APPLICATIONS OF DATA HIDING IN DIGITAL IMAGES

Tutorial for the ISPACS'98 Conference in Melbourne, Australia
November 4-6, 1998

Presenter: Jiri Fridrich

Center for Intelligent Systems
SUNY Binghamton, Binghamton, NY 13902-6000, U.S.A, and
Mission Research Corporation
1720 Randolph Rd. SE, Albuquerque, NM 87105, U.S.A
Fax/Ph: (607) 777-2577
E-mail: fridrich@binghamton.edu
Http://ssie.binghamton.edu/~jirif

CONTENTS

LIST OF ACRONYMS

A/D	Analog / Digital
CCD	Charge Coupled Devices
D/A	Digital / Analog
DC-free	Having zero mean
DCT	Discrete Cosine Transform
DVD	Digital Versatile (Video) Disk
FFT	Fast Fourier Transform
GIF	GIF Graphical Interchange Format
JND	Just Noticeable Difference
JPEG	Joint Photographic Expert Group
LSB	Least Significant Bit
MTF	Modulation Transfer Function
PDF	Probability Density Function
PRNG	Pseudo-Random Number Generator

1. MOTIVATION

The purpose of this tutorial is to introduce data hiding in digital imagery as a new and powerful technology capable of solving important practical problems. The field of data hiding in digital imagery is relatively very young and is growing at an exponential rate. Well over 90% of all publications in this field have been published in the last 5 years. Data hiding is a highly multidisciplinary field that combines image and signal processing with cryptography, communication theory, coding theory, signal compression, and the theory of visual perception. The reason for the tremendous recent interest in this field is quite understandable because of the wide spectrum of applications it addresses.

It is to be expected that digital photographs, videos, and sound tracks will gradually replace their analog counterparts in the near future. For example, the long-term goal of US TV broadcasting is to switch to digital form by the end of the year 2006. Digital representation of signals brings many advantages when compared to analog representations, such as lossless recording and copying, convenient distribution over networks, easy editing and modification, and durable, cheaper, easily searchable archival. Unfortunately, these advantages also present serious problems including wide spread copyright violation, illegal copying and distribution, problematic authentication, and easy forging. Piracy of digital photographs is already a common phenomenon on the Internet. Today, digital photographs or videos cannot be used in the chain of custody as evidence in the court because of nonexistence of a reliable mechanism for authenticating digital images or tamper detection. Data hiding in digital documents provides a means for overcoming those problems.

It appears that data hiding in digital imagery fits into the theme of this conference very well. By embedding almost invisible signals in images, one makes the images “intelligent” in the sense that the hidden message can carry information about the content of the image (thus protecting its integrity), additional information about the author of the image, or other useful data related to the image. In another application, one can achieve a very secure mode of communication by embedding messages into the noise component of digital images. This way, *the very presence of communication becomes hidden*.

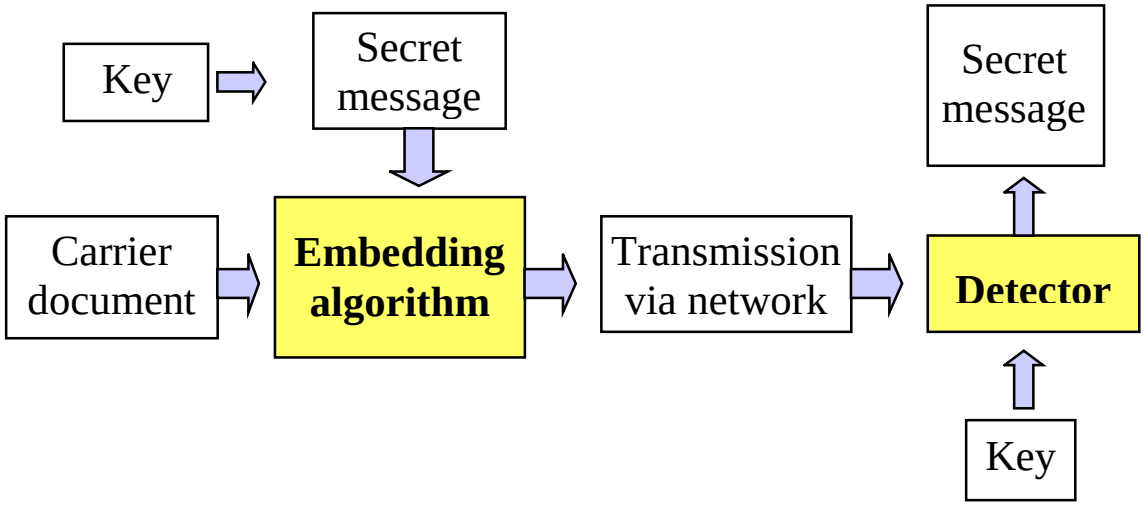
Depending on what information in which form is hidden in the image, one can distinguish at least two types of data hiding schemes: non-robust, undetectable data hiding, and robust image watermarking. In the first case, a digital image serves as a container for a secret message. For example, by replacing the least significant bit of each pixel with an encrypted bit-stream, the changes to a typical image will be imperceptible and the encrypted message will be masked by some innocent looking image. This way, the very presence of communication is hidden. The message embedding can be made much more sophisticated by incorporating the knowledge about the image noise and by using error-correcting codes.

In the second application, robust image watermarking, a short message (a watermark) is embedded in the image in a robust manner. By robustness we mean the ability to survive common image processing operations, such as lossy compression, filtering, noise adding, geometrical transformations, etc. Such robust watermark can be obviously used for copyright protection, fraud detection (verification of image integrity), authentication, etc. At this point we emphasize that cryptographic authentication protocols cannot solve all the issues related to authentication. Cryptographic authentication deals with authenticating the sender of the message over insecure channels. However, once the message (image) is decrypted, the image is unprotected and can be copied and further distributed. Unlike classical paintings that can be studied for authenticity using sophisticated experimental techniques, a digital artwork is just a collection of bits. A visible signature in the corner of the image can be easily replaced or removed with advanced image processing software packages, such as PhotoShop. Additional information in the image header can be erased or changed as well. In other words, any attempt to authenticate the digital image by appending information will fail. Digital watermarking provides an appealing alternative by *embedding* rather than *appending* information directly into the image itself. The embedded information will be transparent to the human eye, but it should be detectable using a sophisticated algorithm provided a secret key is available.

The are many other interesting applications of both non-robust and robust data hiding, and most of them are discussed in this tutorial in detail.

2. DATA HIDING, DEFINITION, TERMINOLOGY

Data hiding also frequently termed “steganography” is closely related to cryptography. The purpose of cryptography is to make messages unintelligible so that those who do not posses secret keys cannot recover the messages. Sometimes, it may be desirable to achieve security and privacy by masking the very presence of communication instead of exchanging encrypted messages. This problem is addressed by steganography. Historically, the first steganographic techniques included invisible writing using special inks or chemicals. It was also fairly common to hide messages in text. By recovering the first letters from words or sentences of some innocent looking text, a secret message was communicated. Today, it seems natural to use binary files with certain degree of irrelevancy and redundancy to hide data. Digital images, videos, and audio tracks are ideal for this purpose. The hidden message may have no relationship to the carrier image in which it is embedded (this is the case in covert, secure communication), or the message may supply important information about the carrier image, such as copyright notice, authentication information, captions, date and time of creation, serial number of the digital camera that took the picture, information about image content and access to the image, etc. The most general scenario for hiding messages is shown in the following diagram:



Each data hiding technique consists of: (1) the embedding algorithm and (2) a detector function. The embedding algorithm is used to hide secret messages inside a cover (or carrier) document; the embedding process is protected by a key-word so that only those who posses the secret key word can access the hidden message. The detector function is applied to a (possibly modified) carrier and returns the hidden secret message. We limit our tutorial to data hiding in digital images. Each data hiding technique must have certain properties that are dictated by the intended application. For example, is there a relationship between the carrier and the hidden message? Who extracts the message? (source versus destination coding) How many recipients are there? Is the key public knowledge or a shared secret? Do we embed different messages into one carrier? Embedding / detection bundled with a key in a tamper-proof hardware? Is the speed of embedding / detection important? The most important properties of data hiding schemes are robustness, undetectability, invisibility, security, complexity, and capacity. We present definitions of those concepts below.

2.1 Robustness

The embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition. Examples are linear and nonlinear filters (blurring, sharpening, median filtering), lossy compression, contrast adjustment, gamma correction, recoloring, resampling, scaling, rotation, small nonlinear deformations (as in StirMark [Kuh1]), noise adding, cropping, printing / copying / scanning, D/A and A/D conversion, pixel permutation in small neighborhood, color quantization (as in palette images), skipping rows / columns, adding rows / columns, frame swapping, frame averaging (temporal averaging), etc. We emphasize that robustness does NOT include attacks on the embedding scheme that are based on the knowledge of the embedding algorithm or on the availability of the detector function. Robustness means resistance to "blind", non-targeted modifications, or common image operations.

2.2 Undetectability

This property is typically required for secure covert communication. We say that the embedded information is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For example, if a steganographic method uses the noise component of digital images to embed a secret message, it should do so while not making statistically significant changes to the noise in the carrier. The concept of undetectability is inherently tied to the statistical model of the image source. If an attacker has a more detailed model of the source, he may be able to detect the presence of a hidden message. Note: the ability to detect the presence does not automatically imply the ability to read the hidden message. We further note that undetectability should not be mistaken for invisibility – a concept tied to human perception.

2.3 Invisibility (perceptual transparency)

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not. A commonly accepted experimental arrangement (so called blind test) frequently used in psycho-visual experiments is based on randomly presenting a large number of carriers with and without hidden information and asking the subjects to identify which carriers contain hidden information. Success ratio close to 50% demonstrates that the subjects cannot distinguish carriers with hidden information.

We note that the concept of invisibility could be defined in other manners leading to more or less strict concepts. The test described above is really a test for visibility of artifacts caused by data embedding schemes. If the visibility of artifacts was tested by presenting both covers (those that do contain hidden information and those that do not) at the same time side by side, a stricter concept of invisibility would result.

2.4 Security

The embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except the secret key), and the knowledge of at least one carrier with hidden message. The concept of security also includes procedural attacks, such as the IBM attack [Cra1], or attacks based on a partial knowledge of the carrier modifications due to message embedding [Fri1].

Finally, we introduce two more concepts of secure black-box public watermark detectors.

2.5 Secure black-box public detector

is a message detector implemented in a tamper-proof black-box (in hardware). It is assumed that the box cannot be reverse-engineered. The secret key used to read the hidden messages is wired-in the black box and cannot be recovered. The availability of the black box should not enable an attacker to recover the

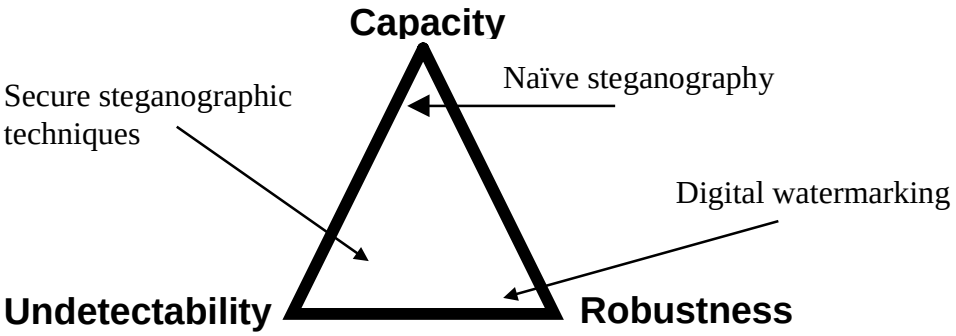
secret key or remove the hidden information from the carrier (again, we assume that the attacker has a full knowledge of the embedding algorithm and the inner workings of the detection function). Of course, any embedding technique that has a secure black-box public detector must also be secure in the sense defined above. At present, it is not clear if a secure black-box public detector can be built at all. Recently, attacks on a general class of data embedding techniques that are based on linear correlators have been described [Kal1, Kal2, Linn1, Linn2, Cox1].

2.6 Secure public detector

is an even stronger concept for which all details of the detector are publicly known. If such a detector is ever built, it would find tremendous applications since it can be implemented in software rather than tamper-proof hardware. It would enable building intelligent Internet browsers capable of filtering images containing certain marks (that would presume the existence of a standard for marking for example X-rated images), automatic display of copyright information with every image, etc. Special care would have to be taken to overcome so called mosaic attack [Pet1]. So far, no secure public detectors exist.

