

# VATTENMÄRKNING

Ahmed Ali                      Eje Svensson  
Linköpings universitet, Sweden  
Email: {ahmal229, ejesv793}@student.liu.se

## Abstract

*This work presents some watermarking techniques and their characteristics. Specific areas of interest will be listed with their advantages and disadvantages. We will try to conclude if the current techniques hold against common attacks.*

## 1. Inledning

Digital vattenmärkning är en relativt ny teknik som nu på senare tid blivit högaktuell i kampen mot den allt mer utspridda piratkopieringen. De första metoderna som skapades för vattenmärkning av digital media kunde kringgå med enkla metoder, men på senare tid har märkningarna blivit smartare och svårare att knäcka.

### 1.1 Bakgrund

Vattenmärkning är en metod för att kunna skydda material som blir kopierade och om så sker kunna spåra kopian tillbaka till vem som ägde originalet. Vattenmärkning kan även användas för att avgöra vem som spridit en kopia genom en unik vattenmärkning i varje kopia.

Vi vill ta reda på hur hållbara dessa metoder verkligen är i dagens samhälle då många processer kan automatiseras med hjälp av datorer. Är det möjligt att filtrera bort skyddet eller förändra det så att det inte går att spåra vem som är skyldig till spridandet av en produkt? Går det lyckas få någon oskyldig verka skyldig?

Nu senast anklagades ett par personer för spridning av filmer i samband med oscarsnomineringen. Detta är ett tecken på att det finns metoder som lyckas med vattenmärkningens mål. Nu börjar även vattenmärkning spridas till mjukvarudistribution som tillämpar unikt distribuerade filer, troligen tillsammans med spårbarhet. CoreAVC [3] är ett exempel på mjukvara som sprids på detta sätt. Det ska bli intressant att se om denna teknik lyckas uppnå någon form av spårning, eller om antalet användare i slutändan kommer överstiga skyddets kapacitet.

### 1.2 Metod

Vi genomfört en teoristudie och tittat på nuvarande tekniker och hur hållbara de verkar vara mot existerande

attacker. Vi har även jämfört olika tekniker för att belysa eventuella fördelar och nackdelar.

Digital vattenmärkning är ett nytt ämne, därför finns det lite tryckt material inom ämnet, samt utvecklingen inom området går snabbt och därför är det lämpligast att använda artiklar och uppsatser från Internet som primära informationskällor.

Rapporten riktar sig främst mot personer med viss teknisk expertis inom dataområdet, gärna med förståelse för kodningsteori.

### 1.3 Frågeställning

Hur hållbara är dagens vattenmärkningstekniker och hur ser framtiden ut för vattenmärkning?

### 1.4 Definitioner

De definitioner vi använder oss av förklaras nedan.

- Watermarking: Vattenmärkning bäddar in information i media som till exempel innehåller information om rättigheter och ägaren till mediet.
- Fingerprinting: Detta är en inbäddad signal i media som kan innehålla information om användaren. Denna information kan användas för att spåra källan till olaglig kopiering.
- Inbäddning av information: Information integreras med innehållet i mediet.

### 1.5 Begränsningar

Rapportens storlek och den begränsade tiden gör att vi inte kan täcka all teknik inom området och därför har vi valt att inte gå in på helt nya områden som t.ex. unik vattenmärkning för media som sänds i broadcast-miljö. Vidare har vi koncentrerat oss mest på film- och musikmedia.

## 2. Användningsområden

I den här delen av rapporten listas olika användningsområden för vattenmärkning tillsammans med deras fördelar och nackdelar. Vi måste även skilja på vattenmärkning i de fall man vill kunna spåra vem som skapade mediet, copyright protection, och de fall där man vill kunna spåra vem som ursprungligen fått en kopia av ett mediet, receiver information även kallad fingerprinting [1].

Det finns många fördelar med vattenmärkning för olika medium. Olika tekniker resulterar i olika mål beroende på de aktuella kraven och detta leder till att olika märkningssätt är bättre i olika fall. Den första varianten av vattenmärkning som uppkom var stenografen. Detta är ingen vattenmärkning om man ser till vanliga mått. Metoden döljer endast extra information i befintlig text och kan därför anses vara en tidig form av vattenmärkning. Den tidigaste användningen av vattenmärkning i stor skala som vi känner till är inom sedeltillverkningen. Där används vattenmärkning som en verifiering att sedeln är äkta, och målet med denna märkning är att otillåten nyskapning av sedlar ska bli svårare.

