Anja Keskinarkaus

DIGITAL WATERMARKING TECHNIQUES FOR PRINTED IMAGES
ANJA KESKINARKAUS

DIGITAL WATERMARKING TECHNIQUES FOR PRINTED IMAGES

Academic dissertation to be presented with the assent of the Doctoral Training Committee of Technology and Natural Sciences of the University of Oulu for public defence in Auditorium TS101, Linnanmaa, on 28 February 2013, at 12 noon

UNIVERSITY OF OULU, OULU 2012
Keskinarkaus, Anja, Digital watermarking techniques for printed images.
University of Oulu Graduate School; University of Oulu, Faculty of Technology, Department of Computer Science and Engineering, P.O. Box 4500, FI-90014 University of Oulu, Finland
Oulu, Finland

Abstract
During the last few decades, digital watermarking techniques have gained a lot of interest. Such techniques enable hiding imperceptible information to images; information which can be extracted later from those images. As a result, digital watermarking techniques have many interesting applications for example in Internet distribution. Contents such as images are today manipulated mainly in digital form; thus, traditionally, the focus of watermarking research has been the digital domain. However, a vast amount of images will still appear in some physical format such as in books, posters or labels, and there are a number of possible applications of hidden information also in image printouts. In this case, an additional level of challenge is introduced, as the watermarking technique should be robust to extraction from printed output.

In this thesis, methods are developed, where a watermarked image appears in a printout and the invisible information can be later extracted using a scanner or mobile phone camera and watermark extraction software. In these cases, the watermarking method has to be carefully designed because both the printing and capturing process cause distortions that make watermark extraction challenging. The focus of the study is on developing blind, multibit watermarking techniques, where the robustness of the algorithms is tested in an office environment, using standard office equipment. The possible effect of the background of the printed images, as well as compound attacks, are both paid particular attention to, since these are considered important in practical applications.

The main objective is thus to provide technical means to achieve high robustness and to develop watermarking methods robust to printing and scanning process. A secondary objective is to develop methods where the extraction is possible with the aid of a mobile phone camera.

The main contributions of the thesis are: (1) Methods to increase watermark extraction robustness with perceptual weighting; (2) Methods to robustly synchronize the extraction of a multibit message from a printout; (3) A method to encode a multibit message, utilizing directed periodic patterns and a method to decode the message after attacks; (4) A demonstrator of an interactive poster application and a key based robust and secure identification method from a printout.

Keywords: compression, geometric attacks, image watermarking, perceptual watermarks, print-cam, print-scan, printout, robustness, synchronization
**Tiivistelmä**


Acknowledgements

The research in this thesis work was conducted in the MediaTeam Oulu research group in the Department of Computer Science and Engineering at the University of Oulu.

I am proud to say that I have been able to work in a team, where it is easy to communicate with colleagues, as well as with the supervisor and directors. I wish to express my sincere gratitude to Professors Jaakko Sauvola and Timo Ojala, who gave a great kick start to my thesis work. Professor Jaakko Sauvola, in particular, my first supervisor, was a great source of innovation and motivation. I will also never forget the support from Professor Timo Ojala, considering both project work and other issues.

From the very beginning, Professor Tapio Seppänen has played an important part in my thesis work. He has served as a valuable source of critic, suggestions and help on algorithm level issues, and from 2006, also as a supervisor of the thesis. I am truly indebted to him and thankful for keeping the thesis work in the right track, but still allowing no shortcuts.

This dissertation would not have been possible without proper funding, of course. Professors Jaakko Sauvola, Timo Ojala and Tapio Seppänen have managed to keep the funding continuous. Over the years, several Tekes and Academy projects, with interesting industrial partners, have supported financially this thesis work.

I owe many thanks to all the team members whom I have been able to work with. Thanks to the watermarking research team with which I have been working during the years, including Marko Brockman, Timo Hirsimäki, Timo Miettinen, Juha Partala and Antti Niskanen. Special thanks to Dr. Tech Nedeljko Cvejic, Dr. Tech Mikko Löytynoja and M. Sc Anu Pramila for fruitful discussions and close co-operation.

This work is dedicated to my family. I thank my parents, sisters, brothers and other close family members for their support. Niina, Sami and Anniina, and of course, Jessiina; you are my greatest joy and source of motivation. Juha, I owe my sincere thankfulness to you for your patience and support.

Oulu, October 2012

Anja Keskinarkaus
### List of symbols and abbreviations

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Autocorrelation function of the image gradients</td>
</tr>
<tr>
<td>bg</td>
<td>Average background luminance</td>
</tr>
<tr>
<td>c</td>
<td>Correlation</td>
</tr>
<tr>
<td>f</td>
<td>Photometric distortion</td>
</tr>
<tr>
<td>f₁</td>
<td>Spatial masking effect</td>
</tr>
<tr>
<td>f₂</td>
<td>Threshold due to background luminance</td>
</tr>
<tr>
<td>g</td>
<td>Grid structure</td>
</tr>
<tr>
<td>G</td>
<td>Affine transformation</td>
</tr>
<tr>
<td>G*</td>
<td>Grid image</td>
</tr>
<tr>
<td>G₀</td>
<td>Directed grid</td>
</tr>
<tr>
<td>I</td>
<td>Cover image</td>
</tr>
<tr>
<td>Iₗₑₜ</td>
<td>Response image after print-cam attack</td>
</tr>
<tr>
<td>Iₚᵣᵉ</td>
<td>Preprocessed image</td>
</tr>
<tr>
<td>I₇</td>
<td>Watermarked image</td>
</tr>
<tr>
<td>Iₗᵳₐᵳᵣₙ</td>
<td>Wiener-filtered image</td>
</tr>
<tr>
<td>H</td>
<td>Harris corner strength measure</td>
</tr>
<tr>
<td>m</td>
<td>m-sequence</td>
</tr>
<tr>
<td>mg</td>
<td>Maximum weighted average of luminance differences</td>
</tr>
<tr>
<td>M</td>
<td>Masking function</td>
</tr>
<tr>
<td>N₀, N₁</td>
<td>Periodicity of repetitions in a periodic watermark</td>
</tr>
<tr>
<td>N</td>
<td>Standard normal distribution</td>
</tr>
<tr>
<td>r</td>
<td>Radial distortion</td>
</tr>
<tr>
<td>Rᵢ</td>
<td>Harris response in level i, where each level simulates different scale and contrast conditions</td>
</tr>
<tr>
<td>Rₓᵧ</td>
<td>Correlation</td>
</tr>
<tr>
<td>Rob</td>
<td>Robustness descriptor</td>
</tr>
<tr>
<td>t₀</td>
<td>Threshold in Harris detector</td>
</tr>
<tr>
<td>T</td>
<td>Threshold in watermark detection</td>
</tr>
<tr>
<td>W</td>
<td>Watermark</td>
</tr>
<tr>
<td>W₀</td>
<td>Directed periodic watermark pattern</td>
</tr>
<tr>
<td>W̃</td>
<td>Wiener estimate of the watermark</td>
</tr>
<tr>
<td>Wₑ</td>
<td>Neighborhood in Harris detector</td>
</tr>
<tr>
<td>x, X</td>
<td>Input signal in embedding process</td>
</tr>
<tr>
<td>y*, Y*</td>
<td>Watermarked signal in embedding process</td>
</tr>
<tr>
<td>q₀, q₁</td>
<td>Repetition number in a periodic watermark</td>
</tr>
</tbody>
</table>
Q  Quantization

α  Watermark weighting function
β  Watermark weighting function
β₁, β₂  Translation parameters
γ  Threshold in peak detection
σ  Variance
δ₁, δ₂  Parameters controlling watermark strength
λ₁, λ₂  Scaling parameters
μ  Scale factor in Helmert transform
θ  Rotation angle
η  Noise
φ  Tuning parameter in Noise Visibility Function
Π  Interpolation method
ε  Interpolation error
w  Watermark estimate

ACF  Autocorrelation Function
BER  Bit Error Rate
CIT  Circular Integration Transform
DCT  Discrete Cosine Transform
DFT  Discrete Fourier Transform
DRM  Digital Rights Management
FFT  Fast Fourier Transform
GUI  Graphical User Interface
GS  Guided Scrambling
HAS  Human Auditory System
HVS  Human Visual System
IA  image-adaptive
IDFT  Inverse Discrete Fourier Transform
IFFT  Inverse Fast Fourier Transform
ILPM  inverse log-polar mapping
IPR  Intellectual Property Rights
JND  Just Noticeable Difference
JPEG  Joint Photographic Experts Group
LPM  log-polar mapping
LSB  Least Significant Bit
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPMP</td>
<td>Intellectual Property Management and Protection</td>
</tr>
<tr>
<td>MTF</td>
<td>Modulation Transfer Function</td>
</tr>
<tr>
<td>NVF</td>
<td>Noise Visibility Function</td>
</tr>
<tr>
<td>PS</td>
<td>Print-Scan</td>
</tr>
<tr>
<td>PSPNR</td>
<td>peak-signal-to-perceptible-noise ratio</td>
</tr>
<tr>
<td>RIT</td>
<td>Radial Integration Transform</td>
</tr>
<tr>
<td>RRW</td>
<td>Robust Reference Watermarking</td>
</tr>
<tr>
<td>RSC</td>
<td>Rotation Scaling Cropping</td>
</tr>
<tr>
<td>RST</td>
<td>Rotation Scaling Translation</td>
</tr>
<tr>
<td>SDG</td>
<td>Subjective Difference Grade</td>
</tr>
<tr>
<td>SNR</td>
<td>signal-to-noise ratio</td>
</tr>
<tr>
<td>VIVA</td>
<td>Visual Identity Verification Auditor</td>
</tr>
<tr>
<td>QF</td>
<td>quality factor</td>
</tr>
<tr>
<td>2D</td>
<td>two-dimensional</td>
</tr>
</tbody>
</table>
List of original publications


# Contents

Abstract

Tiivistelmä

Acknowledgements 7

List of symbols and abbreviations 9

List of original publications 13

Contents 15

1 Introduction 17
  1.1 Background ................................................................. 17
  1.2 Research problem and objectives ........................................ 22
  1.3 Research scope and approach ............................................. 23
  1.4 Contributions and summary of original publications .............. 25

2 Literature review 29
  2.1 Robust watermarks and secure watermarks ............................ 29
  2.2 Imperceptuality and perceptual watermarks ........................... 32
  2.3 Robustness to compression attacks ..................................... 35
  2.4 Robustness to geometric attacks ....................................... 37
  2.5 Robustness to print-scan attacks ....................................... 46
  2.6 Robustness to print-cam attacks and algorithms ................. 53

3 Research contributions 61
  3.1 Methods to increase watermark extraction robustness with perceptual weighting ........................................... 61
  3.2 Methods for robust synchronization in the extraction of a multibit message from a printout ............................. 65
  3.3 A method to encode a multibit message utilizing directed periodic patterns and a method to decode the message after attacks ................................................................. 70
  3.4 Value adding application with the aid of a mobile phone camera 75
  3.5 Content identification with feature point based synchronization 79

4 Discussion 87

5 Summary 93

References 95

List of original publications 101
1 Introduction

1.1 Background

Information hiding is a collection of techniques that have been studied extensively since the first academic conference on the subject was organized in 1996 (Petitcolas et al. 1999). Information hiding can be divided into several subareas which all offer interesting challenges and opportunities in varying application areas. Techniques can be used as well for the purposes of protecting digital content, content identification, traitor tracing or system enhancement, to give only a few examples. Most often, the techniques are applied in the context in which the content stays in digital format. However, an interesting subarea of research is context, in which the watermarked content has a physical format, such as a book or a label. Many interesting print media applications from mobile marketing to legitimate product authentication can be envisioned (Hirakawa & Iijima 2009).

Digital watermarking is an information hiding technique, the early definition of which is “the practice of imperceptibly altering a Work to embed a message about that Work” (Cox et al. 2002a). Additional data is embedded in digital media in a sense that it is perceptually undetectable, tightly coupled to the cover media and furthermore the hidden data can be detected or recovered after a set of manipulations (Swanson et al. 1998). This resistance of watermarking to manipulations, commonly called robustness, is an important performance measure of a watermarking algorithm.

The basic watermarking principle is shown in Fig. 1. The figure shows that depending on the application the watermarking system may be secured with a key. Also the detection/recovery may be accomplished without the cover signal (blind detection) or with the help of the original cover signal (nonblind). Moreover, many of the watermark detection methods rely on measuring similarity between the original watermark and the embedded watermark.