2.7 Conflicting requirements

The above requirements are mutually competitive and cannot be clearly optimized at the same time. If we want to hide a large message inside an image, we cannot require at the same time absolute undetectability and large robustness. A reasonable compromise is always a necessity. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden cannot be too long. This observation is schematically depicted in the figure below.



3. COVERT COMMUNICATION (STEGANOGRAPHY)

Typical use: A spy in a foreign country wants to send messages abroad. He needs to use local communication channels in order to send the messages. He should assume that the communication channel is monitored. Sending encrypted messages would raise suspicion and could result in cutting the access to the communication infrastructure. It is therefore in his best interest to hide the presence of communication at all. This could be solved using a clever steganographic protocol.

Requirements: The most important requirement is that the presence of the hidden message be undetectable. This means that images with and without secret messages should appear identical to all possible statistical tests that can be carried out. It is of paramount importance to know as much about the statistical properties of the source from which cover images are being drawn as possible. For example, if the images are scanned photographs, there will be stronger correlation in the horizontal direction than in the perpendicular direction. The details of the noise may be specific for each scanner and need to be taken into account if a reliable and secure steganographic protocol is needed. On the other hand, if the images are taken using a digital CCD camera, the noise will again have certain specific properties induced by the CCD element and the specific data readout. In either case, the data hiding scheme must respect all known statistical properties of the image source and produce images that cannot be distinguished from images that do not contain any messages.

Another important requirement is the capacity of the communication channel. It is clear that one can embed one bit of information into one frame of a digital video without worrying much about noise models. Such communication scheme would however lead to an impractical and low communication bandwidth. The challenge is to embed as much information as possible while staying compatible with the image noise model.

The last important requirement is that it must be possible to detect the hidden message without the original image. Sometimes it may be possible to agree on certain image database from which cover images are drawn (without repetition!) but this obviously limits the applicability of the technique.

3.1 Methods for RGB images

Analog of one-time-pad (absolutely secure steganographic technique)
T. Aura [Aur1] proposed to embed a small message of the order of 8 bits or so, by repeated scanning of a cover image till a certain password-dependent message digest function returns the required 8-tuple of bits. This has the advantage of absolute secrecy tantamount to one time pad used in cryptography. The method guarantees the same error distribution and undetectability. Although the scheme satisfies the requirements of the steganographic holy grail, it is time consuming, has very limited capacity, and is not applicable to image carriers for which we only have one copy.

LSB Encoding
The simplest and the most common steganographic technique is the Least Significant Bit embedding (LSB). The premise here is that changes to the least significant bit will be masked by noise commonly present in digital images. Actually, in the case of color images, there is even more room for hiding messages because each pixel is a triple of red, green, and blue. Again, replacing two or more least significant bits of each pixel increases the capacity of the scheme but at the same time the risk of making statistically detectable changes also increases. Therefore, it is important to study the security of each specific steganographic technique and argue why it is secure. Even the simple least significant bit encoding may under certain circumstances introduce detectable changes.

Aura [Aur1] suggests to change only a small fraction of the carrier bits. For example, modify each hundredth pixel in the carrier by one gray level. Depending on the image noise, these changes will hopefully be compatible with the uncertainties involved with any statistical model of the image.

Before any secret message hiding technique can be claimed as secure, we need to carefully investigate the carrier images and their statistical properties. The noise component may not be uniform within the image but may depend on the pixel position in the image. For example, pixels corresponding to a bright white color may be saturated at 255 even though the overall model of the noise can be Gaussian with a non-zero variance (this is especially relevant for scanned images processed using gamma correction). An example of such an image is shown in Figure 1. The image has been scanned on a scanner and its brightness was adjusted using gamma correction to achieve a pleasing image. Figure 2 is a black and white image with black pixels corresponding to even gray levels and white pixels corresponding to odd values of gray. One can clearly see a large patch of pixels with values saturated at the maximal gray scale level 255. Even if we play it safe and modify only a small fraction of pixels in the image, we may introduce some suspicious noise into the overflowed patch. This problem with over/under flow can of course be avoided by a more careful choice of the carrier image, preprocessing the carrier, or by instructing the steganographic scheme to avoid the over/underflowed areas and adapt it to the image content.

Figure 1 A scanned image after gamma correction adjustment.

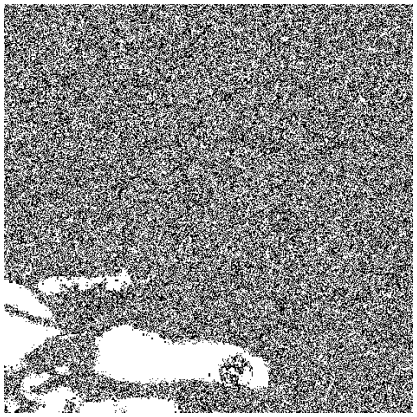


Figure 2 Image from Figure 1 with white pixels corresponding to odd gray levels and black pixels corresponding to even gray levels

While we agree that it is probably impossible to get a complete model of the carrier noise, and that the search for the perfect steganographic method will probably never be complete, we insist that all good secret-hiding schemes must be based on some model of the noise. If it is known that scanned images exhibit larger noise correlations in the horizontal direction and smaller correlations in the vertical direction, while the probability distribution for each pixel, which is neither overflowed nor underflowed, is Gaussian with certain standard deviation, then we have to take this evidence into account and tailor our secret message hiding scheme so that the carrier modifications are consistent with the statistical evidence. It is

certainly possible that somebody will, with great effort, create even more sophisticated noise model and detect the presence of messages, but only at the price of painstaking time-consuming and possible expensive investigation. It is rather unfortunate but understandable, however, that most detailed technical information regarding noise in CCD arrays and scanners is proprietary and rarely published.

Steganographic technique based on PDF of the noise
To give an example how one can incorporate statistical evidence into the construction of a secret message-hiding scheme is as follows. Let us assume that the noise component of pixels with gray levels within the range [L, H] can be modeled with a uniformly valid probability density, *f*, that is symmetric around zero. If the secret plain-text message $\{p_i\}^N_{i=1}$ is encrypted, the cipher-text $\{c_i\}^N_{i=1}$ should be a random sequence of ones and zeros. By averaging several scanned versions of the carrier image (or using adaptive Wiener filter, wavelets, or other noise removing techniques), we obtain a "zero noise" image Z. Using a pseudo-random number generator, we can choose at random *N* pixels in Z with their gray levels in [L, H]. Then, we can modify the LSB of those pixels by the amount of $(2b_i - 1)\,|\eta_i\,|$, where η_i is a random variable with probability distribution *f*. The remainder of the pixels will be modified by η_i. The modifications should be consistent with the statistical model. To recover the hidden message, we need the seed for the pseudo-random number generator. By following the path of random pixels, we can read the encrypted message by comparing the image with its Wiener-filtered version.

3.2 Methods for palette-based images

In general, the more colors in a digital image, the easier is to hide messages. The most difficult images from the point of view of data hiding are images with singular histogram or a small color depth. For example, palette-based images with small number of colors in the palette are in general very difficult to modify without introducing some statistically detectable changes. Unfortunately, a large portion of images on the Internet is available in palette-based formats, such as GIF, PNG, etc. A secure steganographic technique for embedding messages in palette-based images is currently not available. Some software routines that hide information in GIF images are available on the Internet [Mac1]. However, the implementations are not supported by security proofs or any other evidence that hidden messages cannot be detected. Secure steganography for palette-based images remains an unsolved problem.

3.2.1 Embedding messages into the palette
The advantage of palette embedding is that it will probably be easier to design a secure method under some assumptions about the noise properties of the image source (a scanner, a CCD camera, etc.). The obvious disadvantage is that the capacity does not depend on the image and is limited by the palette size.

Permuting the palette entries
It has been suggested in the past that secure message hiding in palette-based images can be obtained by permuting the image palette rather than changing the colors in the image. While this method does not change the appearance of the image, which is certainly an advantage, its security is questionable because many image processing software products do order the palette according to luminance, or some other scalar factor. Also, displaying the image and resaving it may erase the information because the software routine may rewrite (and reorder) the palette. Another disadvantage is a rather limited capacity.

LSB encoding in the palette
A better approach may be to hide encrypted (random) messages in the least significant bits of the palette colors. One would need to guarantee that the perturbed palette is still consistent with the noise model of the original 24-bit image. This, however, could be established in each particular case by studying the sensitivity of the color quantization process to perturbations.

3.2.2 Embedding into the image data
These methods have higher capacity, but it will be harder to prove security of such schemes. In order to prove security of an embedding scheme, we need to understand the details of algorithms for creating palette-based images. Virtually all algorithms consist of two steps: color quantization (also called vector quantization) and dithering. Color quantization selects the palette of the image by truncating all colors of the raw, 24-bit image to a finite number of colors (256 for GIF images, and 216 for Netscape version of

GIFs, 2 for black and white images, etc.). Dithering is used for apparent increasing of color depth (trading spatial resolution for apparent color depth). It is based on the ability of the human visual system to integrate colors scattered in small neighborhood. The best results are obtained using dithering algorithms based on error diffusion [Fol1].

EZ Stego
EZ Stego is a name of a computer program that embeds bits of information into GIF images. The method first sorts the palette so that neighboring entries have similar colors. Message embedding then proceeds with changing the LSB of the pointers to palette entries rather than changing the colors themselves. Since the palette is sorted according to the colors, typically invisible changes will be introduced using this algorithm. The code is available for download at http://www.stego.com/.

So far, we discussed the case when the communication channel is error free (passive warden scenario). This is certainly the case for many computer transfer procedures, such as ftp protocol that already contain error-correcting schemes. The situation complicates when there is noise in the communication channel. This noise could be a random noise with known statistical properties or a result of a deliberate effort to prevent steganography from being used (the active warden scenario). For example, the monitoring agency can actively perturb the messages while staying consistent with the noise model of the carrier image. It can be shown that in that case, the capacity of the steganographic channel decreases but stays above zero [Ett1].

4. DIGITAL WATERMARKING (ROBUST MESSAGE EMBEDDING)

4.1 Copyright protection of digital images (authentication)

Typical use: The author of a digital image wants to "sign" the image so that no one else can attribute the authorship of the image to himself. The signature cannot be appended to the image file, nor can it be visibly imprinted on the image because such signatures can be easily removed or replaced. Cryptographic digital signatures cannot be applied because images are to be viewed by others and, therefore, will be distributed "in plain". Cryptographic digital signatures can be used for authentication of a communication channel but cannot protect an image posted on a web page.

Solution: Robust, secure, invisible watermark is imprinted on the image and the watermarked image W is distributed. The author keeps the original image I. To prove that an image W' or a portion of it has been pirated, the author shows that W' contains his watermark (to this purpose, he could but does not have to use his original image I). The best a pirate can do is to try to remove the original watermark (which is impossible if the watermark is secure), or he can embed his signature in the image. But this does not help him too much because both his "original" and his watermarked image will contain the author's watermark (due to robustness property), while the author can present an image without pirate's watermark. Thus, the ownership of the image can be resolved in the court of law.

Requirements: The watermark must be robust, secure, invisible, and it has to depend in a non-invertible manner on the original image (to prevent the IBM attack see Section 5 on attacks). The watermarking technique can use the original image for watermark detection. This simplifies image registration before watermark detector can be applied. Other requirements: relatively small capacity (1–100 bits).

4.2 Fingerprinting (traitor-tracing)

Typical use: Movies are distributed to different people (as in pay-per-view distribution system). One wants to identify those that make illegal copies and sell them. Other scenario includes distributing sensitive information (images, videos) to several deputies and trying to trace down a traitor who leaks information to the enemy. One cannot use visible (audible) marking because such would look suspicious and could be easily removed. The marks must be perceptually invisible and must be present in every frame or image that

is being distributed. The marks must be embedded in a robust way so that multiple copying or editing cannot remove them.

Solution: The same as in the previous case.

Requirements: Robust, secure, invisible watermark that depends in a non-invertible manner on the original is embedded in the document. The watermarking technique should not use the original for watermark detection. Since possibly a large number of documents marked with different marks will be distributed in the public domain, the technique must be resistant with respect to the collusion attack (averaging copies of documents with different marks, see Section 5 on attacks). Other requirements: relatively small capacity.

4.3 Adding captions to images, additional information to videos

Typical use: Movie dubbing in multiple languages, subtitles, tracking the use of the data (history file). For example, one copy of a movie can be distributed with subtitles in several languages. The VCR, DVD player, TV set, or other video device can access and decode the additional text (subtitles) in real time from each frame, and display it on the TV screen. Although this could be arranged by appending information rather than invisibly embedding it, bandwidth requirements and necessary format changes may not allow us to do so.

