kombination med kryptering. Några av dessa steganografiprogram är EZStego, MP3Stego och White Noise Storm (Lindkvist, 2001a). Man bör dock vara försiktig vid valet av program, då många av dessa inte uppfyller alla krav som ställs på en säker steganografisk metod[28].

[28] http://www.hanshusman.nu/smm/smmoktober.html#s1

5.3 Vattenmärkning

Digital vattenmärkning, som teknik för skyddande av digitala dokument, dök för första gången upp i en vetenskaplig publikation 1993 (Tirkel et al., 1993). Intresset var i början ganska svalt, men allt eftersom Internet ökade i popularitet började man se fördelarna med att kunna skydda och urkundsmärka sina dokument. Den digitala vattenmärkningen används för autenticering och ägarbevisning av olika typer av multimediadokument och i viss mån även textbaserade dokument. Själva vattenmärket består av en kod eller en signatur som det även kallas, vilken i princip kan innehålla vilken information som helst. Vanligast är att den innehåller information om något av följande alternativ: copyrightägaren, skaparen av dokumentet, den berättigade användaren eller vad som behövs för att hantera äganderätten till en viss typ av information (Barni et al, 1998). Vattenmärket kan även innehålla information om hur själva bilden såg ut från början genom att bädda in valda delar av bilden (Fridrich, 1999). Informationen bäddas in och sprids över hela dokumentet med hjälp av en nyckel (Eggers & Girod, 2001), för att ingen del av dokumentet ska vara oautenticerbar.

Vattenmärkning är en utveckling av olika kryptografiska metoder inom området informationsdöljande [eng. Information Hiding] såsom t.ex. steganografi. Vattenmärkning utgår dock från andra filosofiska grunder vad gäller krav och därmed även design av tekniken (Cox et al., 2002). Vattenmärkning genererar dock mer motstånd mot försök att avlägsna den gömda informationen från dokumentet (Katzenbeisser & Petitcolas, 2000). ”Där kryptering och kopieringsskydd misslyckas, ger vattenmärkning en möjlighet att spåra dokumentet till den ursprungliga ägaren” (Su et al., 1998). Cox et al. definierar vattenmärkning på följande sätt (Cox et al., 2002, s.2):

Tekniken att oupptäckbart förändra ett verk för att bädda in ett meddelande om verket.

Alla moderna sedlar har till exempel ett vattenmärke inbäddat i sedelpapperet. Detta vattenmärke innehåller information om sedeln, bl.a. vad den har för

värde och dess existens kan bevisa att sedeln är äkta. Samtidigt är vattenmärket omärkbart om man inte håller upp sedeln mot ljuset.

Digital vattenmärkning är användbart inom ett flertal områden där man på något sätt vill skydda digitala dokument. Då tekniken med vattenmärkning är förhållandevis enkel och då många olika kombinationer och system finns att använda sig av, har vattenmärkning ett stort antal tillämpningsområden. De viktigaste av dessa är dock (Cox et al., 2002):

Ägaridentifiering/informationsmärkning: Att kunna lägga in extra information, vilken ger möjlighet till att spåra dokumentets ursprungliga ägare.

Kopieringsskydd/kopieringskontroll: Att kunna identifiera och spåra obehöriga kopior, samt att begränsa eller hindra kopiering.

Autenticering: Att kunna kontrollera om en kopia av en bild blivit förändrad på något sätt och i så fall kunna lokalisera vilken/vilka delar som har förändrats.

Övriga tillämpningsområden kan vara övervakning av t.ex. TV-sändningar av en film eller att en transaktion av ett speciellt digitalt dokument har skett. Det finns många olika algoritmer för att lägga in ett vattenmärke i ett digitalt dokument och fler utvecklas ständigt. Detta kan medföra att vattenmärkning kommer att bli tillämpbart på många fler områden i framtiden än vad som nu är fallet.

5.3.1 Olika kategorier

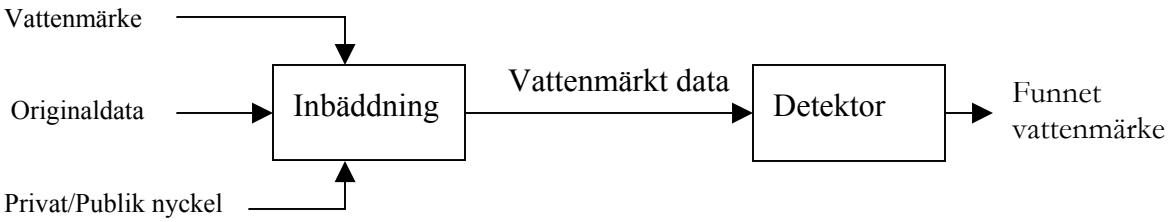
Vattenmärken kan delas in i ett flertal olika kategorier beroende på vilket sätt de bäddas in i dokumentet eller efter hur de extraherar information om vattenmärket ur dokumentet. Alla vattenmärkningssystem använder sina egna speciella lösningar, där alla behöver sin egen specifika information för att kunna hitta ett eventuellt existerande vattenmärke. Några vattenmärkningssystem

kräver att originaldokumentet finns tillhanda vid autenticering, vilket ökar säkerheten då en jämförelse med ursprungsdokumentet möjliggörs, men är opraktiskt då originalet kanske inte finns tillgängligt eller ens existerar. Vattenmärken som inte behöver ursprungsdokumentet för autenticering brukar kallas för *blinda vattenmärken* (Barni et al., 1998).

Vi ser framförallt fyra olika typer av vattenmärken. Dessa är robusta, sköra, halvsköra och borttagbara vattenmärken. Utöver dessa finns det ett flertal varianter av olika vattenmärken som t.ex. självinbäddande vattenmärken som antingen kan vara sköra eller halvsköra. Robusta vattenmärken, vilka används för autenticering brukar bädda in kännetecken från bilden i märket. Detta ökar robustheten ytterligare genom att man här kan avgöra skillnaden mellan de avsiktliga och oavsiktliga manipulationerna (Fridrich, 1999). Sköra vattenmärken kan upptäcka förändringar i alla enskilda delar av dokumentet och ge exakt information om bildens integritet. Däremot klarar de inte av att särskilja ofarliga förändringar som t.ex. förstoring, komprimering etc., från manipulationer där saker läggs till eller tas bort i bilden. Halvsköra vattenmärken är däremot mer robusta till skillnad från de sköra då dessa till stor del klarar av många av de vanliga bildbehandlingsmetoder som i allmänhet används, som t.ex. komprimering. De borttagbara vattenmärkena är praktiska då man vill räkna ut en checksumma av ett dokument och sedan bädda in ett vattenmärke. Vanligtvis skulle checksumman vara ogiltig eftersom själva inbäddningen av vattenmärket producerar en viss störning i dokumentet. Borttagbara vattenmärken går att avlägsna från dokumentet så att en kopia av originaldokumentet kan erhållas och en korrekt checksumma kan räknas ut.

5.3.2 Grundläggande principer

Det finns många olika typer av vattenmärkning och många olika kombinationer av dessa typer. Alla olika former bygger dock på samma princip. Nedan visas en konceptuell bild över hur vattenmärkning av ett digitalt dokument fungerar.



Figur 5.3: Konceptuellt schema över vattenmärkning (Cox et al., 2002; Katzenbeisser & Petitcolas, 2000)

Inbäddaren [eng. embedder] använder sig av ett ursprungsdokument samt ett vattenmärke, som den med hjälp av en privat eller publik nyckel lägger samman till ett vattenmärkt dokument. Om det bara är den som har äganderätten till dokumentet som ska kunna spåra vattenmärket så bör denne använda sig av nycklar för att lägga in vattenmärket. Denna nyckel måste sedan användas för att hitta märket. För att ytterligare öka säkerheten kan informationen krypteras innan den läggs in i dokumentet (Götberg & Smith, 2000).

Detektorn, vilken används för spårning och extrahering av vattenmärket är specialdesignad för det vattenmärkningssystem den är ämnad för. I vissa fall ska detektorn endast bevisa existensen av vattenmärket i dokumentet, medan den i andra fall ska utvinna den data vattenmärket bär med sig (Götberg & Smith, 2000). Outputen från detektorn är beroende av det vattenmärke som använts. Från en robust teknik ska outputen, om inga lyckade attacker genomförts, vara det vattenmärke som ursprungligen bäddades in i dokumentet. Ett skört eller ett halvskört vattenmärke ska, om ingen manipulation skett, ge samma resultat som ett robust. Om en manipulation av dokumentet skett är det mycket troligt att vattenmärket på något sätt har förstörts i de områden av dokumentet där en manipulation har skett (Cox et al., 2002). De allra flesta sköra och halvsköra vattenmärken kan lokalisera var i dokumentet en förändring har skett. Vissa kan till och med återställa det ursprungliga dokumentet (Lin & Chang, 2001).

Utseendet på det vattenmärke som bäddas in i dokumentet är starkt beroende på vilken typ av dokument som ska vattenmärkas. En digital bild kräver en helt annan sorts vattenmärke än ett ljudspår eller en film. Vid vattenmärkning av ett ljud- eller videodata kan vattenmärket läggas ut på ett större antal segment av filen (Katzenbeisser & Petitcolas, 2002).

För att vara effektivt bör ett vattenmärke vara:

Diskret: Vattenmärket ska vara osynligt både statistiskt och för det mänskliga ögat så att kvaliteten på datan inte förändras och för att inte pirater ska kunna hitta och förstöra det (Barni et al, 1998; Cox et al., 2002).

Utskiljbart: Den som är ägare av datan eller någon annan med behörighet ska lätt kunna hitta vattenmärket (Barni et al, 1998).

Robust: Vattenmärket bör vara robust mot acceptabla manipulationer som komprimering och andra signalhanterande tekniker (Barni et al, 1998; Lin & Chang, 2000; Cox et al., 2002).

Säkert: Vattenmärket ska vara mycket svårt, helst omöjligt, att avlägsna av en person som utför en attack (Barni et al, 1998). Vattenmärket ska även vara omöjligt att kopiera från ett dokument till ett annat (Lin & Chang, 2000; Cox et al., 2002)

Ett vattenmärke är säkert så länge inte oauktoriserade personer kan ta bort eller modifiera det (Su et al, 1999). De attacker som vattenmärken kan råka ut för och vara känsliga mot är relativt många. Ett flertal former av dessa är dock kända och det finns möjligheter att stoppa samtliga. Nedan anges de mest förekommande attackerna som ett vattenmärke designat för autenticering kan utsättas för.

- Blind modifiering - Detta är den allra vanligaste typen av attack som ett vattenmärke måste klara av, d.v.s. att personen som utför attacken

förmodar att dokumentet är omärkt och genomför en förändring. Detta är en attack som alla vattenmärken ska kunna upptäcka (Lin & Delp, 1999).

- Oupptäckta modifieringar - Personen som utför attacken gör en förändring av dokumentet på ett sådant sätt att förändringen inte upptäcks av det vattenmärkningssystem som använts (Lin & Delp, 1999; Fridrich, 2002). En av de mest kända av dessa attacker är känd som ”the Holliman-Memon attack” i vilken små bildblock flyttas inom en digital bild eller mellan två olika bilder vattenmärkta med samma nyckel. Denna attack är mer noggrant beskriven i (Holliman & Memon, 2000).