Nästa användningsområde är bilder. I bilder det att lagra mer eller mindre synlig information som helst inte ska vara störande, men ändå går att använda för identifikation av olika saker. Ett närliggande exempel på Linköpings universitet är de tidigare öprintade IDA® alla utskrifter. Målet för vattenmärkningen ledet till hur synligt vattenmärkningen är. I IDA:s fall var målet att begränsa användandet av utskrifter till studierelaterade ändamål, så då var den enklaste lösningen en genomskinlig text över hela sidan. I andra fall vill utgivaren troligen inte att vattenmärkningen ska vara synlig, utan kunnas ta fram om det blir en fråga om vem som äger bilden. Ett vanligt fall på detta är bilder på Internet. Där förekommer det mycket användande av andras bilder. Om tvist uppkommer om vem som äger originalet till en bild är det en stor fördel om den rätta ägaren kan peka på ett eget vattenmärke i bilden [1].

Efter bilder är det naturliga steget att gå till rörliga bilder, med andra ord film. Här är det media som det i dagsläget förekommer mycket jobb för att skapa bra vattenmärkning. Som tidigare nämndes åklagades nyligen ett par personer för olaglig kopiering av film i samband med oscarsnomineringarna. Detta är ett tecken på att det finns tekniker som både är svåra att upptäcka och ta bort men ändå ger bra spårnings-möjligheter och som används i industrin. Inom film går det att använda tidsaxeln för att dölja information, vilket skapar en helt ny dimension till vattenmärkningen.

Nu är det logiskt att ta steget till ljudmediumet. Analogt ljud är ganska svårt att vattenmärka utan att det märks. Det vanligaste fallet är att det införs ett högfrekvent brus ovanför ljudet vilket i mer eller mindre utsträckning förstör ljudkvaliteten. I andra fall läggs det in eller tas det bort ljud i vissa delar av ljudet eller skapas det hopp. Dessa modifikationer stör på ett annat sätt men är kraftfullare mot förlust av ljudkvalité vid kopiering av ljudet. I och med införandet av digitala medium och därmed perfekta kopior går det att skapa ett vattenmärke genom att ibland ändra på minsta signifikanta bit i ljudströmmen. Dock klarar ett sådant vattenmärke sig

extremt dåligt mot förluster vid t.ex. komprimering eller medvetet tillagt brus.

När vi nu har tagit steget in i den digitala världen kommer det naturliga steget vattenmärkning av program i spårningssyfte. Microsoft har länge använt sig av signering av program vilket inte är något vattenmärke i sig, men detta minskar viljan att istället skapa bra vattenmärken. Spårning är annars användbart då utgivaren vill hindra spridandet av förhandsversioner av program, eller ha möjlighet att hitta vem som är skyldig till spridandet. Spårningsmöjligheten blir vanligare även för slutversioner av program som exempelvis fallet med CoreAVC enligt ovan. Enligt förespråkarna ska detta leda till mindre piratkopiering och därmed fler betalande kunder [10].

Dagens samhälle har i större utsträckning den synliga vattenmärkningen som används för verifiering av vem som gjort en produkt ersatts av hologram, detta eftersom sådana är svårare att kopiera. Dock så är hologrammen svåra att integrera i själva produkterna, därför brukar dessa följa med som klisterlappar, vilka i sin tur är lätta att flytta på. I dagens sedlar har hologram integrerats helt, men samtidigt finns vattenmärkningen fortfarande kvar.

Ett exempel på användandet av vattenmärkning för spårning är kopieringsapparater och skrivare som har en mer eller mindre osynlig märkning på sina utskrifter i form av punkter som representerar serienumret. Detta för att det ska gå att spåra utskrifter till en specifik maskin.[4]

## 2.1 Fördelar

I detta stycke beskrivs fördelarna man får med vattenmärkning för de givna mediumen.

I alla fallen för de olika mediumen är största och ibland även den enda fördelen bara själva skapandet av skyddet mot kopiering och/eller spårningsmöjligheten.

I sedelfallet kan man identifiera att sedeln troligen är äkta, men i detta fall går det att argumentera att själva vattenmärket skapar en ökad artistisk känsla. Det blir även lättare för maskiner att på ett säkert sätt identifiera äktheten och valören på en sedel.

I bildfallet går det att använda vattenmärket för att visa på ägande, men inte mycket mer eftersom det är svårt att säkert lagra de relativt stora mängder data i en bild som krävs för fingerprinting.

Inom film däremot går det att ändra lite på den enorma mängden bildinformation som finns för att kunna spåra enskilda kopior av filmen.

Inom ljud är det mer komplicerat att bädda in information eftersom vattenmärkning på ljud oftast påverkar ljudkvaliteten markant.

När det gäller mjukvara finns det inga direkta nackdelar med vattenmärkning, och det är en stor fördel i sig. Mjukvara behöver inte fungera sämre för att man har

integrerat ett vattenmärke i koden, eftersom det finns mycket information som aldrig eller sällan visas för användaren.

## 2.2 Nackdelar

Här listas nackdelar med vattenmärkning för de givna mediumerna.

