Digital vattenmärkning

- Utvärdering av befintliga metoder för synlig digital vattenmärkning av statiska bilder

LUNDS UNIVERSITET
Lunds Tekniska Högskola

LTH Ingenjörshögskolan vid Campus Helsingborg
Datateknik

Examensarbete:
Tobias Bengtsson

LTH Ingenjörshögskolan vid Campus Helsingborg
Lunds universitet
Box 882
251 08 Helsingborg

LTH School of Engineering
Lund University
Box 882
SE-251 08 Helsingborg
Sweden

Tryckt i Sverige
Media-Tryck
Biblioteksdirektionen
Lunds universitet
Lund <2012>

Sammanfattning

Syftet med examensarbetet är att göra en utvärdering av befintliga metoder för synlig digital vattenmärkning av statiska bilder för att undersöka dessa metoders funktionalitet.

Undersökningen behandlar följande punkter:

- Robust och fragil vattenmärkning.
- Detektering av dessa vattenmärkningar.
- Attacktyper såsom olika former av bildtransformation och editering.
- Möjligheter att kontra dessa attacker.
- Lagliga aspekter rörande upphovsrätt .
- Vad färgkanaler är och hur dessa utnyttjas vid vattenmärkning
- Hur en bilds kvalité och kvalitén på vattenmärkningen kan påverka resultatet av skyddet som vattenmärkningen ger.
- En undersökning av vilka metoder för synlig vattenmärkning som finns tillgängliga i nuläget.
- Grunderna för hur metoderna fungerar och för vilka ändamål dessa metoder är menade att användas.

Informationen ovan användes sedan för teoretiska scenarion som påvisar fördelar och brister med de undersökta metoderna. Slutligen ska en utvärdering göras med hänsyn till nedanstående punkter:

- Är metoderna lämpade att användas för de ändamål de används?
- Bästa vattenmärke i syftet att stoppa en viss typ av attacker.
- Kan alla typer av attacker kan förebyggas och är det värt kostnaden att investera i en dyrare lösning?
- Är det möjligt eller relevant att utveckla en ny typ av vattenmärkning?

Dessa frågeställningar resulterar slutligen i ett resonemang kring varför monoton transparent vattenmärkning är den mest optimala typen av vattenmärkning och varför en utveckling av en ny metod inte utfördes.

Nyckelord: Digital, Vattenmärkning, Utvärdering, Bilder

Abstract

Digital watermarking is done by adding a piece of data to a signal, which depending on the target media type may be a picture, audio or video signal. The purpose of this additional signal is to provide a consistent signature linked to the original source which then remains through the act of copying. This allows the author to obstruct the act of theft by adding this signal to his or her creation. This report will focus on information regarding the visual watermarking of static visual images. There are several aspects to be considered when applying this kind of watermarking.

There are two kinds of watermarking, robust and fragile. Despite the fact that both of these types are intended to work with the same purpose in mind they achieve this through different means. Detection is also a vital factor when speaking of digital watermarking. This is because if you lack the possibility to detect your watermark, it might not be enough in legal disputes for you to be proclaimed the author. Malicious attacks will always exist and to prevent these kinds of attacks, it is vital to have knowledge about how these attacks work, how to prevent them and if that is not possible, add an obstruction that makes the process of removing considerably harder.

Using the information above I produced a collection of information where the methods for watermarking are evaluated. The conclusions explain why it's not possible to set one specific method as the one best solution. Some information is also included that explains why the monotone transparent method is most adaptable, if you have to make a pick. Finally I explain why I did not proceed to create a new method for visible watermarking.

Keywords: Digital, Watermarking, Evaluation, Pictures.

Förord

Detta examensarbete har skrivits under våren och hösten år 2011 och är en del av Högskoleingenjörsutbildningen inom datateknik på Lunds Universitets i Helsingborg, Campus Helsingborg.

Arbetet med denna uppsats har varit upplysande och jag har fått en djupare förståelse för hur många faktorer som spelar in i samband med produktionen av synliga digitala vattenmärken.

Jag vill även tacka författare av de referenser som funnits tillhanda, deras verk var den källa som behövdes för att undersöka detta problem.

”Detta examensarbete är dedikerat till de vänner och familjemedlemmar som stöttat mig på livets väg.”

- Tobias Bengtsson

Innehållsförteckning

1 Inledning

Bakgrund

Många av dagens digitala artister vill liksom alla sina föregångare få sina verk bedömda av personer för att få kritik och reflektioner kring sina verk. Tack vare Internet är det möjligt för gemene man att utan större bekymmer lägga upp sina verk för visning. Dock har denna lättillgängliga visningsmonter ett pris. Dessa verk kan lätt kopieras av personer som lägger upp dem på en annan webbplats och utger sig för att själva ha skapat dem. Även välmenande personer som fattat tycke för bilden kan använda den som en del av dekorationen på en egen webbplats. Oavsett bakgrunden till denna kopiering är det likväl ett bekymmer då personen som är den egentliga upphovsmannen till bilden fått sitt verk stulet.

Självfallet finns det individer som vill sprida sina verk på detta sätt. De påverkas inte i någon större utsträckning av denna kopiering, men de som ämnar att sälja sina verk har stora besvär med illegal kopiering av dessa. Det är inte heller alltid som det slutar vid kopiering, ty med hjälp av bildediteringsverktyg såsom Photoshop kan man med enkelhet foga samman bilder, lägga till effekter som påverkar bildens datastruktur eller på annat vis ändra bilden. Denna förändring leder till att personen som nu förändrat bilden kan ses som skapare av den nya bilden, eftersom det nu saknas bevis för att den manipulerade bilden ingår i den nya. Därefter kan den distribueras utan att manipulatören löper någon som helst risk för rättsliga påföljder.

Digital vattenmärkning, principen

För att förhindra eller åtminstone försvåra denna form av vandalism och stöld används digital vattenmärkning [Ref. 5]. Precis som sin analoga förlaga är poängen med digital vattenmärkning att lägga till extra information som ska påvisa objektets äkthet samt förhindra kopiering. Denna extra information lagras som en del av originalet. Generellt för all vattenmärkning gäller att man har ett objekt A, som man avser att skydda. Genom att sedan lägga till en signal på objekt A erhåller man ett objekt med en signal som kopplar samman objekt A med en viss upphovsman.

I fallet med presentation av verk på nätet sker detta genom att lägga till ett ytterligare lager ovanpå det ordinarie mediet som innehåller information som binder objektet till skaparen [Ref. 4].

I samband med bilder innefattar detta oftast att upphovsmannen lägger ett halvt transparent bildlager, föreställande en logo eller signatur, ovanpå

ordinarie bild. Dessvärre är denna metod långt ifrån säker om man vill skapa en vattenmärkning som är svår att ta bort. Anledning till att denna metod kan ses som otillräcklig är bland annat följande. Utvecklingen av bildbehandlingsprogram går i rasande fart. På samma sätt som de fina funktioner som tar bort diverse skavanker på bilder kan programmet ta bort vattenmärkningar om de inte är tillräckligt avancerade [Ref. 5].

Eftersom ett transparent överlappande lager kan ses som en blekning av det undre lagret kan skillnaderna i färgnivåerna enkelt uppmätas och förändras.

Faktorer att ta hänsyn till

Kvalitén på en digital vattenmärkning kan bero på flera faktorer och dessa faktorer är olika relevanta beroende på objektet som ska skyddas. Faktorer som bildens och vattenmärkningens visuella kvalité och eventuella hotbilder för den specifika produkten är bara några exempel på faktorer som kan påverka skyddets stabilitet och effekt [Ref. 4]. Det är också viktigt att ta hänsyn till vad vattenmärket ska användas till vid design av ett vattenmärke.

Det finns även rent praktiska problem med en vattenmärkning. Synlig vattenmärkning har det problemet att det skapar en störing i den visuella upplevelse som man vill förmedla med bilden. Osynlig vattenmärkning har sina egna problem. Detta gäller i synnerhet om man vill skydda den visuella informationen. Eftersom skyddet just är osynligt finns det inget som förhindrar manipulation och redigering av bilden och problemet med att bilder förändras och återpubliceras under annat namn kvarstår.

Problemformulering

Kan ett vattenmärke skapas på sådant vis att det går att tillämpa för alla typer av bilder och är detta vattenmärke i så fall ett skydd som som är likvärdigt för alla dessa bilder? Kommer detta skydd att vara tillräckligt för att en person med avsikt att avlägsna/förstöra vattenmärket, ska bedöma skyddet som ett tillräckligt stort hinder för att låta bli att försöka utnyttja bilden?

Rapporten utvärderar de metoder som finns tillgängliga för att skydda digitala bilder med hjälp av synlig digital vattenmärkning i syftet att presentera metodernas effekter och optimala användningsområden. I anslutning till denna utvärdering kommer ytterligare information inhämtas kring hur man bör gå tillväga för att tillverka ett vattenmärke som ger största möjliga skydd. Vad som också kommer att vara en viktig faktor att ta hänsyn till, är att vattenmärket inte förstör den visuella upplevelsen. Kort sagt att skydd/kostnad-kvoten inte är för stor.

Den visuella upplevelsen är en individuellt beroende faktor, men i denna rapport innebär en god visuell upplevelse att hela bilden ska synas och inget ska vara 100% övertäckt.

Rapporten ska även innehålla en analys av de attacker som kan förkomma mot vattenmärkningar för att ge en insikt i hur dessa attacker kan försvåras eller förhoppningsvis förebyggas.

Ytterligare aspekter som behandlas är detektering av vattenmärken och viss information om bildernas struktur.

Detekteringen krävs för att kunna bevisa ett vattenmärkes förekomst. Information kring detta är relevant för att analysera om de visuella metoder som används är tillräckliga för att bevisa en upphovsrätt till materialet.

Ovanstående faktorer analyseras för att bestämma vilken metod som är lämpligast för ett visst problem och varför det är så. Analysen klargör också de problem som uppstår kring dessa lösningar och teorier kring om dessa problem är relevanta att lösa och om så är fallet tillvägagångssättet för detta. Detta förklaras ytterligare genom exempelscenarion.

Metodik

Informationshämtning

De första veckorna med detta arbete kommer att ägnas åt informationshämtning kring vattenmärkning och metoder för vattenmärkning. Informationen behöver innehålla fakta kring följande ämnen:

- Eventuell benämning av metoder för vattenmärkning
- Användningsområde
- Hur metoden fungerar och hur metoden påverkar bilden
- Hur metoden påverkas av attacker, vilka attacker som metoden är resistent respektive svag mot.
- Lagliga aspekter rörande upphovsrätt och vattenmärkning
- Bildkvalité och dess inverkan på vattenmärkningar

Analysmomenten

Analysmomenten är flera, men ska inledas med att först ge en grundläggande förståelse för hur vattenmärkning fungerar och hur man kan använda vattenmärkning. Därefter påbörjas fördjupningsarbete för att förstå hur detektering fungerar.

Den inhämtade informationen används till att granska de typer av attacker som finns. Denna granskning innebär att djupare förståelse fås kring de olika sätt som ett vattenmärke kan förändras. Vidare kommer det vid detta tillfälle även vara nödvändigt att studera delar av Sverige rikes lag för att klargöra vad som egentligen är tillåtet att göra med digitala bilder.

Därefter behövs förståelse för hur bilder är uppbyggda. Därför ska begrepp som luminositet, mättnad, färgkanaler, färgspektra, kontraster och dylikt studeras.

När all ovanstående information är samlad ska detta sedan utnyttjas för att granska de metoder som finns.

Bilder

Samtliga bilder i rapporten, med undantag av Lunds Universitets Sigill är fotograferade, omarbetade och tecknade av undertecknad.

Exempelscenarion

Alla de föreliggande analysmomenten kommer dessutom att ge upphov till exempelscenarion. Dessa scenarion ska innehålla ett exempel på en vattenmärkt bild. Därefter ska dessa vattenmärkningar analyseras med hjälp av den tidigare vunna kunskapen. Detta för att ge en tydligare insikt i hur dagens vattenmärkning fungerar och hur den kan förbättras.

Slutsatser

Som en avslutning finns ett stycke med slutsatser kring arbetet. Dessa slutsatser innefattar vad som är allra viktigast att ta hänsyn till vid vattenmärkning och varför det är fallet.

Avsnittet kommer även innehålla reflektioner kring vad som kunde gjorts annorlunda.

Källkritik

Nedanstående källor är de som använts som informations under examensarbetet. Fler tryckta verk har undersökts, men visat sig innehålla samma information. De verk jag valde att utnyttja var de verk som fördjupade sig i vattenmärkning.

Webbkällorna som användes valde jag att använda eftersom de innehöll information utöver den information som fanns i tryckt format.
[1] Watermarking

http://www.angelfire.com/electronic/kfrank/water/index.html
Denna källa uppfattades inte först som en pålitlig källa, men efter att ha prövat de nämnda teorierna i bildhanteringsprogram och funnit att de fungerade som nämnt i källan, användes denna information

[2] Sveriges lag på nätet
https://lagen.nu/1960%3A729
Sverige rikes lag anses vara en pålitlig källa. Källan ska utnyttjas för att reda ut problem i samband med upphovsrätt.

[3] Steganography And Digital Watermarking
http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf
Finns på University of Birminghams hemsida. Källan har upprättats i syfte att undersöka steganografi. Bakgrundsinformationen i rapporten innehåller information om hur man kan dölja och lagra extra information i objekt såsom bilder.

[4] Techniques and applications of digital watermarking and content protection Av Michael Konrad Arnold,Martin Schmucker,Stephen D. Wolthusen
Tryck verk av ansett bokförlag (Artech House). Verket förklarar grunderna inomvattenmärkning, men ger även en mer ingående förklaring till redan existerande metoder för osynlig vattenmärkning.

[5] Digital watermarking and steganography Av Ingemar J. Cox
Tryck verk av ansett bokförlag (Elsevier Inc). Även detta verk förklarar grunderna för vattenmärkning. I detta verk beskrivs dock metoder och dylikt på ett mer övergripande sätt. På så vis blir det enklare anpassa information för synlig vattenmärkning.

2 Fragil och robust vattenmärkning

Huvudtyper

Det finns två huvudtyper av digital vattenmärkning. De två typerna är fragil vattenmärkning och robust vattenmärkning. Båda typerna kan användas för att, genom jämförelse med originalet, upptäckta eventuell påverkan på materialet. Varje typ har sitt eget specifika användningsområde där det lämpar sig bäst.

Fragil vattenmärkning

Fragil vattenmärkning bygger på principen att en ändring av det vattenmärkta materialet ska göra det direkt omöjligt att detektera den tidigare befintliga vattenmärkningen i sin helhet[Ref. 4]. Denna typ av vattenmärkning fungerar alltså på det sättet att detekteringsfunktionen returnerar ett svar som innebär att vattenmärket inte längre återfinns på samma form som i originalbilden.

Denna form av vattenmärkning gör att den lämpar sig väl för att detektera föremåls äkthet[Ref. 4]. Man kan också se på bilden vad som manipulerats.

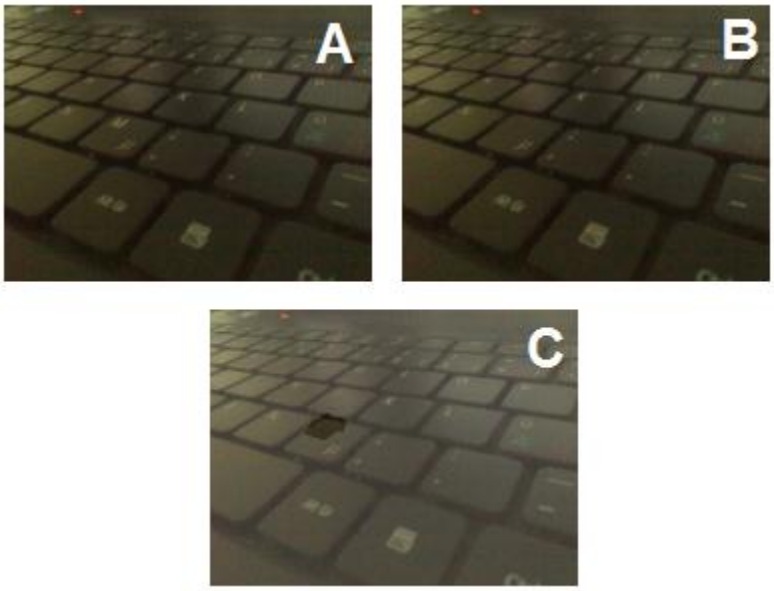

Fig. 2.1 Ovan visas ett exempel på hur manipulation av en vattenmärkt bild uppfattas vid fragilvattenmärkning. A visar en bild i sitt ursprungliga format. B visar samma bild efter att en del av bilden manipulerats. C är en visuell representation av hur denna manipulation uppfattas vid detektion av vattenmärket.