As a driving force for development of watermarking technology has been its potentiality in preventing piracy of digital works. Consequently, watermarking has been widely studied as a component of DRM (Digital Rights Management) systems. A daydream of a watermarker and content owner is a robust copyright mark that would protect IPR (Intellectual Property Rights). Copying of digital material like images, music and movies is easy and the copies are identical
compared with the original data. The copied data does not lose its quality no matter how many copies are taken. Also communication channels like the Internet has made the unauthorized copying, reading, manipulation, and delivering of digital information far too easy. It is commonly noticed that the previous methods for solving IPR issues are not satisfactory anymore, but new techniques must be researched instead. (Hartung & Kutter 1999).

![Watermarking principle](image)

**Fig. 1. Watermarking principle.**

Watermarking has been extensively studied as a means for providing at least a partial solution for the copyright protection problem, with applications on copy/access control, owner identification, proof of ownership and traitor tracing. Extensive studies of the methodology have been done for example by Bender *et al.* (1996) and Swanson *et al.* (1998). When a copyright message is inserted as a watermark, it is not perceptible and cannot be removed easily. Even after data manipulations, the watermark should be usable for copy prevention, for identifying the owner of the rights or for revealing the leakage point of pirated copies in a distribution chain.

The complexity of the problem of copyright protection has however ensured that also other potential watermarking applications have been widely studied. Below is taken a short look into the variety of application opportunities from traditional watermarking to print media applications enabled by watermarking technology.
Owner identification and proving ownership

The embedding of an owner identification mark using watermarking technology is fairly straightforward and has also resulted in commercial implementations. One example is the Digimarc software which exists also as a plug-in component in Paintshop Pro (Perry et al. 2002). The purpose of this software is the insertion of owner identification codes into digitally produced images. The embedded watermark has also the potential to be used not only for identification of the owner but also for actually proving the ownership. This, however, is not a simple problem as the availability of a public detector can be used for attempts to remove the original watermark and then it is easy to insert another one as a replacement (Cox et al. 2002a).

Transaction tracking (Traitor tracing, Fingerprinting)

In owner identification, the embedded watermark is the same in all copies of the content. In fingerprinting, an individual watermark is embedded in every copy sent to the customer. Consequently, it can be used for identifying individual customers. Using this method the source of illegal copying or distribution can be tracked. (Cox et al. 2000). A practical example of a system where watermarking as a method to create an audit trails has been extensively studied is MPEG IPMP (Intellectual Property Management and Protection) (Lacy et al. 1998).

Broadcast monitoring

Information hiding techniques offer also new means for broadcast monitoring systems. Cox et al. (2002a) consider different types of monitoring systems and point out the main difficulties in the past solutions. Passive monitoring based on comparison of the received data on databases being the main difficulty. With watermarking, active monitoring, where comparison is not needed, is possible. Watermarking methods can be used in strengthening the active approach by adding the identification information inside the content so that it is not lost during the transmission due to format changes, and thus, the verification of the usage of the broadcasted material will be more reliable. One example of the earliest comprehensive efforts done on this area was VIVA (Visual Identity Verification Auditor) project in which the aim was to build up a technical solution and
demonstration/testing environment for a very large scale professional broadcast system utilizing watermarking techniques (Depovere et al. 1999).

Content authentication, integrity checking, content identification

Cryptographic techniques have been traditionally used for authentication of digital data by creating a digital signature of the content. This signature can, however, be lost for example due to format transformations. Digital watermarking methods have been introduced to strengthen the weaknesses in content authentication techniques (Cox et al. 2002a). Robustness requirements vary depending on the application (Podilchuk & Delp 1999) and consequently watermarking methods with varying properties have been proposed. Fragile watermarks are suitable when even slight modifications must be detected. In this case, mere lack of presence of a digital watermark can immediately indicate tampering and likely counterfeiting.

However, in many applications the watermark information should be robust to some well-defined set of attacks, such as compression. Usually, such semi-fragile watermarking methods are used to detect manipulations of the objects in a scene, and not directly on checking the integrity of the content (Cox et al. 2002a). In security community, an integrity service is used to determine whether the examined data is exactly identical to the original (Rey & Dugeley 2002). Watermarking community, in its turn, considers malicious versus non-malicious manipulations of data. Watermarking itself makes modifications to the original data. Accordingly, in some applications, like medical applications there is a requirement for reversibility; after content authentication, the watermark should be removable.

Content identification refers to applications, where the watermark can uniquely identify each specific item or instance of content and carry information on the item, routing of shipments or intended destinations. Watermarks can be encrypted and secured so that only authorized reading devices can detect and access the data.

System enhancement, device control, value adding

Additionally to the previous methods, which commonly are classified to watermarking applications, information hiding can also be used to device control, adding captions or some other auxiliary information. Muharemagic & Furht (2006)
refer to such applications as digital watermarking for system enhancement. The non-security nature is usually the main distinguishing factor compared with traditional watermarking applications. Usually, in such application examples, the cover signal carries information that is beneficial to the user. For audio data, Phillips (van der Veen et al. 2001) has demonstrated an application where watermark is used for identifying a song from music played. Löytynoja et al. (2008) proposed an application, where a user can record the music with a mobile phone from radio loudspeakers. The extracted watermark can contain value adding metadata about the song or a link to an external server.

*Applications of watermarking in print media*

Image watermarking applications, where the watermarked images appear in a printed format and provide a portal from printed media to the Internet (Alattar 2000), have gained more interest. In these applications, no adversary is expected, and accordingly, intentional attempts to remove the watermark need not to be considered (Cox & Miller 2002b).

The huge opportunity has been recognized by companies like Digimarc, which is the leading company on development and patenting of watermarking technology. Digimarc were the first to put the idea of linking watermarked printed images to digital world into practice. In software called MediaBridge, the watermark detection is accomplished in PC with the aid of a web camera (Alattar 2000, Perry et al. 2002).

The applications for printed materials are not restricted to system enhancement, with no adversary. The payload of watermark can have various objectives, also in a sense of traditional watermarking. Now, however, the context is different, a watermarked image can be in a published book, in a product label, a newspaper, a magazine or in a catalogue. An example is a security-printing application where watermarking is used for authentication (Ho et al. 2003). A photo in an identification card has hidden information, which will be destroyed by photo substitution or other manipulation. Consequently, watermark can be used to verify the authenticity of the card.
1.2 Research problem and objectives

Challenges for watermarking in print media applications

In their article, Cox & Miller (2002b) pick up some milestones in digital watermarking research. First years were heuristic and various algorithm proposals were introduced as understanding of the issue increased. Significant development was the introduction of the so-called perceptual watermarks and spread spectrum techniques. Late 1990s was the startup of the research on tackling with compression and geometrical attacks. Steady progress has been made in these areas, but still, geometrical attacks, in particular, remain challenging. Geometrical attacks cause synchronization errors in watermark detection/extraction. A synchronization error has a drastic effect on watermark detection/extraction reliability (Zheng et al. 2007).

In order to realize print media applications, the watermarking method should be robust to extraction from printed output. After printing process, the watermarked image is in analog format and in order to be able to extract the watermark, the analog data have to be digitized. In print-scan process, the device making the capturing process is a scanner, whereas in print-cam process, it is a mobile phone camera. Both the printing process and capturing process cause distortions that make watermark extraction challenging. There is a combination of attacks involved, including geometrical attacks and distortions caused by devices. Some of the distortions are of low-pass type, like the pixel value distortion caused by printing, and compression in storing images in mobile phones. Although some progress has been made, the work is still in its infancy. Various issues make the watermark interpretation hard, especially in practical applications.

The research problem of this thesis is: How to realize watermarking method that is robust to synchronization error in printed image applications? In the thesis, especially the following sub-problems are considered:

1. What kind of methods can be used to ensure robust watermarking against low-pass type attacks, and especially, robust extraction from a printout?
2. How to ensure robustness of the synchronization?
3. How to embed a multibit watermark robust to extraction from printout?
4. How to meet application specific demands; robust and secure identification with a scanner/secondly value adding application with the aid of a mobile phone camera?
Thus far, the main watermarking research is almost entirely focused on digital format and the possibilities on applying techniques to applications where data is no longer digital are still quite unexplored. In this thesis, the main objective is to provide technical means to achieve high robustness and to develop watermarking methods robust to printing and scanning process. A secondary objective is to develop methods where the extraction is possible with the aid of a mobile phone camera. The focus is on developing blind watermarking methods, where the original image is not needed for watermark extraction.

1.3 Research scope and approach

There is always a trade-off between capacity, imperceptuality, and robustness in a watermarking scheme. This trade-off is usually visualized with a “magic triangle” (Fridrich 1999), as illustrated in Fig. 2. In this thesis, the main emphasis is on robustness to print and capture process. The focus is on full color images, binary or few-color images are not considered. The performance of the developed image watermarking methods is evaluated against print-scan and print-cam attack. Also a print-scan/print-cam attack combined with additional attacks is considered both in methods and tests. Both processes cause distortions to the watermarked image, which are inherent to the process and as such considered as unintentional attacks. In a real application, the watermarked image seldom exists orphan in a printout, so background variations are also considered. These are issues that have got minimal attention in the watermarking literature. The concentration is in multibit watermarking, and the capacity is measured against attacks. To attain imperceptuality, JND (Just Noticeable Difference) models are used and the quality of the watermarked images is measured either with objective or subjective measures.
The framework for the experimental system is illustrated in Fig. 3. Any inside mechanisms, like halftoning in printers, are considered as attacks. The experiments are conducted in an office environment, using standard office equipment. Two possible application scenarios are explored:

1. Content identification: The robustness of an identification code embedded in an image is examined from the printed media. A predefined watermark is readable with a corresponding secret key. In addition to robustness, invisibility and capacity, the security issue is considered as well. Only an authorized reader can detect and access the data.

2. Value adding service for carrying information in a printed image and using a mobile phone to extract the information: Here, the watermark acts like a barcode, which is hidden into the image. In the demonstration application, the extracted watermark links the user to a webpage, where various value adding services can reside. The performance is evaluated with robustness tests. User tests; subjective quality evaluation, reliability and feasibility are realized in small scale.

In both cases, unintentional attacks are considered, attacks that happen during the layout processing, or print-scan or print-capture process. In the content identification case, the focus is on identifying the images published in the print format, consequently, digital malicious manipulations are not considered. In value
adding, the malicious attacks are not expected, as the watermark information is beneficial to the user.

Fig. 3. Framework for the experimental system.

In this thesis, the constructive work approach is taken. Relevant techniques are taken advantage of when progressing towards the two defined application scenarios.

1.4 Contributions and summary of original publications

The following is the summary of research contributions in this thesis:

1. Methods to increase watermark extraction robustness with perceptual weighting.
2. Methods to robustly synchronize the extraction of a multibit message from a printout.
3. A method to encode a multibit message utilizing directed periodic patterns and a method to decode the message after attacks.
4. A demonstrator of an interactive poster application and a key based robust and secure identification method from printout.

Paper I presents a spatial spread spectrum method with perceptual shaping. Spatial watermarking is not inherently robust to low-pass type attacks like compression. In the paper, it is shown that with the proposed pixel by pixel calculated strength factor also spatial watermarking can be made robust to compression. For spreading, two-level spreading is used. M-sequences are used for spreading and correlation based watermark extraction is enhanced utilizing prefiltering. The author was responsible for algorithm design and development. The expertise of Dr. Cvejic on m-sequences was taken advantage of in the design. Testing was conducted with the aid of Mr. Niskanen. Prof. Seppänen and Prof. Sauvola supervised and participated in the finalization of the manuscript of the work.

Paper II introduces a method robust to print-scan and JPEG (Joint Photographic Experts Group) compression attack. The multilevel approach is taken, where a spatial watermark carries a reference watermark and the multibit message is embedded in wavelet domain. In the paper, the perceptual shaping as developed in Paper I is taken advantage of to embed the spatial reference watermark. In the extraction, methods to improve the estimation of affine parameters are proposed. Also, the effect of different parameters on the performance is evaluated. The author was responsible for algorithm design, development and testing. Ms. Pramila contributed to the introduction of the paper and Prof. Seppänen and Prof. Sauvola supervised and participated in the finalization of the manuscript.

In Paper III, a method robust to print-scan and compound attacks is presented. Methods developed in the previous papers are exploited and a method to encode the message using directed periodic patterns is presented. The proposed method provides a blind message extraction method, where autocorrelation function, filtering, masking and adaptive line search with Hough transform is taken advantage of and the message is interpreted from the estimated peak orientation. Both embedding and extraction are adaptive, with no need to change parameters settings for different images. It is shown that background variation, or a change of printer/print material (two printers, two materials) has no significant effect on the performance of the method. The author was responsible for the design, implementation and testing of the algorithm. Ms. Pramila participated in the
literature review of reference techniques. Prof. Seppänen supervised and participated in the finalization of the manuscript.