Den största nackdelen med vattenmärkning på sedlarna är att det är ett extra steg i produktion och denna blir då dyrare.

Inom bilder är nackdelen att bilden försämras jämfört med originalet. I vissa fall är detta själva skyddet, men oftast är målet att så mycket som möjligt av originalinformationen ska förbli intakt. I andra fall är målet att ändringarna endast ska upptäckas om man jämför bilden med originalet, dvs. inte störa vid betraktning av bilden.

Inom film finns det mycket bildinformation att en liten förändring i en eller ett par bildsegment oftast inte märks. Skyddet ska helst kunna klara förstörande omkodningar till andra format. Detta kan förstöra för nästan osynliga vattenmärknings, eftersom komprimering till stor del kommer filtrera bort dessa.

Inom ljud är det svårt att få bra vattenmärkning som inte hörs, dock går det att luras om vattenmärkningen integreras så att det blir en naturlig del i ljudet och på så sätt komma ifrån att märket stör lyssnaren.

I mjukvaruvärlden finns inga direkta nackdelar med vattenmärkning, eftersom dessa kan bestå av extremt små förändringar, men ändå innehålla mycket information. Dock slår den digitala perfekteten emot systemen, eftersom personer som vill kringgå systemen kan gå ihop med flera kopior och direkt hitta de ställen där källorna skiljer sig. Bra val av digital kodning kan dock delvis lösa detta vilket vi ska ta upp senare i rapporten.

Ett allmänt problem med vattenmärkning är att det i många fall är lätt att kringgå teknikerna. En attackerare kan till exempel i många fall med samma teknik som användes vid första märkningen lägga till ett nytt vattenmärke över originalmärkningen och på så sätt skriva över denna.

## 3. Olika tekniker

Här ska vi lista existerande tekniker och vad som utmärker dessa.

Olika tekniker har tagits fram för att generera och använda vattenstämplar. Vi ska i det här kapitlet redovisa för de viktigaste teknikerna och förklara kortfattat hur de fungerar för att i ett senare kapitel gå in på djupet i en av teknikerna som vi finner intressant. Det finns för närvarande ingen standard som följs överallt, utan olika företag har tagit fram olika tekniker som passar deras produkter och bransch på bästa sätt. Tekniker skiljer sig

åt på många sätt, men det finns vissa gemensamma egenskaper som alla tekniker använder sig av och det är:

- Skapandet av själva vattenmärket med hjälp av en privat "nyckel" som ägaren till objektet har
- Inbäddning av vattenmärket i objektet
- En teknik för detektering av vattenmärket.

Olika tekniker:

- Private or nonblind watermarking schemes: en teknik som kräver tillgängligheten av originalobjektet för att kunna jämföra och fastställa legitimiteten. Denna teknik är oftast inte användbar med dagens användning av media på Internet då det oftast inte är möjligt att ha originalobjektet publikt tillgängligt.
- Public or blind watermarking schemes: en teknik som i motsats till tekniken ovan inte kräver att originalobjektet är tillgängligt under detekteringsfasen. Det enda som behövs då är en nyckel från ägaren. Denna teknik är mer användbar än den förra eftersom originalobjektet inte behövs och då kan detektering och fastställning av objektets legitimitet göras lättare.

Ett exempel på en inbäddningsteknik som används för att "lägga in" information i ett objekt heter "the least significant bit insertion (LSB)" [8]. Digitala bilder sparas vanligen i en 24-bits eller en 8-bits fil. För de bilder med 24 bitar som är flerfärgade, skapas pixelvariationen med hjälp av tre primära färger: röd, grön och blå (RGB). Varje primär färg tar upp en byte och då tar en RGB pixel tre bytes. En RGB pixel kan exempelvis se ut som följande ( 11000110 10111000 10000100). Det krävs tre pixlar för att "dölja" en byte information eller data när LSB-tekniken används. Om exempelvis bokstaven B ska bäddas in i tre pixlar i en bild med värdena:

```
(11000110 10111000 10000100)
(11000110 10111000 10000100)
(11000110 10111000 10000100)
```

Där den sista biten till höger ändras.

```
(11000110 10111001 10000100)
(11000110 10111000 10000100)
(11000111 10111000 10000100)
```

Genom läsning av den sista biten till höger på varje byte i denna grupp av pixlar ovan kan man se att det binära värdet 01000010, där resten av "byte" inte används i det här fallet. Principen är att ändringarna som

tillförs ska vara små att ändringarna på färgerna som resulterar inte går att märka med det mänskliga ögat.

En intressant teknik är användandet av vanlig löpande text i en bild för att koda in information. Små förändringar som exempel olika avstånd på rader eller förändrad utformning av enskilda tecken är svåra att upptäcka om man inte har en annan källa att jämföra med.