Antag att du skulle ta emot bild B i Fig. 2.1. Utan tillgång till originalet A skulle det vara svårt att se om bild B är manipulerad. En detektering på bild B skulle dock resultera i ett resultat som påminner om bild C. Med andra ord

skulle det fragila vattenmärket inte finnas på den manipulerade ytan och man skulle på så vis kunna bekräfta att bilden blivit manipulerad.

Robust vattenmärkning

En robust vattenmärkning är till skillnad från den fragila, en vattenmärkning som är designad för att motstå alla de transformationer som den fragila är designad att brista vid [Ref. 4]. Med andra ord så ska eventuella detekteringsmetoder kunna detektera vattenmärkningen även om bilden påverkats på något sätt. En god robust vattenmärkningsmetod kräver en god detekteringsmetod, dvs. en funktion som kan utvinna märket även efter attack.

Poängen med den höga detekteringsförmågan är att förhindra någon som ej har tillstånd att använda föremålet, från att göra detta utan upphovsmannens tillstånd. Grundprincipen för en robust vattenmärkning är att med hjälp en kryptonyckel och vattenmärkningssekvens baka in ytterligare en signal i en önskad bild, för att bilda en vattenmärkt bild. Vattenmärkningssekvensen är vattenmärket beskrivet som en signal. Om man skulle applicera detta på en synlig vattenmärkning skulle det kunna liknas vid man tar vattenmärkets bild (inklusive allt tomrum på det tänka målet som märket inte sitter på) och sedan omvandlar detta till en lång sträng med en pixel som bredd. Oftast tar dessa robusta metoder även hänsyn till objektets egenskaper för att minska möjligheten att detektera vattenmärkningen utan den exakta metoden för detekteringen. För att extrahera och detektera vattenmärket krävas alltså tillgång till både vattenmärkningssekvensen och nyckeln [Ref. 5].

Tillämpning vid synlig vattenmärkning

Såväl fragil som robust vattenmärkning är metoder som används vid osynlig vattenmärkning. Anledningen till att teori rörande dessa typer av vattenmärkning är beskrivna med det osynliga formatet som grund, är sättet de fungerar på. Strikt visuell vattenmärkning kan lätt påverkas eftersom den är synlig. En robust struktur är därför svår att uppnå via strikt visuella medel.

Fragil vattenmärkning och synlig vattenmärkning är lika på det sättet att båda kan användas för att bevisa en bilds äkthet, dvs. att ingen har påverkat bilden.

3 Detektering

Bakgrund

Likt fragil och robust vattenmärkning har detektering fokus på osynlig vattenmärkning. Beroende på typen av vattenmärkning går det dock även att tillämpa teorin vid visuell vattenmärkning. Ett fall då osynlig vattenmärkning påminner om synlig vattenmärkning är vid användning av så kallad Least Significant Bit-märkning som ofta benämns steganografi.

Detta innebär att man påverkar den minst signifikanta biten i en färgmängd för att lagra information. Rent visuellt är dock denna information osynlig.

Vad detektering i grunden innebär är att man via en funktion ska försöka läsa ut vattenmärket ur en bild. Denna funktion är i samband med osynlig vattenmärkning fullständigt datoriserad och innebär att man reverserar metoden man använde för att lägga till vattenmärket. För synlig vattenmärkning kan det också röra sig om datoriserade metoder, men även direkt iaktagelse (mänsklig) kan visa sig fungera för synlig vattenmärkning.

Värden av vikt

Det finns två viktiga värden som man använder vid detektering av vattenmärkning. Värdena benämns som FNP och FPP.
FNP (False Negative Probability) är sannolikheten att ett vattenmärke inte kan detekteras och FPP (False Positive Probability) sannolikheten att ett vattenmärke som inte producerats detekteras. FPP betecknas vanligtvis med α och FNP med β [Ref. 3]. Båda dessa värden bör ha ett litet värde.

FNP skulle också kunna ses som toleransvärdet för vilken nivå av förändring som vattenmärket ska tillåta. Vid en utveckling av en vattenmärkningsmetod måste man alltså ta hänsyn till vilka attacker som anses sannolika för objektet och utveckla vattenmärkning därefter. FNP är inte ett känt värde för personen som attackerar bilden och därför är attacker som tar hänsyn till FNP inte möjliga.

Tillämpning av sannolikhetsvärden

Antag till exempel att vi har en bild som vi kombinerat med en vattenmärkning. Om vi vid detektering då uppmäter ett för stort värde på β (ett för stort antal försök krävs för att hitta vattenmärket) när vi använder vår detekteringsfunktion på det vattenmärkta objektet, kan man dra slutsatsen att sannolikheten är stor att bilden utsatts för en attack [Ref. 3]. När man utnyttjar dessa sannolikhetsvärden bör man låta mätningen hanteras av dator.

Detekteringen avgör alltså om vattenmärket är skadat eller inte, medan sannolikhetsvärdena avgör om det är en attack eller naturlig påverkan.

Att mäta just α kan vara något problematiskt då detta innebär att man skulle hitta ett vattenmärke som inte finns. Detta innebär då att analysen får göras på ett av två sätt. Det första vore att testa om vattenmärket kan detekteras utan att det är applicerat på bilden. Det andra vore att göra en undersökning kring existerande vattenmärken (som inte finns på bilden) och se om dessa kan upptäckas i bilden. Mätningen för både α och β involverar statistik. Ett flertal försök måste göras att iaktta de förändringar som uppstår vid inbäddning och komprimering. Fler undersökningar innebär ett mer statistiskt korrekt värde för både α och β.

Attackens syfte kan ofta ses på sannolikhetsvärdet som erhållits då ett högre värde innebär en större sannolikhet för att attackens syfte var att avlägsna vattenmärket. På samma sätt kan man även jämföra β med ett resultat som uppnås efter en detekteringsfunktion som körts på det vattenmärkta objektet tillsammans med vattenmärket. Ett större värde på β i detta läge skulle innebära att detekteringen inte kan uppmäta en tillräckligt stor mängd av det ursprungliga vattenmärket i bilden. Värdet på α kan liksom med β också tolkas för att bedöma syftet med attacken [Ref. 3].

I korta ordalag kan man beskriva en beräkning av α och β enligt följande:

Antag att vi har ett vattenmärke V som vi tillåter i bilden och en funktion D som vår detekteringsfunktion. Vi har även en samling B som är bilder med vårt V inbäddat och en annan samling B’ som inte har vårt vattenmärke applicerat. En ytterligare faktor A representerar en attackfunktion. Jag väljer att benämna detta som en funktion pga. den varierande karaktär som attacker kan ha. För fallen nedan innebär 0 att ett vattenmärke inte hittas och 1 att ett vattenmärke hittas.

För α gäller:
Sannolikheten för att D(V, B’)=1 ska vara mindre än α.

För β gäller:
Sannolikheten för att D(A(V, B))=0 ska vara mindre än β.

Metoder

En av metoderna som används för detektering är det så kallade 0-bitarsprotokollet [Ref. 4]. Metoden fungerar på så sätt att man ger funktionen tillgång till den vattenmärkta bilden, den omärkta bilden och vattenmärket. Jämförelsen kommer alltså resultera i en kontroll om det nämnda märket finns

i bilden. En kontroll av den här typen kommer endast att kunna returnera två svar. Om vattenmärket finns kommer funktionen att returnera true/ja och om inte fås false/nej till svar. Visserligen innebär detta att man inte får någon djupare information kring vad som förändrats i bilden, men metoden är nog för att bevisa att bilden blivit påverkad och inte längre befinner sig i sitt ursprungskick [Ref. 4]. Återigen beror dock vad som menas med ursprungskick på den mängd tillåten förändring som detektionen tillåter.

Alternativet till 0-bitarsprotokollet är flerbitarsprotokollet [Ref. 4]. Protokollet bygger på att man ska kunna extrahera vattenmärket ur bilden genom att nyttja nyckeln som användes vid tillverkning av vattenmärket, vattenmärket, den vattenmärkta bilden och originalbilden. Genom att producera den sekvens (mha. krypteringsnyckeln och vattenmärket) som skapades vid produktionen av den vattenmärkta bilden, kontrollerar man ifall samma punkter förekommer i den potentiellt attackerade bilden, som i den sekvensen. Det innebär att denna detektionsfunktion kommer att returnera en bitsekvens. Om denna sekvens överensstämmer med den som uppstod under produktionen av vattenmärket bevisar det alltså att vattenmärket fortfarande finns kvar.

Fördelen med denna metod är alltså att man i detalj kan se hur mycket av vattenmärket som förändrats genom en direkt jämförelse av de två sekvenserna [Ref. 4]. Även i detta fall är det upp till varje enskild person att bedöma hur mycket som är tillåtet att förändra utan att det tolkas som en attack.

Generellt för båda de ovannämnda metoderna är dock att man inte kan tolka en förändring som en attack om den inte överstiger den förändring som kan uppstå via inbäddning av vattenmärket eftersom detta skulle vara trivialt [Ref. 5]. Konsten vid tillverkningen av en vattenmärkning ligger i att ta hänsyn till alla faktorer som kan påverka bilden, såväl attacker som naturliga förändringar som kan uppstå.

Detektering vid synlig vattenmärkning

Vid synlig vattenmärkning kan det vara svårare att tillämpa ovanstående då vattenmärkningsmetoden oftast är väsentligt enklare än vid osynlig. Därför används också två relativt enkla metoder för detektering.

Den första av de två metoderna är att helt enkelt iaktta bilden och se om man kan urskilja sitt vattenmärke. Efter en attack är detta oftast en mindre lämpad metod eftersom vattenmärket kan vara dolt av editering av olika slag.

Därför är det bättre att vid ett sådant tillfälle använda sig av jämförelse mellan bilder mha. program som klarar av att göra subtraktion mellan två bilder och sedan presentera resultatet. Man inleder med att subtrahera den utsatta bilden med originalbilden (utan vattenmärke). Detta ska under perfekta förhållanden resultera i att utvinna vattenmärket, men eftersom bilden nu kan vara påverkad av en attack fortsätter detektering med att analysera resultatet av subtraktionen. Analysen innebär en jämförelse med vattenmärket för att kontrollera om det finns spår av det.

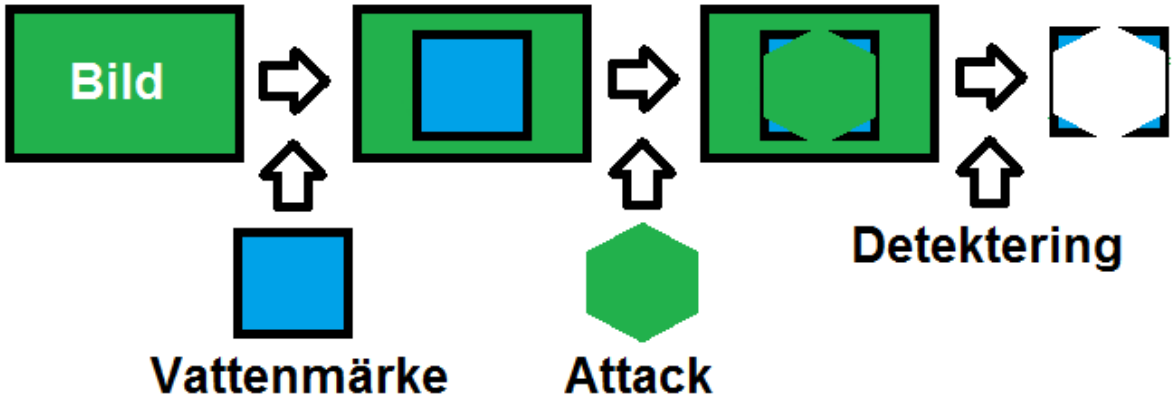

Fig. 3.1 Denna bild förklarar förloppet mellan en omärkt bild till detektering av ett vattenmärke på en bild utsatt för en attack.

Sökandet efter vattenmärket sker på ett flertal sätt. En första kontroll kan vara att jämföra skillnader i färgnivåer för att se om de förhåller sig på samma sätt som i vattenmärket. Ifall attacken var noga med att lämna så mycket som möjligt av bildmotivet intakt, går det även att med ögat se, att resultatbilden av subtraktionen påminner om vattenmärket. Det finns även en möjlighet för en dator att köra en direkt jämförelse vid detta tillfälle för att se om den kan ”se” vattenmärket.

4 Attacker

Första grundtypen

Precis som med huvudtyperna för vattenmärkning finns det två grundtyper för attacker mot vattenmärkningar [Ref. 5]. Dessa har likt vattenmärknings-metoderna också skilda syften. Den första typen kallas för avlägsningsattack och är den typ som de flesta tänker på när man nämner attacker mot vattenmärkning. Precis som namnet antyder går den i princip ut på att man i största möjliga mån avlägsnar vattenmärket från det märkta objektet. Metoden är något som oftast tillämpas vid borttagning av osynliga robusta vattenmärkningar, men kan beroende på vattenmärkets komplexitet, även tillämpas vid synlig vattenmärkning. Syftet med metoden är alltså i grunden att direkt motverka principen med en robust vattenmärkning. Attackens syfte är att förhindra detektering av vattenmärket [Ref. 4]. Kan märket inte detekteras visuellt eller med en detekteringsfunktion har attacken lyckats. Problemet med det sistnämnda är dock att det kan vara svårt att försäkra sig om att en attack lyckats.

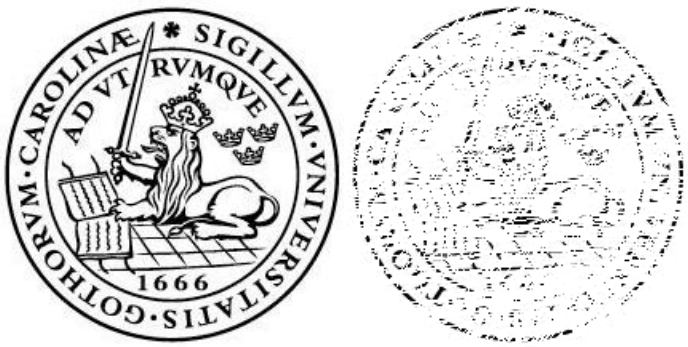

Fig. 4.1 Bilden visar hur ett vattenmärke kan skadas av till exempel en brusattack.

Antag till exempel att ett vattenmärke ser ut som bilden till vänster i Fig. 4.1. En avlägsningsattack skulle kanske lyckas åstadkomma förändringen till höger på vattenmärket. Jämförelsen som görs vid detektering är alltså att kontrollera om denna vattenmärkning kvarstår. Bilderna ovan ger förstås upphov till en trivial jämförelse. Svårigheten ligger i att kunna göra denna jämförelse utan tillgång till detekteringsfunktionen, dvs. när vattenmärket ligger inbäddat i en annan bild. I bilden Fig. 4.2 är bilden till höger i Fig 4.1 inbäddad i en annan bild och kan vara svår att urskilja.

Fig. 4.2 Ett skadat vattenmärke kan vara svårt att detektera.

Den andra grundtypen

Det specifika med den här metoden är att man inte fokuserar på att avlägsna vattenmärket [Ref. 4]. Fokus lägger istället på att försöka uppnå det resultat som syntes i Figur 4.2, dvs. att förändra så att vattenmärkningen blir svår eller omöjlig att urskilja. Man skulle kunna säga att den första metoden kan liknas vid att man försöker dra av ett plåster från bilden och metod två försöker dölja det faktum att plåstret sitter på bilden.

Detta är självfallet möjligt att uppnå denna effekt genom att utnyttja den första metoden. Dock är detta endast möjligt om metod ett tillämpas på en relativt enkel vattenmärkning, t.ex. om vattenmärkningen är monoton eller solid. Vad gäller synlig vattenmärkning är den andra metoden oftast mer än tillräcklig för att ta bort vattenmärket så att någon olovligen kan använda den. Därför är det just denna typ av attacker som är vanligast vid attack mot synliga vattenmärkningar. Problemet med den här typen av attacker ur defensiv synpunkt är att de är alltför lätta att genomföra utan större erfarenhet av bildhantering. Några exempel på hur dessa attacker kan genomföras följer nedan.

Exempel på attacker

Rotation

Problemet en rotationsattack orsakar är av den grad att det påverkar detekteringen av vattenmärket. Detta kan förklaras mha. Fig. 4.3.

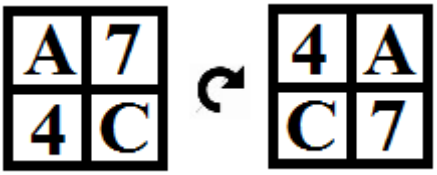

Fig. 4.3 En roterad bild innebär en annorlunda datamängd.