- Avlägsnande av vattenmärket - Om ett försök att avlägsna ett vattenmärke lyckas kan det få stora följder för syftet med vattenmärkningen, nämligen autenticeringen. Personen som utfört attacken kan då ta bort märket, modifiera dokumentet och sedan åter inbädda märkningen i dokumentet (Lin & Delp, 1999). Detta kan medföra att ett förfalskat dokument uppfattas som autenticerat. Möjlighet finns även att flytta ett vattenmärke från ett dokument till ett annat och på så sätt autenticera även detta dokument (Lin & Delp, 1999).

- Informationsläckage - Systemet för vattenmärkning måste vara säkert på sådant sätt att ingen information om de nycklar som använts eller det sätt på vilket vattenmärket bäddats in i bilden kan erhållas genom att analysera ett vattenmärkt dokument (Fridrich, 2002). Detta kan medföra sådana säkerhetsproblem som möjliggör modifieringar av dokumentet eller avlägsnande av vattenmärket. Skulle en nyckel erhållas ur ett vattenmärke skulle det inte vara svårt att förfalska märkningen och inbädda denna i ett annat dokument.

Autenticering, som denna uppsats inriktar sig mot, har som nämnts ovan ett flertal olika vattenmärkningslösningar beroende på vilken form av autenticering

man vill genomföra. Alla dessa varianter har både för- och nackdelar. Alla kan påvisa att en manipulation har skett, dock kan ingen förhindra att en sådan sker. Vi kommer att gå igenom ovan nämnda i detalj nedan.

5.3.3 Robusta vattenmärken

Robusta vattenmärken används framförallt vid copyrightskydd, där information som identifierar ägaren bäddas in i dokumentet (Yin et al, 2001). De robusta vattenmärkena är designade för att ingen ska klara av att ta bort dem ur dokumentet och för att klara av andra typer av tänkbara attacker (Lin et al, 2000). Hur robust vattenmärket bör vara beror på syftet med märket. Är syftet ägaridentifiering har robustheten större betydelse än om syftet skulle vara att föra vidare information till den slutliga användaren, då robustheten inte spelar någon större roll (Yin et al, 2001).

Ett robust vattenmärke ska i princip vara omöjligt att ta bort men om så ändå skulle ske ska dokumentets kvalitet förändras till det sämre i den grad att det inte längre spelar någon roll att vattenmärket tagits bort. En vattenmärkt bild ska inte försämras i kvalitet i jämförelse med dess original, men vid kopiering ska däremot kopian försämras. För att öka säkerheten ska nycklar användas både vid införandet och vid verifiering av vattenmärket. Robusthet innebär framförallt att vattenmärket ska klara av de allra vanligaste manipulationerna så som komprimering, filtrering, kopiering och geometriska förändringar. Informationsförlorande komprimeringar minskar kvaliteten på vissa områden i bilden. Vattenmärket måste därför placeras på en visuellt betydelsefull plats. För att klara geometriska förändringar som rotationer, förminskningar och förstoringar använder sig teknikerna av ett mönster eller en signal som bäddas in tillsammans med vattenmärket. Det kan däremot bli svårt att hitta märket om signalen förstörts. Man ska heller inte kunna bädda in fler vattenmärken i ett dokument som redan är vattenmärkt (Götberg & Smith, 2000).

Barnis system för robusta vattenmärken

Några av de robusta vattenmärkningsmetoderna använder sig av Discrete Cosine Transform (DCT) vid vattenmärkning av bilder. Vattenmärket sprids antingen över hela bilden eller så väljs ett antal DCT-koefficienter ut ur s.k. bildblock där vattenmärket placeras.

En av de tekniker som använder sig av DCT för robust vattenmärkning tar Barni et al. upp i sin artikel *A DCT-domain system for robust image watermarking* (Barni et al, 1998). Denna teknik verkar inom frekvensdomänen och gömmer en pseudoslumpmässig sekvens av reella tal i ett antal valda DCT-koefficienter. Resultat har visat att deras vattenmärke är robust mot de allra flesta av de attacker som ett robust vattenmärke bör motstå. Deras system använder blinda vattenmärken och passar framförallt in på svart-vita fotografier. Till skillnad från andra system ser Barnis et al. system alltid till att bädda in märket i samma serie av koefficienter för att undvika behovet av originalbilden vid avgörandet av var den pseudoslumpmässiga koden är gömd. På detta sätt är det svårare att hitta märket då de ursprungliga DCT-värdena inte är kända. Nedan beskrivs kortfattat detta system.

Inbäddning av vattenmärket

1. Generera ett vattenmärke med längden M bestående av en pseudoslumpmässig sekvens av reella tal.
2. Dela in en bild i ett antal lika stor kvadrater, vilka bildar ett antal block. Dessa block utgör sedan indata för att räkna ut DCT:n[29].
3. Beräkna DCT-koefficienterna.
4. Genomför en zig-zag scan på DCT-koefficienterna.
5. Välj ut en sekvens av DCT-koefficienter efter den ordning zig-zag scannern lagt in dem i vektorn. Den plats man väljer att börja inbäddningen av sekvensen på i vektorn är valfri, men för att uppnå en perceptuell osynlighet på märket utan att förlora robusthet mot

[29] http://www.tfe.umu.se

signalbehandlingstekniker hoppar man alltid över den första platsen i vektorn. De koefficienter man väljer ut ska så alltså ligga mellan platserna (L+1) och (L+M) i vektorn, där L är en valfri plats och M är längden på den pseudoslumpmässiga sekvensen som ska bäddas in.

6. Genomför slutligen en omvänd zig-zag scan för att få fram den vattenmärkta bilden.

Autenticering

1. Givet en möjligt vattenmärkt bild. Dela in bilden i ett antal lika stor kvadrater.
2. Beräkna DCT-koefficienterna.
3. Genomför en zig-zag scan på DCT-koefficienterna..
4. Välj ut koefficienterna mellan (L+1) till (L+M) för att återskapa den pseudoslumpmässiga sekvensen.

Barni et al. har testat sin teknik, genom att märka en bild med ett visst vattenmärke. Bilden utsattes därefter för ett antal olika attacker för att kunna se om detektorn klarade av att avslöja vattenmärket (se bild 5.3). Detektorn tog in 1000 st slumpmässigt genererade vattenmärken och resultatet visade att dekodern utan tvekan kunde hitta vattenmärket i de attackerade bilderna. Resultatet av Barnis et al. teknik visade sig vara så bra att den anses vara mycket starkare än andra metoder inom området (Barni et al., 1998).

Robusta vattenmärken för autenticering

Tills idag har majoriteten av alla robusta vattenmärkningstekniker riktat sig just mot copyright och inte så mycket mot autenticering, trots att det i många fall är lika viktigt att skydda innehållet i ett dokument som att skydda dess copyright. Går det inte att skydda innehållet mot förändringar så borde man åtminstone kunna se vilka förändringar som gjorts med hjälp av ett vattenmärke (Rey & Dugelay, 2000).

Bild 5.1: Originalbild

Bild 5.2: Vattenmärkt bild

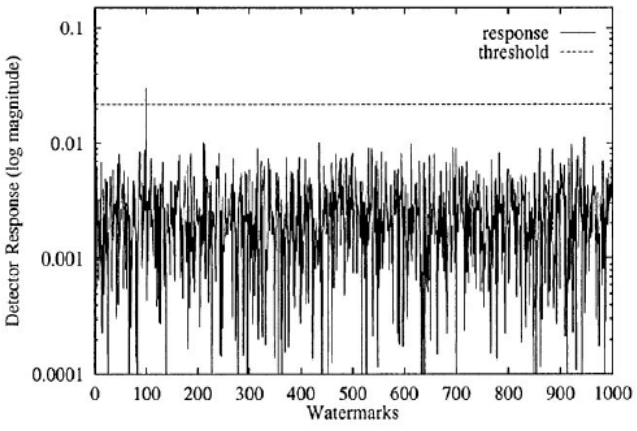


Bild 5.3: Test på en JPEG komprimerad bild. Alla testerna av de attackerna bilderna visade ungefär samma magnitud, där vattenmärket nummer hundra matchade det inbäddade märket.

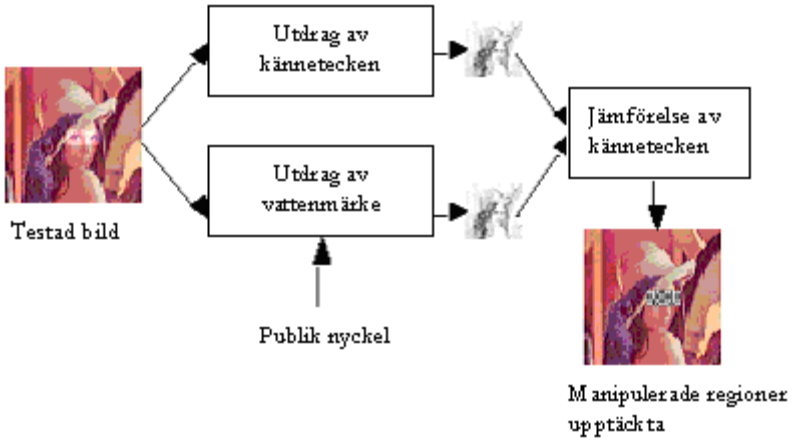
Av de tekniker som tagits fram är det mest sköra eller halvsköra vattenmärken som används vid autenticering. Rey och Dugelay (2000) har däremot föreslagit en teknik vilken bygger på robust vattenmärkning av bilder. Tekniken använder

sig av ett blint vattenmärke och är oberoende av vilken vattenmärkningsalgoritm som används. Till skillnad från de vanligaste vattenmärkena används inte ett fast förutbestämt märke utan detta tas fram beroende på vilken bild vattenmärket är ämnat åt. Idén går ut på att man väljer ut olika kännetecken och speciella drag i bilden som man sedan gömmer i ett robust och osynligt vattenmärke. Vattenmärket krypteras sedan med en privat nyckel innan det bäddas in i bilden. (Se figur 5.4).

Figur 5.4: Generell beskrivning av Rey & Dugelays teknik för autenticering med hjälp av robusta vattenmärken (Rey & Dugelay, 2000).

Vad som inte syns i bilden ovan är att framtagningen och inbäddningen av vattenmärket är en iterativ process, eftersom svagheten i metoden är att originalbilden påverkas av inbäddningen. För att komma runt detta tar man ut nya kännetecken från den vattenmärkta bilden, lägger dessa i ett nytt vattenmärke som därefter bäddas in i den tidigare vattenmärkta bilden. Detta görs ytterligare en gång för att vattenmärkets och bildens kännetecken ska stämma överens.

För att sedan avgöra om bilden blivit förändrad på något vis, jämför man dess kännetecken med dem som finns i vattenmärket, vilka ursprungligen kommer från originalbilden. Är det några skillnader är ett rimligt antagande att bilden på något vis manipulerats för att ändra dess innehåll.



Figur 5.5: Generell bild över autenticering av en digital bild med Rey & Dugelays teknik (Rey & Dugelay, 2000).

Beroende på hur detaljerad informationen i vattenmärket är så kan man hitta olika förändringar, d.v.s. om man fört in mycket information i vattenmärket så är chansen större att man kan upptäcka eventuella förändringar. För mycket information kan man dock inte bädda in i en bild då detta kan påverka vattenmärkets robusthet. Det får däremot vara tillräckligt mycket för att kunna avslöja de möjliga förändringarna.