Det finns metoder för att klara av flera samtidiga pirater som går samman med flera olika kopior som har olika vattenmärken. En metod kallas spread spectrum watermarking [1] och är i grunden att utgivaren lägger in flera vattenmärken i mediet. Det gör att när flera pirater kombinerar sina kopior kan utgivaren ändå se vilka kopior som används för att skapa den kopia som spridits genom att använda sig av en korrelation mellan originalfilen och denna skapade kopia.

#### **4. Synlig och osynlig vattenmärkning - en jämförelse**

Vanlig vattenmärkning på papper räknas som synlig vattenmärkning. Största fördelen med synliga vattenmärken är att personer snabbt kan se varifrån ett dokument kommer ifrån, dvs. identifikation av källan. Ett vanligt exempel på detta är loggan i övre hörnet på tv-sändningar. En logga används ofta för att visa på att materialet är upphovsrättskyddat och samtidigt som en bonus skapa lite reklam för utgivaren. Tanken med detta är att om någon kopierar materialet ska märket finnas kvar så personen inte senare kan hävda att materialet kommer från någon annan källa. Ägarna till originalet kan även för varje kopia variera vattenmärkningen lite och på så sätt kunna identifiera olika kopior. Ett sådant skydd kringgås dock lätt genom att helt enkelt ersätta hela vattenmärket med t.ex. en konstant färg eller ett medel av omgivande färger. Denna typ av vattenmärkning finns ofta i förhandsutgåvor av filmer. I filmfallet är loggan vanligtvis ersatt med en text som även uppmanar att rapportera olagliga kopior.

En fördel med synliga vattenmärken är att upphovsmannen kan välja storleken på vattenmärket och var det ska placeras i bilden. Skyddet blir lättare att ta bort om det befinner sig i ett hörn, eftersom det då går att kapa bort kanterna för att kringgå märkningen helt och hållet.

En annan fördel med synliga vattenmärkning är att det är svårare att ta bort vattenmärket utan att bilden får märkbara defekter.

Ett problem då vattenmärkning används för att antyda om källan, är att en enkel vattenmärkning kan förfalskas. I fall då källan verkligen är viktig är det bättre att använda externa signaturer som använder bilddatan för att skapa en verifieringsbar hashning [2].

Osynlig märkning kan vara små förändringar i råa bitströmmen eller väldigt små färgförändringar i en bild. Det mänskliga ögat har svårt att skilja på små förändringar i färger men märker kontrastförändringar lätt. Detta används även vid komprimering av bilder, så ett vattenmärke som enbart beror på färger har en stor risk att suddas ut vid komprimering eller filter som smetar ut just små avvikelser.

Osynlig vattenmärkning är svårare att upptäcka och kan därför användas för att spåra vilken källa som kopierats. Nackdelen med osynlig märkning är att vanliga filter eller komprimering kan förstöra de små förändringar märkningen är uppbyggd av. Vidare kan många metoder för att skapa osynliga märkningar automatiskt upptäckas genom det brus som skapas [5].

En allmän metod för att förstöra eventuella vattenmärken är att först blanda flera olika källor och skapa ett medelvärde och sedan applicera en brusfunktion på resultatet. Bilden förstörs väldigt lite, men vattenmärken i mediet blir kraftigt skadade.

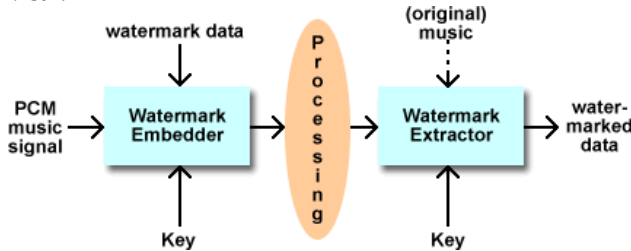
Målet med osynlig vattenmärkning är att originalbilden ska förändras så lite som möjligt, men ändå vara så svår att ta bort så att en borttagen vattenmärkning resulterar i att mediet är obrukbart för det tänkta ändamålet [1].

#### **5. En teknik på djupet - Vattenmärkning av ljud/Mp3**

Att bädda in vattenmärken i en ljudsignal kan genomföras med två olika metoder. Bädda in vattenmärket innan kompression av ljudsignalen så kallad PCM-watermarking eller att bädda in vattenmärket efter kompressionen så kallad Bitstream watermarking. Vattenmärkning av ljud gör att information eller data kan bäddas in i ljudsignalen. Informationen kan sedan användas till att skydda upphovsrätten till ljudet (MP3-filen) och att visa annan data som är kopplat till filen som exempelvis namn, artist, utgivare och för att visa den legitima ägaren till filen. Vattenmärkningen måste vara robust och överleva vanliga operationer på ljudfiler som exempelvis digital/analog konvertering, filtrering och tidsskiftningar. Detta gör att det blir lite svårare att avlägsna vattenmärket från filen.