Antag att en detekteringsfunktion ska söka efter en vattenmärkning som är konstruerad på så sätt att den ska detektera en sekvens som ser ut som bilden ovan till vänster. En rotation kommer därför göra att denna sekvens inte längre existerar i bilden längre [Ref. 4]. Visuellt finns dock vattenmärket kvar. En rotation av hela bilden fungerar alltså inte. Om man däremot avlägnsar en del av bilden, roterar denna och sedan utnyttjar denna del i en ny bild finns alltså mönstret inte tillängligt.

Destruktiv komprimering

Filtyper såsom t.ex. JPEG som nyttjar destruktiv komprimering kan påverka vattenmärkning på flera sätt. Beroende på kvalitén av bilden kan destruktiv komprimering skada den visuella vattenmärkningen [Ref. 4]. Anledningen till detta är att destruktiva komprimeringsmetoder kan skala bort delar av den visuella märkningen. Detta beror på att destruktiv komprimering ofta skalar bort information som kan ses som onödig. Exempel på detta kan vara färgskillnader som det mänskliga ögat inte uppfattar.

Beskärning

Beskärning har liksom rotation en begränsad effekt beroende på vad det är som beskärs och hur detekteringen fungerar [Ref. 4]. Ett trivialt exempel är att man klipper bort en signatur som kan finnas någonstans i utkanten av bilden. Vid sådana tillfällen är skyddet brutalt avlägsnat. Skulle dock vattenmärkningen vara placerad på så sätt att den täcker en vital del av bilden får en beskärning en mer begränsad inverkan, men effekten kan vara tillräcklig för att förhindra detektering. Detta förklaras med Fig. 4.4

Fig. 4.4 Det orangea området ovan visar toleransnivån för hur mycket av vattenmärket som kan saknas innan det blir svårt för detekteringsfunktionen att upptäcka vattenmärket.

Den övre bilden visar ett exempel på hur mycket av den vattenmärkta bilden som kan saknas och fortfarande vara tillräckligt för att vattenmärket ska kunna detekteras av detektionsfunktionen.

Det orangea området visar denna toleransnivå för den skyddade bilden. Skulle man nu avlägsna en tillräckligt stor del av vattenmärket genom beskärning (se bilden med det gråa området i Fig. 4.4), kan detta förhindra detektering av vattenmärket eftersom metoden för att hitta vattenmärket inte kan hitta tillräckligt med information.

Histogramanalys

Är trots sitt namn inte en särskilt komplex metod för att avlägsna synlig vattenmärkning. Denna metod är speciellt effektiv när man önskar avlägsna vattenmärkningar som är av transparent karaktär. Antag till exempel man avläser en bild och uppmäter färgnivåerna enligt Fig. 4.5.

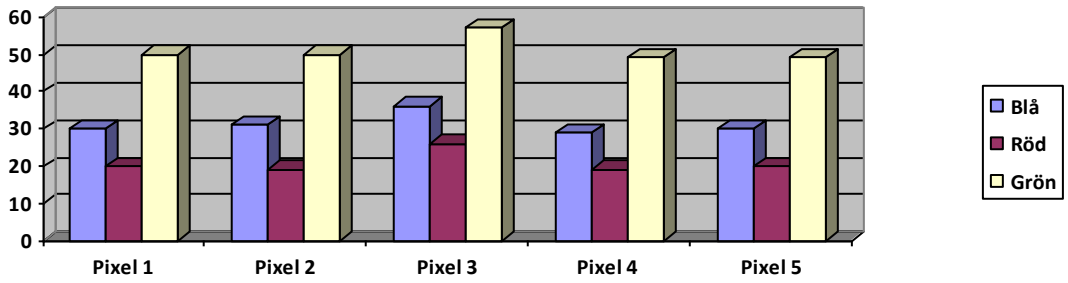

Fig. 4.5.

Man kan ur denna bild utläsa att färgnivån vid pixel 3 är något högre än i närliggande pixlar. Detta betyder att färgen är något ljusare än de övriga. Genom att balansera färgnivån där detta fenomen uppstår kan man avlägsna vattenmärkningar av denna typ [Ref. 4]. Fallet ovan kan ses i bilder där man utnyttjar ljus transparent vattenmärkning.

Brus

Syftet med denna attack är att tillföra en signal till originalet i ett försök att förstöra inbäddade signaler. Är en attack som kan tillämpas relativt enkelt med dagens bildhanteringsverktyg. Se bara på nedanstående bilder, Fig. 4.6.

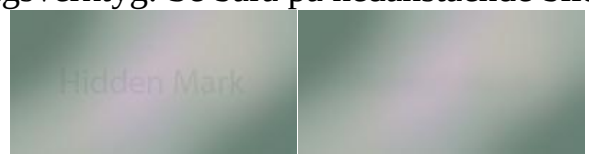

Fig. 4.6 Bilden ovan visar ett vattenmärke före och efter brus. Bilden till vänster är innan attacken inträffat.

Iakttar man den första bilden kan man skymta texten ”Hidden Mark”, men om man iakttar den andra bilden är det omöjligt att se att något står där. Bruset tillför även en effekt på detektionspunkterna. Bildens struktur har förändrats pga. bruset och på så vis flyttat de punkter där detekteringen förväntat sig hitta referenspunkter för att verifiera att vattenmärket finns där [Ref. 4]. Det går

inte heller att finna märket på andra färgnivåer eftersom brusets signalvärde överlappar vattenmärkets signal.

Direkta Editeringsattacker

Den här typen av attack sammanfattar i princip resterande typer av attacker och fungerar i princip på samma sätt som grundtyperna för attacker. Det första alternativet är alltså att försöka återställa bilden som den var innan vattenmärket adderades [Ref. 4].

Den andra typen av editeringsattack fungerar även den på det viset att man ersätter det vattenmärkestäckta materialet med eget material, men i detta fall är målet att förstöra vattenmärket. Därför kan det ofta fungera att bygga över vattenmärket med närliggande bildinformation. Rent principiellt kan det förklaras med Fig. 4.7.

Fig. 4.7 Om man utnyttjar närliggande information kan man ersätta märkta områden utan att få en onaturlig bild. Ovan har jag utnyttjat det blåa området för att ta bort informationen i det röda fältet.

Bilden ovan visar att vi kan ersätta materialet i den röda markeringenen (som kan antas vara vattenmärket för bilden) med bildinformationen i den blåa. Genom att utnyttja det faktum att nyanserna för de båda områdena är snarlika kan vi ersätta informationen utan problem eftersom det mänskliga ögat saknar förmågan att särskilja bildinformation med denna minimala skillnad. Vattenmärket kan inte heller detekteras mha. dator eftersom den informationen man söker helt ersatts av irrelevant information. Det enda man kan detektera är att vattenmärket inte längre finns där.

5 Lagliga aspekter

Upphovsrätten

Upphovsrättslagen är självklart viktig för digital vattenmärkning eftersom en del av syftet med vattenmärkning är förhindra stöld eller missbruk av digital egendom [Ref. 2].
Det är flera delar av lagen som är relevanta. Först och främst är det följande som gäller:

1 § Den som har skapat ett litterärt eller konstnärligt verk har upphovsrätt till verket oavsett om det är:

- skönlitterär eller beskrivande framställning i skrift eller tal,
- datorprogram,
- musikaliskt eller sceniskt verk,
- filmverk,
- fotografiskt verk eller något annat alster av bildkonst,
- alster av byggnadskonst eller brukskonst, eller
- verk som har kommit till uttryck på något annat sätt.

Teoretiskt fungerar denna lag förstås som tänkt, men tyvärr kan den kringgås eftersom det är svårt att verifiera en persons skapande av materialet. I ett fall där en person har offentliggjort verket, utan att nämna att verket inte får användas utan tillåtelse, har personen ifråga gjort det möjligt för andra parter att ta del av och återge verket i annat format utan att detta ses som ett brott mot upphovsrättslagen.

Dock ska det nämnas att verket inte är offentliggjort förrän det som skapats har överförts från en annan plats som inte är offentlig [Ref. 2]. Med andra ord betyder detta att om någon kommer över skapat material utan det först överförts till ett medium som är tillgängligt för allmänheten så är detta stöld. Materialet anses inte heller offentliggjort efter en presentation, om man inte i samband med presentationen gör materialet tillgängligt [Ref. 2]. Ett undantag från detta är förstås om verket säljs eller utlånas till annan person utan upphovsrätt.

Bevis för att verket är ditt

Att bevisa att man är just den individen som skapat verket kan vara svårt. Det smidigaste sättet är att offentliggöra sitt verk. Genom att offentliggöra ett verk presenteras du som upphovsmannen till verket vid just det datum och den tid som verket offentliggjorts [Ref. 2]. Skulle en person sedan presentera ett verk utan upphovsmannens direkta medgivande, kan denna tidsstämpel användas för att verifiera just vem som är upphovsmannen. På så vis kan man även

undvika att en annan part använder verket med sin egen vattenmärkning på objektet. Om ingen uppvisar en publikation med en tidigare tidpunkt för skapandet har man avvärjt just denna risk.

Omfattas inte av lagen

Ett besvärligt problem, som det för tillfället inte finns en lösning på, är framställning av snarlika kopior. Eftersom dessa kopior skapas från grunden, med ett annat verk endast som förebild, omfattas detta inte av upphovsrättslagen. Det betyder att någon vars bild blivit kopierad, inte kan utnyttja lagen till sin fördel. Detta problem är inte unikt för digitala bilder utan förekommer självfallet vid andra typer av produktioner.

Problemet som uppstår i samband med den digitala bildbehandlingen är att verket som påminner om ditt faktiskt inte är ditt och att du på inget sätt kan bevisa att det är en kopia av ditt verk såvida kopian inte är skapad utifrån din bild och har bearbetats till en ny bild. Anledningen till detta är att de referenspunkter som uppstått i din bild vid produktionen och infogandet av vattenmärkningen inte kommer att synas i kopian eftersom de aldrig funnits där.

Ett alternativ för fotografering

När det gäller fotografering finns det en speciell lösning att tillgå för att försäkra sig om upphovsrätten till sin bild. Detta är visserligen ingen lösning som tillämpar vattenmärkning för att fungera, men metoden är likväl intressant. Lösningen kallas RAW-format. Det som händer kan jämföras med de analoga kamerorna. När bilden tas sparas ett negativ, men för fallet med digital information är detta inte en inverterad version av bilden [Ref. 4]. Det som skapas är istället en RAW-fil.

RAW-formatet är en fil som innehåller extremt mycket information om själva bilden och situationen då bilden togs, såsom färgnivåer, modell för kameran, inställningar för lins och liknande [Ref. 4]. Den informationen kompletteras sedan ytterligare med en tidsstämpel och i vissa fall även kryptering. Fördelen med detta format (det ska nämnas att RAW-formatet inte är ett och samma format utan existerar i flera olika filtyper) är att all den ytterligare information som är kopplad till bilden gör bilden väldigt unik och ger många möjligheter till identifiering. Det finns för övrigt inte ett standardiserat bildhanteringsprogram för editering av samtliga RAW-typer [Ref. 4].

Vissa typer av attacker blir även alltför uppenbara vid attacker på RAW-format. Detta eftersom formatets extra information ger upphov till vissa förutsättningar för bilden. Brus-attacker skulle till exempel påverka färgnivåerna och därmed skulle den sparade informationen i filen om bildens

färgvärden inte längre stämma överens med det som finns i den faktiska bilden [Ref. 4]. Det är i princip samma problem som skulle uppstå med ett passfoto där personen på bilden har blå ögon, men informationen intill passfotot säger att personen har bruna ögon.

En bild i RAW-format skulle alltså klara sig utan vattenmärkning, men är på grund av sin storlek inte lämplig att utnyttja till annat än tryck.

Överlagrande vattenmärkning

Två eller flera vattenmärkningar på samma bild behöver inte betyda att vattenmärkningarna är olagliga eller bryter mot upphovsrätt. Tvärtemot kan det i flera fall vara en nödvändighet för att bevisa äganderätt av flera parter [Ref. 5]. Problemet uppstår om ägandepartner har olika typer av vattenmärkning och de blockerar varandra på något vis. Ett exempel på hur det bör fungera följer nedan.

Exempel på fungerande dubbel vattenmärkning

Fungerande dubbel vattenmärkning är då två vattenmärkningar förekommer på samma bild och båda är urskiljbara i sin helhet.

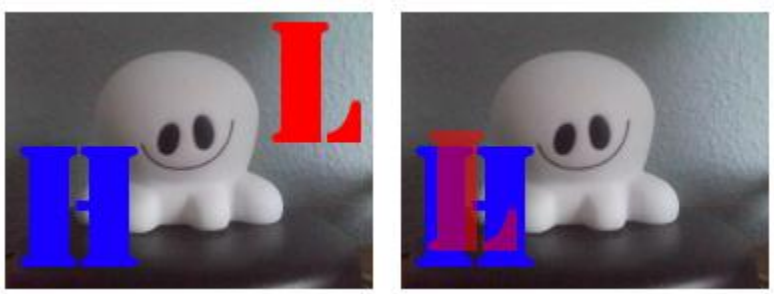

Fig. 5.1 Ovan är ett exempel på tillåten dubbel vattenmärkning.

På båda bilderna i Fig. 5.1 kan man tydligt se båda märkena L och H i sin helhet. Även då L är transparent i bild 2 kan man tydligt se märkets struktur.

Exempel på icke fungerande vattenmärkning

Felaktig dubbel vattenmärkning är ett exempel på ett olagligt tillvägagångssätt att lägga till en andra vattenmärkning. Detta kan dölja den ursprungliga upphovsmannens vattenmärkning och är på så vis också troligen mot reglerna som upphovsmannen angav när han eller hon publicerade bilden.

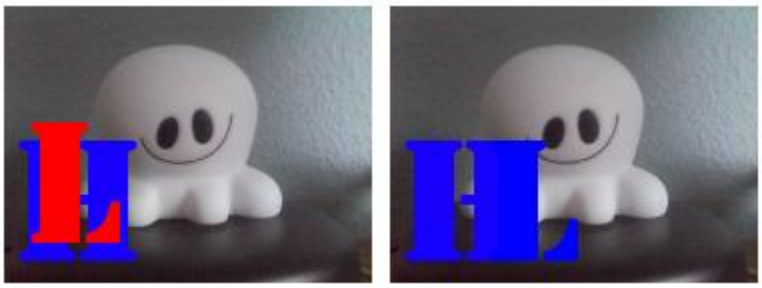

Fig. 5.2 Detta är exempel på dubbel vattenmärkning som kan orsaka besvär eller lagliga disypter.

I den första bilden i Fig. 5.2 överlappar vi stora delar av vattenmärkningen, vilket kan jämföras med en beskärningsattack som nämndes i kapitel 4. I den andra bilden ovan så överlappas också vattenmärkningen, men här utnyttjas den ursprungliga vattenmärkningen för att bilda en del av en ny vattenmärkning.

Bilden till vänster ovan kan vara lätt att bevisa olaglig inverkan på, eftersom en del av det ursprungliga vattenmärket finns kvar, om än endast delar av den. Den andra bilden är något mer problematisk. Eftersom bilden endast ser ut att ha en vattenmärkning kan personen som utfört attacken hävda att det är hans vattenmärke som finns på bilden och upphovsmannen har en beskärd version av hans vattenmärke [Ref. 5]. I ett sådant fall kan en handling om att bilden offentliggjorts med endast märket H vara avgörande för att vinna tvisten.

Även om en person har tillgång till information om den ursprungliga vattenmärkningen skulle detta inte leda till mer än man kan bevisa äganderätt till en viss del av bilden.

6 Färgkanaler

RBG-Modellen

Elektroniska media har många olika sätt att beskriva färger, men till grunden för de flesta ligger RGB-modellen. Detta innebär att färgerna representeras av en summa av de tre primära färgerna röd, grön och blå. Dock baseras representationen på vad det mänskliga ögat uppfattar. Det innebär att färgen som uppfattas som vit är en blandning av färger där röd motsvaras av 30% av färgblandningen, grön 59% och blå 11% [Ref. 4].

För de flesta skärmar är den procentuella fördelningen som nämndes ovan redan tagen hänsyn till. Detta betyder att färgerna istället visas på en skala där alla har samma max- och minimumvärden. Hur dessa skalor ser ut beror dock på vilken filtyp/färgskala som används. En GIF-bild har bara 256 färger att tillgå, till skillnad från t.ex. JPEG som har miljontals färger att tillgå.

Bildformat

Om man ser till detaljerna kring nedanstående filformat finns det ett antal aspekter som kan påverka resultatet vid vattenmärkning.