Paper IV presents a print-cam resilient watermarking method, with an application example of an interactive poster. The method in Paper III was modified to attain resiliency to the strong signal deterioration due to air interface, mobile phone camera properties and human interaction. The algorithm design, implementation and testing were done together with Ms. Pramila. Subtractive-additive embedding designed by the author, perceptual adaptation modified from the author’s previous work by Ms. Pramila were used in order to attain robustness against camera-based extraction. In the extraction, the processed autocorrelation reveals the two-level coded message hidden with periodic patterns. The tests include both incremental change on tilt and distance to find performance limits, where author’s main interest and contribution was on the combined effect of perspective distortions on geometry with accompanied pixel value distortions. The main interest of Ms. Pramila was in the effect of camera properties, as well as in implementation issues. Also performance tests with real users were conducted. Prof. Seppänen supervised and participated in the finalization of the manuscript.

Paper V presents a method robust to print-scan attack and a set of compound attacks. For synchronization purposes, the location of the watermark is tied to a coordinate system defined by robust feature points. A measure describing the robustness of the feature points is described. In detection, the interplay between feature extraction and watermarking ensures reliability. The message sequence is mapped to the directional angle of periodic patterns, where methods developed in the previous papers (III, IV) are taken advantage of. For security, the watermark information is embedded in triangles in permuted locations. Accordingly, in decoding, a key is needed to recompose the triangles for message extraction. The author was responsible for the design, implementation and testing of the algorithm. Ms. Pramila contributed to the introduction of the paper. Prof. Seppänen supervised and participated in the finalization of the manuscript.
2 Literature review

This chapter provides an overview to the literature related to the research topic. In Section 2.1, some general watermarking terminology is explained to relate the thesis work focus area to a wider concept. The next sections give a literature review of the research work concentrating on the focus area.

2.1 Robust watermarks and secure watermarks

An important performance measure of the watermarking algorithms is robustness. Methods that try to remove the watermark or to destroy the value of it are commonly called attacks. Some of these attacks are very media specific, such as frame dropping and frame averaging for video, and others are common to more than one media type. Some are very simple (addition of noise, non-linear filtering, etc.) and other more sophisticated (mosaic) or combinations of several different attacks (Stirmark, Unzign). As Wu et al. (2001) state, an attack on the watermarking system is successful if the original goal of embedding watermarks cannot be achieved.

Attacks can be classified to different categories. Kutter et al. (2000) propose a classification to four different attack types. Removal attacks are attempts to remove the watermark completely from the cover data and, in contrast, geometrical attacks are attempts to distort the watermarked data so that it cannot be detected reliably. Cryptographic attacks are brute force methods for finding a secret, and protocol attacks are meant for confusing the application specific purpose.

Hartung et al. (1999) propose another classification scheme, with four different types of attacks. By simple attacks, the watermarked data is manipulated as an entity of watermark and the host data and they attempt to impair the embedded watermark by manipulations. There is no attempt to isolate or identify the watermark. Detection-disabling attacks most commonly affect so that the detection part loses synchronization and ambiguity attacks make fakes of original data or the watermarked data. The fourth class of attacks is removal attacks that are attempts to isolate the watermark and discard it.

Cox et al. (2002a) make a distinction between robust and secure watermarks. A secure watermark is robust, but also secure in a sense that it can resist intentional tampering. A robust watermark, in its turn, is designed to be resilient
against legitimate and everyday usage of the content. This two level distinction is the most suitable categorization in this thesis.

To attain the robustness to print and capture process, the watermarking method has to be robust to a variety of attacks. In the developed non-secure application, the robustness of the watermarking is a sufficient condition. In the content identification application, robustness is also the main issue. Security considerations are restricted to an unauthorized attempt to detect and access the hidden data.

Several actions can be taken to make the watermarks more robust. It was an early observation that perceptually significant components carry the watermark data most reliably (Cox et al. 1997). The authors suggested spread spectrum techniques as a method to modify a perceptually significant component of the frequency spectrum. A pseudorandom sequence is used to spread a narrowband signal into a wider bandwidth. Accordingly, the watermark is spread in very many frequency bins so that the energy in any one bin is very small and certainly undetectable (Cox et al. 1997).

In the original paper presenting the spread spectrum idea, the detection is non-blind and based upon the knowledge of watermarked locations. In non-blind methods, the original image is available in detection. The knowledge of the original is advantageous in a sense that many of the manipulations the watermarked image has gone through can be at least approximately inverted. Respectively, methods that do not use original cover are called blind methods.

Hanjalic (2000) describes the pixel domain watermarking process by

\[ I_w(x, y) = I(x, y) + k \cdot W(x, y) \]

where a pseudorandom pattern \( W(x, y) \) is added to cover image \( I(x, y) \) to produce the watermarked image \( I_w(x, y) \). The watermark information is spread over the whole image area. The strength of watermark and accordingly imperceptuality versus robustness can be controlled with the small gain factor \( k \). Watermark detection process involves the calculation of correlation \( R_{xy} \) between the possibly distorted watermarked image \( I_w(x, y) \) and the embedded watermark \( W(x, y) \). With a correctly chosen threshold \( T \), the existence of the watermark can be determined

\[ R_{I_w(x, y)W(x, y)} > T \rightarrow \text{watermark detected.} \]
\[ R_{I_w(x, y)W(x, y)} < T \rightarrow \text{watermark not detected.} \]
Spreading is one way of adding controlled redundancy. Another simple way to make the watermarking more robust to processing is adding the same watermark several times. In detection, it is then possible to make a decision of the existence of a watermark based on several observations. The image can be divided into sub-images, where a watermark is repeated and detection can include both local and finally a global decision on the watermark.

The straightforward extension of the previous to multibit watermarking is to increase the payload dividing the image into sub-images, and embed a string of watermark bits \( b_0b_1…b_{l-1} \) sequentially in the sub-images. One commonly used method to represent bits \((0,1)\) in watermarking is to either add or subtract the pattern accordingly. In detection, the bits can be distinguished similarly with correlation and by applying threshold based decision. (Hanjalic 2000).

Another one of the early observations was that a constant strength watermark is not optimal in the sense of robustness and imperceptibility. In frequency domain, the weight of the watermark in coefficient can be tuned according to the principles of HVS (Human Visual System) (Cox et al. 1997, Podilchuk 1998). In pixel domain, equation (1), this refers to parameter \( k \). Suggestions to use perceptual watermarks emerged, where the choice of transform domain plays an important part (Podilchuk 1998, Wolfgang et al. 1999).

In designing a watermarking algorithm, the requirements of the particular application are very important. A priori knowledge of the types of the attacks that the watermarked media will undergo can be taken advantage of. In order to realize print media applications, the watermarking method should be robust to extraction from printed output. Both the printing process and capturing process cause distortions that make watermark extraction challenging. There is a combination of attacks involved, including valumetric distortions and geometrical attacks.

The literature covering watermark embedding and detection/multibit extraction from a printout is quite narrow. However, similar problems, although not simultaneously applied, have been researched for some time. The effect of compression and other low-pass type attacks on watermarking has been widely studied. Also, progress to obtain watermark robustness against geometrical attacks has been made. Obviously, these research results serve as a background and a starting point, also to the development of print-scan and print-cam resilient algorithms.
2.2 Imperceptuality and perceptual watermarks

Cox et al. (2002a) point out two types of measures for evaluating perceptual impact of watermarks: fidelity and quality. Fidelity is the measure for similarity between the original content and the processed content. Quality, in its turn, is how the observer sees or hears the particular content. Thus, for example, the video of a surveillance camera usually is not very appealing and so has a low quality, but a watermarked version of the same content may be similar to the original and thus has a high fidelity (Cox et al. 2002a). Whether the metric is either fidelity or quality, the usual requirement for all watermarking schemes is that when embedding information in another signal, the distortions generated by this hidden information must basically be such that they cannot be heard or seen. The actual imperceptibility criteria can largely depend on functionality of the algorithm (data hiding, image authentication, robust watermarking, fingerprinting, copyright marking) and on the value of the content to be watermarked. (De Vleeschouwer et al. 2002)

Whether the perceptibility is in the context of measuring fidelity of a watermarking (Cox et al. 2002a) or designing a watermarking scheme (De Vleeschouwer et al. 2002) the models for HVS (Human Visual System) and HAS (Human Auditory System) have a central role. Various techniques for adaptation have been adopted from previous research, developed compression schemes, for instance, and successfully utilized in conjunction with watermarking. The complete understanding of human perceptual system is out of the scope of this thesis and so in here only some basic properties referred to in the watermarking literature and their usage in watermarking are presented. The usability of different models for the perceptual system requires application specific considerations as in some cases a simple model is more suitable and in other cases usage of a more complex one is justified. For example, the computational complexity of the algorithm might be restricted and therefore full exploitation of all the aspects of visual modeling would not always be rational (De Vleeschouwer et al. 2002).

Human Visual System is a complex system and although well studied, it has still properties that remain partly as a mystery to scientists. As stated in (De Vleeschouwer et al. 2002), a complete model simulating HVS should also integrate, in addition to modeling encoding and representation stages, some form of interpretation, which is the highest level of human vision and is very complex. However, there are some basic properties that are quite well understood. One of them is frequency sensitivity, which has been widely used in perceptual models.
for image coding, as well as for perceptual models for watermarking. Frequency sensitivity is a property of the human eye that depends only on viewing conditions and can be described by MTF (Modulation Transfer Function), which measures the human eye’s sensitivity on sine wave gratings at various frequencies. Using a fixed condition of viewing, image-independent thresholds can be determined for each frequency band, according to which the change or distortion is not noticeable (Wolfgang et al. 1999).

Another property of the human eye that is well understood is luminance sensitivity, which measures the detectability of noise on a constant background and depends on the average background luminance, as well as the luminance level of the signal. (Wolfgang et al. 1999). Visibility of the noise is larger in dark areas than in light ones, as indicated by Weber-Fechner law (De Vleeschouwer et al. 2002).

Additionally to these basic properties, which give a starting point to utilizing imperfections in human visual system, an important concept in vision modeling is masking, which models the response of the visual system to the combination of different signals. When combined with the frequency sensitivity and luminance sensitivity, more effective exploitation of human visual system is possible. Different kinds of masking phenomena are involved in human vision. Spatial masking refers to the situation where the decrease in the spatial uniformity of the background luminance reduces the visibility of stimuli (Chou & Li 1995). Thus, edges can mask signals out and contrast masking describes the detectability of the signal in the presence of another one (Wolfgang et al. 1999).

Usually, when talking about perceptuality, the metrics used is JND (Just Noticeable Difference), which is a threshold for perceivable distortion. There exist differences in perceiving the distortion (golden eyes, golden ears) and so by the definition 50% of observers would not sense the distortion measured by 1 JND (Cox et al. 2002a). The formulation of calculation for JND has as many possibilities as there exists variations in modelling the perceptual system and therefore range from very simple ones (Lie & Chang 1999) to utilizing only one feature to utilizing several of the previously mentioned features (Suthaharan et al. 1999). In advanced models, the JND-threshold consists of image-independent part based on frequency sensitivity and image-dependent part based on luminance sensitivity and contrast masking.

The utilization of the models can be done on spatial domain or in some transform domain. Wolfgang et al. (1999) present image-adaptive watermarking algorithms both in DCT (Discrete Cosine Transform) and wavelet-domain. In
their approach, the adaptation to the human visual system is based on the visual model for image compression originally introduced by Watson (1993), in which the quantization matrix in the compression scheme is based on the properties of the human eye and is image adaptive. Utilizing the luminance and contrast masking properties, a JND profile is calculated, which gives the estimate of how much the coefficient can be perturbed without the distortion becoming annoying.

Voloshynovskiy et al. (1999) determine a coordinate domain (spatial domain) content adaptive watermarking method based on stochastic modeling of the cover image. The image regions of interest are considered to have different local features and the watermark estimation is considered as to be equivalent to image denoising. In addition to theoretical analysis, a fast method to utilize the theory in practice is presented. The rule of embedding is proposed to be based on

$$y' = x + \left(1 - NVF\right) \cdot w \cdot \delta_2 + NVF \cdot w \cdot \delta_1, \quad (3)$$

where NVF (Noise Visibility Function) is calculated through

$$NVF(i, j) = \frac{1}{1 + \varphi \sigma_i^2(i, j)} \quad (4)$$

and \(\varphi\) is a tuning parameter, \(w\) is the watermark and \(\sigma_i^2\) is image variance. \(\delta_1\) and \(\delta_2\) control the watermark strength. According to the adaptive rule, the watermark is embedded more strongly in texture. The method does not take into account luminance sensitivity and consequently NVF in flat regions approaches zero. The second summation term in embedding rule ensures robustness also in flat regions.