Grundidén till att bädda in informationen i ljudfilen använder sig av en teknik som gör det möjligt att "gömma" information om vattenmärkningen i de ohörbara frekvenserna för det mänskliga örat. På så sätt märker inte den vanliga användaren ens av vattenmärket. Nackdelen här är att ljudfilen kommer att innehålla lite "brus" som kanske inte märks i ljudfiler med populärmusik, men som kan upptäckas av expertlyssnare och/eller med andra typer av musik.

En allmän bild av hur vattenmärkning av ljud kan gå till visas i figur 1. Från vänster i figuren kommer originalljudet in, i sin okomprimerade form, och där bäddas vattenmärket in med en privat nyckel. Efter detta kan ljudet komprimeras eller på annat sätt förändras. Nu kan en användare med sin publika nyckel återskapa vattenmärkets innehåll. I vissa fall kan originalljudet behövas för att extrahera informationen som figuren visar.

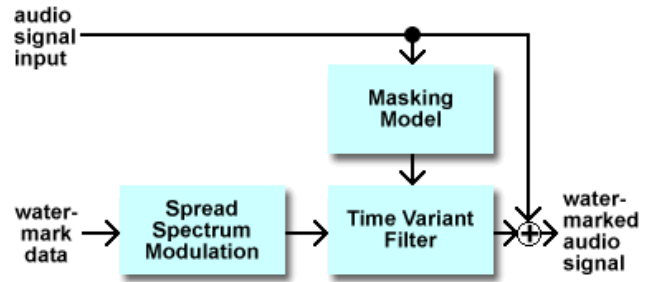


Figur 1 – Vattenmärkning av ljud

Ett exempel på vattenmärkning av ljudfiler som används på marknaden är Sony/Phillips SACD-format som har tagits fram för att möta dagens krav på ljudkvalité och skydd mot kopiering. SACD använder sig av tre olika typer av vattenmärkning. Ett synligt vattenmärke som upplyser köparen eller konsumenten att det är en original kopia. Den andra vattenmärkningen finns digitalt mellan spåren och innehåller "tillstånd" för att använda filen/filerna och till sist en analog vattenmärkning. De två första typerna av vattenmärkningen påverkar inte själva ljudfilerna alls och sänker därmed inte kvaliteten på ljudet. Det är den analoga vattenmärkningen som lägger till ett brus i ljudfilerna. Om den analoga vattenmärkningen verkligen behövs eller inte är upp till musikutgivare att bestämma uppger Sony/Phillips. [6]

## 5.1 PCM watermarking

PCM tekniken bäddar in informationen som innehåller vattenmärket linjärt in i ljudfilen dvs. innan ljudfilen har blivit komprimerat till exempelvis MP3-format. Den grundläggande idén är att gömma en lågfrekvent signal som befinner sig under mediats lägsta uppspelningsbara nivå vilket illustreras av figur 2. Detta säkerställer att signalen inte kan höras. Extraktionen av vattenmärket sker enkelt med hjälp av en bredbandsmottagare implementerad i mjukvara. Vattenmärket kan ses som en sekvens av informationsbitar. Tolkningen av informationssekvensen är vad utgivaren gör den till. Detta betyder att all information som går att visa/uttrycka med bitar går att bädda in i vattenmärket.



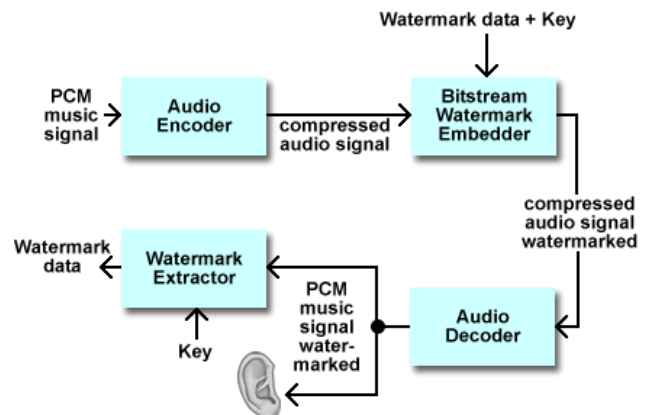
Figur 2 – En variant på hur vattenmärkning av ljud kan gå till