GIF

GIF (Graphics Interchange Format) är ett icke-destruktivt filformat. Vad detta innebär är att data som förloras vid komprimering går att återställa. Därför kan man alltså dra slutsatsen att detta format skulle lämpa sig väl för användning vid osynlig vattenmärkning. På grund av den begränsade färgskalan kan bilder dock förstöras om de sparas till detta format från ett tidigare format som hanterar större mängder färginformation.

PNG

PNG (Portable Network Graphics) kan beskrivas som en uppgradering till GIF och kan hantera transparens samt en bredare färgskala (32-bitar). Filformatet kan även komprimera bilder till samma färgskala som GIF ifall man söker ett filformat med begränsad storlek, men även då PNG stödjer fler färger är det viktigt att komma ihåg att övergången till en annan färgskala fortfarande orsakar viss förlust av data. Där ska man inte lägga på ett vattenmärke innan denna komprimering.

JPEG

JPEG (Joint Photographic Experts Group), använder till skillnad från ovanstående filformat destruktiv komprimering. Detta innebär att dold

information fullständigt kan förloras vid komprimering. Filformatet erbjuder ofta en möjligthet för användaren att spara med olika hög kvalité. Vid högsta möliga kvalité innebär detta att en större datamängd sparas, men också att färginformationen återges väldigt precist. Det innebär att formatet lämpar sig väl för synlig vattenmärkning eftersom det är dessa data som är väsentliga för detektering. Vad som dock bör tas hänsyn till är att JPEG utnyttjar så kallade chroma-data. Chroma-data filtrerar bort färgskillnader som är omöjliga för det mänskliga ögat att särskilja. Därför är det viktigt att se till att både vattenmärke och bild är av samma kvalité innan de slås samman för att få en korrekt återgivelse när man senare försöker avlägsna vattenmärket från bilden.

Tillämpning för vattenmärkning

Eftersom färgernas varians kan bero på bilden själv eller andra faktorer, som till exempel vattenmärkning, kan variansen vara svår att urskilja även för ett datorprogram. Detta gäller definitivt då programmet inte har en aning om hur vattenmärkningen ser ut. Anledningen till att det skulle vara enklare med tillgång till vattenmärkningen är den additiva karaktären som färgerna i en bild har. Med andra ord skulle man kunna avlägsna en synlig vattenmärkning av denna karaktär genom en subtraktion av vattenmärket (eller addition om vattenmärket är mörkare än originalet).

Ett vattenmärke är betydligt svårare att avlägsna om det innehåller både mörkare och ljusare nyanser än originalet. Orsaken till detta visas i Fig. 6.1.

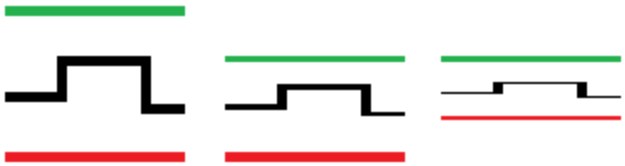

Fig. 6.1 Bilden demonstrerar hur ljusare och mörkare nyanser kan ge ett bättre skydd. Bilden ovan demonsterar hur den vattenmärkta bilden (den svarta linjen), påverkas av ljusförändringar med både ljus (grön) och mörk (röd) vattenmärkning. Ökar vi ljusstyrkan kommer den ljusa vattenmärkningen att glida närmre färgspektret för den övriga bilden medan den mörka vattenmärkningen inte påverkas alltför mycket. Gör vi sedan samma för de mörka nyanserna kommer motsvarande att hända där. Vid det här laget är dock bilden betydligt mer vanställd än vad den skulle varit om bara ljus eller bara mörk vattenmärkning använts.

Luminositet och Mättnad

Luminositet är kort sagt ljusstyrka. Denna kan variera ofta i en bild och används för att ge ett större färgspektra. Mättnad däremot är mängden färg i en bild. Mindre mättnad innebär svaga kontraster och färgskalan placeras närmre gråskala. Mättnaden kan givetvis också variera i en bild, men mättnad används oftast för att förändra hela bilden. Det gör bilden mer enhetlig då den förändrar färgspektret för hela bilden. Bilden 6.1. förklarar fenomenet ytterligare.

Luminositet och mättnad ändras ofta vid digital bildbehandling för att nå den färgnyans man vill. Vad som är viktigt att förstå är att användning av mättnad och luminositet inte ger tillgång till ett vidare färgspektra, utan är endast verktyg för att förenkla bildbehandling. Detta kan enkelt visas med Fig. 6.2.

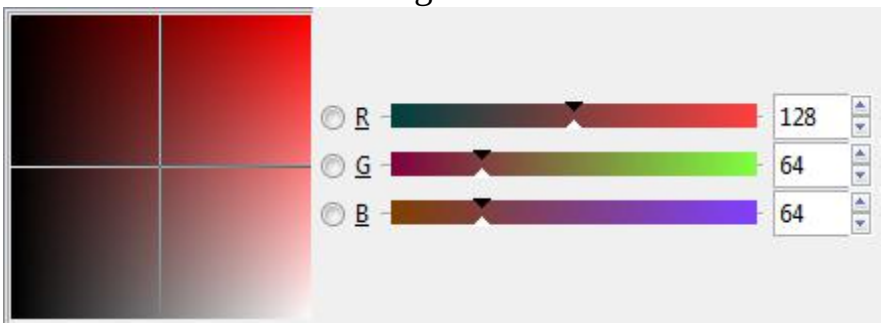

Fig. 6.2 Denna bild används som utgångspunkt för luminositet och mättnad. Bilden har 50% mättnad och 50% luminositet.

Denna första bild visar enbart ett val av färg som vi har som utgångspunkt för att demonstrera vilken effekt luminositet och mättnad. Färgen anges av den punkt där de två linjerna i rutan till vänster möts.

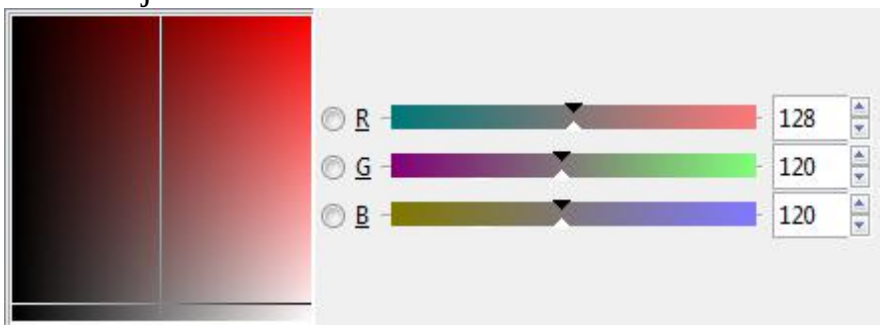

Fig. 6.3 I denna bild är mättnaden sänkt markant. Det resulterar i att man får en något färglös nyans.

I rutan till vänster i Fig. 6.3 ovan har vi nu sänkt mättnaden för bilden. Mättnadsminskning uppnås genom att man låter värdena för de minst signifikanta färgerna gå mot värdet av den mest signifikanta. I exemplet ovan är värdet för G och B lika och de kommer därför att behålla den likheten oavsett värdet för mättnaden, men antar vi att de två mindre signifikanta

värdena skulle inneha ett värde som innebär att de inte längre är lika skulle förändringen ske enligt följande exempel:

Antag till exempel att R, B och G skulle ha värdena 200, 50 respektive 100. Detta skulle då innebära att värdet för B ökar snabbare än G eftersom de båda ska sammanfalla när de uppnår värdet R.

Antar vi nu istället att målet är att maximera mättnaden kommer värdena istället att gå mot noll. R kommer dock fortfarande att vara konstant och den proportionella förändringen kommer att vara densamma som vid minimering av mättnaden. Maximal mättnad uppstår när det minst signifikanta värdet når noll. Dvs. om G och B i detta fallet inte är lika kommer båda aldrig att komma inneha värdet noll.

När man ändrar luminositeten är inget värde konstant. Minskad luminositet innebär att alla värdena kommer att röra sig mot nollpunkten med en sådan hastighet att de kommer nå nollpunkten samtidigt.

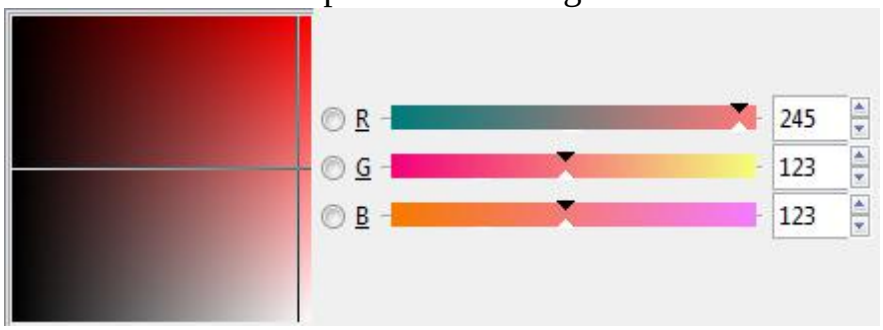

Fig. 6.4 Denna bild demonstrerar vad en höjning av ljusstyrkan innebär.

Proportionalitetskontstanterna är desamma vid ökande luminositet, men när det mest signifikanta värdet når 255 kommer resterande värdena att stanna på det värde de har.

Luminositet har dock tre specialfall. Det är när man justerar luminositeten på de klara färgerna röd, grön och blå. Justeringen innebär då endast en förändring av den angivna färgen. Dvs. vid luminositetsförändring av färgen röd kommer detta endast innebära en förändring av värdet R.

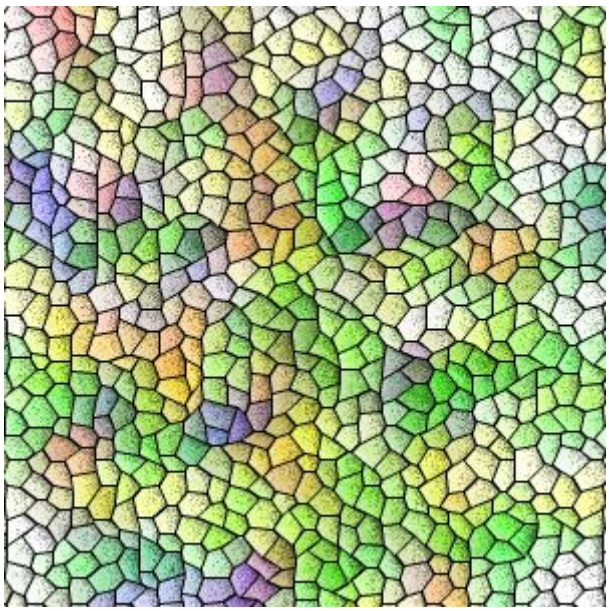

Fig. 6.5 I en bild som denna löper man liten risk att utsättas för en attack som förvandlar bilden till gråskala eftersom färgsättningen är en vital del av bilden.

Vad luminositet och mättnad i grunden innebär för vattenmärkning är alltså att man drastiskt kan förändra färgvärdena i bilden utan att egentligen påverka bildens struktur. Detta i sin tur innebär att om färgen inte är en vital del av bilden kan det bli betydligt svårare att skydda objektet eftersom det innebär att en person som har för avsikt att avlägsna vattenmärket medvetet kan justera bildens färginformation till den nivån att färgerna begränsas till gråskala och därefter kan vattenmärket lättare avlägsnas. Ett exempel på bild där färgen är en vital del av bilden kan till exempel vara Fig. 6.5.

.

7 Bildkvalité

Inverkan på vattenmärket

Där finns ett flertal faktorer som påverkar hur svårt det synliga vattenmärket är att få bort. Beroende på både objektet som skyddas och vattenmärket blir skyddet olika starkt med hänsyn till de olika faktorerna.

Upplösning

Den skyddade bildens upplösning inverkar inte på det sättet att en högre upplösning ger en säkrare bild. Det viktiga är att låta vattenmärkets och bildens upplösning ligga på samma nivå. Notera att detta inte nödvändigtvis innebär att bilderna är av samma storlek utan bara att bildkvalitén ligger på samma nivå. Anledning till detta är följande.

Antag att vi har en bild A som skall skyddas av ett vattenmärke V. V är väsentligt mindre till storleken än objektet på bild A som vi vill skydda. Den omedelbara lösningen till detta vore att skala upp V till att täcka en större yta. Vattenmärket ska vara detekterbart med samma funktion som tidigare, men detta är inte det kritiska med denna lösning.

Antag att en pixel i A tidigare motsvarades av en pixel i V. Nu motsvaras samma yta i V med en yta på 4x4 pixlar i bild A. Problemet är inte det att det blir lättare att urskilja vattenmärket rent visuellt och på så sätt manuellt ta bort märket. Detta skulle i princip vara lika svårt som tidigare eftersom färgnivåerna fortfarande är desamma för den vattenmärkta bilden.

Problemet är istället följande. Ytan på 4x4 pixlar kommer nu ha exakt samma färgavvikelse. Detta innebär att ett program som kan analysera färgkanalerna för bilden enkelt kan urskilja var vattenmärket ligger mha. en histogramanalys. Liknande problem uppstår också om man lägger till en entonig vattenmärkning på en bild som har ett rikt färgspektra.

Färgspektra

Färgspektrat är också det en faktor som måste balanseras mellan vattenmärket och bilden som skyddas. Precis som i exemplet ovan kan man få liknande problem om bilden som ska skyddas har ett begränsat färgspektra. Se t.ex. Fig. 7.1.

Fig. 7.1 I fall då bilder har enkel struktur får transparenta vattenmärkningar försämrad effekt.

Bilden har alltså i sin helhet fem färger (vit inkluderas). På grund av bildens skarpa kontraster är det svårt att använda sig av synlig vattenmärkning på bilden som i Fig 7.1. Även en transparent vattenmärkning som täcker hela bilden skulle vara lönlöst eftersom det låga antalet färger bidrar till att vem som helst skulle kunna reproducera bilden eller avlägsna märkningen utan några som helst problem. Som nämndes tidigare löser man dock problemet genom att använda en vattenmärkning av samma kvalité som bilden har dvs. en heltäckande vattenmärkning som gömmer en vital del av bilden, som i Fig. 7.2.

Fig. 7.2 Heltäckande vattenmärkningar likt den blåa ovan ger ett bra skydd, men förstör också bilden.

Problemet blir istället då att man inte klart kan visa upp hela sin bild. Liknande fall kan uppkomma även med vidare färgspektra, men med ett begränsat antal färger.

Antag att vi har en svartvit bild S. S har ett färgspektra med tusentals nyanser mellan svart och vitt. Problemen med vattenmärkning av bilden är precis desamma som med den enklare bilden. Om man iakttar bilden nedan kan man se att en färgskala mellan två färger är väldigt begränsad även om färgspektret är betydligt bredare än för Fig. 7.2.

Fig. 7.3 Det är en enkel presentation av färgerna tillgängliga vid användning av gråskala.

Problemet kan liknas vid ett koordinatsystem. Med två färger kan man bara förflytta sig mellan två färger. På denna nivå har man komplexiteten av en linje. Skulle ett vattenmärke adderas på denna typ av bild skulle man kunna återställa bilden till original genom att förflytta sig längs denna linje för att hitta färgerna som används för bilden. Detta innebär också att ett vattenmärke med fler än dessa färger skulle vara lönlöst. Personen som utför attacken skulle kunna skilja dessa delar av bilden direkt eftersom dessa pixlar skulle ha en annorlunda färgsammansättning.

Detta gäller i synnerlighet för svartvita bilder eftersom färgkanalernas värde alltid kommer vara lika för alla nyanser på gråskalan. Låt oss säga att de RGB-värden vi har varierar mellan 0 och 256. Detta skulle innebära att vi för en bild i gråskala endast kan uppnå 256 olika färger. Detta är en väsentlig skillnad i jämförelse med om ingen begränsning skulle sättas på de RGB-värden vi har för bilden. Nu har vi istället 3 färgkanaler som kan variera på från 0 till 256 hel oberoende av varandra. Det skulle alltså innebära att fler än 16 miljoner fler färger att variera emellan.

Ett exempel på en presentation över möjliga färger skulle i stället kunna ses som följande Fig. 7.4.

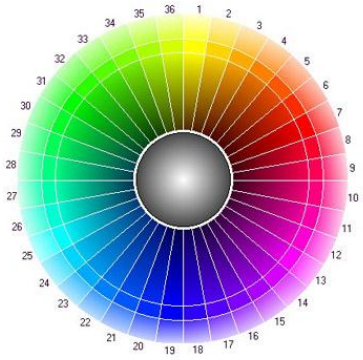

Fig. 7.4 Detta är endast ett exempel på hur man kan presentera alla tillgängliga färger vid användning av ett fullständigt färgspektra.