Requirements: A moderately robust, most importantly with respect to lossy compression, and noise adding, transparent watermark with moderate to large capacity. The original images (frames) are not available for message extraction. Since the hidden information is beneficial for the consumer, there is no need to require security - the consumer is not motivated to remove the hidden information. Since the watermark must be recovered in real time, fast detection is necessary. On the other hand, watermark embedding can be more time consuming.

4.4 Methods for Robust Data Hiding (Watermarking)

Digital watermark is a perceptually transparent pattern embedded in an image using an embedding algorithm and a secret key. The purpose of the watermark is to supply some additional information about the image without visibly modifying the image (compare with date and time imprinting on negatives) or without the need to change the file format. Information appended in a visible form in the image or added to the header of a corresponding image format can be easily erased or replaced. Digital watermark is embedded in the image in an invisible form yet in a persistent, robust manner. The process of embedding a watermark depends on a secret key so that only those possessing the key can access the information hidden in the watermark. With the key, the information carried by the watermark can be read and decoded using a detection algorithm.

An important property of a watermark is robustness with respect to image distortions. This means that the watermark should be readable from images that underwent common image processing operations, such as filtering, scaling, noise adding, cropping, etc. Watermarks that are to be used for copyright protection, fingerprinting, or access control must also be embedded in a secure form. This means that an attacker who knows all the details of the embedding algorithm except the secret key should not be able to disrupt the watermark beyond detection. In such applications, the watermarking scheme is an example of a symmetric encryption scheme with private key[1]. In other applications when it is desirable that the watermark information be publicly accessed by a large number of people, such as adding additional captions to images or subtitles in several languages to movies, there is no motivation for intentional removal of the watermark, and the security of the watermark is not an issue. Although some candidates for a secure public detector have been proposed [Fri1], almost all watermarking schemes that have been described in the literature so far have the property that the ability to read the watermark automatically implies the ability to remove the watermark [Linn1–3, Kal1–2]. The number of bits carried by the watermark could be as low as one bit or several hundred bits or more. Obviously, there is a trade-off between robustness and the capacity of the watermark.

Another important attribute of watermarking is the computational complexity of the embedding and extracting procedures. In some applications, it is important that the embedding process be as fast and simple as possible (e.g., embedding serial numbers of digital cameras into images for the purpose of tamper detection) allowing the extraction to be more time consuming. In other applications, the speed of extraction is absolutely critical (e.g., extracting subtitles from movies). To summarize, the required properties of digital watermarks are:

- Robustness to common image processing operations – untargeted attacks
- Security – targeted attacks (application dependent)
- Perceptual invisibility
- Restrictions on computational complexity of embedding/extraction (application dependent)

Non-oblivious watermarking schemes must access the original image in order to extract the watermark. The original image is usually subtracted from the suspected image before a detection algorithm is applied. The original image can also be used for registering the suspected image if it has been cropped, rotated, scaled, or transformed in some more general manner (e.g., as in StirMark [Kuh1]). Obviously, the availability of the original image makes non-oblivious watermarking schemes much more robust than oblivious schemes, which extract watermarks without accessing the original image. Non-oblivious watermarking is at present the only option for reliable copyright protection. Currently, there is no computationally efficient oblivious scheme that would be able to reliably extract watermarks from images that underwent general non-linear geometric transformations, such as those introduced by a general-purpose watermark removing software StirMark. The quest for StirMark resistant oblivious watermarking scheme remains an active research topic. O' Ruanaidh et al. [Her1] have described an oblivious technique that uses a calibration pattern embedded into the amplitude of Fourier transform in log-polar coordinates. This enables them to register the suspected image after a combination of a shift, rotation, and change of scale. A second, spread-spectrum type of watermark embedded in the middle frequencies is used to carry a message of up to 100 bits or longer.

Most watermarking techniques can be roughly divided into two groups depending on whether the watermark is inserted by modulating the coefficients of some transform or directly the pixel values. In some techniques, the modulation is adjusted according to properties of the human visual system so that no perceptually visible distortions are introduced by the watermark. Transform-based techniques may use DCT, DFT, Hadamard transform, wavelets, or general, key-dependent transforms. The watermark pattern itself can have its energy mostly concentrated in low or high frequencies depending on the technique. Noise-like watermarks generated using spread spectrum methods in the spatial or frequency domains are statistically orthogonal to the original image, and can be extracted by performing a simple dot product with the watermarked image or a portion of its spectrum.

Low-frequency watermarks interfere with the image and it is thus necessary to have the original image for watermark extraction. On the other hand, the low-frequency character of the watermark does not increase the noise level of the image and increases the robustness with respect to image distortions that have low-pass character (filtering, nonlinear filtering such as median filter, lossy compression, adaptive Wiener filtering, etc.). Low-frequency watermarks also have fewer problems with synchronizing the watermark detector with the image and are less sensitive to small geometric distortions. On the other hand, oblivious schemes with low-frequency watermarks are more sensitive to modifications of the histogram, such as contrast/brightness adjustment, gamma correction, histogram equalization, and cropping.

Watermarks inserted mostly into middle and high frequencies are typically less robust to low-pass filtering and small geometric deformations of the image, but are extremely robust with respect to noise adding, nonlinear deformations of the gray scale, such as contrast/brightness adjustment, gamma correction, and histogram manipulations.

It is understandable that the advantages and disadvantages of low and middle-to-high frequency watermarks are complementary. It appears that by embedding both watermarks into one image, one could achieve extremely high robustness properties with respect to a large spectrum of image processing

operations. Indeed, inserting a high-frequency spread spectrum signal on top of an image previously watermarked with a low-frequency watermark could lead to a scheme that enjoys the advantages of both watermarks. There will be very little interference between both watermarks since they will be inserted into two disjoint portions of the spectrum. However, it is not entirely clear how one would build an oblivious technique with low-frequency watermarks.

4.4.1 Watermarking in the spatial domain vs. transform domain

Watermarking techniques can be divided into different categories based on their attributes. For example, the watermark can be embedded directly in the spatial domain or in some transform space using common transforms, such as FFT, DCT, wavelet transform, Hadamard transform, or general key-dependent transform [Fri1]. In the first case, the watermark is embedded directly into pixels values, while in transform-based schemes the image is transformed prior to watermark embedding and the watermark is hidden in the coefficients representing the image. The watermarked image is obtained using an inverse transformation.

4.4.2 Watermarking for color images

In case of color-based images, the watermark could be embedded in one or more selected color channels. Some watermarking schemes use the blue channel only because human eye is least sensitive to the blue component. One can also transform the color space from RGB to YUV or HLS, embed the information into the luminance only, and transform the colors back to RGB.

4.4.3 Oblivious vs. non-oblivious watermarking

Watermarking schemes that need the original image for watermark extraction are called non-oblivious. Typically, such schemes are more robust than oblivious schemes that do not need the original image for watermark extraction. On the other hand, the application of non-oblivious schemes is severely limited by the requirement of having the original image available.

The NEC scheme

The watermarking technique proposed by Cox et al. [Cox2] has quickly become one of the most cited schemes. It does need the original image for watermark extraction (i.e., it is non-oblivious). First, a pseudo-random Gaussian sequence $N(0,1)$ with zero mean and unit variance is generated. For security reasons, the pseudo-random number generator should be seeded with a concatenation of author's ID and an image hash. It can be shown that if the watermark does not depend on the original image or depends only in an invertible manner, one could easily construct a false original and a false watermark and create an ownership deadlock (see the IBM attack in Section 5). The watermark is embedded by modulating discrete cosine coefficients with the largest magnitude. The logic behind this technique is to hide the watermark into the most perceptive modes of the image (the largest magnitude DCTs) in order to achieve a high degree of robustness with respect to lossy compression and most common image processing techniques.
In the version described by Cox et al. [Cox2], the highest energy 1000 frequency coefficients v_k are modulated according to the formula

$$v_k' = v_k (1 + \alpha \eta_k).$$

The watermarked image is obtained by applying the inverse DCT to the coefficients v_k'. The parameter α is the watermark strength and can be adjusted to achieve a reasonable compromise between the robustness of the watermark and its visibility. Large values of α lead to more robust schemes but the watermark becomes more visible because the DCT coefficients are modified by a larger amount. Cox et al. suggest the value $\alpha = 0.1$ obtained empirically. In [Fri2], the author studied the visibility of the watermark using a model of the human visual system. The model used was a simplified version of a linearized spatial masking model of Girod [Gir1]. This model accurately describes the visibility of small changes in uniform areas and around edges. It was found that the value of $\alpha = 0.1$ introduces artifacts that are fairly visible even to an inexperienced observer. Over 15% of pixels exhibited visible changes after watermark insertion. A more conservative value would be $\alpha < 0.05$.

Watermark detection is done by subtracting the original image from a suspected image, calculating the DCT of the difference, and extracting the (possibly modified) watermark sequence. If no distortion of the watermarked image is present, the DCT coefficients of the difference are $\alpha v_k \eta_k$. Clearly, by dividing this

difference by αv_k (remember that the original image is known), one can calculate an estimate η_k' of the original watermark. The extracted watermark is compared to the original watermark by calculating a similarity index

$$\mathrm{sim}(\eta,\eta') = \frac{\eta \cdot \eta'}{\sqrt{\eta' \cdot \eta'}} .$$

As an alternative, a classical correlation between η and η' could also be used. Cox et al. [Cox2] report extremely good robustness with respect to all kind of image processing operations, including noise adding, filtering, lossy JPEG coding, dithering, printing/scanning, and dithering. If the image has been cropped, the missing portions are replaced using the original, unwatermarked image before the detection is carried out. The authors also test the robustness of the watermark by inserting multiple watermarks and testing for the presence of all of them. They also pay attention to the collusion attack in which multiple copies of one image with different watermarks are averaged in an attempt to remove the watermark. An exact mathematical analysis of this attack has been performed by Stone [Sto1].

An improvement due to Podilchuk and Zeng

The technique has been somewhat improved by Podilchuk and Zeng [Pod1] who utilized the properties of the human visual system into the scheme. They start by dividing the image into square blocks, and for each block *b* and each DCT frequency bin (*r*, *s*), they calculate the just noticeable difference *JND*(*b*, *r*, *s*) by which the DCT coefficient of that frequency bin can be modified without causing visible changes. The JNDs are calculated using the frequency masking model described by Watson in [Wat1]. The model was originally designed to achieve higher compression ratios for lossy compression schemes. Podilchuk and Zeng propose to modify the DCTs using the following expression

$$v_k' = v_k + JND(b,r,s)\cdot\eta_k \quad \text{if } v_k(b,r,s) > JND(b,r,s)$$
$$v_k' = v_k \quad \text{otherwise}$$

The sequence η_k is Gaussian $N(0,1)$. This implies that the modifications will be sometimes (in 35% of cases) larger than the calculated *JND*s. The authors, however, still report that their method did not introduce visible changes. The detection is done in exactly the same manner as in the original scheme [Cox2]. The authors report slightly better robustness results when compared to the original scheme.

Perceptually invisible watermarking

This scheme uses models of the human visual system to design provably invisible watermarks. The authors utilize spatial and frequency masking phenomena to guarantee watermark's invisibility. An image is first divided into blocks of 8×8 pixels. Each block is DCT transformed and a frequency-masking model [Leg1] is used to calculate maximal allowable changes in each DCT frequency bin. The frequency masking phenomenon relates to the fact that one signal may mask the presence of another, weaker signal of similar frequency thus making it invisible. For example, sinusoidal grating of frequency *f* and contrast *c* will increase the detection threshold for sinusoidal gratings with frequencies close to *f*. The contrast *c* of a sinusoidal grating

$$U(x,y) = U + Ap(x\cos\theta - y\sin\theta)$$

is defined as $c = A/U$. The contrast sensitivity $H(f)$ is the reciprocal value of the contrast. It can be captured as a function of the grating frequency $f = (f_x, f_y)$ [in cycles per degree] by a Modulation Transfer Function (MTF) (normalized)

$$c_0(f)^{-1} = H(f) = (0.31 + 0.69f)e^{-0.29f},\ f = \sqrt{f^2{}_x + f^2{}_y}.$$

The contrast threshold at frequency *f* as a function of *f*, the masking frequency f_m and the masking contrast c_m is expressed as

$$c(f, f_m) = c_0(f)\,Max\{1, [f(f/f_m)c_m]^{\alpha}\},$$

where $c_0(f)$ is the detection threshold at frequency *f*. To find the detection threshold $c(f)$ at frequency *f* due to masking from neighboring frequencies f_m we sum the contributions using a Minkowski norm with parameter $\beta = 4$

$$c(f) = \left[\sum_{f_m} c(f, f_m)^{\beta} \right]^{1/\beta} .$$

The summation is carried over all 9 neighboring frequencies in the DCT matrix. Frequency masking can be used to calculate the maximal allowable change M_{ij} for each DCT coefficient (i,j). An author's ID is concatenated with image digest and fed as a seed into a cryptographically strong PRNG generating numbers uniformly distributed in [−1,1]. The obtained pseudo-noise sequence is then divided into 8×8 blocks and multiplied by the mask M_{ij} for each block. The result is added to the matrix of DCT coefficients and each block is further transformed using an inverse DCT. Since the frequency-masking model is based on idealized assumptions of two sinusoidal gratings on a uniform background, its accuracy for real images may not be sufficient. To guarantee perceptual invisibility of the changes, the linearized spatial masking model of Girod [Gir1] is used to provide feedback whether or not the changes are visible. If they are, the masking values M_{ij} are multiplied by a factor less than one and the process is repeated till no visible changes are produced.