The advantages of perceptual weighting in watermarking are unarguable. However, using them is not trivial. In multilevel watermarking, where multiple watermarks are embedded in the same cover signal, the problem is sharing the available JND. It may be especially difficult in techniques where multiple transform domains are used. Watermarking, accompanied with a separate synchronization signal, so-called template watermark (discussed in Section 2.4), is one practical example, introducing such problems. The second watermark will be embedded in an image, which has already been doctored with another watermark. The resulting image should however still remain visually pleasing. Also, not every transform domain has an explicitly defined perceptual model suitable for watermarking purposes, which may compromise the choice of transform.
2.3 Robustness to compression attacks

Definitely, one of the most commonly explored properties in the watermarking literature is how the developed algorithms can cope with compression attacks. Compression is one of the attacks that can be classified to so-called unintentional or incidental attacks (Sequeira & Kundur 2001) and is a processing which is involved during the multimedia delivery or storage and not necessarily an attempt to intentionally remove the watermark. As an example of this is usage of compression in Internet transmission and storage of multimedia.

There exists a duality between compression and watermarking. This is because with perceptual coding, used in lossy compression schemes, the main aim is to remove all the irrelevant and redundant information from the signal. The objective for watermarking is, as a matter of fact, quite the opposite, namely, to use the irrelevant information to mask the presence of the hidden data. (Kundur 2000). Luckily enough, compression schemes currently available do not take full advantage of all irrelevancy and redundance available and thus watermarking is possible. As Ramkumar & Akansu (1999) explain, there are holes in compression schemes and data hiding methods utilize these holes to embed additional bits.

In her paper, Podilchuk (1998) proved that usage of HVS models is of advantage to obtain robustness to JPEG compression. Watermarks consist essentially of low power, high frequency noise. Since JPEG allocates fewer bits to the higher frequency components, such watermarks can easily be distorted. Furthermore, these watermarks can also be affected severely by other low-pass type operations. The perceptual watermarks tend to shift the energy of the watermark pattern to the lower frequencies, making them more robust.

Another aspect studied in relation to resistance of watermarking schemes against compression is the choice of watermarking domain. Wolfgang et al. (1998) run a set of experimental tests on color images using two types of IA (image-adaptive) watermarking domains (wavelet and DCT domain) and two types of compression algorithms (wavelet domain) to find out whether it is preferable to use the same domains for watermarking and compression. Watermarking was realized utilizing spread spectrum techniques (Cox et al. 1997). The authors came to a conclusion that at low data rates it is beneficial to match the two transform domains and at high data rates matching is not so critical.

Kundur & Hatzinakos (1999), however, criticized the conclusions and through analysis of their RRW (Robust Reference Watermarking) approach derived quite opposite conclusions. It was stated that, additionally to increasing
robustness by embedding high energy watermark, the robustness can also be increased by mismatching the two transformation domains. In further studies (Fei et al. 2001), the authors derive a quantization attack model and estimate capacity of the watermarking channel. In the case of repetition codes, the mismatching of the domains proves to give better results. Analysis was restricted to spread spectrum watermarking techniques.

No precise conclusions can be drawn as to whether matching the compression and watermarking domain or mismatch gives better robustness. The results may also be quite unpredictable (Jellinek & Uhl 2001). Obviously, the insertion strategy, as well as intelligence in adaptation to HVS, has an impact on the results. As an example, in Fei et al. (2001), the methods explored are restricted to spread spectrum watermarking with fixed visual thresholds. Thus, studies are not general in nature.

In a set of applications, it is preferable to use directly encoder structure for implementing an embedding algorithm. Most often, this is done by modifying the quantized DCT coefficients. The advantage is that in the implementation there is only one module needed for compression and watermarking (Kundur & Hatzinakos 1999), which is efficient in the sense of complexity. Additionally to knowledge for the encoder structure, the known properties of compression can also be utilized in designing optimal embedding schemes. For example, Sencar et al. (2002) propose a method where quantization characteristics are used for modifying embedder and show that watermark payload can be increased provided that the “watermarker” is at the controls of both watermarking and compression processes.

In this thesis work, however, it is assumed that the compression is done after the watermarking process. Compression is considered as a noise adding part in the channel. Generally, it is assumed that the compression ratios are such that image quality is good enough. As an example in print-cam, compression is an inevitable property of mobile phone software for storing the images.

Typically, there are many different valometric distortions (compression, low-pass filtering, amplitude distortion) affecting in the robustness of the extraction of watermark from printouts. The distortions do not treat all the frequencies evenly. The distortions may even change during time, or every distinct scanned printout of the same cover may reveal a slightly different result. The problems in analyzing the distortions are more thoroughly discussed in Section 2.5. Nevertheless, adding redundancy, choice of transform and perceptual watermarking play an important role in recovering watermark after the distortions.
2.4 Robustness to geometric attacks

Among the most challenging issues in watermarking are geometrical attacks, in which the attack desynchronizes the detection or extraction of the multibit message causing a total failure or partial distortion of the information. In a watermarking method for printouts, there is an unavoidable geometrical attack involved. This section covers the watermarking literature discussing the issue of synchronization. This serves as a necessary background, although both print-scan and print-cam as such are more complex problems.

Many methods have been suggested to improve digital watermarking methods under RST attacks. In RST (Rotation Scaling Translation) attack, a more general geometrical attack has been restricted to local or global transform, where transformation can be described with scaling \( (\lambda_1, \lambda_2) \), rotation \( (\theta) \) and translation \( (\beta_1, \beta_2) \) parameters:

\[
\begin{bmatrix}
\lambda_1 \\
\lambda_2 \\
\end{bmatrix}
\begin{bmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta \\
\end{bmatrix}
\begin{bmatrix}
t_1 \\
t_2 \\
\end{bmatrix}
+ 
\begin{bmatrix}
\beta_1 \\
\beta_2 \\
\end{bmatrix}.
\]

Zheng et al. (2007) classify the existing techniques to invariant domain-based, radon transform-based, template-based, salient feature-based, image-decomposition based and stochastic-analysis-based algorithms. Here, we use a slight modification of this classification to provide an overview of the methods. It is noted that many methods combine techniques. An explanation of an exhaustive search is included. It is commonly used in the proposed methods as a last step to ensure robustness. Mainly, the expressed techniques are blind methods. For non-blind methods, also image registration techniques can be utilized. When the original image is available, the geometric distortions can be estimated and inverted prior to watermark detection/extraction.

**Exhaustive search**

In an exhaustive search method, prior to watermark detection, an inverting transform is applied to the image. The process is repeated with varying the parameters of the inverting transform while the watermark is detected. In the simple case of the detector receiving a cyclically shifted sequence \( (r) \), the process is about repeating the correlation \( (c) \) calculations to every shifted version of the received sequence.
where \( w \) is the watermark, \( w = \{ w_0, ..., w_{n-1} \} \) and \( n \) is the length of the watermark signal. A watermark exists if the \( c_{wr}(l) \) exceed a threshold \( T \) for at least one \( l \) (Barni 2005). 

In a more general case of RST, applying exhaustive search would mean finding an estimate transform \( G^{-1} \) to affine transformation \( G \) which enables watermark detection. Consequently, the search base is large, and the computational complexity increases. Additionally, the amount of false positives will increase (Lichtenauer et al. 2003). In practice, the search base is restricted by some means. The constraints may be determined by the application, for example by quality requirements. Also, the search can be limited to one transform, like translation. One of the earliest examples is a method introduced by Kutter (1998). Rotation and scaling parameters are found prior to exhaustive translation search. Kutter uses two bits of the signature as a fixed and known pattern and the existence of the pattern is examined prior to a watermark can be detected.

**RST invariant domain**

O’Ruanaidh & Pun (1998) were the first to introduce the idea of transform-based invariants to gain invariance to RST attacks. A well-known property of the Fourier representation is that the DFT (Discrete Fourier Transform) amplitude is not affected of spatial shifts (translation). Also, a change to the log-polar coordinate system relates point \((x, y)\) with point \((\rho, \theta)\) by

\[
\begin{aligned}
\rho &= \log \sqrt{x^2 + y^2} \\
\theta &= \arctan \frac{y}{x}
\end{aligned}
\]

in which \( \rho \) and \( \theta \) are usually calculated in reference to origin and x-axis, respectively. This kind of change of the coordinate system converts scaling and rotation operations to simple translation, provided that scaling is isotropic. By combining Fourier transform property and log-polar mapping (LPM), in other words, taking Fourier transform of a log-polar map, a RS invariant can be derived. The operation is equivalent to calculating modulus of Fourier-Mellin transform. For RST invariance, the Fourier-Mellin transform has to be preceded by an additional Fourier transform.
A straightforward way to realize the watermark embedding would apply FFT-LPM-FFT, then, embed, followed by inversion of the processes by IFFT-ILPM-IFFT. However, both LPM and ILPM (inverse log-polar mapping) cause image quality distortion through interpolation processes involved. Additionally, there exist no human visual models for adjusting the strength of the watermark in the defined invariant domain. Also, computation of the modulus of the Fourier-Mellin transform of a Fourier transform is problematic (O’Ruanaidh & Pun 1998).

Several proposals have followed, to conquer the implementation difficulties and image quality impairment, in the otherwise so novel idea. O’Ruanaidh & Pun (1998) suggested an alternative of implementation, where only the watermark goes through ILPM. Also other methods have followed, where usually the proposed method involves log-polar mapping, but as a whole, some semi-invariant domain (not truly RST-invariant) is used. The leftover problems are resolved with additional means. In Zheng et al. (2003), the watermark is embedded in LPM domain, an approximate IPLM is used to eliminate the imprecision caused by IPLM. The actual watermarks are embedded in the Fourier magnitude of the original image. As the LPM is not followed by Fourier transform, the translation is the leftover problem. To resolve it, non-blind detection with phase correlation is suggested.

In Liu and Zhao (2004), the researchers take advantage of the properties of the LPM transform and suggest a rectification scheme to determine RST-parameters prior to watermark extraction. A piece of image is taken, LPM is applied on DFT coefficients and used as a template, which is available in the extraction process. When the actual watermark is embedded in Fourier domain, the information provided by template, rotation and scaling parameters is enough for synchronized extraction of the watermark. A spatial domain watermark would require an additional template, to determine spatial shifts. The method is not totally blind, as the extractor needs a template, computed from the original image. However, the information needed is less than in non-blind detection.

Methods based on the projection of the transform space

Lin et al. (2001) state that it is advantageous to represent the watermark as a one-dimensional projection of the image space. The main advantages are computation savings because of the change of 2-D space to one dimension. This type of watermarking methods can be seen as a special case of Radon transformation. In the proposed method, the authors transform the image first by log-polar mapping
of the Fourier magnitudes. Change to one-dimension is realized by summing the result along the log-radius axis. Accordingly, the result is translation and scaling invariant and rotation is handled through exhaustive search. Due to log-polar mapping, similar problems as in the previous methods are involved in the inversion process. The authors have resolved the problem with an iterative method.

Simitopoulos et al. (2003) propose another technique based on one-dimensional projections. RIT (Radial Integration Transform) is used to provide resistance to rotation attacks and CIT (Circular Integration Transform) for resistance against scaling attacks. Origin of transformation, which is performed over the whole image, is determined by a modified Harris corner detection method. Detection may need to be repeated over more than one corner point, where maximum of the correlation is the final detection result. The watermark locates in the same selected robust feature point as an origin. From the distorted (geometrically transformed) image, the detection algorithm calculates characteristic values, based on which rotation and scaling parameters can be calculated and are used to synchronize watermark detection.

**Templates**

In template based approaches, a special template watermark is used to detect transformations undergone by a watermarked image. In Kutter (1998), the template was a 2 bit-pattern used for translation search. Mostly templates are however two dimensional, and as such more suitable for images. The idea is that the template undergoes the same distortions than the watermark. The template has special properties for detecting those distortions.

Pereira & Pun (1999) proposed an algorithm to embed the template in the Fourier domain. The template points are chosen to lie between radii, which have been experimentally chosen. The exact position in frequency domain is pseudo randomly selected. These points can then be used to estimate the geometric transformations the image has gone through. The transformation estimation involves search over the peak-pairs detected on the distorted image. Pereira and Pun report that magnitude of Fourier transform domain has also some drawbacks: every embedded point affects the whole image in spatial domain, and so the amount of peaks and their strength at which they are embedded is restricted by the watermark’s visibility constraint. In addition, the template in magnitudes of Fourier transform domain cannot be used to detect translation. In Pereira & Pun
(2000), a modified template is proposed. Similarly to Pereira & Pun (1999),
template points lie between experimentally determined radii, but instead of a
random arrangement, the points are chosen along two lines.