Kontraster

Kontrasterna är en viktig faktor som tills viss del bygger på samma resonemang som förekom i det ovanstående stycket om färgspektra dvs. att kontrasterna på både bilden och vattenmärket bör vara av samma typ för att försvåra borttagning. Skarpa kontraster på bilden utan skarpa kontraster i vattenmärket gör det lätt att återställa bilden eftersom färgspektret är väldigt tydligt. Ett vattenmärke med skarpa kontraster på en bild med lite kontraster gör att vattenmärket är lätt urskiljbart. Det gör det lätt att avlägsna vattenmärket. För att göra det hela mer trivialt kan man anta att vattenmärket är schackrutigt och bilden består av en solnedgång. Precis som med exemplet

där kontrastmängden var inverterad är det är det lätt att återställa underliggande bild eftersom den har väldigt lite kontraster.

Matchande kontraster

Det finns tillfällen då vattenmärkningens kontrastskiften kommer att vara placerade på exakt samma plats som de underliggande kontrastskiftena. Detta ger en bild som befinner sig lite i gråzonen för om det är en effektiv lösning eller inte.

Anledningen är att vattenmärket ligger i fas med bilden och därför är det lätt att avlägsna vattenmärket utan att det blir några tydliga märken på bilden. Dock kan det däremot bli svårt för personen som försöker återställa den vattenmärkta bilden till korrekt nivå eftersom vattenmärket täckt över hela det närliggande området mellan två skarpa kontraster. Ett exempel på detta är:

Antag att en bild har tagits av en person som står bakom en ledstång. Man önskar nu ta bort ledstången ur bilden. Det är inte någon större svårighet att manipulera bilden så att ledstången försvinner. Problemet är att ersätta vad som fanns bakom ledstången. Om ledstången var av glas (vattenmärket kanske är transparent) kan man se att personen hade ett grönt bälte, men eftersom hela bältet är övertäckt och inget annat är det, är det mycket svårt att beräkna vilken färgnyans bältet egentligen hade. Färgnyansen på bältet har uppkommit genom ljusets infallsvinkel och brytning mot glasledningen för den specifika dagen och tidpunkten.

8 Analys av synliga vattenmärkningsmetoder

Information om kapitlet

Detta kapitel är en sammanställning av olika tillgängliga vattenmärkningstekniker för synlig vattenmärkning. Sammanställningen ger information om hur metoden kan tillämpas, vilka typer av attacker vattenmärkningen är känslig för respektive motståndskraftig mot och under vilka omständigheter metoden bör användas för ett optimalt resultat. Metoderna har i sig inga officiella namn eftersom teorin kring synlig vattenmärkning inte är standardiserad utifrån mer än de punkter som är desamma för osynlig vattenmärkning. Namnen som används här för metoderna kommer därför endast vara en kort beskrivning av respektive metod.

Målet är att slutligen nå fram till en slutsats om vilken av metoderna som skapar största möjliga hinder för eventuella attacker i förhållande till hur stor inverkan vattenmärket har på bilden. Därefter dras slutsatser om huruvida metoden kan vara lämplig att utnyttja för samtliga fall av vattenmärkning eller endast det fallet där vattenmärkningen fungerar bäst och om det kan vara relevant att kombinera metoder för en bättre lösning.

Metod 1: Heltäckande vattenmärkning

Bakgrund

Denna typ av vattenmärkning diskuterades till viss del i kapitel 7 under avsnittet *Färgspektra*. Principen innebär att man adderar ett icke transparent lager till bilden man avser att skydda. Detta för att på så vis fullständigt täcka över den delen av den ordinarie bilden. Vattenmärket är relativt enkelt att tillfoga då det i princip är samma metod som att sätta en stämpel på ett brev.

Styrkor

På grund av att metoden fullständigt skriver över den informationen som den täcker kan man inte återställa objektet till sitt original utan tillgång till just originalet. Dock skulle återställningen i så fall vara redundant eftersom vi redan har tillgång till objektet [Ref. 4]. Detta innebär också att vid alla attacker som har för avsikt att avlägsna denna typ av vattenmärkning så tvingas personen som utför attacken att gissa sig till hur bilden såg ut där märket finns. Antag till exempel att jag har en bild som ser ut enligt Fig. 8.1.

Fig. 8.1 Heltäckande vattenmärkningar kan vara lätta att ersätta om underliggande material har ett logiskt mönster.

Att avlägsna vattenmärket kanske inte är någon större svårighet. I detta fall skulle det kanske inte heller vara någon större ansträngning att skapa en kvalificerad gissning för hur det underliggande materialet kan se ut, men om metoden används korrekt det vara omöjligt att producera en bild som liknar originalet utan tillgång till just originalet. Ett bra exempel på detta kan vara det klassiska exemplet som innebär att censurera en person enligt Fig. 8.2.

Fig. 8.2 Svarta censurblock kan också ses som en typ av heltäckande vattenmärkning. Att ersätta vad som finns under är i dessa fall svårare utan ett logiskt mönster att tillgå.

Att göra en kvalificerad gissning skulle troligtvis resultera i ett helt annat innehåll än i originalet. Metoden är utmärkt när man vill förhindra att bilden dupliceras utan tillstånd från upphovsmannen.

Svagheter

En av svagheterna har redan nämnts. Det är det faktum att eftersom vattenmärket är så enkelt är det också enkelt att avlägsna. Om syftet med en

attack ej är att utnyttja hela bilden utan kanske bara att avlägsna vattenmärket och sedan utnyttja resterande del av bilden till ett kollage eller annan typ av sammansättning är denna lösning poänglös.
I sådana fall krävs en kompletterande osynlig vattenmärkning som täcker en större yta än den synliga vattenmärkningen.

Ett annat problem med denna lösning är även metodens styrka. Att bilden inte går att återställa utan tillgång till originalet innebär också att bilden inte direkt kan sägas vara densamma som originalbilden. Det negativa med detta är att rättsliga mål kan vara svåra att vinna eftersom personen som utnyttjat din bild lika gärna kan skulle kunna ha ett original som du. Detta eftersom det vattenmärkta objektet inte avslöjar hur den egentliga informationen under vattenmärket ser ut (se Fig. 8.3).

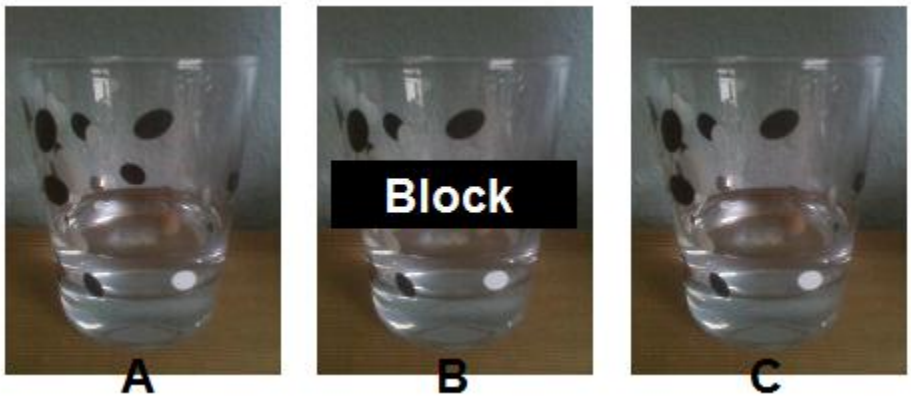

Fig. 8.3 Denna bild demonstrerar vad som kan gå fel när man märker ett område som inte har något logiskt mönster, men har en enkel struktur.

Iaktta Fig 8.3 och antag att vi har en person som tillverkat bild A och den vattenmärkta bilden B. Det finns nu inget som hindrar en annan person att ta bild B och ändra den till att se ut som bild C eftersom B innehåller för lite information om bild A.

Optimala användningsområdet

Det optimala användningsområdet för denna typ av märkning är alltså för att förhindra fullständig kopiering och utnyttjning av originalobjektet och där intresset för vad som händer med resterande delar av bilden inte spelar någon större roll. Exempel på tillfällen då något sådant kan vara lämpligt kan vara vid försäljning av fotografier. Detta beror på just det faktum att målgruppen för bilderna endast är intresserade av det fotot föreställer och inte någon manipulerad gissning av objektet [Ref. 4]. Kort sagt skulle det inte vara värt besväret att avlägsna vattenmärket och ersätta det med egenhändigt tillverkat innehåll.

Metod 2: Entonig transparent vattenmärkning

Bakgrund

Entonig transparent vattenmärkning är den vattenmärkning som tillämpas mest för att skydda ett objekt, men som ändå tillåter en viss insyn i hur objektet ser ut. Vattenmärket kan skapas på olika sätt, men resulterar i snarlika resultat.
Det första alternativet är att utnyttja en additiv metod för att placera vattenmärkningen ovanpå bilden man avser skydda. Praktiskt sett inträffar följande vid skapande av till exempel en klarvit transparent vattenmärkning.

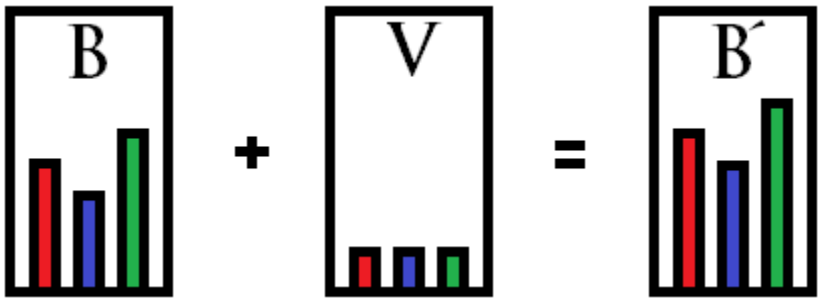

Fig. 8.4 Enkel transparent vattenmärkning kan liknas vid addition. B motsvarar bilden vi vill skydda, V vattenmärket och B´ den vattenmärkta bilden.

En bild B märkt med en entonig vattenmärkning V producerar en vattenmärkt bild B´ [Ref. 3]. Processen är som synes väldigt enkel. För att detektera närvaron av en vattenmärkning är det nog att justera ovanstående exempel till B´ - B = V. Dock förutsätter detta att ingen inverkan förekommit på bilden.

En mer korrekt representation vore B´´ - B = V´´, där B´´ representerar den vattenmärkta bilden med inverkan och V´´ representerar de delar av vattenmärkningen som erhålles genom att subtrahera bort bildinformationen från vattenmärket [Ref. 3]. Den andra metoden för att uppnå liknande resultat består av att man raderar en del av bilden på ett område som motsvarar vattenmärket.

Fig. 8.5 Bilden till vänster är tillverkad med den additiva metoden och ett transparent vitt vattenmärke. Den högra bilden är producerad genom att radera en procentuell del av bilden.

Som synes i Fig. 8.5 är resultat av de två metoderna väldigt svåra att särskilja. Bilden till vänster är tillverkad med den additiva metoden och bilden till höger använder metoden med radering. I fall som med bilden ovan har valet av metod ingen större inverkan, men om vi antar att grundfärgen skulle vara synlig i bakgrunden (i detta fallet är den vit, varav den andra bilden ovan fick en effekt liknande den första) kan det bli problem. Med grundfärg avses färgen på det material som bilden tillverkats på. I verkligheten skulle detta motsvaras av färgen på pappret man ritar på. Detta innebär att personen som avser att avlägsna vattenmärkningen har tillgång till exakt samma färgnysans som utnyttjades för vattenmärkningen.

Är färgen klarvit är det ingen större svårighet att avlägsna märket då det endast innebär en direkt minskning av alla färgvärden i det markerade området. Därför är det en fördel att använda en färg där färgnivåerna inte ligger på samma nivå. Effekten av detta är att om någon nu försöker återställa bilden genom att endast öka eller reducera alla färgnivåer kan få ett resultat som för det mänskliga ögat uppfattas som en icke vattenmärkt bild. Man kan dock mha. att använda B´´ - B = V´´, som nämndes ovan, uppmäta minimala skillnader. Antag att vi skulle göra ett snitt på en pixelrads bredd (se det svarta strecket i Fig. 8.6) för att kontrollera om denna bild utsatt för någon attack.

Fig. 8.6 Det svarta strecket mostvarar ett snitt som kan användas för kontroll av pixelvärdena för denna linje.

Antag även att vi använt oss av en färg som var snarlik klarvit för vattenmärkningen. Med snarlik menas en nyans som för det mänskliga ögat kan uppfattas som klarvit även om där finns en viss skillnad i nyans där man har teknologi till att uppmäta färgnivåerna. Resultatet kommer då att bli enligt Fig. 8.7. Bilden visar färgnivåerna för den svarta markeringen i ett tvådimensionellt diagram.

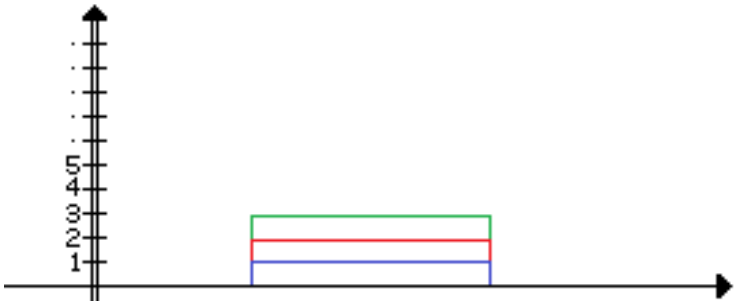

Fig. 8.7 Detta är ett tvådimensionellt diagram som visar hur en entonig vattenmärkning kan ses om en attack misslyckats med att återställa färgnivån till exakt rätt värde.Y-axeln i detta diagram motsvarar nivåer i färgskalan och X-axeln motsvarar den sträcka som det svarta strecket på föregående bild markerar.

Styrkor

Den främsta styrkan med denna metod är att man behåller den enkla strukturen från den föregående metoden, men samtidigt tillåter visning av hela objektet. Den enkla strukturen gör att, precis som det framgick i diagrammet ovan, att all förändring lätt kan kontrolleras. Detta eftersom man vet på vilken nivå som färgen bör ligga och denna nivå är konstant för hela vattenmärket. Erhåller man färger på andra nivåer än den avsatta kan man bekräfta inverkan på bilden.

Styrkan med den enkla kontrollen av inverkan, gör att om en person skulle utföra en attack som resulterar i ett inverkansdiagram som det ovan (Fig 8.7) och sedan adderar ett brus över hela bilden för att dölja attacken, skulle nivåerna som förekommer i diagrammet ovan adderas till bruset och därmed skulle förskjutningen vidarebefordras in i denna del av attacken.

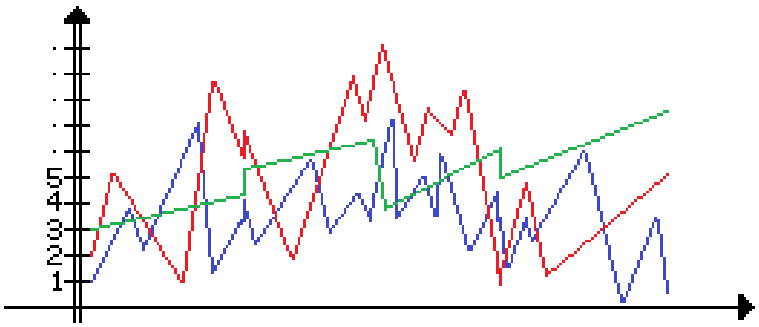

Fig. 8.8 Diagrammet demonstrerar svårigheterna med att dölja en attack på en entonig vattenmärkning om inte vattenmärket fullständigt avlägsnats.

I ovanstående diagram (Fig. 8.8) uppträder dessa vidarebefordrade fel som klara kanter, som i förhållande till det artificiella bruset uppkommer vid exakt samma punkt för varje färg. Hade bruset varit naturligt hade dessa avvikelser inte uppträtt på exakt samma punkter.

Svagheter

Denna metod har en väsentlig svaghet. Om någon räknar ut vilken färgnivå vattenmärket har kan det avlägsnas med samma additiva metod som satte dit märket. Det vanligaste sättet detta inträffar på är om en färgnyans sträcker sig från ett område som inte är märkt till ett område under märket (detta kan räcka med att ett antal pixlar ligger på rad precis vid gränsen av märket). Efter att färgnivåerna jämförts får man fram den färgskillnad som man behöver för att ta bort vattenmärket.