## 5.2 Bitstream watermarking

Här bäddas vattenmärket direkt in i komprimerade ljudfiler dvs efter att filerna har blivit komprimerade. Fördelen är att man på så sätt kan spara mängder av diskutrymme, speciellt i stora databaser och på musik-hemsidor, då de okomprimerade filerna som vanligtvis är mycket större inte behövs. Minskad storlek är en fördel eftersom det går betydligt snabbare att överföra de komprimerade ljudfilerna på exempelvis Internet. Trots att inbäddningen av vattenmärkningen sker på komprimerade ljudfiler sker extraktionen av vattenmärket linjärt. Detta för att dekomprimeringen av ljudfilen med bitstream watermarking inte får förstöra själva vattenmärket. Denna egenskap gör att samma extraktion kan användas till filer med både PCM och Bitstream watermarking. Bitstream gör det även möjligt att bädda in personlig information i vattenmärket som exempelvis användar-ID vid nerladdning av ljudfiler på internet [7]. Flera fördelar med denna metod är:

- Snabb inbäddning av vattenmärket som gör att exempelvis en server kan bädda in vattenmärken dynamiskt vid nedladdning.
- Kompatibilitet med PCM vattenmärkning.

Metoden kan ses som en digital variant av den allmänna metoden och visas i figur 3.



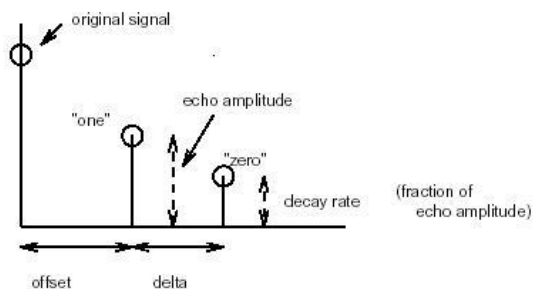
Figur 3 – Vattenmärkning av komprimerat ljud

Flera tekniker som använder digital vattenmärkning med ljudfiler använder en typ av echo hiding eller att bädda in extra information i tidsaxeln. Anthony Lu, Daniel Grohl, och Walter Bender som har skrivit en artikel om digitalvattenmärkning med ljudfiler förklarar att det mänskliga örat trots sin känslighet har några "hål" i vad den kan höra eller urskilja [9]. Tekniken utnyttjar dessa "hål" för att lägga in den önskade extra informationen i ljudfilen. Exempelvis maskerar högt ljud lågt ljud.

### 5.3 Echo hiding

Det mänskliga örat är känsligt för störningar som brus, men uppfattar inte eller rättare sagt filtrerar bort naturliga fenomen som eko. Detta kan man använda för att dölja information i en ljudsignal. [9]

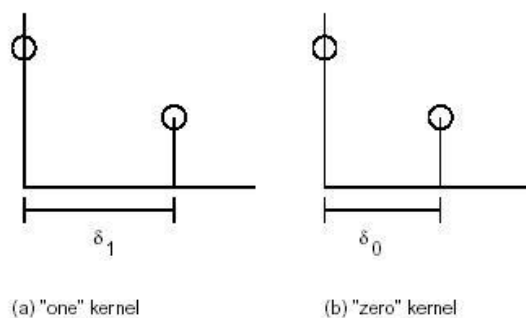
Några begrepp som används här är initial amplitud för originalsignalen,  $\alpha$  decay rate  $\delta$  som «r hur mycket av ursprungliga amplituden som är kvar efter tiden delta.  $\delta$  one offset  $\delta$  «r tiden  $\delta$  första ekot borde komma.  $\delta$  zero offset  $\delta$  (one offset + delta) är då det andra ekot borde komma. Signalen minskar med decay rate. För varje eko. Förskjutningen (offset) av ekot är en viktig komponent här eftersom det mänskliga örat i ett visst ögonblick inte kan höra originalljudet och ett eko samtidigt, utan det som uppfattas är en enda signal med lite brus i bakgrunden och därför är ljudkvaliteten på signalen eller ljudet med vattenmärket av lite sämre kvalitet än originalljudet. Figuren nedan beskriver termerna nämnda där x-axeln är tids och y-axeln är amplitud.



Figur 4 ¶ Echo Amplitude, olika val av parametrar

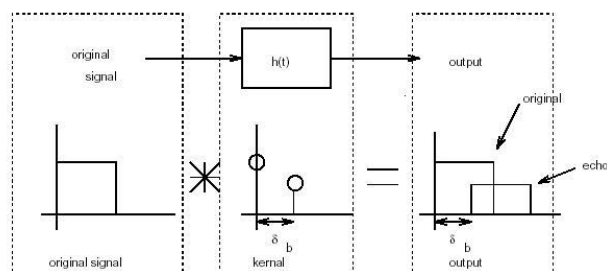
Kodningsprocessen använder sig av diskreta tidsvariabler (en fördröjning mellan pulserna) med endast två impulser. En puls kopierar källan eller original signalen och den andra pulsen representerar själva ekot. För att bädda in den binära koden med ettor och nollor används en av två systemfunktioner,  $\delta$  zero kernel  $\delta$  eller  $\delta$  one kernel  $\delta$ , enligt figur 5 Figuren visar på den signal man lägger till för att lägga till ett eko. Den binära koden som innehåller det digitala vattenmärket är kodat med en blandning av systemen. Därför är fördröjningen mellan

den originala signalen och ekot beroende av både vattenmärket och originalsignalen. [9]



Figur 5 ¶ Olika fördröjning i Echo hiding

Figur 6 beskriver kodnings processen i sin helhet från originalsignal till signal med inbäddat eko som beror på vattenmärket.