Kutter (1998) proposed that a separate template signal is not always
necessary and used the watermark itself as a calibration signal. The watermark is
embedded several times at different, horizontally and vertically shifted, locations
in the blue image component and has a form of a weighted spread spectrum signal.
Prior to watermark detection, the periodic structure of the watermark is used to
estimate rotation and scaling. Autocorrelation function is calculated as

\[
R_{w,w} (u,v) = \sum_{x} \sum_{y} \tilde{w}(x,y) \tilde{w}(x+u,y+v),
\]

where \( \tilde{w} \) is the watermark estimate. Due to periodicity of the watermark, there
will exist peaks in the autocorrelation function, which are localized. Periodic
insertion shows in the autocorrelation function as peaks, which are detected by
first computing gradient of the autocorrelation function. The locations of the
gradient maxima are marked as peak locations. By zeroing out all values but
maximums, a structure is constructed, where the location of the peaks reflects the
rotation and scaling that the watermarked image has undergone. This is illustrated
in Fig. 4.

![Fig. 4. Marked peak locations A) when no geometrical transformations are applied and
B) after rotation and scaling.](image)

The strength of the watermark depends on the luminance value of the pixel and
the weighting function is attained by dividing the luminance value \( L(x,y) \) with a
fixed value \( \kappa \) as
\[ \alpha(x, y) = \frac{L(x, y)}{\kappa}. \] (9)

Kutter (1998) uses a prediction filter to calculate the estimate of the watermark. It should be noticed that two sets of corresponding locations before and after geometric transformation are enough to calculate transformation coefficients for successful inversion of rotation and scaling. However, for robustness against translation and cropping, full correlation search is needed.

Kutter (1998) repeated the watermark pattern to four locations, to introduce a nine peak structure (Fig. 4), which is then used to estimate rotation and scaling. Due to attacks, the estimated grid will be affected by noise caused by attacks. Mainly attacks lower the distinguishing of the peaks from the noise. Some peaks may be lost, location of the peak may be inaccurate and additional wrong peaks may appear. Accordingly, Deguillaume et al. (2002) took the original idea further and embedded a periodical watermark structure with many repetitions in order to get a high number of peaks. Such a grid can be represented by two vectors, the direction of which indicates main axes and norm correspond to the periods. Under affine transformation, the distortions change the main axes, and periods, as illustrated in Fig. 5.

Fig. 5. A) A high number of peaks in a reference grid and B) the distorted grid after affine transformation (Deguillaume et al. 2002).
The authors reasoned that a larger number of peaks survive, even under severe signal fading. Additionally, an intentional removal of peaks by local interpolation becomes more difficult (Voloshynovskiy et al. 2000). Opposed to Kutter’s (1998) spatial embedding method, the embedding of the repetitive pattern is realized in a wavelet decomposed multiresolution image. To keep the periodicity, also the watermark is wavelet decomposed. Perceptual weighting is modified from NVF (Equation 4) to be suited for multiresolution embedding. As a downside of the very high number of repetitions, the watermark is periodic in structure, so it is not pseudorandom anymore.

The peaks can be detected from the local maxima of autocorrelation function or from the magnitude spectrum. Ideally, all the peaks are extracted as in Fig. 5, but in practice, distortions affect peak detection. Consequently, the approach will be more robust since random points are less likely to present significant alignments than correct ones. In other words, it is robust to noise; missing some peaks, or insertion of some false peaks. With Hough transform or Radon transform combined with a robust extraction of periods from aligned points, a robust estimator of the correct underlying grid can be found. First, the main axes of the underlying, possibly distorted grid are estimated. Then, periods of the principal directions are estimated. Due to the estimation process, the affine parameters can be computed and inverted prior to the watermark detection process. Similarly to Kutter (1998), translation or cropping has to be handled with exhaustive search.

Alvarez-Rodríguez & Pérez-González (2002) take a more analytic approach to the watermark synchronization issue and concentrate on theoretical understanding of the performance limits for template (pilot) based watermark synchronization algorithms. Analysis from the main parts is applicable to at least methods basing on a repetitive watermark pattern (Kutter 1998, Deguillaume et al. 2002, Chen et al. 2006). The authors determine a theoretical boundary for estimating rotation and scaling parameter and prove the results with comparing empirically vs. theoretically attained values. The results illustrate that there exists a clear quantization effect on estimating affine synchronization parameters. That is, resolution of the synchronization algorithm is a significant parameter when assessing the quality of the algorithm. In the case of periodic watermark, the resolution is dependent on the offsets that are used in watermark embedding. The further apart the autocorrelation peaks appear, the better the resolution. However, large offset causes peaks to be less distinguishable, and accordingly watermark strength should be well designed.
Salient feature-based methods

The introduction of second generation watermarking (Kutter et al. 1999), have generated a bunch of techniques, in which the synchronization relies in detecting salient feature points. Unlike first generation watermarking schemes, the second generation watermarking employ the notion of data features as defined in (Kutter et al. 1999). The salient points either determine the location of the watermark or determine the origin to apply a transform. In (Kutter et al. 1999), feature points are used to perform tessellation on the image. Each emerging Voronoi cell is watermarked using spread spectrum watermarking independently of the other regions. The extracted feature point locations serve as the origin for the watermark. Accordingly, the method is robust to translation and cropping. For robustness against rotation and scaling, the authors suggest using log-polar transformation. Spread spectrum watermark is highly vulnerable to a synchronization error. The added watermark may change the location of feature points, so limited search is proposed to compensate the inaccuracy.

Bas et al. (2002) proposed another tessellation based watermarking method. In their proposal, watermark image segments are the result of feature point detection and Delauney tessellation. Triangular shape of the area provides the advantage over polygonal area of Voronoi tessellation, that is, the watermark itself can be shaped through affine transformations to fit to the resulting tessellation triangles. In detection, similarly affine transform can be utilized to shape triangles to the original shape prior to calculating correlation.

In the other category of second generation watermarking techniques, regions to be watermarked are centered at the extracted feature points. Commonly, non-overlapped regular, such as circular regions, are used. The actual embedding methods vary from spatial to transform domain to stochastic-analysis-based methods. A good representative of the proposed methods is a method by Seo & Yoo (2004). A circularly symmetric watermark is repeated on N circular areas, located around N strongest feature points. Similarly to many of the proposed second generation watermarking techniques, a modification of the Harris measure is used for feature point detection:

\[
H(x,y,s_n) = \det A(x,y,s_n) - 0.04 \times (\text{trace}A(x,y,s_n))^2,
\]

where the calculus gives the Harris corner strength measure \(H(x,y,S_n)\) at scale \(s_n\) at point \(x,y\) and \(A\) is the second-moment matrix of the image gradients. In each level in the scale space
where $W_c$ is the neighborhood in which the maximum is evaluated and $t_h$ is a threshold. A feature point gives only position information (translation), so additionally the proposed method performs a search over scale space to find the Laplacian maximum. If a normalized scale-space maximum (characteristic scale) is at $(x_0, y_0; s_0)$ in the scale-space representation of an image, then in the scaled image it is assumed to be at $(tx_0, ty_0; ts_0)$. This is a utility that can be taken advantage of to attain scale invariance. In Seo & Yoo (2004), the actual watermark is circularly symmetric for easier detection under rotation.

In the basic 1-bit model for watermarking images (Equation 1), the watermark pattern $W(x, y)$ is of the same type and dimension as the cover image (square, rectangular). However, when taking advantage of feature points, the shape of the watermark usually is of a more complex type, as illustrated in Fig. 6. The watermark has to be of a certain shape to fit to the elementary patch (Celik 2001). Bas et al. (2002) fit the triangular watermark $T_w$ to triangularly shaped tiles by warping. In detection, unwarping is used prior to calculating the correlation between $T_w$ and $\tilde{T}_w$. In (Seo & Yoo 2004), the radius of the embedded circular watermark relates to the characteristic scale, so assuming an isotropic affine transformation, the watermark can be detected.

\[
\begin{align*}
H(x, y, s_x) &> H(x, y, s_y) \quad \forall x, y \in W_c \\
H(x, y, s_x) &> t_h
\end{align*}
\]  

(11)

\[
H(x, y, s_x) > t_h
\]

Fig. 6. Second generation watermarking approaches by A) Kutter et al. (1999) B) Bas et al. (2002) and C) Seo & Yoo (2004).

In every case, repeatability (robustness of feature point extraction) is of importance. Also accuracy of the feature point location affects the performance of the algorithms. An example of geometric manipulation that may deteriorate
watermark detection is aspect ratio change. For example, Delauney triangulation procedure is not independent of such a non-uniform scaling (Celik 2001). In general, the shape of the watermark should correspond to the expected geometric transformations; consequently, for example, a circle shape watermark as such will not be effective against non-isotropic scaling (Seo & Yoo 2006).

**Stochastic-analysis-based algorithms**

Alghoniemy & Tewfik (2000) proposed another approach to deal with geometric distortions. Their method is based on watermark embedding and detection on a normalized image. The parameters for normalizing the image are calculated from geometric moments of the image. In the original method, the normalization process has been designed to take care of correct detection independent of the image size, orientation, and flipping direction. Dong & Galatsanos (2002) and Kim & Lee (2003) also propose a watermarking method based on normalization. The former concentrates on generalization of the geometric attack and resilience to affine transformation, using a larger set of moments. Similarly to (Alghoniemy & Tewfik 2000), in Kim & Lee (2003), the image is normalized on translation, scaling and rotation. Translation invariance is achieved by translating the image to image centroid, and scaling invariance by using a standard size in watermark embedding and detection. For rotation invariance, the authors propose to use the magnitude of Zernike moments instead.

### 2.5 Robustness to print-scan attacks

In the print-scan process, an image goes through a format change from digital format to printed format and back to digital. The process is of interest to watermarking research as print-scan can be both considered as an attack to remove a hidden copyright mark or as a possibility to authenticate an image that appears in paper format, for instance. As far as watermarking is concerned, a priori knowledge of the attacks can be taken advantage of on design. In the focus area of this thesis, the more deeply the print-scan process is understood, the better watermarking methods can be designed. However, the complexity of analyzing the process is revealed from the few studies published so far.

Lin & Chang (1999) propose a model for the print-scan process by considering a pixel value and geometric distortions separately. During printing and scanning process, the watermarked image undergoes several attacks,
including distortion of pixel values caused by luminance, contrast, gamma correction and chrominance variations, blurring of adjacent pixels. In the mathematical formulation of the pixel distortion, the authors consider the effect of different factors and model it by

\[ x^\prime(t_1, t_2) = K\left[ x(t_1, t_2) * \tau_1(t_1, t_2) + x(t_1, t_2) * \tau_2(t_1, t_2) \right] \cdot \eta_1 \cdot s(t_1, t_2), \quad (12) \]

where \( x(t_1, t_2) \) is the virtual finite support image describing the continuous image in the physical domain, \( \tau_1 \) models the combined effect of point spread function of the printer and scanner, \( \tau_2 \) represent higher noise around the edges, \( \eta_1 \) is white Gaussian random noise and \( s(t_1, t_2) \) is the sampling function. \( K \) represents a combined nonlinear effect of the AC, DC and gamma adjustments of the printer and scanner and is formulated by

\[ K(x) = \alpha \cdot (x - \beta_1)^\gamma + \beta_2 + \eta_2(x), \quad (13) \]

where \( \eta_2 \) describes the power of the noises (thermal and dark current noises) and \( K \) is a function of pixel value and adjustable parameters \( \alpha, \gamma, \beta_1, \beta_2 \). The authors estimate the parameters of responsivity function experimentally using image registration with the aid of the original image.

The other attack considered related to print-scan process by Lin & Chang (1999) is the RSC (Rotation Scaling Cropping) attack, which illustrates the process of scanning an image. The image area to be scanned is defined by the user using a GUI (Graphical User Interface), which means that a significant portion of background, additionally to the actual image, is also cropped during scanning process. Additionally, the image can be rotated and scaled. The general formulation of affine transformations (Equation 5) can be applied also for printed and scanned images. In Lin & Chang (1999), however, the effect of cropping has also been taken into account by

\[ x_p = \begin{cases} x', (t_1, t_2) \in M \\ 0, \text{ elsewhere} \end{cases} \quad (14) \]

In the equation, \( M \) is a masking function. In experiments, the concentration is on popular PS (print-scan) devices such as color inkjet printers and flatbed scanners.

Yu et al. (2005) summarize the problems in print-scan resiliency of watermarking to three points. Firstly, randomness: every time an image is printed and scanned, even with proper placement of the paper into the scanner bed, the resulting image is different. Secondly, user-dependency: the selection of the
printing and scanning parameters is a matter of taste of the one operating on the
printing and scanning. Also placing a printout in the scanner bed is user-
dependent, as is also the manual selection of the scanning area. Thirdly,
indistinguishability, i.e. printing and scanning operations cannot be separated from
each other.

In the analytical section, Yu et al. (2005) classify the attacks involved in the
print-scan operation to systematical and operational. Systematical distortions are
those related to the devices. The authors concentrate on the characteristics of laser
printers, in particular. The authors relate to printing the following distortions;
grayscale conversion attack related to halftoning, low-pass type attack causing
blur due to the print device and geometric distortions. Similarly as during printing,
in scanning, a low-pass filter attack is present, and it causes blurring. Additionally,
in scanning, there exist geometric distortions which are man-dependent.