5.3.4 Sköra vattenmärken

Ett skört [eng. fragile] vattenmärke är per definition ett vattenmärke som med lätthet kan förstöras (Lin & Delp, 1999). Designat för en digital bild upptäcker ett skört vattenmärke med hög sannolikhet alla tänkbara förändringar i bildens pixlar (Fridrich, 2002; Lin & Delp, 1999). Detta är speciellt lämpligt inom området autenticering av digitala dokument då man med stor säkerhet kan fastställa om dokumentet på något sätt blivit förstört eller förändrat sedan vattenmärket bäddades in (Cox et al., 2002; Lin & Delp, 1999). Detta skulle vara till stor nytta vid känslig bildhantering då vattenmärket skulle kunna bäddas in i bilden redan vid tagningsögonblicket. Detta skulle leda till att bilden redan från det att den sparas i digitalkamerans flash-minne är autenticerad.

Skulle ett ur bilden utdraget vattenmärke vid något tillfälle visa på förstörelse, kan man med stor sannolikhet säga att bilden på något sätt har förändrats.

Lin och Delp räknar i en artikel upp flera olika funktioner som system vilka använder sig av sköra vattenmärken bör innehålla (Lin & Delp, 1999). Bland dessa kan nämnas:

- Vattenmärket ska upptäcka förändringar. Ett system för sköra vattenmärken måste med stor sannolikhet kunna upptäcka samtliga förändringar som sker i ett digitalt dokument då detta är det fundamentala användningsområdet för sköra vattenmärken.

- Vattenmärket måste vara genomskinligt för blotta ögat. Vattenmärket bör inte var synligt under normal observation eller på något sätt lägga sig i det digitala dokumentets funktionalitet.

- Detektering av vattenmärket ska inte kräva originalbilden. Detta bör krävas då originalbilden kanske inte finns tillgänglig eller ens existerar. Det kan även vara så att ägaren av bilden inte litar på en tredje part.

- Detektorn ska kunna lokalisera och karaktärisera förändringar gjorda av det märkta dokumentet. Detta inbegriper även att finna de områden som utsatts för förändring.

- Vattenmärken genererade från olika nycklar ska vara ”ortogonala” vid detektering. Ett vattenmärke inbäddat med en speciell nyckel ska endast upptäckas av detektorn vid givande av den korrekta motsvarande nyckeln. All annan möjlig sidoinformation som ges till detektorn ska misslyckas med att upptäcka det inbäddade vattenmärket.

- Inbäddning av ett vattenmärke av oauktoriserade parter ska vara mycket svårt. Att ta bort ett vattenmärke från ett dokument och

sedan inbädda detsamma i ett annat bör vara nästintill omöjligt att genomföra.

För att ett system för vattenmärkning ska fungera på ett tillfredsställande sätt måste det inneha de funktioner som nämnts ovan, samtidigt som det kan motstå alla de attacker mot vattenmärken som tidigare nämnts, samt alla de andra attacker som finns kända. Ett sådant system presenteras av Jessica Fridrich i (Fridrich, 2002).

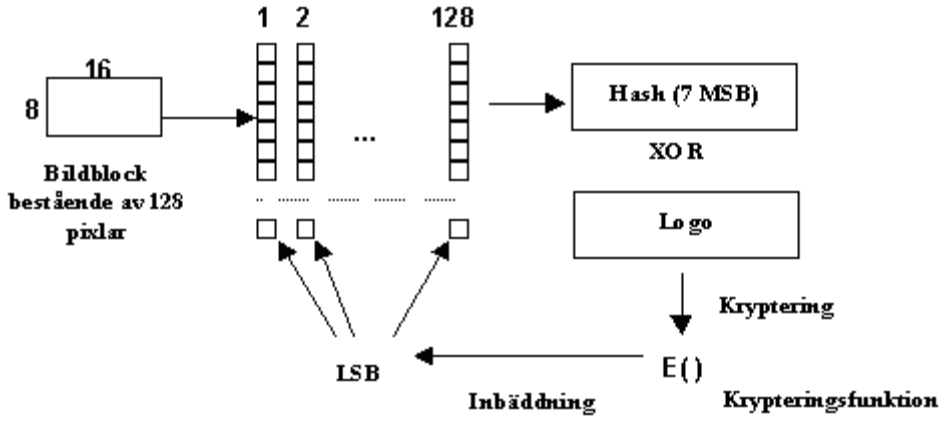
Fridrichs system för sköra vattenmärken (Fridrich, 2002)
Systemet är från början utformat för digitala bilder, men är enligt Fridrich lätt expanderbart till andra typer av multimediala dokument. Systemet, baserat på ett system utvecklat av Ping Wah Wong, klarar enligt Fridrich de attacker som ovan beskrivits samt ytterligare inte nämnda attacker.

Inbäddning av vattenmärket

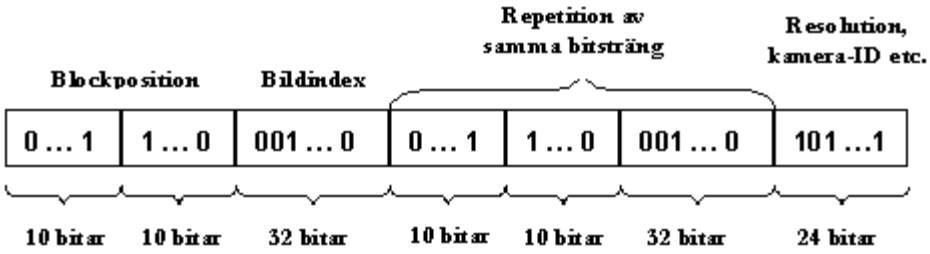
1. Dela upp bilden i 8x16 pixlar stora bildblock (128 pixlar totalt).
2. För varje bildblock, räkna ut ett hashvärde H för de sju mest signifikanta bitarna för samtliga av de 128 pixlarna.
3. Genomför en XOR-beräkning på H tillsammans med motsvarande binära logoblock, vilket resulterar i H'.
4. Kryptera H' och bädda in i de minst signifikanta bitarna för de 128 pixlarna.

Inbäddningen av vattenmärket är densamma som Wong använde sig av (se figur 5.6), dock med skillnad i utseende på det binära logoblocket. Strukturen på detta redovisas närmare i figur 5.7. Varje logoblock kommer att innehålla information om bildblockets ursprungliga position, bildindexet, bildens resolution, eventuellt kamera-ID, eventuellt fotograf-ID m.m. De första 52 bitarna i logoblocket är exakt samma som de följande 52 bitarna, vilket möjliggör att det går att autenticera vilket 8x16 pixlars bildblock som helst,

oberoende av dess position. Sannolikheten för en felaktig autenticering är därigenom $1:2^{52} \approx 10^{-15}$.



Figur 5.6: Den av Fridrich föreslagna metoden för inbäddning av vattenmärke (Fridrich, 2002).



Figur 5.7: Den av Fridrich föreslagna strukturen av det binära logoblocket (Fridrich, 2002).

Autenticering

1. Dela upp bilden i 8x16 pixlar stora bildblock (128 pixlar totalt).
2. För varje block, räkna ut ett hashvärde H för de sju mest signifikanta bitarna för samtliga av de 128 pixlarna.
3. Dekryptera LSB för att få fram H'.
4. Genomför en XOR-beräkning på H tillsammans med H', vilket resulterar i logoblocket för det aktuella bildblocket.
5. Om de 52 första bitarna i det erhållna logoblocket överensstämmer med de följande 52 bitarna är innehållet i bildblocket autentiskt.

6. Eftersom innehållet i blocket är autentiskt kan vi anta att informationen om bildindexet, resolutionen, blockets position och övrig sidoinformation stämmer. Informationen i blocket innehåller därför tillräcklig information för att autenticera att blockets position är den korrekta.

Om inga autentiska block hittas skulle man kunna söka manuellt genom att låta ett 8x16 pixlar stort fönster ”glida” över bilden och försöka hitta autentiska block på detta sätt. Om en säkrare autenticering önskas eller mer information behöver bäddas in i varje block finns möjlighet att ändra storlek på varje använt block till önskad storlek.

5.3.5 Halvsköra vattenmärken

Halvsköra [eng. semi-fragile] vattenmärken är en form av vattenmärke som är specialdesignat för autenticering av dokument. Termen halvskör reflekterar att vattenmärket är robust mot en sorts attacker och skört mot andra (Eggers & Girod, 2001). Med halvskör vattenmärkning menas att märket är robust mot vissa tillåtna attacker som komprimering, medan det är skört mot otillåtna attacker som t.ex. utbyte av data i dokumentet (Cox et al., 2002). Halvsköra vattenmärken värnar om informationens autenticitet, inte om dokumentets exakta representation (Ekici et al., 2001). Anledningen att man definierar en attack som tillåten är att den inte ändrar på den information som dokumentet innehåller, utan endast skapar en viss grad av störning. Former av detta kan t.ex. vara jpeg-komprimering av bilder (Lin & Chang, 2000) eller mpeg-komprimering av film (Lin & Chang, 1999).

Robusta och sköra vattenmärken är inte ideala vad gäller att skilja på tillåtna förändringar av dokument och otillåtna. Ett exempel kan vara om en person gör en mindre, otillåten förändring av ett dokument och sedan genomför en tillåten komprimering av dokumentet. Om vattenmärket var robust skulle detektorn kunna avfärda den mindre förändringen som en störning, medan ett skört vattenmärke helt skulle förstöras av komprimeringen och förklara hela

dokumentet som manipulerat (Lin et al, 2000). Detta är även anledningen till att det inte går att använda multipla vattenmärken i form av att först bädda in ett robust och sedan ett skört vattenmärke i ett dokument för att kunna autenticera och samtidigt kunna ha en viss grad av robusthet. En komprimering av dokumentet skulle förstöra det sköra vattenmärket och därefter skulle det inte gå att autenticera dokumentet (Lin et al, 2000). Ordningen av inbäddningen är oväsentlig då, om ordningen varit den omvända, det sköra vattenmärket skulle förstörts redan vid inbäddningen av det robusta vattenmärket.

Ett exempel där användning av halvsköra vattenmärken skulle vara lämpligt är om en fotograf vill kunna autenticera en bild och samtidigt skicka den över Internet. Detta scenario skulle kunna inkludera en digital kamera som vid tagningsögonblicket lägger in ett specifikt kamera-ID i bilden i form av ett halvskört vattenmärke. Fotografen kan då komprimera bilden till jpeg-format om så önskas och fortfarande kunna autenticera bilden. All information för autenticering skulle förstöras av komprimeringsproceduren om man använt ett skört vattenmärke (Lin et al, 2000).

De egenskaper vi ser som önskvärda hos ett halvskört vattenmärke är i princip samma som de hos sköra vattenmärken; det ska upptäcka förändringar, vara genomskinligt, originalbild ska ej krävas för detektering, kunna lokalisera förändringar, nycklar ska vara ”ortogonala” samt att inbäddning av vattenmärke av oauktoriserade ska vara mycket svårt. Kärnegenskapen hos halvsköra vattenmärken är dock att det måste kunna bestämma autenticiteten på innehållet i ett dokument (Ko & Park, 2002). Medan sköra vattenmärken autenticerar hela dokumentet, koncentrerar sig halvsköra vattenmärken på att informationen som dokumentet innehåller inte skiljer sig från det dokumentet ursprungligen förmedlade.

Den stora skillnaden ligger i, som nämnts ovan, att vattenmärket ska tåla vissa förändringar av dokumentet. På samma sätt måste vattenmärket klara av alla de attacker som gäller för ett skört vattenmärke såsom; blind modifiering, oupptäckta modifieringar, avlägsnande av vattenmärke samt informations-

läckage. Ekici et al. (2001) beskriver mer detaljerat vilka manipulationer som kan betraktas som tillåtna för en digital bild:

- Mild kompression. Till exempel jpeg-komprimering upp till 70%.
- Histogramutjämning.
- Lågpassfiltrering.
- Gaussiskt brus.
- Slumpmässiga bitfel vid överföring eller lagring.
- Förändringar i skärpa.