The security of the scheme is in the secret autohor's ID that is used to produce the pseudo-noise sequence that is modulated by the mask M_{ij}. The detection proceeds by regenerating the pseudo-noise sequence and the masking matrices M_{ij} from the original image. One then evaluates the pseudo-noise sequence and correlates it with the original sequence S. Detection of the watermark is achieved via hypotheses testing

$$H_0 : X = R - S = N \qquad \text{(No watermark)}$$
$$H_1 : X = R - S = W' + N \quad \text{(Watermark)}$$

where R is the potentially pirated signal, W' is the potentially modified watermark, and N is noise.
The scheme is remarkably robust with respect to all kinds of image processing distortions. The authors report that the watermark could be extracted from images degraded by simultaneous noise adding, lossy JPEG compression (10% quality) and cropping to 15% of the whole image.

Oblivious watermarking schemes almost always utilize some form of spread spectrum approach because such watermarks are typically orthogonal to the original image.

Watermark embedding in wavelet space
Kundur and Hatzinakos [Kun1,Kun2] embed message bits into disjoint triplets of wavelet coefficients chosen from the same resolution level. The choice of the triplets is based on a pseudo-random number generator initialized with a secret key. The middle coefficient is adjusted so that its relative position with respect to the other two coefficients falls into intervals of length $(c_{max}-c_{min})/(2Q-1)$, where c_{max} and c_{min} are the largest and the smallest wavelet coefficients from each triplet, and Q is a fixed integer. The number Q can be adjusted to obtain a good trade-off between robustness and watermark visibility.

Watermark embedding in general key-dependent spaces
Schemes that embed watermarks into the projections onto smooth orthogonal basis functions such as, discrete cosines, are typically very robust and less sensitive to synchronization errors due to skipping of rows of pixels, and/or permuting of nearby pixels than techniques that embed watermarks using pseudo-noise patterns. However, if the watermark pattern is spanned by a relatively small number of publicly known functions, it may be possible to remove the watermark or disrupt it beyond reliable detection if a portion of the watermark pattern can be guessed or is known[1], or when the embedding key becomes partially available. The plausibility of such an attack is demonstrated in [Fri1]. This observation suggests that techniques based on general, key-dependent orthogonal basis functions may provide more security than techniques based on publicly known bases, such as discrete cosines.

It is not necessary to generate a *complete* set of orthogonal basis functions since only a relatively small number of them are needed to span a watermark pattern. One can calculate projections[2] of the original image onto a set of J orthogonal functions, and modify the projections so that some secret information is

[1] This can happen in a collage consisting of several images.

[2] The dot product of two images A_{ij} and B_{ij} is defined as $\langle A,B \rangle = \sum_{i=1}^{M} \sum_{j=1}^{N} A_{ij} B_{ij}$

encoded. Let us denote such functions f_i, $i = 1, \ldots, J$. Assuming that the functions are orthogonal to each other, the system of J functions can be completed by $MN–J$ functions g_i to a complete orthogonal system. The original image I can then be written as

$$I = \sum_{i=1}^{J} c_i f_i + g, \qquad c_i =< f_i, I >,$$

where g is a linear combination of functions g_i that are orthogonal to f_i. The watermarking process is realized by modifying the coefficients c_i. Furthermore, the watermarked image Iw can be expressed as

$$Iw = \sum_{i=1}^{J} c'_i f_i + g, \qquad c_i' =< f_i, Iw >= (1+\alpha w_i)c_i,$$

where c_i' are the modified coefficients, α determines watermark's strength and visibility, and w_i is a watermark sequence. Given a modified watermarked image Im,

$$Im = \sum_{i=1}^{J} c_i'' f_i + g', \qquad c_i'' =< f_i, Im >,$$

we can calculate the modified coefficients by evaluating the projections of Im onto the functions f_i. A cross-correlation $corr$ of the differences $c''–c$ with $c'–c$,

$$corr = \frac{(c''–c)(c'–c)}{\|c''–c\|\|c'–c\|},$$

is compared to a threshold to decide about the presence of a watermark.

Direct spread spectrum in the spatial domain

All pixels in the image are divided into three disjoint sets A, B, and C with cardinalities $|A| = |B|$. The sets are generated from a pseudo-random number generator seeded with secret key. The gray levels of pixels in set A are increased by k gray levels and pixels in set B are decreased by k. The pixels in set C remain unchanged. The average DC term of the image is unchanged because the cardinalities of sets A and B are equal. The detection is based on the fact that the average gray level over two randomly chosen sets A' and B' are approximately equal

$$\bar{a} = \sum\nolimits_{A'} g_{ij} \approx \bar{b} = \sum\nolimits_{B'} g_{ij},$$

while the averages will be well separated (by k) if $A' = A$ and $B' = B$. Pitas [Pit1] defines a test statistics q as

$$q = \frac{\bar{w}}{\sigma_{\bar{w}}}$$

where $\bar{w} = \bar{a} - \bar{b}$ is the difference between mean values of pixels in A and B. The presence of a watermark is determined by hypotheses testing:

H_0: There is no watermark in the image ($\bar{w} = 0$)
H_1: There is a watermark in the image ($\bar{w} = k$)

Possible improvements of this technique include taking into account the human visual system. For example, the Weber's law says that the sensitivity of the human eyes to small changes in gray is inversely proportional to the gray level. Therefore, it would make sense to choose k adaptively so that the quantity k/g_{ij} stays below certain threshold. Another possibility would be to use the spatial masking by Girod [Gir1] and modulate k according to the spatial sensitivity mask. The masking model can give us the maximal error for each pixel in the image.

Many different watermarks can coexist in one image. This is due to the fact that the superimposed signal is essentially random and random signals will generally have little interference. The watermark has most of its energy concentrated in the high frequencies. It will be robust to nonlinear transformations of the gray scale (gamma correction, contrast/brightness adjustment, and histogram equalization) but it will not be too robust with respect to operations that have low-pass character and to lossy compression.

Patchwork

Bender, Gruhl, and Morimoto introduce a technique called patchwork. Pairs of pixels *A* and *B* with gray levels *a* and *b* are randomly chosen in the image. The expected value of the difference A – B is zero. Repeating this procedure *n* times, we can form the quantity *S*

$$S = \sum_{i=1}^{n} (a_i - b_i)$$

The expected value of this sum is zero with variance $\sigma^2 = 10922.5 \times n$ (for 256 gray levels). Using statistics, it is possible to estimate the probability hat the value of *S* will exceed certain threshold. The watermarking algorithm starts with a secret key used to seed a PRNG. The sequence of pseudo-random numbers is used to randomly select *n* pixel pairs. For each pair, the gray level of one the first pixel is increased by one, while the value of the second pixel is decreased by one. To prove that an image is watermarked with a specific secret key, one generates the sequence of pseudo-random numbers and evaluates the sum *S*. Again, hypotheses testing can be used to confirm the presence of a watermark on a certain confidence level. The method can be improved by adjusting patches of pixels rather than single pixels. This will have the effect of shifting the energy of the watermark towards low frequencies thus making it more robust to JPEG compression and low-pass filtering. As with most spread spectrum methods, the watermark is very robust to nonlinear transformations of the gray scale.

Frequency-based spread spectrum

This method embeds a spread spectrum signal into the Fourier (Cosine) coefficients of an image rather than directly into the image pixels. Frequency-based spread spectrum methods appear to be more robust than their spatial counterparts. This is especially true for low-pass filtering and JPEG compression. A nice feature of spread spectrum methods is that they easily accommodate insertion of more than one bit. An elegant method for coding multiple bits into a spread spectrum signal has been described by Ó Ruanaidh [Rua1] (a similar technique was proposed by Piva [Piv1]). The watermark is inserted by adding a noise-like signal to the middle frequencies of its DCT. The DCT coefficients are converted to a vector and the middle 30% (N_m frequencies) is chosen for marking. The information carried by the watermark consists of *M* symbols and each symbol s_i is represented using *r* bits, $1 \le s_i \le 2^r$. For each *i*, a sequence $\xi^{(i)}$ of pseudo-random numbers of length N_m+2^r uniformly distributed in [0,1] is generated. Symbol *s* is represented using the segment $\eta^{(i)} = \xi_s^{(i)}, \ldots, \xi_{s+N_m-1}^{(i)}$ of consecutive N_m pseudo-random numbers. For each symbol a new sequence of pseudo-random numbers is generated. The seed for the PRNG serves as the secret key. The message of *M* symbols is then represented as a summation

$$S_p = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} \eta^{(i)} .$$

The spread spectrum signal S_p is approximately Gaussian with zero mean and unit standard deviation even for moderate values of *M* (e.g., $M \approx 10$). The signal S_p is further multiplied by a parameter γ (watermark strength / visibility) and added to the middle N_m DCT coefficients d_j. Again, the spatial masking model of Girod [Gir1] can be used to adjust γ so that the double watermarked image is perceptually identical to the original image. The value of $\gamma = 13$ works well for most images. The amplitude of the combined watermark is typically in the range [−20,20] with an average rms of 5 gray levels. In [Rua1], the watermark was repeatedly embedded in blocks of 128×128 pixels.

The detection of the message consisting of *M* symbols proceeds by first transforming the image using a DCT and extracting the middle N_m DCT coefficients. The secret key is used to generate *M* pseudo-random sequences of length N_m+2^r needed for coding the message symbols. For each sequence, all 2^r segments of length N_m are correlated with the middle N_m DCT coefficients. The largest value of the correlation determines the encoded symbol.

This watermarking scheme exhibits very impressive robustness properties with respect to many image processing operations. Brightness/contrast adjustment, gamma correction, histogram operations, dithering, sharpening, noise adding, and high-pass filters leave the watermark almost untouched. The watermark is also fairly robust to lossy JPEG compression. Depending on the watermark strength, the message can

supposedly be extracted untouched after JPEG compression with 15% quality. Low pass filtering, mosaic filter, and median rapidly deteriorate the watermark especially when applied iteratively several times.

Scale, rotation, shift invariant watermarking
Ó Ruanaidh et al. [Her1] describe a variation of this technique to make the watermark robust against arbitrary combination of rotation, shift, and change of scale. The idea is to use Fourier transform in log-polar coordinates. It is possible to show that scaling and rotation are transformed to shifts in the new coordinate system.

1. Divide the image into adjacent blocks of 128×128 pixels.
2. Take logarithm of the gray levels (the logarithm corresponds to the logarithmic sensitivity of the human eye described by the Weber's law).
3. Compute the FFT for each block, obtain the magnitude and phase.
4. Modulate the magnitude of the middle band of frequencies by adding a spread-spectrum signal in a similar way as in the previous method.
5. Add a template to the same band by a second modulation.
   a) Apply log-polar map to the magnitude components
   b) Select a set of magnitude components that will be modulated (guiding principle: the pattern formed by the modulated components should have as small autocorrelation as possible)
   c) Map the pattern back from log-polar space into the frequency space
6. Compute inverse FFT using the modulated magnitude components.
7. Apply exponential function to the image (inverse of the Weber's logarithm)

The detection of the watermark starts with the same steps 1.–3. and then the magnitude components are transformed using log-polar map. In the log-polar space a two-dimensional search is performed to find the scaling and rotation parameters. This could be done by computing simple cross-correlation and locating a peak. Using the found scaling and rotation parameters, the image is then transformed back and the detection algorithm is applied to the middle band of Fourier magnitudes in a similar manner as in the previous method. At present, this technique can survive the widest spectrum of geometrical transformations.

Efficient and robust method for adding captions, audio, and video to videos, and images
This method provides a very high capacity with medium robustness. The high information capacity makes it useful for embedding video-in-video or sound without increasing the bandwidth or requiring two separate information streams.