Detta leder oss till denna metods andra stora svaghet. Eftersom märket visar en viss kontrast i jämförelse med det kringliggande området kan man enkelt tillverka en pixel-exakt kopia genom att förstärka kontrasten till det att man tydligt kan se vattenmärkets struktur. Även då detta kan undvikas genom att placera delar av vattenmärket nära delar på bilden som har liknande färgnyanser leder detta till ett annat problem. Det gör det möjligt att direkt eliminera vattenmärket inom det området genom en bruseffekt. Metoden som användes för detektion under stycket *Styrkor* går då inte längre att använda eftersom ingen annan attack har använts för avlägsnandet inom det området.

Optimala användningsområdet

Metoden skall inte tillämpas för bilder med ett smalt färgspektra och skall inte användas om det finns alltför stora områden (relativt mått beroende på utformningen av vattenmärket) där vattenmärket och bilden smälter samman. Utöver detta finns det många alternativ där denna metod kan utnyttjas och detta är också anledningen till att metoden är väl representerad på internet och andra öppna källor. Eftersom vattenmärket är avsett att skydda material samtidigt som det är transparent är det av vikt att placera märket så att man täcker de områden man anser är nyckeldelen av bilden, dvs. det man inte vill få stulet. Det man bör tänka på är att vattenmärket, om än betydligt säkrare än föregående metod och mer anpassad till att visa upp fullständiga bilder, är väldigt lätt avlägsna om man kommer över färgnivåerna som användes vattenmärket. Vattenmärket är då så gott som borta. Därför bör denna metod, liksom föregående, kompletteras av en osynlig vattenmärkning om man har ett skydd i åtanke som verkar i mer än avskräckande syfte.

Metod 3: Flerfärgad transparent vattenmärkning

Bakgrund

Denna metod kan ses som en kompletterad version av den föregående där man nu avlägsnat den svaghet som gjorde att vattenmärket enkelt kunde avlägsnas genom att man beräknade skillnaderna mellan färgnivåerna i

vattenmärkningen och den skyddade bilden. Anledningen till att det inte fungerar är trivial då det beror på att där helt enkelt är för många färger i de båda källorna (vattenmärket och bilden). Just denna metod innehåller ett flertal olika undermetoder som alla har sina specifika för- och nackdelar.
Nedan beskrivs ett antal av dessa metoder där de är grupperade efter styrkor och svagheter som påminner om varandra.

Delmetod 1: Monoton transparent vattenmärkning

Bakgrund

Detta är den mest begränsade metoden för flerfärgad vattenmärkning och har många likheter med den entoniga vattenmärkningen i det avseendet att färgspektret är begränsat. I detta fall på en skala mellan två färgnyanser. Vattenmärket är dock betydligt svårare att avlägsna. Antag till exempel att en person avser att skydda en bild med 16 miljoner färger och utnyttjar ett skydd som kanske endast har 256 olika färgnyanser. Det innebär i grunden att varje pixel kan ha ett skydd som varierar mellan 256 olika värden, men som tack vare underliggande bilds karaktär försvårar ytterligare för eventuell attack på följande sätt [Ref. 1].
Antag att vi har en variabel v sådan att $1 < v < 256$ som motsvarar färgspektret för vattenmärkningen och en ytterligare variabel b sådan att $0 < b < 16*10^6$. Om vi nu antar att vi har en pixel p som motsvarar värdet i en pixel i den skyddade bilden kan en person som utför en avlägsningsmetod påbörja en beräkning för färgen som ska finnas på platsen. Personen kommer dock snabbt att stöta på ett problem. Antag till exempel att värdet för pixeln är 3400023. Det skulle innebära att man kan ställa upp följande additiva fall.

$$b + v = 3400023$$

Vid första insikt kan problemet tyckas trivialt, men problemet här är det samma som att försöka lista ut ett lösenord där det första tecknet för sig kan variera mellan hundratusentals olika värden som sedan ska kombineras med ett ytterligare värde för att bilda det värdet som sökes. Visserligen går det att uppskatta ett värde inom rimliga gränser för b och genom att iaktta närliggande oskyddade områden, men då kvarstår fortfarande problemet att märkningen inte avlägsnat fullständigt eftersom man genom att använda samma detekteringsmetod som för den entoniga transparenta vattenmärkningen B´´ - B = V´´ i alla fall kommer att returnera en skillnad för objektet [Ref. 3].

Tar man sedan även i beaktande att detta problem uppstår för en enda pixel kan man lätt räkna ut hur besvärligt det blir att avlägsna ett vattenmärke som

täcker ett större område. Såsom framgår ovan blir problemet även svårare att lösa när antalet färgkontraster ökar.

Styrkor

Styrkorna med den här metoden är precis det som nämns i föregående uppgift plus en ytterligare. Denna metod tar en svaghet från förra metoden och åtgärdar denna, nämligen att vattenmärket har en enda nyans. Den nyansen har nu övergått i ett mycket vidare spektrum.

Svagheter

Problemet med ett vidare spektrum är dock att det blir lite besvärligare att särskilja förändringar vid brus. Istället för att mäta förändringarna ifrån en specifik nivå mäts det nu istället utifrån en linje. Denna linje erhålls alltså efter att B´´ - B = V´´ använts för att bryta ut vattenmärket. Linjen i detta fall motsvaras av vattenmärkets nivå för en pixellinje. Har vattenmärket en struktur som är brusigt av naturen kan problemet bli ännu värre.
Antag till exempel att vattenmärket ser ut som diagrammet i Fig. 8.9.

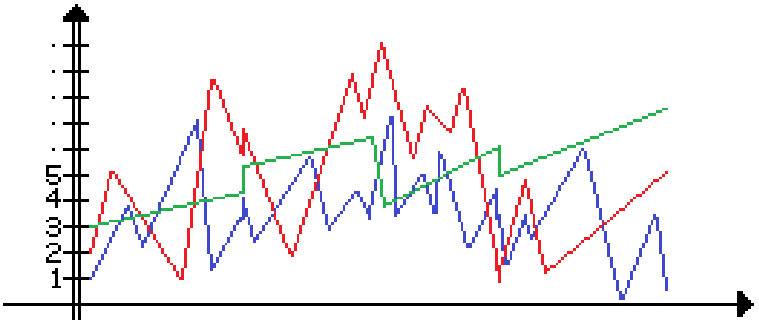

Fig. 8.9 Detta demonstrerar svårigheterna med att tolka ett vattenmärke med fler färgnivåer.

Såsom tydligt framgår ur diagrammet skulle både naturligt och brus från en attack skapa ett problem då det är svårt att skilja på dem när strukturen är enligt ovan. Avvikelserna skulle visserligen ligga kvar precis som vid föregående metod, men chanserna för att brus skulle särskilja sig från en rak linje(ett enkelt värde) är betydligt större än att bruset skulle skilja sig från annat brus.

Delmetod 2: Flerfärgad transparent vattenmärkning

Flerfärgad transparent vattenmärkning där färgspektret ej är begränsat är nästa steg i ordningen. Metoden har principiellt samma struktur som föregående monotona metod. Skillnaden är att ytterligheterna utökas på ett sätt som innebär att vattenmärket blir allt svårare att avlägsna, men samtidigt blir också

förändringar i form av naturligt brus allt svårare att särskilja från brus till syfte att avlägsna vattenmärket. Detta problem blir särskilt tydligt om man återigen listar den additiva funktionen för en pixel.

$$b + v = p$$

I fallet för denna metod har dock det övre gränsvärdet för v uppgått till att bli det samma som det övre gränsvärdet för b. Notera dock att p aldrig kan bli större än det största värdet av v och b, om v och b är bilder konstruerade med samma färgspektra. Ett exempel på detta kan vara om man konstruerat en bild på en skala med färgerna röd och blå, där vattenmärket sedan består av färger på an skala med svart och vit. Röd och blå är visserligen en delmängd av vad som krävs för att uppnå färgen vit, om man ser på hur man uppnår färgen vit genom att maxa att färgskalor.

För att tydligare förklara varför p inte kan anta ett större värde än v och b kan man se de båda variablerna som två vektorer placerade på varsin linje. För enkelhetens antas att dessa två linjer vara placerade i ett och samma plan, linjerna skär varandra i planets origo och vinkeln mellan de två linjerna är 90 grader. Antag nu att vi har en vektor v som kan variera i längd längs med en av dessa linjer och en vektor b som variera längs med den andra. Var för sig skulle de aldrig kunna nå ett värde som övergår maxvärdet för deras respektive linje, men vektorsumman (förutsatt att v och b inte sammanfaller med nollpunkten) skulle resultera i en punkt som inte befinner sig på någon av linjerna [Ref. 3]. Detta resulterar också i en förklaring till varför denna typ av vattenmärkning inte är lämplig att använda. Antag att bild b innehåller samtliga nyanser mellan röd och blå, med ett vattenmärke som varierar i samtliga nyanser mellan svart och vitt. Problemet är då att någon som analyserar denna bild kommer att upptäcka att färgerna endast varierar mellan ett antal punkter kan man också dra slutsatser kring vilka färgkombinationer som inte kan finnas i sambandet och därför begränsa spektret, som i sin tur förenklar avlägsnandet av en vattenmärkning.

För att få största möjliga skydd med den här metoden skall alltså v, b och p ha samma övre gränsvärde och använda samma färgspektra. Antag till exempel att vi använder 16 miljoner färger. Liksom med föregående metod innebär detta att vi har en additiv metod där vi har två variabler som tillsammans bilder resultatet p. Skillnaden mellan denna metod och föregående är att möjligheterna för att uppnå resultatet nu i ökats drastiskt.

Styrkor

Styrkan med den här metoden, vid jämförelse med den föregående metoden, är ungefär densamma som att jämföra olika krypteringsmetoder där skillnaden är

antalet bitar som krypteringen sker med. Det går att erhålla nyckeln för dekrypteringen oavsett antalet bitar att lägga till ett större antal bitar gör det dock betydligt svårare att beräkna lösningen.

Svagheter

Denna metod har samma svagheter som flerfärgad transparent vattenmärkning. I takt med att skyddet blir mer avancerat (ett vidare färgspektra tillämpas), blir det också svårare att särskilja specifika nivåer av färger från varandra vid till exempel en brusattack. Genom att subtrahera bort originalbilden från den utsatta bilden kan man få en skillnadsbild för att uppmäta förändringar. Problemet som uppstår när för många nivåer används är att den skillnadsbild som erhålls också innehåller fler nivåer. Därför blir det svårare att bevisa att denna skillnadsbild är den samma som den som erhålls om man gör samma subtraktion på det vattenmärkta originalet. Detta kan förklaras med följande exempel.

Antag att vi har ett vattenmärke där vi erhåller följande sekvens i skillnadsbilden:
23 - 24 - 25 - 12 - 23 - 12 - 13

Efter en brusattack erhåller vi istället denna sekvens:
23 - 25 - 26 - 11 - 22 - 13 - 12

Jämför man dessa sekvenser ser man tydligt att resultaten skiljer sig, men är fortfarande snarlika varandra.

Om vi listar ett exempel för entonig transparent vattenmärkning skulle det istället se ut såhär:

Den egentliga skillnadsbilden skulle då resultera i en sekvens som bara kan anta två värden. Där vattenmärket finns eller där det inte finns. Exemplet kan då se ut såhär:

23 - 23 - 23 - 0 - 23 - 23 - 23

Efter en attack med samma brus som ovan får vi följande sekvens:

23 - 24 - 24 - 0 - 22 - 24 - 22

Såsom tydligt ses på dessa exempel ovan blir det konstanta mönstret från en entonig transparent lösning mycket mer konstant eftersom kontrollvärdet är detsamma för hela bilden, till skillnad från den flerfärgade där varje

individuell pixel kan ha ett eget kontrollvärde. Det blir alltså svårare att bevisa att någon avlägsnat ett märke eftersom varje del kräver ett eget bevis.

Metod 4: Hybridmetoder

Bakgrund

En del av lösningarna ovan kan kombineras för att skapa alternativa lösningar. Dessa hybridmetoder används eftersom olika metoder kan komplettera såväl styrkor som svagheter hos andra metoder. Andra typer av hybridlösningar försöker uppnå en viss effekt vid vattenmärkning genom att använda delar av andra metoder. Ett exempel på detta är metoden nedan.

Delmetod 1: Heltäckande vattenmärkning med additiv metod

Bakgrund

Denna metod består av att man genom användning av en additiv metod producerar ett heltäckande vattenmärke. Ett exempel på hur man producerar en heltäckande klarvit vattenmärkning med denna metod följer.

Antag att vi vill skapa följande bild (Fig. 8.10) som ett vattenmärke på ett objekt vi vill skydda.

Fig. 8.10 Ett exempel på ett vattenmärke man vill uppnå.

Vi förutsätter att vi endast vill använda de svarta delarna som ett skydd för bilden. Detta innebär att vi ska skapa ett märke där färgkanalerna är nollställda för att uppnå svärta. Hade vi nu använt den förstnämnda, heltäckande, metoden hade vi helt enkelt klistrat in denna bild ovanpå bilden vi önskar skydda, men för den här metoden tar vi hänsyn till hur bilden som skyddas ser ut. För att producera detta resultatet ser vi nu till att skapa en additiv funktion som gör att färgkanalerna skapar detta märket på objektet vi vill skydda. Antag till exempel att vi har en enkel röd bild som i Fig. 8.11.

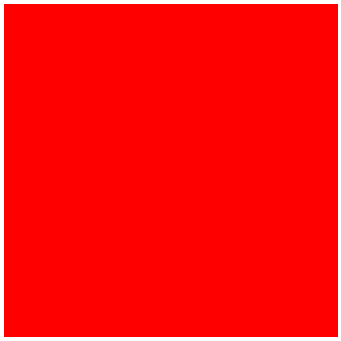

Fig. 8.11 Ett exempel på en enkel röd bild.

För att skapa den nämnda vattenmärkningen skapar man en funktion som förminskar färgvärdet i den röda kanalen tillräckligt för att nollställa kanalen. Det är dock av yttersta vikt att man inte reducerar värdet med mer än det värdet som finns i kanalen. Detta för vi vill kunna återställa bilden till sitt ordinarie format genom att addera vattenmärkningens värden till det vattenmärkta objektet. För exemplet ovan innebär detta att vattenmärket har samma form som ovan (Fig 8.10), men färgen kommer att vara röd.
Hade man velat skapa en heltäckande vit vattenmärkning, med samma mönster, så hade man adderat ett direkt inverterat värde i förhållande till det värde man önskar skapa vattenmärket för. För exemplet ovan detta inneburit att vi adderat ett vattenmärke där den röda färgkanalen är nollställd och de övriga kanalerna maxade.

Precis som med den svarta vattenmärkningen är det av största vikt att inversen är korrekt beräknad eftersom det i annat fall resulterar i ett felaktigt original när vattenmärket avlägsnas med samma metod.

Styrkor

I förhållande den förstnämnda heltäckande metoden har även denna metod den fördelen att underliggande bildformation inte alls kan avläsas eftersom metoden ligger i samma lager och täcker all information. Utöver detta har den här metoden också fördelen att den kan återställa den skyddade bilden till sitt originalstadium eftersom vattenmärket alstras på matematiskt vis istället för att produceras som ett inklistrat objekt. Genom att kunna nå originalstadiet utan tillgång till originalet kan man bevisa ägande.

Svagheter

Dessvärre har denna metod fortfarande ett problem som gör denna metod svår att utnyttja för rättsliga ärenden. Heltäckande vattenmärkningar täcker över all underliggande information och därför kan det inte bevisas att din version är den korrekta, utifall en dispyt skulle utlösas kring vem som har den korrekta vattenmärkningsfunktionen. Dock skall nämnas att risken för att detta sker med mer avancerade bilder är väldigt låg eftersom personer som försöker

avlägsna vattenmärkningar ofta saknar förmågan att producera liknande verk. Därför är det hela en balansgång mellan arbete och kostnad för personen som utför attacken.

Delmetod 2: Vattenmärkning av multipla färgkanaler

Bakgrund

Denna metod är en hybridmetod där den ordinarie metoden används upprepade gånger för att nå en ny effekt. Metoden kräver dock en viss strukturell design på vattenmärket för bästa effekt. Syftet med denna metod är att plantera delar av en vattenmärkning i flera färgkanaler, men samtidigt inte låta någon del ha en naturlig övergång till en annan [Ref. 1]. Till exempel kommer det vid en övergång från röd till blå inte förekomma några mellanliggande nyanser såsom lila. Anledningen till att man skapar vattenmärket på detta sätt är man vill förhindra detektion av vattenmärket för personer som inte har tillgång till den ordinarie detektionsfunktionen. Problemet med detektion uppstår eftersom vattenmärket inte kan tolkas som en hel bild. Varför märket inte kan tolkas som en hel bild visas av bilden nedan (Fig. 8.12).