På samma sätt beskriver Ekici et al. (2001) vilka manipulationer som kan betraktas som otillåtna:

- Samtliga medvetna manipulationer. Detta inkluderar borttagning, ersättande eller tillägg av information.
- Geometriska manipulationer. Detta inkluderar t.ex. rotering eller förändringar i upplösningen.
- Färgmanipulationer. Förändringar i färger, skuggning eller annat som ändrar utseendet av bilden.
- Bakgrundsmanipulationer. Ändringar i bakgrunden t.ex. tid på dygnet eller dylikt.
- Beskärning.

De allra flesta multimediafiler ligger idag i komprimerad form och det är främst dessa halvsköra vattenmärken inriktar sig mot. Många av de sköra vattenmärken som finns bygger på att ett hashvärde beräknas på dokumentet. De karakteristika detta hashvärde har innebär att två olika input inte kan producera samma output. Detta leder till stora problem när man komprimerar ett dokument (Ko & Park, 2002). Utmaningen med halvsköra vattenmärken ligger i att förändra en robust märkningsmetod till att kunna upptäcka och lokalisera förändringar i ett dokument (Lin et al., 2000). Nedan redovisar vi ett system för halvsköra vattenmärken utvecklat av Eggers och Girod. I en undersökning genomförd av Ekici et al. fick Eggers och Girods system mycket

bra testvärden vad gäller ovan nämnda tillåtna och otillåtna manipulationer (Ekici et al., 2001).

Scalar Costa Scheme för halvsköra vattenmärken

Eggers och Girod (2001) presenterar ett system som har sin grund i ett system utvecklat 1983 av Costa. Detta system använder sig av en kodbok, vilken genererar en slumpmässig nyckel, som måste finnas tillgänglig för både inbäddaren och detektorn. Eggers och Girod menar dock att för att Costas metod ska kunna vara effektiv måste denna kodbok vara alltför stor för att vara praktiskt användbar. De använder sig i stället av en mer strukturerad kodbok och kallade detta nya system för Scalar Costa Scheme - SCS.

Inbäddning av vattenmärket

1. Dela in en bild i ett antal lika stor kvadrater, vilka bildar ett antal bildblock.
2. Beräkna DCT-koefficienterna.
3. Genomför en zig-zag scan på DCT-koefficienterna.
4. Ett lämpligt vattenmärke *v* kodas om till en sekvens av binära tal *d*.
5. Bädda in de binära talen i bildblockens andra till åttonde DCT-koefficienter.
6. Genomför slutligen en omvänd zig-zag scan för att få fram den vattenmärkta bilden.

I korthet går detta ut på att inbäddaren härleder en vattenmärkessekvens *v* från ett vattenmärke och värddatan *x*. *v* adderas sedan till *x* för att få fram en vattenmärkt data *s*. *v* måste väljas på ett sådant sätt att skillnaden mellan *x* och *s* är så liten som möjligt. Algoritmen repeteras för samtliga block som dokumentet består av. Blockstorleken bestäms av användaren och är viktigt för hur säker autenticeringen kommer att vara. Större block ger mindre noggrannhet vid eventuell lokalisering av förändringar. SCS är starkt beroende av olika parametrar som används vid inbäddningen av de binära talen. Dessa parametrar bör optimeras för att en bra jämvikt av detekteringssäkerhet och

den störning som kan resultera av inbäddandet av vattenmärket i dokumentet. Formler för optimala värden för parametrarna redovisas i Eggers et al. (2000).

Autenticering

En detektor designad för SCS är av formen sannolikhetsdetektor. Detektorn bestämmer för varje element i den data som ska autenticeras riktigheten i om det binära talet som bäddats in var inbäddat med en speciell nyckel ur den använda kodboken. Om det binära talet och nyckeln inte stämmer överens kan man anta att datan på något sätt blivit otillåtet manipulerat. Detta kan genomföras genom att låta ett ”fönster” av en viss storlek glida över testdatan. Storleken bestäms av vilken blockstorlek man valt för de olika blocken av ursprungsdokumentet i inbäddningen av vattenmärket.

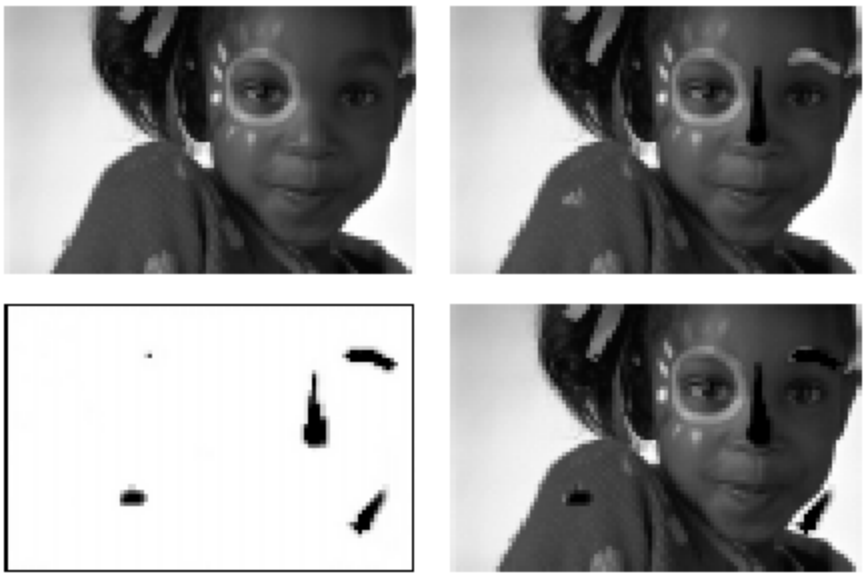


Bild 5.4: Övre vänstra: En vattenmärkt bild. Övre högra: Manipulerad och jpeg-komprimerad vattenmärkt bild. Nedre vänstra: Upptäckta manipulerade regioner av bilden. Nedre högra: Upptäckta manipulerade regioner ovanpå den manipulerade bilden.

I bild 5.4 visas resultatet av ett experiment av SCS genomfört av Eggers och Girod. De mörka fläckarna indikerar manipulerade områden av bilden. Även ett område som inte varit manipulerat har indikerats som sådant. Detta visar på ett av de fundamentala problem som halvsköra vattenmärken har som verktyg för autenticering av bl.a. bilder, då robust vattenmärkning av plana områden nästan är omöjlig (Eggers & Girod, 2001).

5.3.6 Borttagbara vattenmärken

Borttagbara vattenmärken är definitionsmässigt en kombination av vattenmärkning och digitala signaturer (Cox et al., 2002). I vissa applikationer kan även den minimala distorsion som införs av att man bäddar in en signatur i en bild vara oacceptabel. Exempelvis inom sjukvården skulle minsta lilla förändring av en bild kunna ligga till grund för en stämning för felbehandling. Den kanske är lätt att övertyga en tekniskt kunnig person om att ett inbäddat vattenmärke inte skulle ändra en läkares tolkning av bilden, men skulle samma argument vara övertygande i en rättssal?

Under sådana förutsättningar är det enda sättet att garantera att ingen betydande förändring skett att inte förändra något alls. Detta har lett till ett intresse för *borttagbara vattenmärken* för autenticering, d.v.s. vattenmärken som kan avlägsnas från det verk där de bäddats in så att man får exakta kopior av det omärkta originalet.

Om man kan konstruera ett borttagbart vattenmärke blir det inga problem med att kryptografiska signaturer blir ogiltiga efter inbäddningen.

Följande steg beskriver ett generellt protokoll (Cox et al., 2002):

1. Skaparen av ett verk räknar fram en signatur baserad på all information i verket. Signaturen bäddas sedan in i verket på ett borttagbart sätt.
2. Verkets mottagare extraherar och sparar den inbäddade signaturen.

3. Mottagaren tar bort vattenmärket från verket. Vid det här steget bör verket vara identiskt med det ursprungliga omärkta verket.
4. Som verifiering på det föregående beräknar mottagaren en ny signatur på verket och jämför den med den signatur som extraherats ur verket.
5. Om och endast om den beräknade och den mottagna signaturen är identiska är det mottagna verket autentiskt.

Cox et al. beskriver en variant av en algoritm föreslagen av Fridrich et al. som försöker lösa problemet med borttagbara vattenmärken (som ovan). En noggrannare beskrivning av algoritmen finns i (Fridrich et al., 2001). I stora drag kan deras algoritm beskrivas som följer:

Låt A representera den information som förändras i verket c när vi bäddar in ett meddelande m om N bitar. Den här informationen måste vara mindre än eller lika med 2^N. Om exempelvis inbäddningsalgoritmen ersätter LSB planet av en bild eller ljudsignal, så är A den information som LSB planet innehåller. Fridrich et al. har visat att borttagande är möjligt i de fall där A är komprimerbart. Kan A förlustfritt komprimeras till M bitar, så kan ytterligare N-M bitar borttagbart bäddas in i verket.

Inbäddning och autenticering (Cox et al., 2002):

1. Hitta den information, A, som kommer att förändras i inbäddningsprocessen.
2. Konstruera det meddelande, m, som är en sammansättning av en förlustfri komprimering av A och en kryptografisk signatur, S, beräknad på det ursprungliga verket c.
3. Bädda in m i c.
4. För att verifiera verket extraherar man meddelandet m (och dess beståndsdelar A, i komprimerad form, och S) ur verket.
5. Genom den komprimerade versionen av A och det vattenmärkta verket kan man rekonstruera originalet av verket.

6. Beräkna signaturen på det rekonstruerade verket och jämför den med den extraherade signaturen *S*.
7. Om de två signaturerna stämmer överens är verket autentiskt.

Då Fridrichs et al. lösning innebär både användandet av digitala signaturer och möjligheten att fullständigt återställa verket till sitt ursprungliga skick lämpar den sig väl för de syften vi undersöker.

5.3.7 Självinbäddande vattenmärken

Självinbäddande vattenmärken kan vara sköra eller halvsköra och har främst utvecklats för autenticering av dokument och för att skydda dokumentets innehåll. Enkelt förklarat kan man säga att vid denna typ av vattenmärkning bäddar dokumentet in en kopia av sig själv på ett sätt som gör att man vid ett senare tillfälle inte bara kan upptäcka var manipulationer gjorts utan även rekonstruera dokumentet för att få fram dess ursprungliga innehåll (Fridrich, 1999).

Jiri Fridrich har tillsammans med Miroslav Goljan (1999) utvecklat en metod för autenticering av svartvita bilder med hjälp av ett självinbäddande vattenmärke. Då det skulle ta alldeles för mycket plats att bädda in hela bilden i sig själv, väljer man ut speciella kännetecken och områden som ofta utsätts för manipulationer och bäddar in informationen om dessa i bilden. Inbäddningen av vattenmärket påverkar originalbilden ytterst lite. 50% av pixlarna i bilden kommer inte att påverkas medan resterande hälft bara kommer att förändras en nivå på gråskalan. Metoden bygger på att man delar in bilden i 8x8 pixlar stora block. För varje block beräknar man DCT-koefficienterna, vilka därefter kvantifieras och läggs in i LSB. Man kan antingen användas sig av två eller bara en LSB. Använder man sig däremot av två, kan större mängder information bäddas in i bilden och då också få fram en rekonstruktion med högre kvalitet. Nedan beskrivs metoden för att använda sig av en LSB, då denna är enklare att förstå (Fridrich & Goljan, 1999).