In the beginning, a secret key is specified, which is used to generate author's signature S – a pseudo-random sequence of $M \times N$ numbers in the interval [0,1]. Each $M \times N$ video-frame is divided into blocks of 8×8 pixels. Each block B is transformed using a DCT together with author's signature S. The transformed signature is normalized so that its maximal values are within the unit interval. The DCT transform of B is analyzed using a frequency-masking model [Leg1]. Maximal allowable changes of all 64 DCT coefficients are calculated. Let T denote the minimum of those allowable changes. The transformed block is projected onto a random direction that is obtained as a DCT transform of the normalized signature S. The projection value p is modified to p' by quantizing with T and adjusted by $\pm T/4$ to encode a 1 or –1, respectively. The new, modified DCT block D' is calculated as

$$D' = D + (p' - p)Dct(S).$$

Since $|Dct(S)|<1$, the changes to D are at most $3/4T$ (1/2 for truncating and ¼for adjust ment). The watermarked block is obtained simply by applying inverse DCT to D'. This technique can survive common video distortions, such as high MPEG and noise adding. It is also reasonably fast and secure. Techniques similar to this one will undoubtedly find more applications, such as in tamper detection in digital images.

4.5 Image integrity protection (fraud detection)

Typical use: An imaging device, such as a digital camera, digital video-camera, or a scanner marks an image with a unique, robust, secure watermark before it is saved on a flash card, DAT tape, small mechanical hard drive or sent to output to another device such as computer, video capture board, etc. Embedding watermarks into digital images with the intent to detect the place and extent of image modifications will play an important role in detecting digital frauds, and it can be used to establish a chain of custody in the court of law. Digital images cannot be currently used in the court of law as proofs because of the ease of making digital forgeries and the impossibility to detect image manipulation. The advantage of using digital watermarks is clear: the watermarks are independent of the image format, do not increase the bandwidth (as opposed to adding a header), and cannot be removed to prevent the proof of forgery.

Requirements: Robust, secure, transparent watermark with a detector that does not need the original image.

Solution: The image is divided into blocks, and each block is watermarked with a different watermark. The watermarks depend on a secret, camera-specific key and on the original image. The secret key is embedded in a tamperproof box inside the camera. To prove authenticity of an image, the manufacturer provides the key, and the image integrity is checked by testing the presence of a watermark inside each block. If some blocks exhibit correlation values below a certain threshold, we have evidence that the image has been tampered with – a portion of the image has probably been replaced, or some features have been added or removed. If the correlation is decreased by approximately the same amount in each block but stays above threshold, the image was probably modified using a filter. It may be possible to estimate the filter type (kernel size and kernel values) by comparing the differences in watermark correlations from different blocks.

Powerful publicly available image processing software packages such as Adobe PhotoShop or PaintShop Pro make digital forgeries a reality. Feathered cropping enables replacing or adding features without causing detectable edges. It is also possible to carefully cut out portions of several images and combine them together while leaving barely detectable traces. Techniques such as careful analysis of the noise component of different image segments, comparing histograms of disjoint image blocks, or searching for discontinuities could probably reveal some cases of tampering, but a capable attacker with enough expertise can always avoid such traps and come up with an almost perfect forgery given enough time and resources. This is one of the reasons why digital imagery is not acceptable as evidence in establishing the chain of custody in the court of law. There are other instances, of mostly military character where image integrity is of paramount importance.

Digital images typically contain a lot of redundant information due to large spatial correlations. It is possible to introduce a large MSR error but still be able to identify important features in the image. A good method for detection of tampering should be able to distinguish small, unimportant changes due to common image processing operations from malicious changes, such a erasing features, adding new features, etc. The newly emerged field of information hiding provides new, versatile, and powerful tools for detection of tampering in digital images.

Digital watermarking can be used as a means for efficient tamper detection in the following way. One could mark small blocks of an image with watermarks that depend on a secret ID of that particular digital camera and later check the presence of those watermarks. The “fragility” of the watermark against various image distortions determines our ability to measure the extent of tampering.

4.5.1 Embedding check-sums in LSB

One of the first techniques used for detection of image tampering was based on inserting check-sums into the least significant bit (LSB) of image data. Images taken using CCD elements or scanned on a scanner always contain a noise component. Hiding check-sum bits in the LSB will not produce visible changes. Walton [Wal1] proposes a technique that uses a key-dependent pseudo-random walk on the image. The check-sum is obtained by summing the numbers determined by the 7 most significant bits and taking remainder operation with a large integer N. The probability that two groups of pixels will have the same check-sum is $1/N$. The check-sum is inserted in a binary form in the LSB of selected pixels. This could be

repeated for many disjoint random walks or for one random walk that goes through all pixels. To prevent tampering based on exchanging groups of pixels with the same check-sum, the check-sum can be made "walk-dependent". The method is very fast and on average modifies only half of the pixels by one gray level. Although check-sums can provide a very high probability of tamper detection, they cannot distinguish between an innocent adjustment of brightness and replacing a person's face. Increasing the gray scales of all pixels by one would indicate a large extent of tampering, even though the image content has been unchanged for all practical purposes.

4.5.2 Embedding m-sequences

Van Schyndel et al. [Sch1] modify the LSB of pixels by adding extended m-sequences to rows of pixels. The sequences are generated with a linear feedback shift register with n-stages with periods as high as 2^n. M-sequences have known desirable autocorrelation and randomness properties. For an $N \times N$ image, a sequence of length N is randomly shifted and added to the image rows. The phase of the sequence carries the watermark information. A simple cross-correlation is used to test for the presence of the watermark. This technique is robust to small amount of noise and can accommodate more than one watermark because different segments of m-sequences are uncorrelated. The watermark can, however, be easily removed or replaced by manipulating the LSB. In addition to that, the method does not have good localization properties. Wolfgang and Delp [Wol1] extended van Schyndel's work and improved the localization properties and robustness. They use bipolar m-sequences of –1's and 1's arranged into 8×8 blocks and add them to corresponding image blocks. Their technique is moderately robust with respect to linear and nonlinear filtering and small noise adding. Since the watermark is inserted in the last two LSBs, again, it can be easily removed.

4.5.3 Distortion measure based on perceptual watermarking

Zhu et al. [Zhu1] propose two techniques based on spatial and frequency masking. Their watermark is guaranteed to be perceptually invisible, yet it can detect errors up to one half of the maximal allowable change in each pixel or frequency bin depending on whether spatial [Gir1] or frequency [Leg1] masking is used. The image is divided into blocks and in each block a secret random signature (a pseudo-random sequence uniformly distributed in [0,1]) is multiplied by the masking values of that block. The resulting signal depends on the image block and is added to the original block. The changes are thus always less than or equal to the maximal allowable change and do not introduce visible artifacts. Errors smaller than one half of the maximal allowable change are readily detected by this scheme. The error estimates are fairly accurate for small distortions. It is unclear, however, if this technique would provide any useful information for images that have been distorted by more than a perceptually invisible amount. Even though the image has been visibly distorted, we might want to argue that the image content is essentially the same and no large malicious changes occurred. This could be done using a robust watermarking scheme applied to larger blocks. The watermark in this method [Zhu1] depends on the image in a weak manner. The secret signature does not depend on the image – it is modulated by the masking values of each block. But those masking values are available to anybody to compute. Marking a large number of images with one secret key would be obviously insecure. Such a technique would not be suitable for marking images in digital cameras.

4.5.4 Block-watermarking technique

This technique [Fri3, Fri4] embeds a robust watermark into larger blocks (i.e., 64×64 pixels). To prevent unauthorized removal or intentional distortion, the watermark depends on a secret key S (camera's ID), block number B, and on the content of the block. The content of each block is represented with M bits extracted from the block by projecting it on a set of random, smooth patterns and thresholding the result. This extraction process gives similar M-tuples for similar blocks enabling thus a successful synthesis of the spread spectrum signal from the watermarked / tampered image. The spread spectrum signal for each block is generated by adding M pseudo-random sequences uniformly distributed in [−1,1]. Each sequence depends on the secret key, block number, and the bit extracted from the block. If k out of M bits are extracted incorrectly due to image distortion, the spread spectrum signal will still have large correlation with the image as long as $k << M$.

The spread spectrum signal is rescaled, made DC-free, and added to the middle third of DCT coefficients for each block. The detection proceeds by blocks by recovering *M* bits from each block, generating the spread spectrum signal, and correlating it with the middle third of DCT coefficients of that block.

If watermarks are present in all blocks with high probability, one can be fairly confident that the image has not been tampered with in any significant manner (such as adding or removing features). If the watermark correlation is lower uniformly over all image blocks, one can deduce that some image processing operation was most likely applied. Based on the image content and the watermark strength in each block one can further attempt to classify which image operation was applied (e.g., low-pass filter, high-pass filter, gamma correction, noise adding, etc.). If one or more blocks show very low evidence for watermark presence while other blocks exhibit values well above the threshold, one can estimate the probability of tampering and, hopefully, with a high probability decide whether or not the image has been tampered with.

4.6 Copy control in DVD

Typical use: A commercially distributed movie will carry a robust, transparent watermark that will specify whether or not the movie can be copied. A DVD player able to access the watermark would then refuse to copy the disk to another disk.

Requirements: Robust, transparent, secure watermark embedded in the frames. The original frames are of course unavailable for extraction of the watermark. It is also necessary to have a secure black-box public detector without a secret key built-in a tamper-proof black box in hardware.

4.7 Intelligent browsers, automatic copyright information

Typical use: After an image is downloaded but before it is displayed by a browser, it is checked for presence of watermarks. If certain watermarks are present, the image is not displayed and is automatically erased from computer memory. The screening could be adjusted according to the user that is logged on to the computer. Another application is display of copyright information with every image rendered by browsers, image manipulating software, such as PhotoShop or PaintShop, etc.

Requirements: The most stringent requirements: robustness, invisibility, secure public detector implemented in software. Currently, it is not clear if a secure public watermark detector implemented in software can exist at all.

5. ATTACKS ON WATERMARKS

5.1 The IBM attack.

It is probably best explained on an invertible non-oblivious scheme. Let us assume that Alice watermarks her image I_A by adding her watermark W_A to I: $I_A = I + W_A$. Bob generates his watermark W_B using his key and creates a fake original $I' = I_A - W_B$. Since $I_A = I + W_A = I' + W_B$ and since the watermarking method must be robust with respect to small changes, Bob can argue that Alice's original I contains his watermark W_B if he uses his forged original I' for the detection. Of course, Alice can claim that her watermark is contained in Bob's original if she uses her I as the original image. This creates a deadlock and one cannot unambiguously decide who owns the image. This attack can be thwarted by making the watermark W depend on the original image in a non-invertible manner. In order to forge an original and a watermark, an attacker would have to solve the equation $I_A = I' + W(I')$ for I', which may be computationally very difficult if W for example depends on image hash. Care needs to be taken, however, how the image hash is applied. In some circumstances, if multiple watermarked copies are available, an attack can still be mounted [Cra2]. Craver has also shown that oblivious schemes, such as the direct spread spectrum technique by Pitas are also vulnerable to this attack. If the seed used to divide the image into three sets *A*, *B*, and *C* does not depend on the image, one could carefully exchange the pixels from arbitrarily chosen

sets *A*', *B*', and *C*' to forge a watermark inside any image. Of course, if the seed depends on the image in a non-invertible manner, this attack will not be possible.

The collusion attack becomes relevant whenever one image is watermarked with different watermarks and those copies are distributed. For example, fingerprinting movies with the intention to identify the customer requires marking the frames with a different watermark that is unique to the customer. If many customers average together the frames from their movies, the watermarks will cancel out and a non-watermarked copy could be obtained. This is called the collusion attack. In some situations, the collusion attack is not relevant simply because only one watermarked copy of a digital image will be ever made and distributed. But for fingerprinting and traitor tracing, the collusion attack needs to be taken into account.

5.2 StirMark

This powerful attack has been designed by a research group (R. Andersson, F. Petitcolas, and M. Kuhn) at University of Cambridge. The attack simulates image distortions that commonly occur when a picture is printed, photocopied, and rescanned. The image is slightly stretched and compressed by random amounts, a small amount of noise is added to simulate quantization errors of A/D and D/A conversion. The strongest part of this attack is the small geometrical change. They cause loss of synchronization between watermark detector and the image. For low-frequency watermarks, small geometrical deformations can cause large differences in DCT coefficients. StirMark does not pose any threat to non-oblivious watermarking because the original image can be used for registration of the watermarked/attacked image. Oblivious watermarking methods, however, may be seriously disturbed by this attack. Currently, there is no oblivious watermarking scheme that would be able to withstand the StirMark attack.