Solanki et al. (2006) model the print-scan attack with three components:
geometric transformations, nonlinear effects and colored noise. From geometric
transforms, the research concentrates on the effect of cropping. As in Lin &
Chang (1999), the cropping is thought as a multiplication with a masking window.
Cropping is considered to cause blurring. The main sources of nonlinear
distortions are gamma tweaking, dot gain in the printer and gamma compensation
in the scanner. With experimental studies, the authors verify that a low-pass
filtering type attack is involved in the print-scan process. Colored noise is the
cause of digital halftoning, accompanied with the uncertainties of printing process
itself. Both are considered to cause high-frequency noise. In the experiments, the
authors study the effect of print-scan process with simulations and real tests with
un-calibrated devices. This is to mimic more the real situation; most of the
devices used by common users are un-calibrated. Specially, the effect of PS
(Print-Scan) process on DFT coefficients is experimented. Best preserved are,
according to their experiments, high magnitude low frequency coefficients. Tests
also show that there is a discrepancy on the image size when printed, the aspect
ratio of the image may change for a small amount.

He & Sun (2005) also examined the print scan process in order to develop a
print-scan resilient watermarking method. The authors emphasize that the
distortions during PS process are very much device dependent and also time
variant. Due to complexity of analyzing the process, an experimental approach is
taken. In addition to the findings of Solanki et al. (2006), some new findings are
depicted in the article. Using different scanners and printers He & Sun (2005)
found out that most of the textures are preserved, dynamic range of the intensity values is reduced and that change is nonlinear.

Altogether, in addition to geometrical distortions, printer/scanner optical and mechanical distortions, like ink spreading, are challenging. This difference, although barely visible to eyes, makes a difference when extracting the message or detecting the existence of a watermark compared to message extraction/detection without print-scan attack. (Yu et al. 2005).

**Print-scan resilient watermarking algorithms**

The watermarking methods, where the intention is that the watermark is readable from printouts, can be coarsely divided into two categories. In the first category, are methods, which are based in direct manipulation of halftone cells, like the method proposed by Xu & Wan (2008). In the second category, are methods which considerer print-scan, including halftoning process in the printer, as an attack and do not combine watermarking with the printing process.

These two approaches are very different from each other. Halftoning is a process that converts a multitone image into a bi-level image. As a consequence, problems related to watermarking directly halftone images, resemble the ones with watermarking binary images, such as black and white documents. Flipping pixels in a binary images require rules for how the changes are made so that they are not disturbing (Wu & Liu 2004). Similarly, in halftone watermarking, there has to be a controlled way to introduce bi-level changes in halftone patterns. In extracting a halftone watermark, however, the resolution of the scanned image has to be in a halftone dot level, requiring very high quality scanning and preprocessing to synchronize the extraction. Because of the synchronization problems, halftone watermarking methods are not necessarily robust to print-scan process, but some are used for watermarking scanned material. The great potential of halftone watermarking is on detecting forgery, and consequently, methods are often fragile in nature.

In this thesis, because of the clear differences in basis, the work concentrates on the methods belonging to the second category, on methods that are robust to print-scan process, including halftoning to produce the print. Due to the complexity of the print-scan attack, the watermarking literature on print-scan resilient watermarking is quite narrow. In Table 1, the majority of the proposed methods are presented, with a short description of basic properties.
It can be seen from the synchronization methods that most of the methods take advantage of the work done on resolving RST resiliency in digital domain. Templates, semi-invariant domain, and salient feature-based methods have been suggested. Because of the strong distortions, however, additional means have to be used to ensure robustness to pixel value distortion. Also man-dependency when selecting the area to be scanned, makes the problem more complex. Generally, this reflects in the approaches with a need of some preprocessing. Often, for example, edge detection is used for detecting the boundaries of the image area.

Table 1. Print-scan resilient watermarking algorithms (ED refers to edge detection).

<table>
<thead>
<tr>
<th>Authors</th>
<th>Synchronization</th>
<th>Multibit Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solanki et al. (2004, 2006)</td>
<td>halftone cells+ED</td>
<td>Y (few hundred bits)</td>
</tr>
<tr>
<td>He &amp; Sun (2005)</td>
<td>ED</td>
<td>Y (1024 bits)</td>
</tr>
<tr>
<td>Bas et al. (2002)</td>
<td>feature points</td>
<td>N</td>
</tr>
<tr>
<td>Chen et al. (2006)</td>
<td>spatial template+ED</td>
<td>Y (64 bits)</td>
</tr>
<tr>
<td>Chiu &amp; Tsai (2006)</td>
<td>frequency domain peak</td>
<td>Y (serial number 888)</td>
</tr>
<tr>
<td>Lin (1999)</td>
<td>log-log mapping</td>
<td>Y(14*3 bits)/N</td>
</tr>
<tr>
<td>Lefebvre et al. (2001)</td>
<td>frequency domain template</td>
<td>Y</td>
</tr>
<tr>
<td>Lin &amp; Chang (1999)</td>
<td>invariant features</td>
<td>N</td>
</tr>
<tr>
<td>Hu (2008)</td>
<td>feature points</td>
<td>Y(~20bits) *)</td>
</tr>
<tr>
<td>Pramila et al. (2008)</td>
<td>templates</td>
<td>135 bits</td>
</tr>
</tbody>
</table>

In Solanki et al. (2004, 2006), the synchronization has been specially designed for detecting watermarks from printout. It is based on detecting orientation of halftone cells for correcting the geometric rotation. The method is, however, not applicable to digital rotation. In watermarking, the authors rely on analysis of the effect of print-scan process and experiments. A method to selectively embed in low frequencies (SELF) of DFT coefficients is proposed.

Lin (1999) and Lin & Chang (1999) propose methods based on invariant features, where invariance is gained through appropriate transformation. In this sense, they belong to the class of methods originally proposed by O’ Ruanaidh & Pun (1998). Authors use log-log Lin (1999) and log-polar Lin & Chang (1999) map of Fourier coefficients. Method in Lin & Chang (1999) is accompanied with projection of log-polar coefficients. In Lin (1999) all images are resized to a standard size prior to DFT. Due to inherent aspect ratio change in print-scan process, Fourier-Mellin (log-polar mapping of Fourier coefficients), as such, is inappropriate and causes problems. The change of image size, the information
loss of discarded area (cropped), and translation of the origin point of the image are considered to be the main sources of distortion affecting the DFT coefficients.

Bas et al. (2002) and Hu (2008) base their approach on feature (salient) point detection. Both methods are dependent on the repeatability of feature point detection. As well as print-scan attack effects on watermark detection/message decoding, it also deteriorates feature point detection. Specially challenging are images with textured regions.

Chen et al. (2006) and Lefebvre et al. (2001) rely on templates and place into the image two watermarks, where one is the synchronization template and the other the actual watermark. In Chen et al. (2006) for the actual watermark to be detectable, the synchronization watermark (periodic pattern) is embedded first. NVF (Equations 3 and 4) is used for perceptual weighting of the pattern. The autocorrelation function is used to find peaks and Radon transform is utilized to invert skew prior to decoding of the actual spatial domain message. Additionally, image pixel density is used to remove the white margins and black margins caused by both the translation and because of the inversion process.

Lefebvre et al. (2001) use a circularly arranged frequency domain peak structure for synchronization. The actual watermark is a 2D pattern embedded in spatial domain. In Chiu & Tsai (2006), the watermark is also a circular frequency peak structure. To get some gain on capacity, concentric circular stripes are used. Rotation and scaling are handled with one peak outside the ring region acting as a reference for the rotation and scaling.

Pramila et al. (2008) investigate the possibility of taking advantage of properties of different domains in designing a print-scan and additionally JPEG resilient watermarking scheme. Two templates are used to enable robust watermark carrying in wavelet domain. Wavelet domain has properties that are of advantage against JPEG attacks. Circularly arranged peak structure in Fourier domain is used for detecting rotation and scaling and spatial domain template is used for translation search.

Commonly, methods taking advantage of templates are based on inverting the transformations prior to watermark detection. Inversion of rotation is also used in Solanki et al. (2004, 2006). The inversion process of rotation and scaling is illustrated in Fig. 7. The figure also depicts that, if the watermark is not embedded in translation invariant domain, there is still a need to define the exact position of the watermark. In all of the methods presented in Table 1, the experiments are restricted to images in a white background and mostly it is expected that the
actual watermarked image area is not cropped. To our knowledge, Pramila et al. (2008) are the only ones considering also a combination of JPEG and PS attack.

Fig. 7. Scanner user interface on the left and watermarked image after inverting rotation and scaling on the right.

In overall, methods represented in Table 1 differ with respect to how well they respond to the challenges caused by both the inherent geometrical transform in PS attack, as well as the pixel value distortion. In Table 2, the performance of the methods against geometrical distortions is summarized. Pixel value distortion is mostly handled with proper weighting of the watermark and/or choice of coefficients in the appropriate domain. In Table 2, mark ++ is utilized if the method is robust to specific geometric transform, + if the method is at least partly robust or there are some restrictions, and – if the issue is not considered and the effect is not predictable. If the effect has actually been measured, the numerical value is given. The results in Table 2 indicate that most of the methods have restrictions. In the sense of robustness to all transforms (rotation, scaling, translation, cropping) the best performing seems to be Hu (2008), where capacity of the method for the Lena image is approximately 20 bits. The method proposed
in Bas et al. (2002) is a 1-bit watermarking method and highly dependent on the success of the detection of the feature points.

Table 2. Print-scan resilient watermarking algorithms (ED refers to edge detection).

<table>
<thead>
<tr>
<th>Authors</th>
<th>Rotation</th>
<th>Scaling</th>
<th>Translation</th>
<th>Cropping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solanki et al. (2004, 2006)</td>
<td>*</td>
<td>+</td>
<td>ED</td>
<td>(+)</td>
</tr>
<tr>
<td>He &amp; Sun (2005)</td>
<td>–</td>
<td>–</td>
<td>ED</td>
<td>–</td>
</tr>
<tr>
<td>Bas et al. (2002)</td>
<td>&lt; 10%</td>
<td>80%</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Chen et al. (2006)</td>
<td>++</td>
<td>–</td>
<td>ED</td>
<td>–</td>
</tr>
<tr>
<td>Chiu &amp; Tsai (2006)</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>Lin (1999)</td>
<td>-</td>
<td>*(+)</td>
<td>(+)</td>
<td>0.8</td>
</tr>
<tr>
<td>Lefebvre et al. (2001)</td>
<td>++</td>
<td>+</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Lin &amp; Chang (1999)</td>
<td>-3°/+3°</td>
<td>0.1–2.0</td>
<td>&gt; 2.5</td>
<td>&lt; 0.6</td>
</tr>
<tr>
<td>Hu (2008)</td>
<td>*</td>
<td>0.5–2.0</td>
<td>+</td>
<td>40%</td>
</tr>
<tr>
<td>Pramila et al. (2008)</td>
<td>++</td>
<td>+</td>
<td>++</td>
<td>–</td>
</tr>
</tbody>
</table>

2.6 Robustness to print-cam attacks and algorithms

Pramila et al. (2008) define ‘print-cam’ as a process where the watermarked image is printed on a paper and then read with a camera phone by taking a picture of the printed image. Nuutilen & Oittinen (2009) propose a method to simulate the printing and imaging channel (print-cam process). The model shows the effect of different elements involved in the process. In their model, response image \( I_{est} \) is given by

\[
I_{est}(x, y) = g[s(x, y)] + \eta[s(x, y)]
\]

(15)

\[
s(x, y) = v[w(x, y)]
\]

(16)

\[
w(x, y) = f[r(x, y)]
\]

(17)

\[
\eta(x, y) = \sigma[s(x, y)] \cdot \mathcal{N}
\]

(18)

In the simulation model, the image goes in the camera through the optics module and through a printing and imaging module. The input to the printing and imaging module is an image that is radially distorted (\( r \)) and the quality of which has been
lowered by photometric distortion \( (f) \). In the simulated imaging device, the input image is sampled to the resolution of the imaging device, which is described with spatial sampling \( (v) \). The effects of the printing and imaging module have been considered to consist of the response function \( (g) \), which determines the dependency between the input signal and measured response of the printing and imaging channel and noise \( \eta \) in the printing and imaging channel. The response of the noise is approximated with variance \( \sigma \) and \( \mathcal{N} \) refers to the standard normal distribution.

According to the authors, the effect of the printing and imaging module had a stronger effect on BER (Bit Error Rate) of the watermark than optics module. However, as authors state, as the model does not take into account watermarking principle, the results can be explained by the choice of watermarking principle (in this case modification of pixel intensity values in blocks of image). In order to make use of the previous model, a large set of parameters have to be estimated and the parameters have to be reset, with a change of devices or environment. But after this has been done, the load of manual experiments will be smaller.