Inbäddning av vattenmärket

1. Förbered bilden för inbäddning genom att placera in bildens gråskala i ett passande intervall och sätt värdet för varje LSB till 0. Dela in bilden i 8x8 stora block och gör sedan följande punkter för varje block B.

2. Beräkna DCT för varje block och kvantifiera de elva första koefficienterna enligt den ordning som zig-zag scannern skapar. Räkna därefter om de kvantifierade värdena till binära koder. Skapa en matris innehållande bitlängden för varje kod. Denna matris ska sedan användas för att de första elva koefficienterna ska kodas med exakt 64-bitar. Använder man sig i stället av två LSB och 128 bitar kan man bädda in större mängder information.

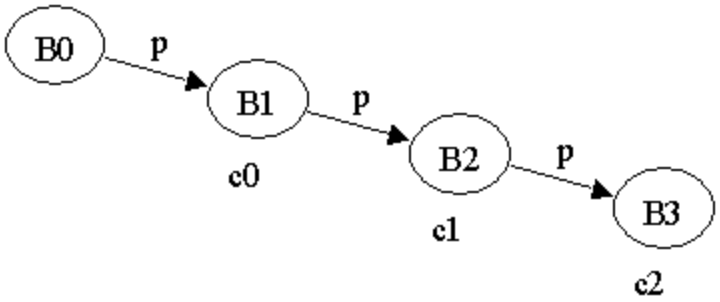
3. Kryptera 64-bitars sekvensen skapad ovan och bädda in den i LSB:n i blocket B. Nästa bäddas in på platsen B + p, där p talar om hur långt ifrån föregående plats nästa kod ska bäddas in.

Informationen om block B bäddas alltså in i block B + p. Informationen om pixlarna i block B + p bäddas i sin tur in i block B + p + p, osv. Det blir ungefär som en lång kedja innehållande olika koder. Åt vilket håll denna kedja kommer att gå slumpas fram innan själva inbäddningen startar.

Autenticering

Autenticering av bilden går sedan ut på att jämföra den inbäddade koden, med koden för blocket i den befintliga bilden. Antag att någon ändrar registreringsnumret på en fotograferad bil. Blocken i bilden betecknar vi som tidigare B och de inbäddade koderna betecknar vi c. Registreringsnumret finns på plats B1. Koden c1, som är gömd i B2, kommer nu inte stämma överens med koden för B1. Koden för B0 kommer heller inte stämma med koden gömd i B1 eftersom blocket inte kan behålla den gömda informationen efter att det manipulerats. Om koden c2 som är gömd i B3 överensstämmer med B2:s

befintliga skick och koden c0 som är gömd i B1 inte stämmer med den B0:s befintliga skick kan vi konstatera att platsen B1 på något vis har manipulerats. Med hjälp av koden c1 som är gömd i B2 kan vi nu rekonstruera innehållet i B1 för att få fram den ursprungliga registreringsskylten på bilen. Under rekonstruktionen bäddar man åter in den korrekta informationen för B0 i B1.



Figur 5.8: Princip för inbäddning och autenticering med självinbäddande vattenmärken.

De höga krav som finns på självinbäddande vattenmärkena medför dock att det är omöjligt att få fram en teknik som ger en bra rekonstruktionskvalitet, osynliggör vattenmärket och som är robust på en och samma gång (Fridrich, 1999). Metoden som ovan beskrivits kan skapa en bra rekonstruktionsbild och påverkar inte originalet nämnvärt vid inbäddningen, däremot har den ett flertal robusta svagheter. Om större områden i bilden förändras i samma riktning som p går är risken stor att flera av blocken i kedjan förändras, vilket medför att det inte går att göra en rekonstruktion av originalbilden. Detta på grund av att för mycket av den inbäddade informationen förstörts. En annan nackdel är att det inte går att upptäcka de förändringar som gjorts på de områden vars information inte bäddats in på en annan plats i bilden (Fridrich & Goljan, 1999).

6 Diskussion

I detta kapitel avser vi diskutera det vi kommit fram till om myndigheternas användning av IT och deras förhållningssätt till medborgarna. Vi kommer även att ta upp en del moraliska betänkanden när det gäller de tjänster som myndigheterna lägger ut på Internet, samt användarnas attityder mot dessa. Slutligen går vi igenom de tekniker som vi redovisade i kapitel 5 och jämför hur de svarar mot vår kravlista.

6.1 Myndigheternas och medborgarnas användning

Det har gått trögt för myndigheterna vid utvecklingen av en 24-timmarsmyndighet och orsakerna har varit många. Man måste hitta en säker teknik med ett antal funktioner, skapa ett förtroende gentemot medborgarna och utbilda personal m.m. Den information myndigheter administrerar är såpass viktig att man inte kan ta några risker.

För att idén med e-tjänster ska fungera förutsätts i många fall att personen som använder tjänsten kan identifiera sig. Vår litteraturstudie har visat att detta kan göras med en digital signatur. Signaturen ska ha samma betydelse som den fysiska namnunderskriften och möjligheten för någon annan att kunna använda denna identifiering måste vara obefintlig. En annan förutsättning är att överföringen och lagringen av de elektroniska dokumenten är säker för att tjänsten ska fungera. Det får inte finnas någon möjlighet till manipulation av dokumenten utan att detta upptäcks.

För att de mer personliga tjänsterna inom e-demokratin ska vidareutvecklas anser vi att det måste bli enklare att skaffa sig en unik elektronisk identitet. Det bästa vore om EID och vårt vanliga ID-kort eller körkortet kunde kombineras så att där både finns en bild, personnumret och nyckeln för den elektroniska identifieringen. Detta har funnits som förslag från IT-kommissionen, men ytterligare framsteg med detta har vad vi erfar inte gjorts. Införandet av ett

sådant kort anser vi inte får medföra några större investeringar från medborgarnas sida vad gäller inköp av kringutrustning då detta skulle kunna utesluta stora delar av befolkningen och även hindra utvecklingen och spridningen av EID.

Tyvärr löser inte digitala signaturer problemen helt då mycket av säkerheten beror på hur informationen lagras efter det att det digitala dokumentet har fyllts i och skickats iväg. Som vi ser det lagras antingen hela formuläret som ett enda dokument och det är här de digitala signaturerna är användbara för autenticering. Delas däremot informationen upp och lagras i olika delar av en databas kan inte denna teknik tillämpas. Istället blir det här fråga om hur man på bästa sätt kan skydda själva databasen mot intrång för att förhindra manipuleringar, något som vi inte har tagit upp i denna uppsats.

För digitala bilddokument inom bl.a. polis- och sjukvårdsmyndigheten anser vi att vattenmärkning lämpar sig bättre än signaturer då här även finns möjlighet att återställa bilden till dess ursprungliga skick med hjälp av självinbäddade vattenmärken. Mycket beror självklart på syftet med och innebörden hos bilden. Prioriterar man säkerhet framför återställandet av originalbilden bör man kanske välja sköra vattenmärken för att kunna upptäcka minsta lilla förändring. För att alla myndigheter ska kunna autenticera de digitala dokumenten är det viktigt att de samarbetar. De som kommit längst bör hjälpa de andra och myndigheterna bör försöka dra lärdomar av varandra. Det är viktigt att man skapar gemensamma lösningar som alla kan använda sig av då kommunikationen mellan myndigheterna i framtiden kommer att öka. Vi anser därför att det är viktigt att Statskontoret fortsätter ta den samordnande rollen och ansvarar för hela utvecklingen av Sveriges e-demokrati.

Vi har under vår studie kommit fram till att bl.a. polisen är en av de myndigheter som bör kunna dra nytta av de lösningar vi tidigare redogjort för, då deras utredningsmaterial spelar en viktig roll för framtida beslut. De har även på senare år mer och mer börjat använda sig av digitalt material vid brottsplatsundersökningar och dylikt, vilket gör att de bör vara i behov av olika

lösningar för att autenticera digitala dokument. Detta gäller inte bara de dokument som kommer in från utomstående utan även deras eget material. Som polis kan man bli mutad eller hotad till att göra saker till andras fördel. Som exempel kan man ta en polisman som varit ute och tagit bilder på en brottsplats. Denne ska då inte ha möjlighet att på vägen till stationen ändra på något i bilden innan den kommer in i polisens eget datasystem. En lösning på detta problem hade kunnat vara att man i samband med att fotografiet tas, vattenmärker det med ett självinbäddat vattenmärke där hela bilden ingår för att kunna återställa den förvanskade bilden till dess ursprungliga original. Därefter kan man beräkna en checksumma som läggs in för att enklare kunna upptäcka samtliga förändringar. Tyvärr är detta än så länge inte möjligt eftersom det inte går att bädda in en hel bild, utan endast utvalda delar, i sig själv. Däremot är tekniken med checksummor en fungerande lösning som redan finns implementerad i ett flertal digitalkameror.

6.2 Moraliska aspekter

Vår uppsats visar på hur man behöver olika tekniker för att kunna säkerställa att ett digitalt dokument inte är förvanskat när dokumenten allt mer försvinner från den fysiska världen och flyttas till den digitala. Vi visar även på hur förtroende är en viktig del i 24-timmarsmyndigheten och hur man behöver dessa olika tekniker för att etablera detta förtroende i en digital miljö. Förtroendet kommer av att man genom de olika teknikerna känner sig säker på att den information man får eller de uppgifter man lämnar på nätet är korrekta och säkra. Dock måste det även finnas ett förtroende för teknikerna som sådana för att de ska fungera som en garant i nättransaktioner. Här uppstår ett problem som måste lösas. De tänkta användarna av en 24-timmarsmyndighet är gemene man, alltså varje svensk (i vårt fall), och för att gemene man ska tro på pålitligheten hos 24-timmarsmyndigheten behöver det utvecklas ett förtroende för de olika säkringsteknikerna som finns. En metod för detta kan vara att institutioner med redan uppbyggt förtroende ställer sig bakom de olika typerna av lösningar som presenteras. Ett bra exempel på detta är bankernas BankID-

tjänst, där flera stora och erkända banker ställt sig bakom en gemensam lösning för personidentifiering som redan i år använts för inkomstdeklaration på nätet.

Myndigheter har alltid en serviceplikt gentemot oss medborgare. Alla ska ha en möjlighet att kunna delta och utnyttja de tjänster som tillhandahålls. Myndigheternas användning av e-demokratin får därför inte skena iväg. Även om Sverige har en av de högsta siffrorna per invånare vad gäller PC-datorer i hemmen så finns här fortfarande en stor digital klyfta. Många menar ofta att den äldre generationen varken har kunskap eller intresse att följa med i den digitala utvecklingen och därför inte har en chans att kunna delta. För oss är den äldre generationen våra far- och morföräldrar, men det gäller inte bara denna generation. En stor grupp av människorna i åldrarna 40 år och uppåt har fortfarande ingen eller väldigt dålig kunskap om hur Internet fungerar. Trots att dessa människor så sakteliga börjar lära sig kommer det ta många år innan alla får så stort förtroende och förståelse för den digitala tekniken att de kan börja använda myndigheternas service på nätet. Vi anser därför att myndigheterna inte kan flytta över alla sina servicetjänster på Internet innan medborgarna är redo. För att alla fortsättningsvis ska kunna delta måste myndigheterna därför ha kvar delar av servicen på de fysiska kontoren.