5.3 The mosaic attack

This attack was motivated by an automatic system for copyright piracy detection – a special program (a crawler) that will search through the Internet, download pictures, and look for illegal copies of images watermarked with a certain watermark. The idea behind the mosaic attack is to simply break an image into small portions and correctly assemble them on a web page so that a complete image without spaces is obtained. This is easily done because most browsers can paste images without any spaces in between them. Because images with dimensions smaller than a certain limit cannot be reliably watermarked, the crawler would not detect the watermark in any mosaic piece. Another possibility is to "wrap" images into Java applets, Active X objects so that they would not be recognized as images to the crawler. The applet can even descramble the image in real time.

This attack can only be overcome by a system that would render the complete web page on a computer screen, detect the images, and search for watermarks in them.

5.4 The histogram attack

This attack applies mostly to fix-depth watermarks that are applied to images with some singularities in the histogram. The histograms of some images after scanning exhibit regularly distributed peaks. If such an image is watermarked with a fixed depth watermark [Pit1,Ben1], the peaks will essentially double and one can correctly estimate a large portion of the watermark pattern by simply counting the number of pixels occupying neighboring gray level bins. The attack can be easily thwarted if images are preprocessed before watermarking to get rid of the histogram peaks. Details of this attack can be found in [Mae1].

5.5 Attack based on partial knowledge of the watermark

It is important that a partial knowledge of the watermark should not enable a pirate to remove the entire watermark or disturb it beyond reliable detection. It might indeed be possible in certain cases to reconstruct the watermark pattern based on the assumption that the watermark becomes partially known. This assumption is not that unreasonable as it may seem at first. For example, one can make a guess that certain portion of the original image had pixels of uniform brightness or of a uniform gradient, or an attacker may be able to foist a piece of his image into a collage created by somebody else. If this is the case, then the

knowledge of a portion of the watermark pattern may give us additional constraints to disturb or eliminate the whole watermark. This is especially relevant for watermark patterns spanned by publicly known functions. In [Fri1] an attack is described that can be applied to any non-adaptive robust watermarking technique, invertible or not, if some portion of the original unwatermarked image is known or can be guessed, and if the watermark is mostly spanned by some small number of Fourier modes. The attack attempts to find the coefficients of the lowest frequency DCT coefficients based on the "known" pixel values. A set of linear equations completed with a stabilizing functional makes the inversion possible.

6. OPEN PROBLEMS AND CHALLENGES

6.1 Oblivious secure watermarking

State of the art: Reasonable robustness with respect to changes in the gray levels due to filtering, lossy compression, and due to simple geometric transformations, such as shift, scaling, rotation, and cropping. If general nonlinear geometric transformations, such as StirMark, is applied, the synchronization of the watermark detector becomes a very hard problem. Watermark detection is then equivalent to a search in a 6-dimensional space, which is a very computationally intensive task.

Needs to be solved: A robust watermark with a computationally efficient detector that can extract watermarks from images that underwent general geometric distortions.

Possible approaches: *Content Locked Coordinate Systems* (CLCS) being investigated at Phillips Research Labs.

Abandon all pixel-based or coefficient-based techniques and use *feature-based techniques*. For example, one could embed information into edge profiles or into mutual relationship among edges. If an image does not have well defined edges, the contrast or color depth of the image would be adjusted so that features can be defined.

Embedding marks into images and use the marks to learn about the deformation the image underwent. Possible problem: The watermarking strength will only be as good as the marks. Also, one would have to search for the marks, which may still be computationally expensive.

6.2 Watermarking schemes with a secure public black-box watermark detector

State of the art: Virtually all watermark detectors are thresholded correlators. This makes them vulnerable to a variety of general attacks. By feeding the black box with a sequence of images, one first determines a critical image for which a small change to the image flips the watermark detector (the critical image may not be close to the watermarked image). The black box is then implemented in software and a search for the secret key is performed. This can be done in a statistical manner or by solving an overdetermined system of equations.

It is hypothesized that nonlinear detectors that are not based on thresholded correlations will not be vulnerable to this type of attack. Probabilistic thresholds somehow alleviate the problem.

Needs to be solved: Clarify which properties of the watermark detector are important. Is it nonlinearity, discreteness, or non-invertibility? Design a robust watermarking technique and a secure black-box detector. Clarify the relationship between neural nets and public watermark detectors. Another question is whether or not it is possible to find a general procedure for design secure public black-box detectors for a large class of watermarking schemes.

Possible approaches: Key-dependent basis, embedding a pattern into the projections onto the basis functions.

6.3 Watermarking schemes with a secure public watermark detector

State of the art: This is an extremely difficult problem. To the best of my knowledge, no schemes have ever been described in the scientific literature, and no proofs of impossibility have been given. Most likely, cryptographic tools developed for public-key systems must be used.

Needs to be done: Clarify if schemes with such detectors are possible in principle. Design a robust scheme with secure public detector.

Possible approaches: Use one-way trapdoor functions to hide the key or the values of some quantities derived from the image. One could for example hide a key as a large prime masked (multiplied) by another large prime and give the product to public. Of course, there is long way from this simple idea to something practical.

8. REFERENCES

This list contains most of the important and influential papers on data hiding in digital imagery and its applications. Some relevant citations are also included.

[And1] R. J. Anderson, "Stretching the Limits of Steganography", *1st Information Hiding Workshop, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 39–48, 1996.
[And2] R. J. Anderson and Fabien A. P. Petitcolas, "On the limits of steganography", *IEEE Journal of Selected Areas in Communications (J-SAC) – Special Issue on Copyright & Privacy Protection*, (to appear) 1998.
[Ano1] Anonymous (zguan.bbs@bbs.ntu.edu.tw), "Learn cracking IV – Another weakness of PictureMarc", [news:tw.bbs.comp.hacker] mirrored on [http://www.cl.cam.ac.uk/~fapp2/watermarking/image watermarking/digimarc crack.html], August 1997. Includes instructions to override any Digimarc watermark using PictureMarc.
[Arc1] G. Arce, "A Blind Digital Image Signature in Wavelet Compression", University of Delaware.
[Auc1] D. Aucsmith, "Tamper Resistant Software: An Implementation", *1st Information Hiding Workshop, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 317–333, 1996.
[Auc2] D. Aucsmith, "Tamper resistant software: An implementation", In Anderson [2], pp. 317–333.
[Aur1] T. Aura, "Invisible communication", *Proc. of the HUT Seminar on Network Security '95*, Espoo, Finland, Nov 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology. [http://deadlock.hut.fi/ste/ste_html.html], [ftp://saturn.hut.fi/pub/aaura/ ste1195.ps]
[Ben1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding", *Proc. of the SPIE Conference on Storage and Retrieval for Image and Video Databases III*, vol. 2420, pp. 164–173, San Jose, CA, Feb. 1995.
[Ben2] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding", Technical report, MIT Media Lab, 1996.
[Ben3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal **35**(3/4), pp. 313–336, 1996.
[Ber1] H. Berghel and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking", *IEEE Computer* , **29**(7), pp. 101–103, 1996.
[Bla1] R. E. Blahut, The theory and practice of error control codes, Addison-Wesley, 1983.
[Bol1] F. M. Boland, J. J. K. Ó Ruanaidh, and C. Dautzenberg, "Watermarking Digital images for Copyright Protection", *Proc. of the 5th IEE International Conference on Image Processing and its Applications*, no. 410, Edinburgh, July, 1995, pp. 326–330.
[Bon1] L. Boney, A. H. Tewfik, K. N. Hamdy, "Digital Watermarks for Audio Signals", *IEEE International Conference on Multimedia Computing and Systems*, Hiroshima, Japan; pp. 473–480, June 1996.
[Bon2] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals", *European Signal Processing Conference*, EUSIPCO '96, Trieste, Italy, Sep 1996.

[Bor1] A. G. Bors and I. Pitas, “Image watermarking using DCT domain constraints”, *Proc. IEEE Int. Conference on Image Processing*, vol. 3, pp. 231–234, 1996.
[Bra1] R. D. Brandt and F. Lin, “Representations that uniquely characterize images modulo translation, rotation and scaling”, Pattern Recognition Letters, vol. 17, pp. 1001–1015, August 1996.
[Brs1] J. Brassil, S. Low, N. F. Maxemchuk, and L. O’Gorman, “Electronic Marking and Identification Techniques to Discourage Document Copying”, *IEEE J. Selected Areas in Commum.*, vol. 13, no. 8, pp. 1495–1504, Oct 1995.
[Brs2] J. Brassil, S. Low, N. Maxemchuk, L. O’Goram, “Document Marking and Identification using Both Line and Word Shifting”, Infocom95. [ftp://ftp.research.att.com/dist/brassil/1995/infocom95.ps.Z]
[Brs3] J. Brassil, S. Low, N. Maxemchuk, L. O’Goram, “Hiding Information in Document Images”, CISS95. [ftp://ftp.research.att.com/dist/brassil/ 1995/ciss95.ps.Z]
[Brs4] J. Brassil and L. O’ Gorman, “Watermarking document images with bounding box expansion”, *I1st Information Hiding Workshop*, R. Anderson, ed., vol. 1174 of Lecture Notes in Computer Science, pp. 227–235, Springer-Verlag, 1996.
[Brd1] G. W. Braudaway, “Protecting publicly-available images with an invisible image watermark”, *Proc. of the ICIP*, pp. 524–527, Santa Barbara, California, Oct 1997.
[Brd2] G. Braudaway, K. Magerlein and F. Mintzer, “Protecting publicly available images with a visible image watermark”, *Proc. SPIE: Optical Security and Counterfeit Deterrence Techniques*, vol. 2659, pp. 126–133, 1996.
[Bru1] O. Bruyndonckx, J. J. Quisquater, B. Macq, “Spatial method for copyright labeling of digital images”, *Proc. IEEE Workshop on Nonlinear Signal and image processing*, I. Pitas editor, pp. 456–459, 1995.
[Bur1] S. Burgett, E. Koch, and J. Zhao, “A novel method for copyright labelling digitized image data”, *IEEE Transactions on Communications*, Sep 1994.
[Car1] G. Caronni, “Assuring ownership rights for digital images”, *Proc. Reliable IT Systems*, VIS' 95, Vieweg Publishing Company, 1995.
[Cha1] W. G. Chambers, “Basics of Communications and Coding. Oxford Science Publications”, Clarendon Press Oxford, 1985.
[Com1] B. O. Comiskey and J. R. Smith, “Modulation and Information Hiding in Images”, in: *Information Hiding, First International Workshop*, ed. Ross J. Anderson. Cambridge, U.K., May 30–June 1, 1996, Proc. Lecture Notes in Computer Science, vol. 1174, Springer-Verlag, 1996 [http://sunsite.informatik.rwth-aachen.de/dblp/db/conf/ih/ih96.html]
[Cox1] I. J. Cox and J.-P. M. G. Linnartz, “Some general methods for tampering with watermarks”, preprint, 1998.
[Cox2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “A secure, robust watermark for multimedia”, *Proc. of the Information Hiding: First Int. Workshop*, Lecture Notes in Computer Science, vol. 1174, R. Anderson, ed., Springer-Verlag, pp. 183–206, 1996.
[Cox3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, Technical Report 95–10, NEC Research Institute, 1995.ftp://ftp.nj.nec.com/pub/ingemar/papers/watermark.ps.Z.
[Cox4] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, “Secure Spread Spectrum Watermarking for Images, Audio and Video”, *Proc. IEEE Int. Conf. on Image Processing*, Lausanne, Switzerland, vol. 3, pp. 243–246, Sep 1996.
[Cox5] I. J. Cox and J.-P. M. G. Linnartz, “Public watermarks and resistance to tampering”, Proc. of the ICIP, Santa Barbara, California, October 1997. Paper appears only in CD version of proceedings.
[Cox6] I. J. Cox and M. L. Miller, “A Review of Watermarking and the Importance of Perceptual Modeling”, *Proc. of the SPIE Human Vision and Electronic Imaging*, vol 3016, pp. 92–99, 1997.
[Cox7] I. J. Cox and Kazuyoshi Tanaka, “NEC data hiding proposal”, Technical report, NEC Copy Protection Technical Working Group, July 1997. Response to call for proposal issued by the Data Hiding SubGroup.
[Cra1] S. Craver, N. Memon, B. Yeo, and M. Yeung, “Can Invisible Watermarks Resolve Rightful Ownerships?” Technical Report RC 20509, IBM Research Division, July 1996.
[Cra2] Scott Craver, Nasir Memon, Boon-Lock Yeo, and M. Yeung, “Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications”, *IEEE Journal of Selected Areas in Communications*, 1998.