Figur 6 ¶ Kodningsprocessen för Echo hiding

Extraktion eller detektering av vattenmärket kräver en detektering av intervallet mellan ekon. Därför måste korrelationen av den kodade signalens spektrum analyseras vid avkodning.

Metoden är väldigt ny och ska mer ses som en pekare på ett sätt som kan skapa ohörbara vattenmärken i ljud.

### 6. Framtiden

Hur ser det ut i framtiden på vattenmärkningsfronten. Kommer tekniken leva kvar om än i ett annat format?

Som vi har nämnt tidigare i rapporten, befinner vattenmärkningsteknologin någonstans i begynnelsefasen och har inte riktigt mognat. Det finns exempelvis fortfarande inga universella standarder som följs för exakt vilken av de olika vattenmärkningsteknologier som är lämpligast att använda i något givet fall. Det kan bero på att det fortfarande inte finns någon teknik som är lämpligast för "alla" digitala medier. Det kan också bero på att eftersom företagen som producerar medierna vet bäst vad som är lämpligaste tekniken för deras medier använder just denna teknik. På detta sätt är det lättare för dem att använda denna teknik och samtidigt hålls produktionskostnaderna nere då de inte behöver specialanpassa sin övriga teknik. Kommer de stora

företagen överens om en standard som kan användas med olika medier och format kommer vattenmärkning lättare kunna utvecklas vidare och kanske finnas i de flesta medierna som finns till försäljning i framtiden.

Intresset för vattenmärkningstekniken har ökat under de senaste åren i takt med att flera av musik och filmproducenter distribuerar sina produkter direkt över Internet, mot betalning självklart. Samtidigt har antalet användare med tillgång till en relativt snabb internetuppkoppling ökat markant de senaste åren världen över. Det som film och musikproducenterna är främst intresserade av är de förlorade inkomsterna på grund av all olagliga överföringar mellan användare. Det är med stor sannolikhet inte lagen eller moralen de är intresserade av i första hand utan pengar. Därför är det fortfarande värt för dem att sponsra och ge bidrag till nya teknologier och forskningar som gör spridning och kopiering av musik och filmer svårare.

Lite problem finns det med själva tekniken för vattenmärkningen som försvårar en framtida utveckling och utbredning. Vi listade några viktiga nackdelar med vattenmärkning i föregående kapitel och det viktigaste att tänka på när det gäller framtiden är hur säker tekniken är mot attacker och hur svårt det är att kringgå vattenmärkningen. I dagsläget är det möjligt till och med för en "vanlig" användare att "knäcka" koden eller kringgå den så att den skyddade filen kan spridas utan några större risker. Detta gör att tekniken inte är så användbar som många av producenterna till film och musik hade hoppats på från början. Om däremot tekniken utvecklas så det blir svårt att kringgå vattenmärkningen har tekniken en ljus framtid framför sig där konsumenterna går tillbaka till att köpa lagliga kopior, istället för att ladda ner olagliga sådana, i rädslan av de rättsliga följderna då spridningen kan följas till källan. Vi tror att detta är ett möjligt scenario eftersom film- och musikbolagen sponsrar denna teknik med stora summor varje år för att den ska utvecklas och bli säkrare. Det är mycket möjligt att det i en nära framtid kommer en vattenmärkningsteknik som gör det mycket svårare för "vanliga" användare att kringgå, men samtidigt jobbar "hackare" världen över för att "knäcka" de nya teknikerna så att det blir möjligt för dem att sprida filerna relativt riskfritt.

Ett intressant citat som passar in här är: "Every watermark can be hacked and every watermark will be hacked, if there is sufficient motivation and opportunity." [Christian Neubauer på Tysklands Fraunhofer Institute, en av de ledande utvecklarna av vattenmärknings-teknologier].

En fördel med vattenmärkning är att behovet av aktiva kopieringsskydd i framtiden kan minskas. I dagens läge har kopieringsskydden blivit så betungande att det finns personer som väljer piratversioner av mjukvara inte av

ekonomiska skäl utan bara för att slippa problemen med kopieringsskydden. Osynlig vattenmärkning med spårningsmöjlighet istället för kopieringsskydd kan istället komma att hindra själva kopieringen från allra början utan att behöva störa den lagliga användningen.