Fig. 8.12 Detta är en demonstration för hur ett vattenmärke på multipla färgkanaler uppfattas om man ser till varje färglager för sig.

Punkt 1 på bilden ovan visar vattenmärket skulle uppträda infogad i en bild och skulle förstås visuellt vara lätt att urskilja från resterande delar av bilden. Detta är endast ett förtydligande exempel. Skulle vi försöka kontrollera alla 3 färgkanalerna för att se om samma mönster återkommer på alla tre och på så vis avslöja vattenmärket struktur skulle detta vara omöjligt eftersom delarna av vattenmärket skulle uppträda enligt punkt 2.

Nästa steg i denna metod är att göra vattenmärket svårare att upptäcka på respektive färgkanal eftersom en struktur enligt ovan skulle kunna innebära att det är lätt skulle kunna avlägsna vattenmärket med klipp och klistra verktyg [Ref. 1]. För att uppnå den önskade effekten bör man först och främst se till att kanterna inte är skarpa kring vattenmärkningen. Detta för att undvika precis det fenomenet som nämns ovan. Antag då att gränsen mellan två färger skulle se ut enligt Fig. 8.13.

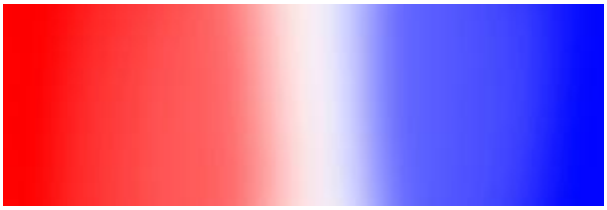

Fig. 8.13 En naturlig övergång mellan två färgnyanser ska inte användas eftersom detta innebär att man kan spåra delar av vattenmärket på flera färglager.

Lagren är nu åtskilda och gränserna är väldigt odefinierade, men på grund av att vattenmärket nu inte markerar något är det fortfarande väldigt lätt att ta bort märket. Därför krävs det även en viss transparens för att återigen införa de fördelar som fanns med metod 3.1.
Antag att vi skapar ett vattenmärke som ser ut som Fig. 8.14 och därefter placerar detta vattenmärke på Fig. 8.15.

Fig. 8.14 Detta är ett exempel på hur ett vattenmärke på multipla färgkanaler kan se ut.

Fig. 8.15 Detta är bilden vi vill skydda med vattenmärket i Fig 8.14.

Därefter erhåller vi då följande resultat (Fig. 8.16) där den inbäddade signalen nu ligger i tre separata lager och inga distinkta kanter kan erhållas genom att justera kontrasten.

Fig. 8.16 Här syns resultatbilden av vattenmärket Fig. 8.14 och bilden Fig. 8.15.

Fördelen är att även om märket uppträder som att det särskiljer sig markant från det skyddade objektet gör ovanstående egenskaper att det blir nästan omöjligt att avlägsna vattenmärket. Utöver det gör användadet av extrema färgvärden för färgkanalerna det lätt att kontrollera hur pass intakt vattenmärket är eftersom nivåerna som avläses vid detektion är så klara.

Styrkor

Separerade färger vid vattenmärkningen gör att vattenmärket är svårt att detektera då värdet för vattenmärkningen är lokaliserat på 3 åtskilda nivåer. Funktionen för vattenmärket är alltså inte kontinuerlig för hela vattenmärket. Färgningen gör även att märket är väldigt resistent mot brus. På bilden nedan (Fig. 8.17) visas ett exempel på hur bild och vattenmärke reagerade på kraftigt RGB-brus. Även om vattenmärket blir något svårare att urskilja händer precis samma sak med bilden man vill utnyttja och därför kan det ses som en effektiv metod mot bruseffekter.

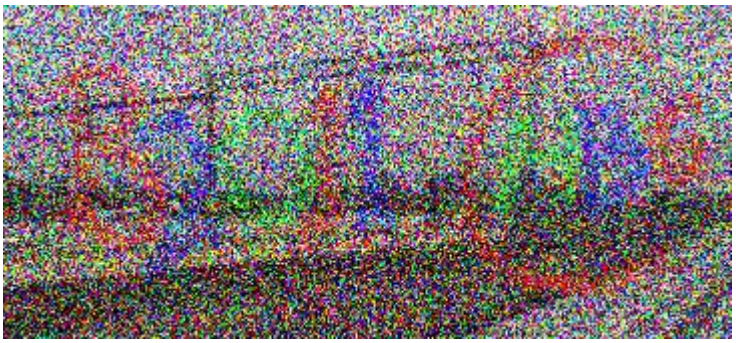

Fig. 8.17 Vattenmärket kan även urskiljas efter extrema bruseffekter.

Samma effekt fås när man försöker förstärka kontrasterna för att få fram vattenmärket (se Fig. 8.18).

.

Fig. 8.18 Förstärkta kontraster kommer inte att avslöja hela vattenmärket eftersom övergångarna är så otydliga.

Vattenmärket bibehåller sin struktur eftersom vattenmärket endast består av klara färger. Det är klart att de färgade områden på bilden som övergår i en mer enfärgad struktur kan avslöja hur delar av vattenmärkningen ser ut, men eftersom vårt vattenmärke till en början har väldigt odefinierade kanter innebär detta följande. Även om den personen som försöker avlägsna vattenmärket klarar av att avlägsna en del, är risken väldigt stor att personen kommer lämna kvar en vag kontur av den del av vattenmärket som avlägsnats [Ref. 1].

Något som kan förstärka denna typen av vattenmärkning ytterligare är om man dessutom använder sig av de extrema färgerna som uppstår vid gråskala, nämligen svart och vit [Ref. 1]. Då dämpar man effekten av en attack som justerar mättnaden. Detta eftersom vitt och svart är betydligt mer resistenta än övriga färger (RBG) då de redan finns på gråskalan. Bilderna nedan (Fig. 8.19 - 8.21) visar hur förändring i mättnad påverkar de olika extrema färgerna.

Fig. 8.19 Denna bild visar hur färgerna röd, grön, vit, blå och svart uppträder vid 100% mättnad.

Fig. 8.20 Denna bild visar hur färgerna röd, grön, vit, blå och svart uppträder vid 50% mättnad.

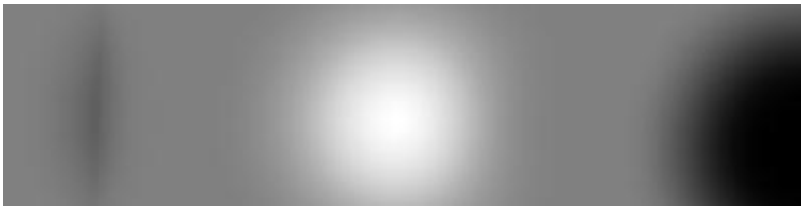

Fig. 8.21 Denna bild visar hur färgerna röd, grön, vit, blå och svart uppträder vid 0% mättnad.

Svagheter

Den största svagheten för denna typ av vattenmärkning är dess ineffektivitet vid gråskala. Anledningen till detta är den samma som att vattenmärkningen fungerar så otroligt bra för färgade bilder. För färgade bilder täcker märket upp de tre mest extrema färgtyperna (röd, blå och grön), vilket gör att om vi adderar någon av dessa färgtyper kommer vi alltid att ha kvar maxvärdet av två andra. Samma gäller bruset som nämndes ovan. Eftersom bruset sällan är statiskt innebär detta att vi kommer ha större statiska nivåer där vattenmärket finns. Bruset kan inte svänga längre än till max för ett färgvärde, vilket gör att svängningarna inte åstadkommer mer än att förvränga hela bilden istället för att sudda ut spår av vattenmärket.

Vad som gör att denna teknik brister vid användning i samband med gråskala är helt enkelt färgspektret. Antag till exempel att vi ser ett fullständigt färgspektrum som ett tredimensionellt rum där röd motsvaras av x-axeln och blå respektive grön representeras y respektive z. I detta spektrum kan färgerna variera i miljontals olika kombinationer. Om vi föreställer oss färgen för en pixel i detta spektrum som en punkt i detta spektrum är det lätt att förstå effekten av en färgpåverkan. Antag att vi har en pixel p med värdet (30, 45, 123). Väljer vi nu att maxa en färg för att försöka bli av med vattenmärket får det följande effekt. Om färgen vi anger maxinställningar för är grön kommer punktens värde att förändras till (30, 45, 256).

Det innebär att vi fortfarande har två variabler kvar där vi kan se vattenmärket. Skulle man sedan upprepa processen en gång till för ännu en färgkanal skulle vi fortfarande ha ett värde kvar att kontrollera emot, medan bilden vid det här stadiet har uppnått en monoton struktur. Ytterligare upprepning resulterar i en helvit bild.
Hade bilden varit i gråskala hade färgrepresentationerna röd blå och grön inte längre representerat extremvärden för färgspektret, som nu ligger på en komplexitetsnivå av en rak linje då värdet endast kan variera mellan två punkter. Eftersom vattenmärket ej är placerat på extremvärdesnivå innebär detta att vattenmärket påverkas hårt av brusattacker.

Tillämpning av nya extremvärden som till exempel svart och vitt hade fungerat till en viss utsträckning, men på grund av den begränsade färgskalan hade det inneburit att vattenmärket på flera ställen smält ihop med bilden man avsett att skydda.

9 Exempelscenarion

Bakgrund

Detta kapitel är ämnat till att förklara varför olika metoder bör tillämpas för olika fall.

Scenario 1: Motiv ur fokus

Fig. 9.1 En exempelbild där vattenmärket för bilden har en dålig placering.

Inledande kommentar

Denna bild (Fig. 9.1) har ett väldigt dåligt placerat vattenmärke, förutsatt att syftet för vattenmärket är att skydda bilden från stöld. Om syftet är att endast meddela iakttagande person att bilden är skyddad och samtidigt låta användaren se huvuddelen av bilden fungerar det.

Placeringsproblem

Anledningen till att placering är olämplig är att den i första hand inte täcker huvudmotivet, utan har istället placerats nere i en hörna. Detta i sig behöver nödvändigtvis inte vara något bekymmer om syftet är att blockera utnyttjandet av bilden som helhet, men eftersom ytan som vattenmärket är placerat på endast täcker lite betongvägg som är ur fokus är bilden speciellt känsligt för beskärningsattacker och direkta editeringsattacker.

Effektivaste attacktyperna

En beskärningsattack på denna bild är förödande. Antag till exempel att vi gör en vertikal avklippning precis till höger om vattenmärket. Då kommer vattenmärket inte längre att finnas kvar, men bilden kan fortfarande utnyttjas eftersom alla vitala delar av motivet finns kvar i bild.

Den andra typen av attack som lätt kan tillämpas på denna bild är editeringsattacker. Vad som gör detta så lätt är vattenmärkets placering på en bakgrund med lite kontraster och dålig fokus. Detta innebär att man inte

behöver analysera angränsande färger för att förstöra vattenmärket. Vad det i stället innebär, är att innehållet där vattenmärket finns enkelt kan ersättas med material från närliggande bildinformation och på så sätt kan man avlägsna alla spår av vattenmärkningen (se Fig. 9.2).

Fig. 9.2 Som synes i figuren är vattenmärket från figur 9.1 avlägsnat.

Utöver detta skulle man kunna addera ett brus för att ytterligare dölja inverkan på bilden.

Åtgärder

Det enklaste sättet att förebygga händelser som dessa är att placera vattenmärket på en position där det ger upphov till problem att avlägsna det.

För att uppnå detta ska man ta hänsyn till följande faktorer:

- Skärpan på kringliggande och övertäckt bildinformation. Är informationen ur fokus är det lätt att ersätta informationen med kvalificerade gissningar. Höga kontraster kommer att avslöja återanvänd bildinformation eftersom det kommer uppträda suddigt eller onaturligt i bildens helhet.

- Kontraster där vattenmärket placeras bestämmer också hur svårt det blir att producera falsk information för området. Detta kan relateras till vad som nämndes kapitlet för *Färgmängder*. Täcker vattenmärket enbart ett område där färginformationen endast varierar mellan brun och vit begränsas den möjliga färginformationen.

- Bestäm vilken del av bilden som anses vara huvudmotivet för bilden och se till att vattenmärket påverkar detta. Att omarbeta motivet för en bild medför att attacken kan skada motivet man önskar stjäla.

Scenario 2: Struktur och vattenmärkning

Fig. 9.3 Detta exempel visar ett monotont transparent vattenmärke på ett inskannat objekt.

Inledande kommentar

Bilden (Fig. 9.3) är ett exempel på en teckning skapat med analoga medel och sedan scannat in för en digital presentation. Bilden jag tecknat har ett enkelt transparent vattenmärke placerat på motivet.

Bildstruktur

En speciell egenskap med analogt producerade bilder är att de oftast erhåller en viss struktur från medlet de är producerade på och med. Detta innebär både fördelar och nackdelar. Till fördelarna hör det faktum att bilden blir svårare att replikera eftersom texturen ger bilden ett sorts heltäckande skydd. Det innebär att förändringar ofta syns genom onaturliga mönster i texturen. Med onaturliga mönster menas till exempel områden där texturen upphör eller bilden innehåller onaturliga kontraster, såsom en fullständigt vit nyans dvs. R, B och G-kanalerna alla har sitt maxvärde. Därför är bilden resistent mot lokala förändringar. Däremot blir det svårare att kontrollera heltäckande förändringar.

Vanliga attacker

Attacker som är typiska för den här sortens bilder är brus och kontrastskiften. Vad som gör dessa typer av attacker specifikt effektiva för bilder med en existerande struktur är att detta är faktorer som kunnat påverka bilden redan till en början. Med detta menas brus och kontrastskiften som uppstår vid komprimering eller inläsning från en analog bild.

På grund av de egenskaper som beskrivits ovan är det alltså viktigt att vattenmärket som utnyttjas inte har samma svagheter eftersom det innebär att bilden och vattenmärket kan påverkas av samma attack. Kan vattenmärket och

bilden påverkas av samma attack innebär det också att förändringen kan uppfattas som naturlig. Bilden som utnyttjas i detta scenario har därför ett problem trots att vattenmärket ligger ovanpå huvudmotivet. Större delen av vattenmärket är placerat på områden som saknar texturer av den anledningen att de ljusa nyanserna i bilden representeras med avsaknad av färg.

Detta medför då att vattenmärket i princip är placerat på en fullständigt vit yta (Fig. 9.4). Med justeringar rörande kontrast och brus innebär det att den lilla yta av vattenmärket som är placerat på en bakgrund med texturer påverkas.

Fig. 9.4 Vattenmärket påverkas i hög grad om det är placerat på ett område som har ett begränsat urval av karaktär, dvs. struktur, färg och kontrast är lika för hela området.

Antag till exempel att det hela vattenmärkta området representeras av procentsats på 100%. Efter avlägsnandet av vattenmärket på det vita området återstår endast 20%. Ytterligare påverkan i form av brus och kontrastskifte kan då resultera i att knappt 10% är detekterbara.

Åtgärder

Färgskalan på vattenmärket fungerar utmärkt eftersom den varierar mellan samma färger som bilden. Därför kan märket inte förstöras genom en förändring av färgbalansen. Vad som istället behövs åtgärdas är ytan som skyddas.

Låt oss kalla den yta av vattenmärket som ligger över en yta på bilden som inte är helvit för effektiv yta. Problemet är alltså att den effektiva ytan inte är en tillräckligt stor del av huvudmotivets yta (vattenmärket täcker inte hela karaktären). Detta kan hade kunnat åtgärdas genom att förstora vattenmärket och sedan använda detta. Dock bör man, om man använder sig av ett förstorat vattenmärke, se till att bildkvalitén behålls. Eftersom vattenmärket endast har

ett fåtal zoner med kontrastskiften är de viktigt att dessa påverkas av ytterligare kontrastskiften i bilden för att skapa ett så stort spektrum för vattenmärket som möjligt.

Ett större färgspektum över ett område med en struktur (från bilden) gör att man erhåller ett skydd som är mer resisten mot brus. Detta eftersom vattenmärket nu ligger över två delar med olika kontrast. Bruset skulle i området med vattenmärket innebära två olika resultat. Ett svagt brus i ett område med kraftiga färgskiften innebär att konstrastskillnaden fortfarande skulle lysa igenom. Ett starkt brus däremot skulle innebära att vattenmärket döljs, men det starka bruset leder även till en drastiskt kvalitetssänkning, vilket är någonting man vill undvika i samband med avlägsnandet av vattenmärket.

Scenario 3: Vattenmärkning av multipla färgkanaler

Fig. 9.5 En vattenmärkning som ligger på multipla färgkanaler och som används på en bild med minst samma färgskala ger ett högresistent skydd.