[Cra3] S. Craver, N. Memon, B.-L. Yeo, and M. Yeung. “Can invisible watermarks resolve rightful ownerships?” *Proc. of the IS&T/SPIE Conference on Storage and Retrieval for Image and Video Databases V*, San Jose, CA, USA, vol. 3022, pp. 310–321, Feb 1997.
[Cra4] S. Craver, “On Public-key Steganography in the Presence of an Active Warden”, IBM Research Report RC 20931, July 1997.
[Dau1] C. Dautzenberg and F. M. Boland. Watermarking Images. Technical report, Department of Electronic and Electrical Engineering, Trinity College Dublin, 1994.
[Dav1] P. Davern and M. Scott, “Fractal based image steganography”, R. Anderson, editor, *Information Hiding, First International Workshop*, Lecture Notes in Computer Science, pp. 279–294. Springer-Verlag, Berlin, 1996.
[Del1] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq, “Digital watermarking”, *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques*, vol. 2659, pp. 99–110, February, 1996.
[Del2] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq, “Digital watermarking of images”, *Proc. of the IS&T/SPIE Symposium on Electronic Imaging Science and Technology*, 1996.
[Dig1] Digimarc home page. [http://www.digimarc.com/], April 1997.
[Dix1] R. C. Dixon, “Spread Spectrum Systems with Commercial Applications”, Wiley, New York, 1994.
[Dug1]R. Dugad, Krishna Ratakonda, Narendra Ahuja, “A New Wavelet Based Scheme for Watermarking Images”, University of Illinois at Urbana-Champaign
[Dvd1] Watermarking for DVD - Call for Proposals see http:// www.dvcc.com/ dhsg/, July 1997.
[Ett1] J. M. Ettinger, “Steganalysis and Game Equilibria”, *2nd Information Hiding Workshop*, Portland, OR, Apr 15–17, 1998.
[Fra1] E. Franz, A. Jerichow, S. Moeller, A. Pfitzmann and I. Stierand, “Computer-based steganography”, *Information Hiding, First Int. workshop*, Cambridge, UK, Springer, Lecture Notes in Computer Science, No. 1174, pp. 7–21, 1996.
[Fri1] J. Fridrich, “Robust digital watermarking based on key-dependent basis functions”, *The 2nd Information Hiding Workshop in Portland*, Oregon, April 15–17, 1998.
[Fri2] J. Fridrich, “Combining Low-frequency and Spread Spectrum Watermarking”, *Proc. SPIE Int. Symposium on Optical Science, Engineering, and Instrumentation*, San Diego, July 19–24, 1998.
[Fri3] J. Fridrich, “Image Watermarking for Tamper Detection”, *Proc. ICIP ’98*, Chicago, Oct 1998.
[Fri4] J. Fridrich, “Methods for Detecting Changes in Digital Images”, *Proc. of The 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems* (ISPACS' 98),Melbourne, Australia, 4–6 November 1998.
[Gir1] B. Girod, “The Information Theoretical Significance of Spatial and Temporal Masking in Video Signals”, *Proc. of the SPIE Human Vision, Visual Processing, and Digital Display*, vol. 1077, pp. 178–187, 1989.
[Gir2] B. Girod and F. Hartung, “Watermarking Method and Apparatus for Compressed Digital Video”, US Patent application, 1996. [http://www-nt.e-technik.uni-erlangen.de/~hartung/watermarking.html]
[Gir3] F. Goffin, J. F. Delaigle, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, “A low cost perceptive digital picture watermarking method”, In Sethin and Jain [50], pp. 264–277.
[Gol1] D. M. Goldschlag, M. G. Reed, P. F. Syverson, “Hiding Routing Information”, *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 137–150, 1996.
[Gru1] Daniel Gruhl, Walter Bender, and Anthony Lu, “Echo hiding”, In Anderson [2], pp. 295–315.
[Gru2] D. Gruhl, A. Lu, W. Bender, “Echo Hiding”, *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 295–315, 1996.
[Kha1] Khaled N. Hamdy, Ahmed H. Tewfik, Ting Chen, and Satoshi Takagi, “Time-scale modification of audio signals with combined harmonic and wavelet representations”, *International Conference on Acoustics, Speech and Signal Processing–ICASSP '97*, vol. 1, pp. 439–442, Munich, Germany, April 1997. IEEE Press. Session on Hearing Aids and Computer Music.
[Han1] T. G. Handel and Sandford [http://www.lanl.gov/users/u078743/embed1.htm
[Har1] F. H. Hartung and B. Girod, “Watermarking of MPEG-2 Encoded Video without Decoding and Reencoding”, *Proc. of the SPIE Conference on Multimedia Computing and Networking*, vol. 3020, pp. 264–274, San Jose, CA, Feb 1997.
[Har2] F. Hartung and B. Girod, “Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video”, *Proc. European Conference on Multimedia Applications, Systems and Technologies (ECMAST 97)*, Milano, Italy, May 1997.

[Har3] F. Hartung and B. Girod, “Digital watermarking of MPEG-2 coded video in the bitstream domain”, *Proc. International Conference on Acoustics, Speech, and Signal Processing (ICASSP 97)*, Munich, Germany, April 1997.
[Har4] F. Hartung and B. Girod, “Digital watermarking of raw and compressed video”, In N. Ohta, editor, Digital Compression Technologies and Systems for Video Communications, *SPIE Proc. Series*, vol. 2952, pp. 205–213, Oct 1996.
[Har5] F. Hartung and B. Girod, “Digital Watermarking of Raw and Compressed Video”, *Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies*, Berlin, Germany, Oct. 1996.
[Har6] F. Hartung and B. Girod, “Digital watermarking of uncompressed and compressed video”, Signal Processing, 1997. Accepted.
[Har7] F. Hartung and B. Girod, “Watermarking of MPEG-2 Encoded Video Without Decoding and Re-encoding”, *Proc. Multimedia Computing and Networking 1997 (MMCN 97)*, San Jose, CA, Feb 1997.
[Har8] F. Hartung and B. Girod. Fast public-key watermarking of compressed video. *Proc. of the IEEE International Conference on Image Processing*, Santa Barbara, CA, Oct 1997.
[Her1] A. Herrigel, J. Ó Ruanaidh, H. Petersen, S. Pereira, T. Pun, “Secure Copyright Protection Techniques for Digital Images,” *Proc. 2nd Int. Information Hiding Workshop*, Portland, Oregon, April 15–17, 1998.
[Hsu1] C.-T. Hsu and J.-L. Wu, “Hidden signatures in images”, *IEEE Int. Conf. on Image Processing*, 1996.
[His1] Hisashi Inoue, Akio Miyazaki, Akihiro Yamamoto, Takashi Katsura, “A Digital Watermark Based on the Wavelet Transform and Its Robustness on Image Compression”, Matsushita Electric Industrial Co., Ltd; Kyushu University.
[Jag1] G. Jagpal, “Steganography in Digital Images”, Thesis, Cambridge University Computer Laboratory, May 1995.
[Jay1] N. Jayant, J. Johnston, and R. Safranek, “Signal Compression Based on Models of Human Perception”, *Proc. of the IEEE*, vol. 81, pp. 1385–1422, Oct 1993.
[Jay2] N. Jayant, J. Johnston, and R. Safranek, “Perceptual Coding of Images”, *SPIE*, vol. 1913, 1993.
[Kah1] D. Kahn, “The Codebreakers”, Macmillan, NY, 1967.
[Kah2] D. Kahn, “The history of steganography”, *1st Workshop on Information Hiding, Lecture Notes in Computer Science*, R. Anderson, ed., vol. 1174, pp. 1–5, Springer-Verlag, 1996.
[Kal1] T. Kalker, “Watermark Estimation Through Detector Observation”, Philips Research Eindhoven, Netherland, preprint 1998.
[Kal2] T. Kalker, J. P. Linnartz, and M. van Dijk, “Watermark estimation through detector analysis”, *Proc. of the ICIP*, Chicago, Oct 1998. Submitted.
[Koc1] E. Koch, J. Rindfrey and J. Zhao, “Copyright Protection for Multimedia Data”, *Proc. Int. Conf. on Digital Media and Electronic Publishing*, Leeds, UK, 6-8 December 1994.
[Koc2] E. Koch, J. Zhao, “Towards robust and hidden image copyright labeling”, *Proc. Nonlinear Signal Processing Workshop*, Thessaloniki, Greece, pp. 452–455, 1995. [http://www.igd.fhg.de/www/igd-a8/pub/IEEE_Hidden.ps]
[Kuh1] M. G. Kuhn, “Stirmark”, available at http://www.cl.cam.ac.uk/~mgk25/stirmark/, Security Group, Computer Lab, Cambridge University, UK (E-mail: mkuhn@acm.org), 1997.
[Kun1] D. Kundur and D. Hatzinakos, “A robust digital image watermarking method using wavelet-based fusion”, to appear in *Proc. Int. Conference in Image Processing*, 1997.
[Kun2] D. Kundur and D. Hatzinakos, “Digital Watermarking Based on Multiresolution Wavelet Data Fusion”, *Proc. IEEE, Special Issue on Intelligent Signal Processing*, under review, 43 pages, 1997.
[Kur1] C. Kurak, J. McHugh, “A cautionary note on image downgrading”, *IEEE Computer Security Applications Conference*, pp. 153–159, San Antonio, TX, USA, December 1992.
[Lag1] R. L. Lagendijk G. C. Langelaar, J. C. A. van der Lubbe, “Robust Labeling Methods for Copy Protection of Images”, *Proc. of the SPIE Conference on Storage and Retrieval for Image and Video Databases V*, vol. 3022, pp. 298–309, San Jose, CA, February 1997.
[Lag2] G. C. Langelaar, J. C. A. van der Lubbe, and J. Biemond, “Copy protection for multimedia data based on labeling techniques”, In 17th Symposium on Information Theory in the Benelux, Enschede, The Netherlands, May 1996.
[Lan1] G. C. Langelaar, J. C. A. van der Lubbe, and R. L. Lagendijk, “Robust labeling methods for copy protection of images”, In Sethin and Jain [50], pp. 298–309.

[Leg1] G. E. Legge and J. M. Foley, “Contrast Masking in Human Vision”, *J. Opt. Soc. Am.*, **70**(12), pp. 1458–1471, 1980.
[Lin1] J. P. Linnartz and M. van Dijk, “Analysis of the sensitivity attack against electronic watermarks in images”, *Proc. of the Workshop on Information Hiding*, Portland, April 1998. Submitted.
[Lin2] J. P. M. G. Linnartz, A. C. C. Kalker, G. F. Depovere, and R. Beuker, “A reliability model for detection of electronic watermarks in digital images”, *Proc. Benelux Symposium on Communication Theory*, Enschede, pp. 202–208, Oct 1997.
[Lin3] J.-P. Linnartz, T. Kalker, G. Depovere, “Modelling the false alarm and missed detection rate for electronic watermarks”, *Proc. of this Workshop*.
[Mac1] R. Machado. Stego. http://www.fqa.com/romana/romanasoft/stego.html
[Mae1] M. J. J. Maes, “Twin peaks: The histogram attack to fixed depth image watermarks”, *Proc. of the Workshop on Information Hiding*, Portland, April 1998. Submitted.
[Mae2] M. J. J. Maes and C. W. A. M. van Overveld, “Digital watermarking by geometric warping”, *Proc. of the ICIP*, October 1998. Submitted.
[Mat1] K. Matsui and K. Tanaka, “Video-steganography: How to secretly embed a signature in a picture”, *Proc. IMA Intellectual Property Project*, vol. 1, pp. 187–206, 1994.
[Mil1] E. Milbrandt, “Steganography Info and Archive”, Available at URL http://indyunix.iupui.edu/¸emilbran/stego.html.
[Mil2] E. Milbrandt. http://members/iquest.net/mrmil/stego.html, October 1997. Steganography Info and Archive.
[Min1] F. Mintzer, Albert Cazes, Francis Giordano, Jack Lee, Karen Magerlein and Fabio Schiattarella, “Capturing and preparing images of Vatican library manuscripts for access via Internet”, *Proc. of the IS&T 48th Annual Conference*, Washington, DC, USA, pp. 74–77, May 1995.
[Mor1] N. Morimoto and Daniel Sullivan. IBM Data Hiding proposal. Technical report, IBM Corporation, September 1997. Response to call for proposal issued by the Data Hiding SubGroup.
[Mor2] D. C. Morris, “Embedding hidden indentification codes in digital objects”, US Patent 5,530,751, 1996.
[Mos1] I. S. Moskowitz, M. H .Kang, “Covert Channels - Here to Stay?”, Compass 94 pp. 235–243
[Nik1] N. Nikolaidis and I. Pitas, “Copyright protection of images using robust digital signatures”, *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol. 4, pp. 2168–2171, May 1996.
[Nil1] N. B. Nill, “A visual model weighted cosine transform for image compression and quality assessment”, *IEEE Trans. Communications*, vol. COM-33, No. 6, 1985.
[Rua1] J. J. K. Ó Ruanaidh and T. Pun, “Rotation, scale and translation invariant digital image watermarking”, *Proc. of the ICIP*, vol. 1, pp. 536–539, Santa Barbara, California, Oct 1997.
[Rua2] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, “Phase Watermarking of Digital Images”, *Proc. IEEE Int. Conf. on Image Processing*, vol. 3, pp. 239–242, Lausanne, Switzerland, Sep 1996.
[Rua3] J. J. K. Ó Ruanaidh, F. M. Boland, and O. Sinnen. Watermarking digital images for copyright protection. *Proc. of the Electronic Imaging and Visual Arts Conference*, Florence, Feb 1996.
[Rua4] J. J. K. Ó Ruanaidh, F. M. Boland, and C. Dautzenberg, “Watermarking Digital Images for Copyright Protection”, *Proc. of the IEE Conference on Image Processing and its Applications*, Edinburgh, pp. 326–330, 1995.
[Rua5] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, “Watermarking digital images for copyright protection”, *IEE Proc. Vision, Image and Signal Processing*, **143**(4), pp. 250–256, August 1996.
[Ohn1] J. Ohnishi and K. Matsui, “Embedding a seal into a picture under orthogonal wavelet transform”, *Proc. Int. Conference on Multimedia Computing and Systems*, pp. 514–521, June 1996.
[Pet1] F. A. P. Petitcolas, “Weakness of existing watermarking schemes”, [http://www.cl.cam.ac.uk/~fapp2/watermarking/image watermarking/], Oct 1997.
[Pfi1] B. Pfitzmann, “Information hiding terminology”, In R. Anderson, editor, *Information Hiding, Lecture Notes in Computer Science*, pp. 347–350. Springer-Verlag, Berlin, 1996.
[Pit1] I. Pitas, “A method for signature casting on digital images”, *Proc. of the IEEE International Conference on Image Processing*, vol. 3, pp. 215–218, Sep 1996.
[Pit2] I. Pitas and T. Kaskalis, “Applying signatures on digital images”, *Nonlinear Signal and Image Processing Workshop*, Thessaloniki, Greece, pp. 460–463, 1995.
[Pit3] I. Pitas, T. Kaskalis : "Signature Casting on Digital Images”, *Proc. IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, June, Greece, 1995.