Det är, enligt vår uppfattning, även viktigt att myndigheter och förvaltningar m.fl. kommer överens om en rimlig teknisk nivå för sina internetbaserade tjänster. Flera av de lite mindre datorintresserade som köpt en dator men som inte gjort så mycket mer har många gånger alltför gamla versioner av de nödvändiga programmen för att använda de tillgängliga tjänsterna. Skulle dessa medborgare uppdatera sina system kanske istället uppkopplingen är ett problem då dessa ofta har alldeles för långsam överföringshastighet. Vi menar därför att man inte ska vara tvungen att använda sig av de senaste versionerna och den snabbaste uppkopplingen för att kunna utnyttja e-tjänsterna. Självklart måste en del krav ställas av säkerhetsskäl, men det ska inte vara det senaste endast för att följa trenden. Det ska räcka med ett vanligt 56 kbit/s modem och ett äldre operativsystem. Även om datorer idag är relativt billiga så är de fortfarande dyra för dem som inte har så god ekonomi. Samma gäller för de

internetuppkopplingar som finns. Modem där du bara betalar taxan motsvarande ett vanligt telefonsamtal är fortfarande billigast men även långsamt. De elektroniska dokumenten och även myndigheternas hemsidor får därför inte innehålla för mycket information i kilobyte för att överföringen ska kunna ske inom rimlig tid.

Förtroendet för myndigheterna är alltså en av grundpelarna för e-demokratins fortsatta utveckling, men även en annan aspekt har kommit fram under arbetet med denna uppsats. Det är den etiska och moraliska aspekten i nättransaktioner. Det finns en ganska stor skillnad i attityd till att sätta sitt namn på ett papper och att signera en transaktion med ett musklick. I det förra fallet finns det en underförstådd aspekt av att man signerar något ”på heder och samvete” och själva processen där man tar fram pennan och skriver under pappret blir som en ceremoni där man synliggör sina handlingar; det hela blir en kulminering till underskriften. Där underskriften känns som en procedur känns ett musklick obetydligt. En normal datoranvändare som använder dator i sitt arbete utför flera hundra musklick per dag, då kan ännu ett för att acceptera en order eller signera ett dokument kännas obetydligt och t.ex. utan bevisvärde. Här finns med andra ord en risk för att användaren tar för lätt på de överenskommelser han ingår med sin digitala signatur och mer lättvindigt bryter dessa utan att tänka på konsekvenserna.

Det vi kommit fram till är att det måste till en attitydförändring, eller en upplysning om betydelsen av en digital underskrift och dess innebörd. Därtill kommer även det faktum att en generell uppfattning är att man har mindre förtroende för text som presenteras på en skärm än text som finns i ett fysiskt dokument. Principiellt borde det inte vara någon skillnad; förtroendet för texten bör bero på källan, inte på mediet, men så är inte alltid fallet idag. Man måste komma åt uppfattningen att en digital överenskommelse väger lättare än en vardaglig. Som vi sett i vår uppsats finns det inga rättsliga hinder för detta, utan bara attityder.

För att exemplifiera detta kan man titta på inlämningen av inkomstdeklarationen. När man i år kunde lämna in sin deklaration på elektronisk väg gjorde drygt 800 000 personer det medan man fortfarande kunde se folk som åkte förbi insamlingsställen i sina bilar och lämnade in deklarationen genom bilfönstret. På något sätt känns det tryggare att lämna in sin inkomstdeklaration till en okänd person genom bilfönstret än att skicka in den via Internet. Det kan finnas en tveksamhet att något verkligen händer när man klickar på skärmen medan det ger säkerhet att ha lämnat sitt papper till personen i reflexväst som lägger den i en tunna full av andra deklarationer.

6.3 Teknisk genomgång

De tekniker som vi beskrivit i kapitel 5 anses av de som utvecklat dem vara säkra och fullgoda metoder för att autenticera digitala dokument. Användningsområdena och funktionaliteten skiljer sig dock relativt mycket åt från teknik till teknik. Nedan kommer vi att diskutera teknikerna med avseende på de kriterier för användbarhet som vi tidigare ställt upp; säkerhet, funktionalitet, överförbarhet och implementerbarhet.

Säkerhet är en viktig del för de digitala dokumentens överlevnad. Avlägsna säkerheten och garantin till ett dokuments äkthet försvinner. Samma gäller för de tekniker vi presenterat. Avlägsna säkerheten och tilltron till de tekniker som används för autenticering försvinner. En teknik utan tilltro kommer aldrig att få stor spridning hos den breda allmänheten och därmed inte bli en vedertagen princip för autenticering. Vi menar att säkerheten är tudelad. Dels måste säkerheten gentemot attacker mot det skyddade dokumentet vara god och dels måste säkerheten gentemot attacker mot den använda skyddstekniken vara tillförlitlig.

Av de vattenmärkningstekniker vi studerat finns det inom samtliga områden implementeringar som har fullgott skydd mot attacker mot själva tekniken, d.v.s. attacker som vill förstöra eller avlägsna vattenmärket. Digitala signaturer

presenterar dock här ett stort problem, då signaturen och dokumentet är separerade. Signaturen och dokumentet måste alltid vara tillsammans för att en autenticering ska kunna ske. Detta kan medföra att signaturen lätt kan avlägsnas från dokumentet, vilket leder till att detta därmed inte längre kan garanteras vara autentiskt. Detta problem kan dock kringgås om dokumentet i fråga är av multimediatyp, då man i detta fall kan använda sig av ett borttagbart vattenmärke och bädda in signaturen i dokumentet. Alternativt fortsätter utvecklingen så att man kan skapa en ny fil som fungerar som ett elektroniskt kuvert i vilket man kan lägga ihop dokumentet och signaturen. Ett annat bekymmer vi ser gäller för steganografi, eftersom denna teknik kan tyckas säker då det stora syftet är att gömma undan dokumenten så att ingen kan se att de ens existerar. Så länge man väljer harmlösa skyddsobjekt som ingen kan tänkas vilja ändra i kan tekniken tyckas säker, men om någon gör stora ändringar i stego-objektet finns risken att det skyddade dokumentet inte går att extrahera. Detta anser vi vara ett stort säkerhetsproblem då man därmed förlorar de dokument man ämnat skydda.

Vad gäller attacker mot de skyddade dokumenten, såsom manipuleringar, kan åsikterna gå isär om vad som är en manipulering. Vi anser dock att bedömningen av vad som är en manipulation eller ej är alltför subjektiv och menar därför att samtliga förändringar av ett digitalt dokument är att betrakta som en otillåten manipulering Detta medför att vi anser att någon av de tekniker som inte tillåter komprimering och dylika informationsförlorande metoder är att föredra. Dessa är digitala signaturer, sköra vattenmärken och borttagbara vattenmärken. De övriga teknikerna som tillåter dylika operationer utgör ett fullgott skydd för autenticering på sitt sätt, men tillåter en viss grad av manipulation av dokumentet.

Funktionaliteten på de tekniker vi valt att redovisa skiljer sig relativt mycket åt från teknik till teknik. Digitala signaturer producerar ny information utifrån dokumentet som sedan bifogas, steganografi gömmer dokumentet bakom ett annat dokument och vattenmärkning gömmer information i dokumentet. Ingen av dessa tekniker kan dock förhindra att en manipulation sker, endast spåra att

en sådan har skett. Den ultimata lösningen hade varit om möjligheten till manipulation inte funnit överhuvudtaget. Det hade varit bra om man kunnat spara dokumentet i ett filformat som bara hade kunnat öppnas av ett specifikt program som bara tillät läsning av själva filen utan möjlighet att kringgå säkerhetsprinciperna. Någon sådan teknik har vi dock inte funnit.

Samtidigt skiljer sig teknikerna en hel del åt vad gäller hur de autenticerar ett digitalt dokument. Detta är något man måste ta i beaktande när man väljer vilken teknik man vill använda sig av. Vill man bara veta om ett dokument är manipulerat, eller vill man vet vad som har blivit manipulerat, eller till och med återställa dokumentet till en någorlunda bra version av hur dokumentet ursprungligen såg ut? Detta kan tyckas självklart. Man vill väl alltid återställa dokumentet? Det är dock dels en fråga om vilken dokumenttyp man ska autenticera, då lokalisering av manipulationer och återställning av dokumenten tyvärr ännu endast finns för multimediadokument och dels en fråga om säkerhet. Vid val av teknik måste man välja mellan att ha ett robust system och ett säkert. Möjligheten att återställa dokumentet minskar ju säkrare system man kräver och vice versa. Denna kompromiss mellan robusthet och säkerhet är något som måste tas i beaktande vid val av autenticeringssystem.

Att tekniken är användbar på alla typer av dokument är, enligt oss, att föredra. Med så många olika format som ett digitalt dokument idag kan vara sparat i är det omöjligt att hitta en teknik som kan användas på alla. Det är inte säkert att alla tekniker för att fastställa ett dokuments äkthet passar lika bra på alla typer av digitala dokument. Det har snarare visat sig att motsatsen gäller. Som vi ser det så kanske en teknik lämpar sig bättre än en annan för ett visst specifikt dokument, både när det gäller implementering och hur säker den är för just det dokumentslaget. Här ser vi ett stort minus för de olika vattenmärkesteknikerna då de, till skillnad från digitala signaturer och steganografi, i första hand är inriktade mot digital multimedia. Någon heltäckande teknisk lösning finns ej inom vattenmärkningsområdet. Digitala signaturer och steganografi kan å andra sidan användas till alla typer av dokument.

Av de tekniker vi gått igenom har vi funnit praktiska implementeringar till digitala signaturer och steganografi. Vattenmärkning är fortfarande på ett forskningsstadium och är ännu inte allmänt spritt. Detta har medfört att vi inte kunnat testa dessa tekniker på ett bra sätt. Vad vi dock har uppfattat av de olika teknikerna är att samtliga är enkla att använda. Steganografi har vi vissa betänkligheter mot vad gäller andra tillämpningsområden än överföringar. Det skulle vara svårt att ha en ordentlig struktur på sina filer om samtliga var inbäddade i olika skyddsobjekt. Att sedan packa upp och ner dokumenten varje gång man vill titta på eller arbeta med dem anser vi vara ett alltför krångligt arbetssätt.

Det är inte bara inom myndigheter behovet av att kunna autenticera digitala dokument finns. Även företag kan dra nytta av fördelarna med digitala signaturer, vattenmärkning och steganografi. Den allmänna uppfattning vi fått när vi studerat de olika tekniker som vi tidigare redovisat är att det inte finns någon optimal lösning till autenticeringsproblemet. De tekniker som finns är bra inom sitt gebit, men alla har sina för- och nackdelar. Digitala signaturer lämpar sig t.ex. bättre vid avtal än vad steganografi gör. Steganografi kan i stället användas för att företagshemligheter inte ska komma ut och vattenmärkning för att autenticera digitala bilder. Vid valet av teknik måste man därför, menar vi, anpassa sig till de speciella behov man har för att på detta sätt avgöra vilken teknik som är den ultimata för just den situationen.

7 Slutsats

Vi har under vårt forskningsarbete kommit fram till att det finns ett antal tekniker för att autenticera digitala dokument. De uppfyller dock inte alla de krav som vi anser bör ställas på en teknik för detta ändamål. Vi menar därför att ytterligare forskning och utveckling inom området kommer att behövas för att framställa en teknik som dels klarar de säkerhetskrav som finns och dels kan användas på samtliga typer av digitala dokument.

Den teknik som har störst utbredning ser vi som digitala signaturer, som även är den teknik som svenska myndigheter idag använder sig av. Även steganografi har en viss spridning och flera implementeringar finns på marknaden. Digital vattenmärkning är fortfarande på ett forskningsstadium och har idag en begränsad användning inom stora forskningsföretag.