## 7. Sammanfattning

Vattenmärkning är en teknik som används för att bädda in information i ett medium. Denna informations används i sin tur för att visa vem som äger original kopian eller för att spåra kopior av ett medium.

Denna rapport börjar med en kort bakgrund till vattenmärkning och dess användningsområden. Några fördelar och nackdelar med vattenmärkning tas upp samt några definitioner som är relevanta för ämnet.

Teknikerna för vattenmärkning som är tillgängliga idag kan kringgå med relativt lätta metoder, vilket gör att vattenmärkningstekniken blir mindre användbar. En övanlig användare kan med hjälp av en dator göra vissa modifieringar för att förstöra eller ta bort vattenmärket.

Det finns lite olika tekniker för vattenmärkningen och vilken teknik som används beror delvis på varför den ska användas samt vilka det är som har tagit fram eller tänkt att använda tekniken dvs. att olika tekniker passar olika ändamål.

Rapporten belyser kort om skillnader och likheter mellan synlig och (nästan) osynlig vattenmärkning. Synlig vattenmärkning är svårare att suddas bort, men upptäcks lätt. Därför kan synlig märkning inte användas för att identifiera enskilda kopior så bra.

Osynlig vattenmärkning består av små förändringar i källan, gärna utanför det område som människor kan upptäcka. Osynliga vattenmärken som endast använder detta kan dock försvinna lättare vid komprimering eftersom det är vanligt att algoritmer komprimerar sådana områden kraftigare.

Senare fortsätter rapporten med att ta upp några vattenmärkningstekniker för att förklara dem närmare. PCM, Bitstream och Echo Hiding som är de vanligaste vattenmärkningsteknikerna idag beskrivs.

Det saknas en standard för vattenmärkning. Detta är troligen eftersom det inte existerar någon teknik som står emot attacker tillräckligt bra. Tekniken för digital vattenmärkning befinner sig i begynnelsefasen och därför kommer det att dröja tills det dyker upp en ny teknik.

## 8. Slutsatser

Efter studierna och undersökningar som har gjorts i ämnet kring vattenmärkning kom vi fram till dessa slutsatser:

- Den digitala vattenmärkningstekniken är en relativt ny teknik som fortfarande inte är helt säker att använda.
- Det går att med relativt lätta metoder kringgå vattenmärkningen eller förstöra vattenmärket.
- Vattenmärkning för ljudmedia kan bli användbar om det utvecklas några vattenmärkningstekniker som kan stå emot eller överleva attacker bättre än dagens existerande tekniker.

## Källförteckning

- [1] K-G Stenborg, Distribution and Individual Watermarking of Streamed Content for Copy Protection, Linköpings Universitet IDA, 2005. ISSN 0280-7971
- [2] Julia Åhlén, Digitala Vattenstämplar, 29-11-2004. URL: [www.hig.se/~jae/grund\\_bildbeh/fls4.pdf](http://www.hig.se/~jae/grund_bildbeh/fls4.pdf) (tillgänglig 2006-04-26).
- [3] CoreAVC, <http://coreavc.corecodec.org/>
- [4] Joel Asblom, Skrivaren förråder dig - utskrifter går att spåra, 2005-11-03 [http://www.idg.se/ArticlePages/200511%5C03%5C07593777710\\_20051103075937\\_CS/20051103075937\\_CS.dbp.asp](http://www.idg.se/ArticlePages/200511%5C03%5C07593777710_20051103075937_CS/20051103075937_CS.dbp.asp) (tillgänglig 2006-04-28).
- [5] Fredrik Wickström, Digital vattenmärkning, KTH Stockholm, 2004. TRITA-NA-E04079.
- [6] Mike Collins, MPEG Audio Watermarking Report, 2002. <http://www.mpg.org.uk/watermarkingreport.htm> (tillgänglig 2006-05-02). Copyright - The Music Producers Guild Ltd.
- [7] Fraunhofer Institut Integrierte Schaltungen, Fraunhofer IIS - Audio & Multimedia, Watermarking, 2006. <http://www.iis.fraunhofer.de/amm/techinf/water/index.html> (tillgänglig 2006-05-02).
- [8] Digital Watermarking World. <http://www.watermarkingworld.org/faq.html#SECTION00028000000000000000> (tillgänglig 2006-05-02).
- [9] D. Gruhl, W. Bender, and A. Lu. "Echo-hiding", Information hiding: 1st International Workshop, R.J. Anderson, Ed., vol. 1174 of Lecture Notes in Computer Science, 1996, Isaac Newton Institute, England, pp. 295-315.
- [10] Thomas Lopatic, Licenturion Technology Whitepaper I, 2001. <http://www.licenturion.com/fileadmin/Tech-1L.pdf> (tillgänglig 2006-04-28)