[Piv1] A. Piva, M. Barni, F. Bartolini, V. Cappellini, “DCT-based watermark recovering without resorting to the uncorrupted original image”, preprint, 1997.
[Pod1] C. I. Podilchuk and W. Zeng, “Digital image watermarking using visual models”, *Proc. of the IS&T/SPIE Conference on Human Vision and Electronic Imaging II*, San Jose, CA, USA, vol. 3016, pp. 100–111, Feb 1997.
[Pod2] C. I. Podilchuk and W. Zeng, “Image Adaptive Watermarking Using Visual Models”, To appear, *IEEE Journal on Selected Areas in Communications*, 1997.
[Pod3] C. I. Podilchuk and W. Zeng, “Perceptual watermarking of still images”, *Proc. The First IEEE Signal Processing Society Workshop on Multimedia Signal Processing*, June 1997, Princeton, New Jersey.
[Pod4] C. I. Podilchuk and W. Zeng, “Watermarking of the JPEG bitstream”, *Proc. of the International Conference on Imaging Science*, Systems, and Technology, Las Vegas, Nevada, USA, pp. 253–260, June 30 – July 3, 1997.
[Pre1] R. D. Preuss, S. E. Roukos, A. W. F. Huggins, H. Gish, M. A. Bergamo, P. M. Peterson, and D. A. G, “Embedded signalling”, US Patent 5,319,735, 1994.
[Rho1] G. B. Rhoads, “Indentification/authentication coding method and apparatus”, World Intellectual Property Organization, WIPO WO 95/14289, 1995.
[Rho2] Geoffrey B. Rhoads, “Steganography methods employing embedded calibration data”, US Patent 5636292, June 1997.
[Rio1] O. Rioul and M. Vetterli, “Wavelets and Signal Processing”, *IEEE Signal Processing Mag.*, vol. 8, pp. 14–38, Oct 1991.
[Pam1] Pamela Samuelson, “Copyright and digital libraries”, Communications of the ACM, **38**(4), April 1995.
[Max1] T. Maxwell Sandford II, Jonathan N. Bradley, and Theodore G. Handel. “The data embedding method”, *Proc. of the SPIE Photonics East Conference*, Philadelphia, Sep 1995.
[Scn1] M. Schneider and S.-F. Chang, “A Robust Content Based Digital Signature for Image Authentication”, *Proc. of the 1996 IEEE International Conference on Image Processing*, Lausanne, Switzerland, Sept 1996.
[Scn2] M. Schneider and S.-F. Chang, “A Content-Based Approach to Image Signature Generation and Authentication”, vol. III, pp. 227–230, in *Proc. ICIP ’96*.
[Sch1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark”, *Proc. of the IEEE International Conference on Image Processing*, vol. 2, pp. 86–90, Austin, Texas, USA, Nov 1994.
[Sch2] R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne, “Towards a robust digital watermark”, *Proc. of the ACCV-95 Conference*, Nanyang Technological University, Singapore, Dec 1995.
[Ser1] S. Servetto and C. Podilchuk, “On the Number of Bits that can be Hidden in an Image”, Technical report, Bell Laboratories, Nov 1997.
[Sig1] “Signum Technologies – SureSign digital fingerprinting”, [http://www.signumtech.com/], Oct 1997.
[Smi1] J. P. Smith, “Authentication of Digital Medical Images with Digital Signature Technology”, Radiology, vol. 194, No.3, pp. 771-774, 1995.
[Smi2] J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images”, *Proc. Information Hiding: First Int. Workshop*, R. Anderson, ed., vol. 1174 of Lecture Notes in Computer Science, pp. 207–226, Springer-Verlag, 1996.
[Sto1] H. S. Stone, “Analysis of Attacks on Image Watermarks with Randomized Coefficients”, NEC Research Institute, Technical Report, 1996.
[Swa1] M. D. Swanson, B. Zhu, B. Chau, and A. H. Tewfik, “Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation”, preprint, Department of Electrical and Computer Engineering, Univ. of Minnesota, Minneapolis, MN 55455, 1998.
[Swa2] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia Data Embedding and Watermarking Technologies”, Invited Paper, to appear in the *Proc. of the IEEE*, 1998.
[Swa3] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Robust data hiding for images”, *Proc. of the IEEE Digital Signal Processing Workshop*, pp. 37–40, Loen, Norway, Sep 1996.
[Swa4] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Transparent robust image watermarking”, *Proc. IEEE Int. Conf. on Image Processing*, vol. 3, pp. 211–214, 1996.
[Swa4] M. Swanson, B. Zhu, and A. H. Tewfik, “Data Hiding for Video in Video”, *Proc. ICIP '97*, vol. II, pp. 676–679.

[Mat1] K. Matsui and K. Tanaka, “Video-steganography: How to secretly embed a signature in a picture”, *Journal of the interactive Multimedia Association Intellectual Property Project*, **1**(1), pp. 187–206, January 1994.
[Tan1] K. Tanaka, Y. Nakamura, and K. Matsui, “Embedding Secret Information into a Dithered Multi-level Image”, *Proc. of IEEE Military Communications Conference*, pp. 216–220, 1990.
[Tao1] B. Tao and B. Dickinson, “Adaptive Watermarking in the DCT Domain”, *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Munich, Germany, April 21–24, 1997.
[Tew1] A. H. Tewfik, M. D. Swanson, B. Zhu, K. Hamdy, and L. Boney, “Transparent Robust Watermarking for Images and Audio”, *IEEE Trans. on Signal Proc.*, 1996.
[Tir1] A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne. Electronic watermark, in Dicta-93, pp. 666–672, Macquarie University, Sydney, Dec 1993.
[Tir2] A. Z. Tirkel, R. G. van Schyndel, and C. F. Osborne. A two-dimensional digital watermark. In ACCV, Singapore, 1995.
[Unz1] Unzign. Available at http://altern.org/watermark/ (E-mail: unzign@hotmail.com), 1997.
[Wal1] S. Walton, “Information authentication for a slippery new age”, *Dr. Dobbs Journal*, vol. 20, no. 4, pp. 18–26, April, 1995.
[Wat1] A. B. Watson, “DCT quantization matrices visually optimized for individual images”, *Proc. of the SPIE Conference on Human Vision, Visual Processing and Digital Display IV*, pp. 202-216, 1992.
[Way1] P. Wayner, “Disappearing Cryptography – Being and Nothing on the Net”, AP Professional, 1996.
[Way2] P. Wayner [http://www.funet.fi/pub/crypt/old/mimic/Peter Wayner]
[Wol1] R. B. Wolfgang and E. J. Delp, “A watermark for digital images”, *Proc. IEEE Int. Conf. on Image Processing*, vol. 3, pp. 219–222, 1996.
[Wol2] R. B. Wolfgang and E. J. Delp, “A watermarking technique for digital imagery: further studies”, *Proc. of the IEEE International Conference on Imaging, Systems, and Technology*, pp. 279–287, Las Vegas, NV, USA, June 30–July 3 1997.
[Wol3] R. B. Wolfgang, Christine I. Podilchuk, Edward J. Delp, “A Wavelet-Based Watermarking Technique for Compressed Color Images”, Purdue University; Bell Laboratories, ucent Technologies
[Xia1] X.-G. Xia, C. G. Boncelet, and G. R. Arce, “A multiresolution watermark for digital images”, *Proc. of the ICIP*, vol. 1, pp. 548–551, Santa Barbara, California, Oct 1997.
[Xio1] Zixiang Xiong, Wenwu Zhu, Ya-Qin Zhang, “Multiresolution Watermarking for Images and Video: A Uniform Approach”,
[Zha1] J. Zhao, “A www service to embed and prove digital copyright watermarks”, *European Conference on Multimedia Applications, Services and Techniques*, pp. 695–710, Louvain-la-Neuve, Belgium, May 1996.
[Zha2] J. Zhao. The syscop home page.[http://syscop.igd.fhg.de/] or [http://www.crcg.edu/syscop/], February 1997.
[Zha3] J. Zhao and E. Koch, “Embedding Robust Labels into images for Copyright Protection”, Intellectual Property Rights and New Technologies, *Proc. of the KnowRight' 95Conference*, pp. 242–51, 1995.
[Zha4] J. Zhao and E. Koch, “Embedding Robust Labels Into Images For Copyright Protection”, *Proc. Int. Congr. on IPR for Specialized Information, Knowledge and New Technologies*, Vienna, Austria, Aug 1995. [http://www.igd.fhg.de/www/igd-a8/pub/EmbedLabel.ps]
[Zha4] J. Zhao, E. Koch, J. Rindfrey, “Copyright Protection for Multimedia Data”, *Proc. of the Int. Conference on Digital Media and Electronic Publishing*, pp. 203–213, London, UK, 1996.
[Zhu1] B. Zhu, M. D. Swanson, and A. Tewfik, “Transparent Robust Authentication and Distortion Measurement Technique for Images”, preprint, 1997.
[Zhu2] B. Zhu, A. Tewfik, and O. Gerek, “Low Bit Rate Near-Transparent Image Coding”, *Proc. of the SPIE Int. Conf. on Wavelet Apps. for Dual Use*, vol. 2491, pp. 173–184, Orlando, FL, 1995.

APPENDIX

Discrete Cosine Transformation

$$D(i,j)=\frac{2}{\sqrt{M\times N}}\sum_{r=1}^{M}\sum_{s=1}^{N}w_1(r)w_2(s)I(r,s)\cos\frac{\pi}{2\times M}r(2i+1)\cos\frac{\pi}{2\times N}s(2j+1),$$

where

$$w_1(r)=1/\sqrt{2}\text{ when }r=0\text{ and }w_1(r)=1\text{ otherwise}$$
$$w_2(s)=1/\sqrt{2}\text{ when }s=0\text{ and }w_2(s)=1\text{ otherwise}$$

the size of the image is $M\times N$
$I(r,s)$ denotes the image matrix of gray values, and $D(r,s)$ denotes the DCT matrix of coefficients.

Inverse Discrete Cosine Transformation

$$I(i,j)=\frac{2}{\sqrt{M\times N}}\sum_{r=1}^{M}\sum_{s=1}^{N}w_1(r)w_2(s)D(r,s)\cos\frac{\pi}{2\times M}r(2i+1)\cos\frac{\pi}{2\times N}s(2j+1),$$