Genom att använda sig av någon av de tekniker vi redovisat i denna uppsats kan man fastställa om ett digitalt dokument är ett original. Dock har alla tekniker, digitala signaturer, steganografi och digital vattenmärkning både för- och nackdelar. Vi menar därför att man vid val av teknik noggrant måste välja vilken teknik man vill använda sig av till den situation man befinner sig i.

I och med införandet av 24-timmarsmyndigheter i vårt samhälle ser vi ett ökande behov av dessa tekniker, då kommunikationen och dokumentöverföringen mellan myndighet och medborgare, i framtiden, allt mer kommer att öka. Utan säkra tekniker mot manipulering kommer inte denna dokumentöverföring att kunna ske på ett tillfredsställande sätt, både vad gäller medborgarnas förtroende för myndigheternas tjänster och vad gäller myndigheternas behov av att dokumenten är oförfalskade.

8 Referenser

Böcker:

Alling-Ode, B, Tubin, E. (1993). *Falska kort? Bilden i dataåldern*. Emmaboda: Styrelsen för psykologiskt försvar.

Bjurwill, C. (1995). *Fenomenologi*. Lund: Studentlitteratur.

Cox, I.J., Miller, M.L., Bloom, J.A. (2002). *Digital Watermarking*. San Fransisco: Morgan Kaufmann Publishers.

Easterby-Smith, M., Thorp, R., Lowe, A. (1991). *Management Research – An Introduction*. London: SAGE Publications Ltd.

European Commission. (2001) *Digital signatures: A survey of law and practice in the European Union,* Cambridge: Woodhead Publishing Limited.

Katzenbeisser, S, Petitcolas, F. A. P. (2000). *Information hiding. Techniques for steganography and digital watermarking*. Norwood: Artech House Inc.

Nydén, M. (2000). *Myndigheter, internet och integritet,* Stockholm: Styrelsen för psykologiskt försvar.

Patel, R., Davidson, B. (1991). *Forskningsmetodikens grunder,* Lund: Studentlitteratur.

Ritchin, F. (1991) *Bildens förändrade värld*, Stockholm: Journal Mediaproduktion.

Artiklar och rapporter:

Barni, M. Bartolini, F. Cappellini, V. Piva, A. (1998). *A DCT-domain system for robust image watermarking.*
[Internet] URL: http://lci.det.unifi.it/Publications/sp98.zip

Ekici, Ö., Coskun, B., Naci, U., Sankur, B. (2001) *Comparative Assessment of Semi-Fragile Watermarking Techniques*.
[Internet] URL:
http://www.busim.ee.boun.edu.tr/~sankur/SankurFolder/SPIE_Denver.pdf

Eggers, J.J., Su, J.K., Girod, B. (2000). *A blind watermarking scheme based on structured codebooks*.
[Internet] URL: http://www.lnt.de/~eggers/texte/SIIA_paper.pdf

Eggers, J.J., Girod, B. (2001). *Blind Watermarking applied to image authentication*
[Internet] URL: http://www.lnt.de/~eggers/texte/icassp01.pdf

Fridrich, J., (1999). *Methods for Tamper Detection in Digital Images*.
[Internet] URL:
http://www.ws.binghamton.edu/fridrich/Research/acm99.doc

Fridrich, J., Goljan, M. (1999). *Protection of digital images using self embedding*.
[Internet] URL:
http://www.ws.binghamton.edu/fridrich/Research/nj_may14.doc

Fridrich, J., Goljan, M., Du, R. (2001). *Invertible Authentication*.
[Internet] URL:
http://www.ws.binghamton.edu/fridrich/Research/InvertibleAuthentication01.doc

Fridrich, J. (2002). *Security of Fragile Authentication Watermarks with Localization*
[Internet] URL:
http://www.ws.binghamton.edu/fridrich/Research/authentication.doc

Grönlund, Å. (2001). *En introduktion till Electronic Government*.
ur: Grönlund, Å, Ranerup, A. (2001). *Elektronisk förvaltning, elektronisk demokrati: Visioner, verklighet, vidareutveckling*. Lund: Studentlitteratur.

Holliman, M., Memon, N. (2000). *Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes*.
[Internet] URL: http://isis.poly.edu/memon/pdf/publi_countr_wtrmrk.pdf

IFCC (2003) *IFCC 2002 Internet Fraud Report*.
[Internet] URL: http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf

IT-rättsliga observatoriet. (2001). *Digitala dokuments bevisvärde, skrivelse till IT-kommissionen*.
[Internet] URL:
http://sirnet.metamatrix.se/material/Hearing/dig_dokument_0102.pdf

Johnson, N.F., Jajodia, S. (1998) *Exploring Steganography: Seeing the Unseen*.
[Internet] URL: http://www.jjtc.com/pub/r2026.pdf

Ko, H.H., Park, S.J. (2002). *Semi-Fragile Watermarking for Telltale Tamper Proofing and Authenticating*.
[Internet] URL:
http://www.kmutt.ac.th/itc2002/CD/pdf/17_07_45/WP2_OD/2.pdf

Lenk, K., Traunmüller, R. (2002). *Electronic Government: Where are we heading?*
ur: Lenk, K., Traunmüller, R. (2002). *EGOV 2002, LNCS 2456*, s. 1-9. Berlin: Springer-Verlag.

Lin, C-Y., Chang, S-F. (1999). *Issues and Solution for Authenticating MPEG Video*
Ur: SPIE (1999) *Proceedings of SPIE Vol. 3657, Security and Watermarking of Multimedia Contents, Ping Wah Wing, Edward J. Delp, Editors,* pp. 54-65. Washington: SPIE.

Lin, C-Y., Chang, S-F. (2000). *Semi-Fragile Watermarking for Authenticating JPEG Visual Content*

Ur: SPIE (2000) *Proceedings of SPIE Vol. 3971, Security and Watermarking of Multimedia Contents II, Ping Wah Wing, Edward J. Delp, Editors,* pp. 140-151. Washington: SPIE, 2000.

Lin, C-Y., Chang, S-F. (2001). *SARI: Self-Authentication-and-Recovery Image Watermarking System.*
[Internet] URL: http://www.ctr.columbia.edu/~cylin/pub/acmmm01demo-sari.pdf

Lin, E.T., Delp, E.J. (1999). *A Review of Fragile Image Watermarks.*
[Internet] URL: ftp://skynet.ecn.purdue.edu/pub/dist/delp/acm99/paper.pdf

Lin, E. T., Podilchuk, C. I., and Delp, E. J. (2000). *Detection of Image Alterations Using Semi-Fragile Watermarks*
Ur: SPIE (2000) *Proceedings of SPIE Vol. 3971, Security and Watermarking of Multimedia Contents II, Ping Wah Wing, Edward J. Delp, Editors,* pp. 158-163. Washington: SPIE.

Lindkvist, T. (2001a) *Steganografi – en översikt.*
[Internet] URL: http://www.cs.kau.se/~stefan/IW/Tina.pdf

Pichon, E., Niethammer, M., Sapiro, G. (2003) *Color histogram equalization through mesh deformation.*
[Internet] URL: http://www.ima.umn.edu/preprints/jan2003/1906.pdf

Rey, C. & Dugelay, J. (2000). *Blind detection of malicious alternations on still image using robust watermarks.*
[Internet] URL: http://www.eurecom.fr/~image/PS/rey-dugelay-IEE00.pdf

Rikspolisstyrelsen, (2000) *Rapport angående elektronisk identifiering.* Stockholm: Rikspolisstyrelsen.

SOU 1999:12. *Elektronisk demokrati.* Stockholm: Fakta Info Direkt, 1999.

Statskontoret 2000:7. *Infrastruktur för säker elektronisk överföring till, från och inom statsförvaltningen*. Stockholm: Statskontoret.

Statskontoret 2000:21. *24-timmarsmyndighet – Förslag till kriterier för statlig elektronisk förvaltning i medborgarnas tjänst*. Stockholm: Statskontoret.

Statskontoret 2002:30. *Utveckling av 24-timmarsmyndigheter – lägesrapport december 2002*. Stockholm: Statskontoret.

Statskontoret 2002:108. *Utveckling av 24-timmarsmyndigheter – lägesrapport juni 2002*. Stockholm: Statskontoret.

Su, J.K., Hartung, F., Girod, B. (1999). *Digital Watermarking of text, image, and video documents*.
[Internet] URL: http://www.cg.cs.tu-bs.de/v3d2/pubs/diwa-shg98.pdf

Tirkel, A.Z., Rankin, G.A., van Schyndel, R.M., Ho, W.J., Mee, N.R.A., Osborne, C.F. (1993). *Electronic Water Mark*.
[Internet] URL: http://goanna.cs.rmit.edu.au/~ronvs/papers/DICTA93.PDF

van Rossum, M., Chauvel, D., Mangham, A. (2002). *BRAINCHILD, Building a Constituency for future research in Knowledge Management for Local Administrations*.
ur: Lenk, K., Traunmüller, R. (2002). *EGOV 2002, LNCS 2456*, s. 26-32. Berlin: Springer-Verlag.

Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M. (2002). *Encouraging citizen adoption of e-government by building trust*.
[Internet] URL: http://www-scf.usc.edu/~pavlou/WarGefPavRosEM.pdf

Westholm, H. (2002). *e-Democracy goes ahead. The Internet as a tool for improving deliberative policies?*
ur: Lenk, K., Traunmüller, R. (2002). *EGOV 2002, LNCS 2456*, s. 240-247. Berlin: Springer-Verlag.

Yin, K. Pan, Z. Shi, J. Zang, D. (2001). *Robust mesh watermarking based on multiresolution processing.*
[Internet] Tillgänglig på: http://www.sciencedirect.com

Östberg, O. (2003) *PM - Lärdomar inför Sveriges fortsatta strävanden att etablera nätverkssamverkande 24-timmarsmyndigheter*. Stockholm: Statskontoret, 2003.

Uppsatser och avhandlingar:

Götberg, O., Smith, H. (2000) *Feature Based Digital Watermarking for Images,* Magisteruppsats. Göteborg: Chalmers tekniska högskola.

Lindkvist, T. (2001b). *Fingerprinting of digital documents*. Doktorsavhandling. Linköping: Linköpings universitet.

Internet:

Altavista. (2003). URL: http://www.altavista.com

Bibliotek. (2003). URL: http://www.bibliotek.se

CiteSeer. (2003). URL: http://citeseer.nj.nec.com

Google. (2003). URL: http://www.google.com

Gunda. (2003). URL: http://www.ub.gu.se/gunda

Libris. (2003). URL: http://www.libris.kb.se

Nationalencyklopedien. (2003). URL: http://www.ne.se

ScienceDirect. (2003). URL: http://www.sciencedirect.com

Bilaga 1 - Definitioner

Autenticering/verifiering - Autenticering är enligt oss då man på ett tillförlitligt sätt säkerställer att ett digitalt dokument inte är manipulerat.

Bitmap - En standard för okomprimerade digitala bilder.

CA - Certification Authority. Ett företag eller en myndighet som fått förtroende att utfärda elektroniska identifikationer. Detta kan jämföras med hur Posten och olika banker får utfärda giltiga identitetskort i Sverige.

Checksumma - Se hashvärde.

DCT - Discrete cosine transform är en omfattande matematisk process, vilken konverterar informationen i ett 8x8 pixlar stort bildblock från den spatiala domänen till frekvensdomänen. All information om den övre vänstra pixelpunkten, vilken kallas DC-komponenten lagras medan man för nästa pixel endast lagrar information om skillnaden mellan den aktuella pixeln och DC-komponenten. På samma vis behandlas resterande pixlar i resten av blocket. Dessa pixlar kallas AC-komponenter. DCT-beräkningen resulterar i en matris av spektrala koefficienter, kallad ett DCT-block, vilken beskriver bildblocket med hjälp av frekvenser. Matrisen är arrangerad som så att de låga frekvenserna samlats i övre vänstra hörnet av matrisen och de höga frekvenserna i nedre högra hörnet[30].