Inledande kommentar

Detta exempel (Fig. 9.5) visar ett exempel på god placering vattenmärket då det täcker alla väsentliga delar av huvudmotivet. Lägg också märke till att ett antal delar av huvudmotivet påverkas av flera delar av vattenmärkningen (flera olika färger av vattenmärket). Det innebär att jobbet med att avlägsna vattenmärket nu kräver arbete med att avlägsna flera olika källor.

Ett annat problem som uppstår vid avlägsnande här är att kanterna inte är skarpa. Det innebär att varje enskild källa i vattenmärket nu även har en viss varians som i sin tur innebär att man måste analysera hur långt den här mindre skarpa konturen sträcker sig för att fullständigt eliminera vattenmärket. Att inte fullständigt beräkna var någonstans vattenmärket upphör kan leda till att vattenmärket kvarlämnar en kontur och därför kan detekteras.

Bildstruktur

Om fokus läggs på bilden kan man se att bilden har en viss textur. Denna textur har inte uppkommit i samband med produktion på papper eller annan inskannad källa. Istället har denna textur erhållits genom komprimering i samband med framställningen av bilden. Denna typ av textur kan utnyttjas för att kontrollera om bilden blivit utsatt för lokala attacker (med lokala attacker menas attacker som endast påverkat bilden på ett antal ställen och inte hela bilden). Dessa lokala attacker kan urskiljas med hjälp av så kallad Error level Analysis.

Error Lever Analysis fungerar som så att man upprepade gånger sparar objektet i ett känt filformat. Genom att göra detta ser man att komprimeringar i vissa områden kommer att vara mer omfattande. Anledningen till detta är att ändringar som gjort vid senare tillfällen inte kommer ha påverkats av lika mycket komprimering som de tidigare skapade områdena av bilden. Om något området inte påverkats så mycket av komprimering, innebär detta att det

området också förändras mer än resterande delar av bilden vid framtida nersparning.

För just denna bilden har vattenmärkets placering bidragit till att man vattenmärkt strukturen. Vilket, liksom i föregående exempel bidrar till att bilden blir svårare att förändra utan att det märks på strukturen. Till nackdel är dock att denna struktur är datorgenererad i samband med komprimering. Detta innebär att texturen går att reproducera genom att utnyttja samma komprimeringsmetoder.

Vanliga attacker

Eftersom denna metod i grunden bygger på att producera ett skydd bestående av ett flertal lager med olika färgnivåer är det vanligt att man försöker kringgå detta med hjälp av att påverka bildens färgmängd. Till exempel resulterar en omvandling till gråskala i följande resultat (Fig. 9.6).

Fig. 9.6 Färgerna i bilden påverkas i omfattande skala när den konverteras till en monokrom färgskala.

Vad som inträffar är att färger vars mättnad inte är tillräckligt hög (relativt beroende på vilken bild som används) kommer att neutraliseras när man sedan sänker mättnaden för hela bilden (gör om bilden till gråskala). Anledningen är den att färgerna i gråskala produceras genom ett lika värde för samtliga RGB-kanaler. Antag nu att färgen vi har är röd (R = 255). För att uppnå ett värde på gråskalan innebär detta att färgnivåerna måste justeras radikalt för att erhålla en nyans som ligger på gråskalan. I bilden ovan används visserligen alla extremtnivåer av färger för RGB-kanalerna, men ändå är det bara på visa delar av bilden som vattenmärket i princip försvinner.

Fenomenent förklaras med det faktum att vattenmärket är transparent. Detta transparenta lager innehåller yttterligare färginformation som påverkar vattenmärket. Kombinationen av vattenmärket och bilden är alltså det som förändras vid mättnadssänkning. Hade målet nu varit att försöka utvinna något i bild som inte ligger under vattenmärket, hade detta varit relativt enkelt, men

man måste också ställa frågan vad det är som man vill utnyttja i bilden. Kan personen som utför denna attack fortfarande vilja utnyttja en bild i gråskala?

Åtgärder

Om en bild med rik färgskala omvandlats till gråskala är det fortfarande fysiskt möjligt att utnyttja bilden, men bilden är nu också väldigt förändrad från sitt ursprung. Eftersom det i detta läge är svårt att återställa bilden till ett färgat format utan att också återställa vattenmärket, är det i detta läge som hela problemet blir subjektivt. Hur stor förändring av objektet är personen som attackerar bilden villig att stå ut med för att få tag i bilden?
I bilden ovan så återstår delar av vattenmärket eftersom det inte innehar samma färgvärden som de övriga färgerna som försvann vid transformationen. Genom att man producerar samma märke med mindre fragment som bygger upp märket, kan man producera ett flertal fält som kvarstår vid en sådan transformation.
Ett exempel på hur detta skulle kunna se ut framgår ur bilderna nedan. Den övre bilden representerar den oridnarie vattenmärkningoch följande bild visar hur samma märke produceras med mindre fragment.

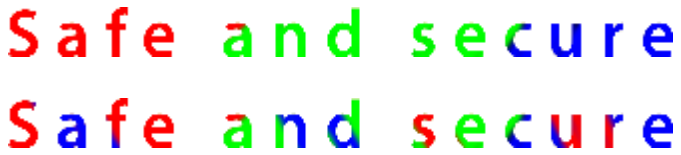

Fig 9.7 Detta demonstrerar hur man kan producera samma vattenmärke med samma färger, men med en skillnad i storlek på de olika fragmenten.

Nackdelen med en sådan lösning är att det blir svårare att placera märket på ett sådant sätt att det inte förlorar sin mening genom att ligga på ett område som inte ger något egentligt skydd. Dvs att ett fragment ligger på en sektion där det endast bidrar till att täcka en yta med enkel information, såsom enfärgade delar av bilden.

10 Ett användbart program

Gimp 2.6.11

Gimp är ett GNU bildbehandlingsprogram som stödjer massvis med funktioner. Några av dessa funktioner var speciellt användbara för att utvärdera såväl vattenmärkningsmetoder som attacker.

Bildjämförelse (subtraktion gjord med bilder)

Denna funktion har en metod som gör en direkt jämförelse mellan två lager och subtraherar det överliggande lagret från det nedre. Funktionen använde jag för att bl.a. se effekten av en attack samt undersöka hur mycket av vattenmärket som kan urskiljas efter attacken. Som ett exempel på detta är här (Fig. 10.1) en jämförelse mellan de två bilderna (Fig 10.3 och 10.4) som förekommer i följande kapitel under sektionen *Placering*.

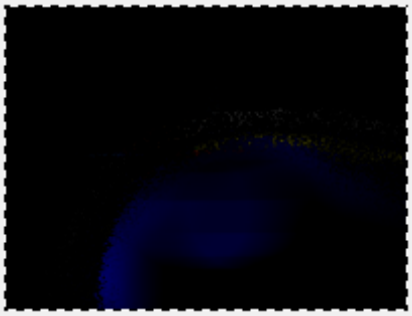

Fig. 10.1 Detta är en bild som visar resultatet av en subtraktion mellan en vattenmärkt bild och en bild där vattenmärket utsatt för en avlägningsattack.

Det svarta i bilden motsvarar en avsaknad av förändring dvs. ingen påverkan har skett på detta område eller så är påverkan så effektiv att bilden har reproducerats med originalkvalité på detta område.

Färglagerfiltrering

Denna funktion låter användaren visa enskilda färglager (rött, grönt och blått). Funktionen var speciellt användbar för att undersöka effekten av kontrastförändringar samt se hur vattenmärkningsmetoderna uppträder i de olika kanalerna.

Fig. 10.2 Detta är en demonstration av en bild visad med enbart en röd färgkanal

Bilden (Fig. 10.2) visar till exempel hur mycket av vattenmärket som finns synligt i den röda kanalen och hur tydligt det uppträder.

Attacker

Programmet har även varit till stor nytta för att producera de attacker som finns. Det går att producera bruseffekter som efterliknar komprimering utan att faktiskt komprimera bilden. På så sätt kan man undersöka komprimerings-effekten utan att skapa en ny grund för hela bilden. Även andra typer av bruseffekter som använts i detta examensarbete har producerats mha. detta program. Detta innebär att jag kunnat undersöka metodernas resistens mot flera typer av brus.
Attacker såsom direkta editeringsattacker, reproduktion av bildmaterial via kloning, klippning, gråskalatransformering, rotation, histogramanalys och dylikt har gjort mha. Gimp.

Histogramanalysen är i sig ingen inbyggd funktion, men går att utföra i även de enklaste av bildediteringsverktyg. Detta beror på att de flesta verktyg har följande funktioner som kan användas för ändamålet.

- Funktionen ”hämta färg” – Denna funktion hämtar värdet av en färg redan existerande i bild och ersätter den aktiva färgen med denna.
- Färgval via inställning av färgkanaler – Denna låter användaren bestämma färg genom att ange värden på de tre färgkanalerna.

Med hjälp av att då för hämta en färg och sedan konfigurera färg kan man erhålla färgen för varje ruta och därefter beräkna skillnaden.

Nackdelar

Dock skall påpekas att även om program av denna typ är till stor hjälp vid produktion av bilder och vattenmärkning (synlig) är dessa program också i lika många fall skyldiga till avlägsnande av vattenmärkningen.

11 Slutsatser

Färgmängder

Färgmängderna i bilden är den absolut viktigaste faktorn i valet av vattenmärke eftersom balansen med vattenmärket är vad som avgör vilken metod som krävs för vattenmärkning. I de flesta fall kan man tillämpa en relativt enkel metod där man använder ett vattenmärke som har ett färgspektra som ligger nära maxvärdet för filtypen, men samtidigt finns det ett antal fall där denna lösning inte kan tillämpas. Detta är fall då bildens färgspektra är väldigt begränsat. I sådana fall bör man tillämpa en vattenmärkning som ligger i samma begränsade färgspektra som bilden ligger. Enkelt uttryckt kan man definiera lösningen enligt följande.

Vattenmärkningen ska använda ett färgspektrum som är på samma nivå som bilden man avser att skydda. Använder man två olika färgspektrum innebär det att det finns vissa färgkombinationer som bara kan uppstå vid kombination av dessa två färgspektra. Problemet blir allt större desto mer begränsat färgspektret är. Ett extremfall för detta kan till exempel vara då bilden är svartvit. I detta fall skulle det innebära att ett vattenmärke som innehåller en färg som avviker från svart eller vit. Det innebär i sin tur att det skulle vara trivialt att avlägsna vattenmärket.

Såsom också kan utläsas i ovanstående exempel innebär ett begränsat färgspektrum för både bild och vattenmärke också att det blir svårare att tillverka ett skydd som är tillräckligt för att skydda bilden med enbart en synlig vattenmärkning. Eftersom bilden i exemplet endast är svart och vit innebär detta att vattenmärket blir enkelt att urskilja (innehåller en färg som inte finns i bilden) eller att man förstör bildens struktur (vattenmärket har samma färg som bilden).

Struktur

En annan viktig aspekt att ha i åtanke är att man bör matcha bildens och vattenmärkets struktur. Detta har till viss del att göra med ovanstående slutsats, men problemet är lite mer lokalt. Till exempel så kan bilden bli extra känslig för attacker om bilden har skarpa konstraster där vattenmärket inte har det och vice versa. Även då färgspektret är det samma gör detta att man kan urskilja tydliga gränser för vattenmärket. Detta i sin tur innebär problem i stil med att vattenmärket lätt kan utsättas för en direkt avlägsningsattack, överlagring av färgvärden eller bortklippning. En slutsats som dock kan dras baserat på *Delmetod 2* för *Hybridmetoder* är att även om vattenmärket är visuellt åtskiljbart, så kan det fortfarande vara svårt att avlägsna.

Placering

Det gäller att iakttaga försiktighet vid placeringen av vattenmärket. Se nedanstående bild Fig. 10.3.

Fig. 10.3 Detta är en exempelbild med en röd vattenmärkning på ett gult fält.

I bilden ovan är huvudelen av vattenmärket (det röda området) placerat på det gula fältet (notera att kontrasten är överdriven för att märket ska vara urskiljbart för studiesyften). Även om jag nu inte vet det exakta värdet för den underliggande färgen för det skyddade området kan en uppskattning lätt göras. Att enbart attackera bilden ovan i avsikt att få bort märket på det gula området skulle dessutom leda till att ca 80% av vattenmärket försvinner. Med återstående 20% kvar kan ett lätt brusfilter ge förödande resultat för alla försök att avslöja en tidigare vattenmärkning. Bilden nedan är ett exempel på hur ovannämnda attack kan påverka bilden.

Fig. 10.4 Såhär kan bild 10.3 se ut efter en editeringsattack och brusattack.

Utveckling av ny metod

Att utveckla en ny metod för synlig vattenmärkning av digitala bilder är inte aktuellt av flera anledningar, men främst av dessa anledningar är det faktum att varje bild har en specifik färgmängd och struktur. Detta innebär att vattenmärket bör vara konstruerat efter bilden man avser att skydda. Konsekvensen av detta skulle bli att varje typ av bild skulle behöva en specifikt utvecklad lösning.

Vilket leder till det andra problemet med att utveckla en ny metod. Antalet sätt en bild kan vara konstruerad på resulterar i ett problem i utvecklingen även för enkla fall. Tag till exempel en bild med begränsad färgmängd och struktur, som i till exempel bild av en logotyp. Såsom nämnt är det effektivaste vattenmärkesalternativet för denna typ av bild ett vattenmärke som är heltäckande i något avseende. Möjligheterna för att producera en heltäckande bild är något begränsade.

Om man istället ser till de transparenta metoderna, som då lämpar sig bättre för bilder med ett mer varierande färgvärde, är det största problemet bildens struktur. På grund av varianserna i struktur, textur, färgintervall, färgmängd, kontraster och dylikt är det svårt att utveckla en metod som lämpar sig för att skydda bilden i den utsträckning som behövs. Istället är det av vikt att förstå teorin kring vad som gör ett vattenmärke svårt att avlägsna och producera ett vattenmärke utifrån dessa grunder.

Bästa nuvarande metod (för alla typer av bilder)

Om ett val måste göras för vilken typ av metod som fungerar bäst för att skydda samtliga sorters bilder, kommer det att vara den metod som för tillfället också används som mest.

Den monotona transparenta vattenmärkning fungerar bäst överlag eftersom chansen för att vattenmärkets spektra finns i bildens spektra är som störst. Det innebär att vattenmärket förblir intakt vid mättnadsförändringar. Även då beräkningarna för att finna vattenmärkets värden är enklare än vid flerfärgad transparent vattenmärkning, så är det av större vikt att färgvärdena inte särskiljer väsentligt från varandra. Gråskalan förekommer till lika stor del i färgade bilder såsom svaritvita då den används för att sätta ljusnivå i bilden. Därför är den bättre lämpad till att användas över lag. Att använda sig av ett färgat spektra i vattenmärkningen om bilden inte är färgad resulterar i samma utgång som i *Exempelscenario 3*.

Vad kunde gjorts annorlunda

En första reflektion var att en djupare insikt i vad som behövdes kring ämnet innan valet av examensarbete påbörjades hade varit till stor nytta. Den parallella inlärningsmetod som utnyttjades för detta arbete gjorde att djupare kunskap kring ämnet saknades och att målbilden var något vag.
Något som också visade sig problematiskt med informationsinsamlingen var det faktum att de flesta källor som behandlar ämnet vattenmärkning fokuserar på osynlig vattenmärkning och så kallad steganografi. Även då viss del av teorin kunde utnyttjas för synlig vattenmärkning var det för ovannämnda områden som den vetenskapliga grunden fanns. Eftersom mitt mål var att undersöka teorin kring förebyggande av stöld av bilder och inte förmågan att kunna spåra bilder efter stöld höll jag fast vid konceptet med synlig vattenmärkning.
Något som visade sig problematiskt med detta beslut var dock hur otroligt subjektiv teorin kring synlig vattenmärkning är. Till skillnad från osynlig vattenmärkning är denna teori beroende av bildens utseende och sålunda visade dig svårt att komma till en klart överlägsen metod.

12 Referenser

Webbkällor:

[1] Watermarking
http://www.angelfire.com/electronic/kfrank/water/index.html
Mars 2011

[2] Sveriges lag på nätet
https://lagen.nu/1960%3A729
Mars 2011

[3] Steganography And Digital Watermarking
http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf
Mars 2011

Litteratur:

[4] Techniques and applications of digital watermarking and content protection Av Michael Konrad Arnold,Martin Schmucker,Stephen D. Wolthusen 2003 Artech House, INC. ISBN: 1-58053-111-3

[5] Digital watermarking and steganography Av Ingemar J. Cox 2008 Elsevier Inc, ISBN: 978-0-12-372585-1