Stach et al. (2002) focus on the use of web cameras for watermark detection. The authors point out two cases where such a linking applications might fall into. Although the considerations are for web cameras, they also apply them to other cameras. In the first case, the camera must be chosen or designed for the particular watermarking application. In the second case, the watermarking application must survive using a range of devices. Both Nuutinen & Oittinen (2009) and Stach et al. (2002) enumerate as one of the most difficult issues the camera software. For example, most of the mobile phone cameras automatically JPEG compress the image, which has since the 1990s considered as a powerful attack on a watermark. Many of the technical parameters of the camera software may be completely inaccessible or some parameters can be adjusted.

The conditions in Nuutinen & Oittinen (2009) are set to a fixed camera distance, constant light conditions and perpendicular direction of the camera to the printed image. In practice, pixel value distortion is accompanied with geometrical distortion. User-dependency is emphasized, as the person holding the camera equipped phone, may cause projective distortion in addition to rotation, scaling, translation and cropping. Systematical distortions related to the devices (printer, mobile phone camera), are accompanied with environmental characteristics, which cause additional pixel value distortions or otherwise decrease reliability of watermark extraction. Pramila et al. (2008) and Perry et al. (2002) enumerate the effect of print material, ink density, lighting conditions and
noise around the image. Due to strong attacks, not many print-cam resilient methods have been proposed. In Table 3, are depicted the published ones.

Table 3. Print-cam resilient watermarking algorithms.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Synchronization</th>
<th>Capturing device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kim et al. (2006), Kim et al. (2005)</td>
<td>spatial template</td>
<td>digital camera, tiff mode, tripod</td>
</tr>
<tr>
<td>Nakamura et al. (2004)</td>
<td>visible frame</td>
<td>mobile phone, freehand</td>
</tr>
<tr>
<td>Liu &amp; Shieh (2011)</td>
<td>visible frame</td>
<td>mobile phone, freehand</td>
</tr>
<tr>
<td>Takeuchi et al. (2005)</td>
<td>visible frame</td>
<td>digital camera</td>
</tr>
<tr>
<td>Pramila et al. (2008)</td>
<td>visible frame + spatial template</td>
<td>mobile phone, freehand</td>
</tr>
<tr>
<td>Horiuchi et al. (2009)</td>
<td>frequency domain template</td>
<td>mobile phone</td>
</tr>
</tbody>
</table>

Print-scan attack, discussed in Section 2.5, restricts the usability of synchronization methods originally designed for handling digital media only. In print-cam, there are even fewer practical possibilities. From Table 3, it can be seen that many of the proposed methods base on the use of a visible frame, which is used to invert the effect of the tilted position of the camera.

In Kim et al. (2006) and Kim et al. (2005), no frame is used, but there is still a need for manual removal of excess area prior to watermark extraction. The watermarking method is based on the self-referencing principle originally proposed by Kutter (1998). A tiling pattern is used for detecting geometrical transformation and the fingerprint code can be detected with cross correlation after image recovery.

Horiuchi et al. (2009) use a frequency domain template, with no visible frame, but do not show the effect of camera tilting in the experiments. The watermark embedding idea follows the principle proposed by Pereira & Pun (1999). The signal pattern structure is circular in the frequency domain. Peak values in two circles of the outside are used to adjust the position and alignment and peak values in three inner circles express the watermark information. In practice, the watermark is embedded in spatial domain by superimposing the IDFT (Inverse Discrete Fourier Transform) transformed pattern to the image.

Nakamura et al. (2004) present a watermarking method based on 2D (two-dimensional) patterns. A 2D pattern, P, visualized in Fig. 8, is used to carry information. According to the sequence of embeddable bits \( t_n \), either \( P^- \) or \( P^+ \) is selected. The size of the pattern is matched to that of image block and superimposed to the image. Consequently, every block carries one error coded and spread spectrum coded bit and capacity depends on the size of blocks used.
The extraction is based on an estimate of which pattern energy is superiorly in the block from blocks of preprocessed and filtered image. Preprocessing, projection distortion correction and scale normalization are needed in extraction and realized with the aid of a frame around the image.

![2D patterns](image)

**Fig. 8. The pair of 2D patterns in the method developed by Nakamura et al. (2004).** A) 2D pattern used to embed $-1$ and B) the pattern used to embed $+1$.

In Katayama *et al.* (2004), a fast frame detection method needed in Nakamura *et al.* (2004) for preprocessing (image recovery) is explained. A blue frame illustrated in Fig. 9 is used for estimating corner points and inverting projective distortion and for clipping the image.
In Liu & Shieh (2011), authors suggest an improvement for the watermarking principle of Nakamura et al. (2004). Robustness and invisibility is proven to get better when the watermark strength is based on Watson’s DCT domain model for JND calculation. Accordingly, the 2D patterns are shaped in DCT domain and IDCT transformed prior to embedding.

In Pramila et al. (2008), the visible frame is accompanied with an invisible spatial template. In the paper, the authors show that a conventional spread spectrum watermarking with cross correlation based message extraction with proper watermark strength can be made robust to print-cam process. The watermark is embedded and extracted in wavelet domain. Preprocessing includes compensation of lens distortions. Also the frame method itself is not accurate enough for detecting translation, so an additional spatial template is proposed.
In addition to Pramila et al. (2008), the systematical nonlinear geometrical distortions related to the properties of the capturing device (mobile phone camera) are considered by Takeuchi et al. (2005). The authors propose a watermarking system involving lens distortion and perceptive distortions correction accompanied with a patented GS (Guided Scrambling) watermarking technique (Kunisa 2009). In the GS technique, the robustness of the watermark is ensured utilizing multiple scrambled candidate sequences, the best one of which is chosen by simulating detection and calculating SNR (signal-to-noise ratio).

In the methods described above, the success of watermark recovery is strongly dependent on the accuracy of the image recovery process. In Fig. 10, this aspect is illustrated related to the use of block wise watermarking techniques. Slight error changes inspected area and the defective effect becomes stronger when the size of the block decreases. Also, successful recovery from geometrical
transformations is not a sufficient condition to watermark recovery, but the watermarking method also has to be robust to the effect of the inverting geometrical transformation during recovery process.
3 Research contributions

In this chapter, the summary of the main contributions of the original publications is given. For publications, the central problem is pointed out, the essential parts of the methods are described and the main results highlighted.

3.1 Methods to increase watermark extraction robustness with perceptual weighting

In the early days of watermarking research in the end of 1990’s, a number of spatial domain watermarking methods were introduced. By far, the most famous techniques were LSB (Least Significant Bit) modification and spread spectrum techniques. Commonly, early spatial domain techniques were, however, very vulnerable to attacks, especially to compression. As compression is one of the attacks that may happen unintentionally, robustness to it is considered particularly important. Simultaneously to robustness, watermarking should also meet the general watermarking definition; “the practice of imperceptibly altering a Work to embed a message about that Work” (Cox et al. 2002a). Paper I presents a spatial spread spectrum method with perceptual shaping, with the goal of improving watermark robustness against compression attack without causing visible distortions.

As well as in all of the later work, the modifications are made on the luminance component of the image. In the center of attention in Paper I, is JND analysis on the host image, which results in a pixel by pixel strength factor for the watermark. For spreading the watermark bits, m-sequences are applied. The strength of the m-sequence is modified according to the JND analysis, resulting in an image-dependent watermark. Accordingly, the amplitude of the watermark is optimized both when considering robustness and for attaining perceptual invisibility of the watermark. The embedding scheme is depicted in Fig. 11.

The scaled m-sequence is added to the host signal line by line as follows:

\[ y'(n) = x(n) + \alpha(i) \cdot m(k), \text{when watermark bit = 1} \]  \hspace{1cm} (19)
\[ y'(n) = x(n) - \alpha(i) \cdot m(k), \text{when watermark bit = 0}. \]  \hspace{1cm} (20)

In the equations, \( y' \) is the watermarked image, \( x \) is the original image, \( \alpha \) is the image dependent adaptive strength factor, and \( m \) is the m-sequence.
For visual adaptation, it is proposed to take advantage of the model by Chou & Li (1995). A JND threshold is calculated for each pixel based on two properties of the human eye, one of them being the spatial uniformity of the background luminance and the other one the average background luminance behind the pixel:

$$JND_{\mu}(x, y) = \max \left\{ f_1(bg(x, y), mg(x, y)), f_2(bg(x, y)) \right\}, \quad (21)$$

where $f_1$ describes spatial masking effect and $f_2$ models the threshold due to background luminance. Spatial masking, $f_1$ is calculated taking account average background luminance ($bg$) around pixel at $(x, y)$ and maximum weighted average ($mg$) of luminance differences in four directions around the pixel. Intensity masking, $f_2$ relies on subjective tests on noise visibility threshold on different backgrounds. (Chou & Li 1995)

The detection scheme is blind and so the original image is not needed for message extraction. If we define $y^*(n)$ as the watermarked pixel values and $m(n)$ as m-sequence samples, the raw cross-correlation values $c_{xy}(m)$ are defined as
The output vector has the format
\[ c(m) = c_{my}(m - N), m = 1, 2, \ldots, 2N - 1. \]  

Furthermore it is shown that the detection results can be improved with an equalization filter, such as a fixed one-dimensional high pass filter of the form \( d(n) = [-1 2 -1] \), which filters out strong low pass components from the \( y'(n) \) (Fig. 12). It is also proposed in Paper I to use an additional level of spatial spreading, controlled by a spreading factor, to make the watermark more secure and to tune the capacity.

![Extraction principle in Paper I. (IJ) 2002 International Workshop on Digital Watermarking. Reprinted with permission.](image)

The effect of prefiltering on robustness was measured with grey level images Diana and Baboon. The results for Diana image, with and without prefiltering are
shown in Table 4. With no compression, the capacity of the 256×168 size Diana image was 127 bits. With increasing the compression, down to the quality factor of 25, drops the capacity to 1/4. Still, the message can be extracted without errors. Due to highly textured areas in the Baboon image, longer m-sequence are needed; $2^{10}−1$ for robustness against compression with QF = 50. In both cases, the PSNR (peak signal-to-noise ratio) of the watermarked images were ~37 dB.


<table>
<thead>
<tr>
<th>m-sequence length</th>
<th>No pre-filtering, QF = 100, BER(%)</th>
<th>Pre-filtering, QF = 100 BER(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^7-1$</td>
<td>12.60</td>
<td>0</td>
</tr>
<tr>
<td>$2^8-1$</td>
<td>1.79</td>
<td>0</td>
</tr>
<tr>
<td>$2^9-1$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$2^{10}-1$</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

In larger scale test the robustness to compression attacks was tested for five categories of color images (facial images, synthetic images, scenery images, textures, document images). In these tests, with altogether 65 images, two important results were obtained. Firstly, image quality remains good, while weighting the watermark as illustrated in Fig. 13A. Secondly, robustness to JPEG compression – even with QF of 50 – can be achieved in near all image categories, with a suitably long m-sequence. This is shown in Fig. 13B, where it is illustrated how the BER approaches zero, when the length of the m-sequence is increased.
Simultaneously to the concern of robustness to compression attacks in the end of the 1990s, aroused also the attention to the drastic effect of geometrical transformations on watermark robustness. Most of the papers published on geometrical attacks considered RST attack, where the attack can be described with rotation, scaling and translation parameters. At the same time, aroused also interest on watermark surviving printing and scanning operation. In print-scan process, there is a geometrical attack inevitably present. This accompanied with
the distortion caused by the devices, and involvement of human in the process, makes watermark detection/extraction from printouts especially hard.

In template based RST resilient methods, a template is used for synchronization purposes. When a separate synchronization watermark is used, the problem is how to efficiently share the available JND with the actual message watermark. The resulting image should still be visually pleasing. Additionally, the template should be robust, and give accurate estimates for RST parameters so that the image can be recovered from affine transformations and the message extracted.

In Paper II, a print-scan resilient template based method is presented. Multilevel watermarking principles are applied in order to embed a reference watermark and the message bits. The reference watermark is a periodic template \( W \) satisfying equations (24) and (25), generated from a pseudorandom sequence of values \([-1, 1]\):

\[
W(x + q_0 N_0, y) = W(x, y); \quad q_0, N_0 > 1 \tag{24}
\]

\[
W(x, y + q_1 N_1) = W(x, y); \quad q_1, N_1 > 1. \tag{25}
\]

In the equations, \( N_0 \) and \( N_1 \) determine the periodicity of repetitions, and \( q_0 \) and \( q_1 \) a repetition number in horizontal and vertical directions. The reference watermark is embedded in the host image in spatial domain, utilizing the equation

\[
Y^*(x, y) = X(x, y) + \lambda_1 JND_{fb} \cdot W(x, y), \tag{26}
\]

where \( Y^* \) is the watermarked image, \( X \) is the luminance component of the original image, \( W \) is the periodic watermark and \( x \) and \( y \) describe the pixel position. \( JND_{fb} \) is the scaling factor attained from the JND profile, and \( \lambda_1 \) is an additional scaling factor. The synchronization template is used to estimate affine transformation parameters.