[30] http://data.uta.edu/~telemm/slides/pdf/M4/M4L1.pdf

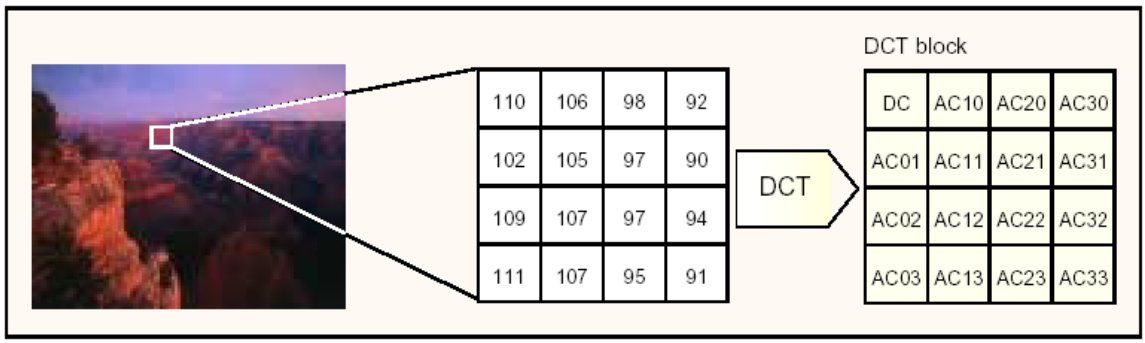


Bild A: Förenklad bild av vad som händer vid DCT-beräkning. Observera att beräkningen sker på ett 8x8 pixlar stort block och inte på ett 4x4 pixlar stort[31].

Detektor - Ett för en vattenmärkesteknik specialdesignat program som extraherar ett vattenmärke ur ett digitalt dokument.

Digital signatur - En teknik för transaktionssäkerhet för digitala dokument, baserad på asymmetrisk kryptering. Se kapitel 5.1.

Digitalt dokument - Ett digitalt dokument betecknar vi som en handling som är lagrad på ett digitalt medium. Till detta räknar vi även textfiler, multimediafiler och dylikt såsom ifyllda webbformulär.

EID - Elektronisk identifikation. Ett sätt att identifiera sig i elektroniska transaktioner, t.ex. med hjälp av en privat krypteringsnyckel. Också en benämning på ID-kort där sådana nycklar är integrerade.

Elektroniskt kuvert - En filtyp i vilken flera filer kan läggas samman. Existerande exempel på elektroniska kuvert kan t.ex. vara en zip-fil[32].

[31] http://www.ite.mh.se/~love/magister/uppsatser/jessica.pdf

[32] Se http://www.winzip.com för exempel på implementering.

Filtrering - En signalbehandlingsteknik vilken syftar till att filtrera bort information ur en digital bild för att t.ex. erhålla bättre eller sämre skärpa (Cox et al., 2002).

Frekvensdomänen - Den representation av en bild som innehåller information om densamma i form av spektrala frekvenser.

Hashvärde - En hashfunktion är en beräkningsalgoritm som omvandlar en variabel mängd data till ett värde av fix längd t.ex. 128 bitar. Värdet kallas hashvärde, hashsumma, checksumma, fingeravtryck m.m. Hashfunktioner gör det möjligt att på ett effektivt sätt skapa digitala signaturer på stora meddelanden genom att komprimera innehållet till en hanterbar mängd. Hashfunktionen skall skapa ett hashvärde från ett meddelande så att det med utgångspunkt från meddelandet är lätt att beräkna hashvärdet, men med utgångspunkt från hashvärdet är omöjligt att beräkna fram det ursprungliga meddelandet, samt att det med utgångspunkt från meddelandet är omöjligt att ta fram ett annat nytt meddelande som genererar ett identiskt hashvärde. De vanligaste hashfunktionerna är MD2, MD5 och SHA-1[33].

Histogramutjämning - En bildbehandlingsteknik för att öka bildens kontrast genom att stärka intensiteten i bildens pixlar (Pichon et al., 2003).

Gaussiskt brus - En additiv störsignal i digital media. Sådana störningar kan vara en effekt av att t.ex. en ljudsändning går över en radiokanal eller en videosändning sänds över ett analogt TV-nät (Cox et al., 2002). Detta på grund av elektriska rörelser i kommunikationskanalen[34]. Även kallat vitt brus.

[33] http://naring.regeringen.se/propositioner_mm/pdf/ds9814.pdf

[34] http://www.computeruser.com/resources/dictionary/

Informationsförlorande komprimering - Viss information förloras vid komprimering. Ofta är det så att komprimeringen inte ändrar hur betraktaren uppfattar innehållet i t.ex. en bild. Denna typ av komprimering är dock inte lämplig för textfiler då innehållet i dokumentet faktiskt ändras.

JPEG - Joint Photographic Experts Group. En standard för komprimering av digitala stillbilder[35].

Kvantisering - Kvantisering är en informationsförlorande komprimerings-metod som genomförs på resultatet för DCT-beräkningen för att reducera antalet bitar som bildblocket består av. Varje koefficient i DCT-blocket divideras med konstanter som bestäms av en kvantiseringstabell innehållande 8x8 värden. Ett värde för varje cell i DCT-blocket. Efter division och avrundning är många av koefficienterna för de höga, för ögat omärkbara frekvenserna i DCT-blocket lika med noll. Detta medför att datamängden med hjälp av olika matematiska metoder kan ytterligare reduceras[36].

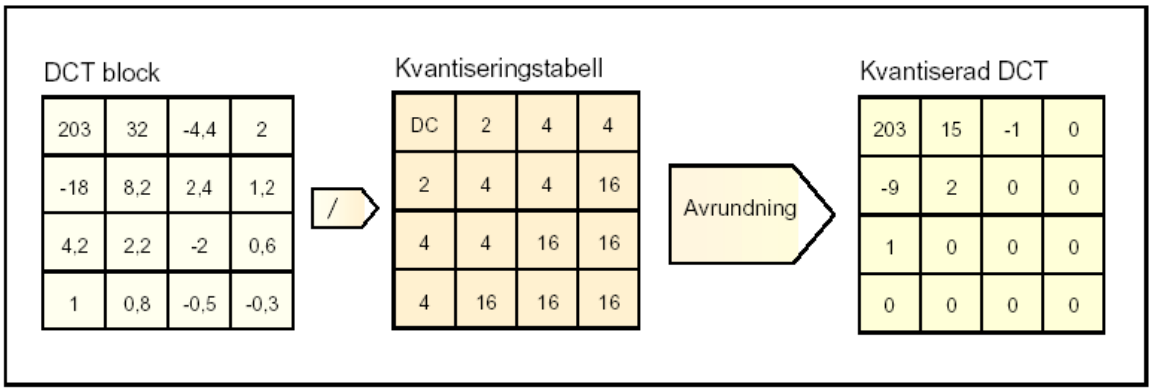


Bild B: Exempel på en kvantisering av ett DCT-block. Observera att beräkningen sker på ett 8x8 pixlar stort block och inte på ett 4x4 pixlar stort[7].

[35] http://www.jpeg.org

[36] http://www.ite.mh.se/~love/magister/uppsatser/jessica.pdf

LSB - Least significant bit. I en binär kod är LSB den bit eller bitposition i koden som representerar den minsta mängden data som kan representeras av koden. LSB är den bit som har minst vikt i koden.

Lågpassfiltrering - En form av *filtrering* vilken låter samtliga frekvenser under en viss specificerad frekvensgräns passera filtret, men som försvagar högre frekvenser[37]. Detta kan t.ex. användas till att simulera VHS-inspelning av en digital film (Cox et al., 2002).

Manipulerat dokument - Ett manipulerat dokument definierar vi som ett digitalt dokument där innebörden ändrats genom att betydande information tillförts eller tagits bort från det ursprungliga originalet.

MPEG - Moving Picture Experts Group. En standard för komprimering av digitala ljud- och filmsekvenser[38].

MSB - Most significant bit. I en binär kod är MSB den bit eller bitposition i koden som representerar den största mängden data som kan representeras av koden. MSB är den bit som har störst vikt i koden.

Nyckel - information, vanligen en sekvens av slumpmässiga siffror, som används för att kryptera eller dekryptera elektroniska signaler.

Pixel - Den minsta enhet som kan beskrivas i en digital bild. Pixeln har en ljusstyrka, position och eventuellt en färg.

PKI - Public Key Infrastructure. Ett begrepp som brukar användas för den infrastruktur som krävs för tillämpningar av säkerhetsfunktioner baserade på kryptering med öppna och privata nycklar.

[37] http://www.its.bldrdoc.gov

[38] http://www.mpeg.org

Spatiala domänen - Den representation av en bild som innehåller värden som representerar intensitet och färg, för ett antal pixlar.

Steganografi - En teknik för att gömma information man vill hålla hemlig inuti annan information. Se kapitel 5.2.

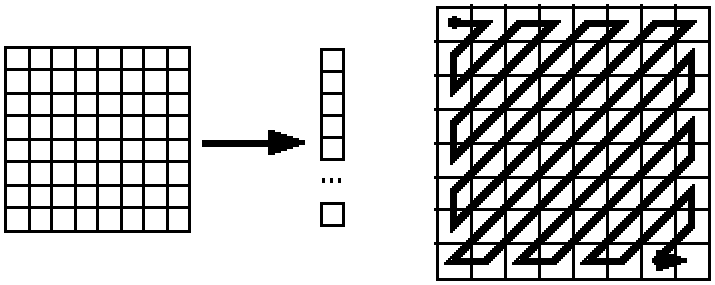
Vattenmärke - En teknik för att oupptäckbart förändra ett verk för att bädda in ett meddelande om verket. Se kapitel 5.3.

XOR - Exclusive OR. En binär logisk operation enligt följande tabell:

Input A	Input B	Output C
0	0	0
1	0	1
0	1	1
1	1	0

Tabell A: Sanningsvärdestabell för XOR-beräkning.

Zig-zag scan - Det mänskliga ögat är mer känsligt för de låga frekvenserna än de höga frekvenserna. Syftet med en zig-zag scan är att gruppera lågfrekventa koefficienter i en kvantiserat DCT-block i början av en vektor och högfrekventa i slutet av vektorn.



Figur A: Zig-zag scan av en 8x8 frekvensmatris till en 1x64 vektor[39]

[39] http://www.cs.cf.ac.uk/Dave/Multimedia/node238.html

Bilaga 2 - Sökord

Följande sökord och olika böjningar av dem (t.ex. autenticera, autenticering) har vi använt oss under våra litteraturstudier.

- Dokument / digitala dokument / digital document
- Autenticering / authenticity
- Manipulering / bild manipulering / förvanskning
- e-demokrati / elektronisk demokrati / digital demokrati / e-democracy / elektronic democracy / digital democracy / e-gov
- 24 – timmarsmyndigheten
- förtroende / tillförlitlighet / trust
- Vattenmärkning / digital vattenmärkning / watermarking / digital watermarking
- Robust vattenmärke / robust vatermarking / sköra vattenmärken / fragile watermark / halvsköra vattenmärken / semi-fragile vatermark / self-embedded watermark
- Digitala signaturer / digital signatures
- Steganografi / steganography
- Verifiera