The message bits are embedded in the image, where reference information has first been embedded, in wavelet domain. Single-level decomposition of the image into subbands using Haar-wavelets is utilized and the message bits are embedded in the approximation coefficients of the wavelet transform utilizing

\[
\begin{align*}
Y_{l_f}^{**}(n) &= Y_{l_f}^{*}(n) + \lambda_2 \cdot m(k), \text{ message bit } = 1 \\
Y_{l_f}'(n) &= Y_{l_f}(n) - \lambda_2 \cdot m(k), \text{ message bit } = 0
\end{align*} \tag{27}
\]

where \( Y_{l_f}^{*}(n) \) is the watermarked subband in the \( l \)th resolution level at \( f \)th frequency orientation and \( Y_{l_f}'(n) \) is the corresponding subband of \( Y^* \). The chip rate for spreading is controlled by the length of the m-sequence, \( m(k) \), and the
addition or subtraction of the m-sequence is weighted using estimated JND profile from the image with the synchronization watermark and a scaling factor $\beta$. $\lambda_2$ is an additional scaling factor. Decomposition of the JND profile is utilized, to derive energy weight for the low resolution subband. Finally, the watermarked image is inverse transformed.

The multibit watermark extraction method is preceded by an image recovery process. Robust extraction of the actual message requires that the inversion process of the geometric distortions is accurate. Accordingly, methods to attain accurate estimation are proposed. A periodicity as formulated in equation 24 and equation 25 can be revealed by calculating autocorrelation for the watermark estimate. Autocorrelation function $R_{\hat{w}, \hat{w}}(u, v)$ is calculated over an area defined by $N_3$, $N_4$, $M_3$ and $M_4$.

$$R_{\hat{w}, \hat{w}}(u, v) = \sum_{x=N_3}^{N_4} \sum_{y=M_3}^{M_4} \hat{W}(x, y)\hat{W}(x + u, y + v),$$

(28)

where $\hat{W}(x, y)$ is a Wiener estimate of the watermark calculated from the watermarked image. Wiener filtering is normally used to enhance noisy image with low-pass filtering, but here it is used to estimate the noise, in other words, the watermark. The filtering is realized using Matlab 2-D Wiener filter. The absolute value of the resulting autocorrelation function is scaled to the range of $[0,1]$ and peak detection is furthermore enhanced using Sobel filtering. Sobel filter, a commonly used edge detection filter, emphasizes horizontal edges and accordingly improves peak detection. A grid structure $g(u, v)$ is generated by thresholding:

$$g(u, v) = \begin{cases} 1, & \text{when } R_{\hat{w}, \hat{w}}^{**}(u, v) \geq \gamma \\ 0, & \text{when } R_{\hat{w}, \hat{w}}^{**}(u, v) < \gamma \end{cases}$$

(29)

where $\gamma$ is the threshold and $R_{\hat{w}, \hat{w}}^{**}(u, v)$ is the scaled and filtered ACF (Autocorrelation Function). The ACF reaches its peak at the origin, and periodicity with every pairs of $N_3$, $N_4$ and $M_3$, $M_4$ is the same, so utilization of overlapping areas and summation as defined in equation 30 is suggested and later proven to improve robustness:

$$g^*(u, v) = \sum_{n, \nu} g^{(N_3, N_4, M_3, M_4)}(u, v),$$

(30)
where summation is origin centric. From the constructed grid structure, the rotation angle is determined by examining the line segments determined from the peaks in the Hough transform matrix. The Hough transform is a method which can be used to isolate features of a particular shape, like a line in an image or in this case, in the grid structure. Printing and scanning process causes noise, and due to the nature of the ACF function, most of the noisy points in the grid are situated along the line going through the origin. It is suggested to calculate the rotation angle utilizing end points of the selected, longest, line in the most dominant direction of lines. The line going through the origin, the blue line in Fig. 14, is excluded. Furthermore, the noise also affects scaling estimation, and a method to reduce the effect of this noise is proposed in Paper II.

After inverting rotation and scaling, the image is still translated (see Fig. 7). This holds true for both periodic spatial templates, as well as for frequency domain templates. In Paper II, the underlying periodic pattern, and especially periodic pseudorandom vectors along the edges of it, are used to determine translation. Edges are found by determining a significant drop in mean removed cross-correlation. The method allows the setting up of the parameters to control the complexity of translation search.

Message extraction is based on a thresholded correlation receiver and is similar to the one presented in Paper I, but realized in wavelet domain. The Hamming coded message is revealed with a zero-thresholding. The extraction process relies on the success of the preceding image recovery.

In the experiments, the capacity of the message was kept constant, the message is error coded and the length of the message is 112 bits. Tests concentrate on measuring the performance with different parameters. Robustness was measured against print-scan attack or print-scan attack combined with JPEG compression. In the experiments, the angle of the image in the scanner bed was varied 0–15° to simulate displacement on the scanner bed. The performance was measured with success ratio and BER. Tests indicated that the success ratios of the tests depend on the suitability of the parameter. It was shown that suitable parameter settings between the strength of the synchronization watermark and the actual watermark can be found. A stronger synchronization grid is needed when the watermarked image is compressed prior to printing. As well as the strength factors, the selection of threshold γ in equation 29 was seen to have a direct effect on the performance. It was pointed out that instead of a manual threshold selection, an adaptive method would be more useful.
The PSNR and PSPNR (peak-signal-to-perceptible-noise ratio) values varied between 34.2 dB to 37.9 dB and 46.7 dB to 54.1 dB, respectively. The PSPNR (Chou & Li 1995) value was suggested for performance evaluation as it takes into account only the part of the distortion that exceeds the JND threshold and as such is suitable for evaluating the effect of multilevel watermarking on quality.

Tests also indicated that, with overlapping areas (Equation 30), the compression ratio can be increased and the success ratio is still quite high. Without overlapping areas, JPEG compression with QF = 50, printing and scanning the result image, resulted in a 0% success ratio with the average of 7.7% BER. Summation patches up missing peaks when calculating RS parameters and consequently the success ratio increased to 83% with an average of 1.78% BER. This offers an interesting performance improvement method that would be worth further development.

Compression, as well as print-scan, are both powerful attacks on watermarking. In Paper II, it was shown that the robustness of a synchronization template to these attacks can be achieved with efficient JND usage, filtering and noise reduction methods. This makes possible the use of multilevel technique,
where the actual message is embedded in wavelet domain. Results also show the importance of the correct threshold settings for estimating affine transform parameters (Equation 29). When the threshold is optimal, the inversion of the geometric transformations is more accurate, and accordingly, the bit error rate approaches zero.

3.3 A method to encode a multibit message utilizing directed periodic patterns and a method to decode the message after attacks

After the turn of the millennium, some scientific publications considered especially print-scan attack. In Table 1, is gathered the majority of proposed approaches where watermarking process does not directly manipulate halftone cells. As an evidence of the difficulty of the problem, the range of proposals is quite narrow. In Paper II, it was noted that, with the proposed multibit message embedding technique in wavelet domain, the need for accuracy for inverting rotation was approximately 0.3 degrees for reliable message extraction. Especially the reliability of spread spectrum based methods relies on the accuracy of the inversion process and recovering the image from geometrical distortions, as well as possible prior to extraction/detection. A usual method to extend a 1 bit watermark to multibit is to increase the payload dividing the image to blocks (sub-images). In block based methods, the inaccuracy of inversion process causes block division error, which may have a tremendous effect on reliability. The smaller the blocks, the more severe the effect is.

Current watermarking literature considers print-scan as an individual attack where experiments have been done from images in a white background (see Fig. 7). In a practical case, images seldom exist orphan against white background. In spatial template based methods, the autocorrelation function, in which the peak maximum is always located at the center, does not give information about the location of the watermark. Similarly, frequency domain template due to translation invariance of Fourier transform does not give information of the position of the watermark. As a result, there is usually a need for some auxiliary method such as edge detection, full search, or correlation to locate the watermarked area, prior to extracting the message or detecting the watermark. Additionally, in practice, for example slight aspect ratio change while layout processing, would confuse most of the current print-scan resilient methods. None of the papers shown in Table 1, expect for Pramila et al. (2008), considers a
combination of attacks, in which print-scan is accompanied with an additional JPEG attack.

In Paper III, a method to embed multibit messages robust to print-scan and print-scan combined with an additional attack is presented. The method takes advantage of autocorrelation properties of periodic patterns and encodes the multibit information in a way that the message can be robustly extracted from printed and scanned images without exact inversion process. This is the case also when the inexactness is caused by an additional attack or the image is translated on a nonwhite background.

A periodic pattern exposes important properties. Firstly, the autocorrelation function reveals peaks that are placed at grid intersections. Secondly, the peaks are equidistantly placed with respect to the fundamental periods \((N_0, N_1)\) in the pattern. Finally, the orientation and fundamental periods are exposed to the same geometrical transforms as the actual image. In Paper III, we define a directed periodic pattern

\[
W^\theta = \Pi \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} W(u,v)
\]

where \(\Pi\) defines the interpolation. A previously non-utilized property in the watermarking literature is that the directed grid \(G^\theta\) has all the preceding properties, but it also keeps the information \(\theta\) of the direction of the periodicity. Accordingly, a method to encode a message by modulating \(\theta\) of the periodic pattern is presented. The original message is divided to be spread over the image blocks and represented by quantized orientation \(Q_i(\theta)\). One block carries reference information to indicate the amount of rotation and scaling the image has undergone. The other image blocks carry information, in which periodic patterns, using different orientations are used to convey a multibit message in the modulated angle. An example of the mapping between message segment and angle information is illustrated in Fig. 15.
Perceptual shaping in embedding and using autocorrelation function, filtering, masking, and adaptive line search with Hough transform ensures robust message extraction. The accuracy of the angle detection has a direct effect on the capacity of the scheme; the more accurate detection, the higher capacity. Or, the other way round, the fewer bits embedded per block, the more error in angle detection is allowed.

In Paper II, the synchronization information is spread over the whole image area. In Paper III, instead of multilevel watermarking, a block based method is used. One block carries reference information for detecting rotation and scaling parameters. The actual message bits are spread over the remaining image area. Suggested filtering, masking and adaptive thresholding techniques ensure that a piece of information is enough for this evaluation. This is illustrated in Fig. 16, where the reference watermark from the left corner (1/9 of image size) of the scanned image area is evaluated for reference information. The attacked image has also a text “Robustness” laid on top of the watermarked image, to simulate local distortion. Portion of the text shows in Fig. 16 A at the bottom. The reference information is still good enough for estimating rotation and scaling parameters, despite the block division error, and even the inserted text on top of the image.

Different methods are proposed to achieve robustness for both synchronization and message information. In Paper III, the information is embedded using a perceptual model similarly as in Paper II. Print-scan process causes more distortion in highly textured image areas, and experiments showed that a suitable set of parameters can be found to compensate the phenomenon. A linear relationship between $\lambda_1$ and the average gradient magnitude in blocks of

![Encoding table:](image)

<table>
<thead>
<tr>
<th>Code</th>
<th>Angle</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>$90^\circ$</td>
</tr>
<tr>
<td>001</td>
<td>$22.5^\circ$</td>
</tr>
<tr>
<td>010</td>
<td>$45^\circ$</td>
</tr>
<tr>
<td>011</td>
<td>$66.5^\circ$</td>
</tr>
<tr>
<td>100</td>
<td>$90^\circ$</td>
</tr>
<tr>
<td>101</td>
<td>$112.5^\circ$</td>
</tr>
<tr>
<td>111</td>
<td>$135^\circ$</td>
</tr>
</tbody>
</table>

Fig. 15. Message encoding. (III.) Copyright© 2010 Elsevier. Reprinted with permission.
size 16×16 is used as explained in Paper III. Accordingly, instead of fixed $\lambda_1$, more watermark strength is placed on textured areas of images.

In extraction a grid image $G'_{\mathbf{u}, \mathbf{v}}$ is calculated as follows:

$$G'_{\mathbf{u}, \mathbf{v}} = \begin{cases} 1, & \text{when } M(\mathbf{u}, \mathbf{v}) \times R_{\phi, \psi}''(\mathbf{u}, \mathbf{v}) \geq \gamma \\ 0, & \text{when } M(\mathbf{u}, \mathbf{v}) \times R_{\phi, \psi}''(\mathbf{u}, \mathbf{v}) < \gamma \end{cases}$$ (32)

where $M(\mathbf{u}, \mathbf{v})$ denotes a masking operation and $\gamma$ is a threshold. For masking, a circular mask is used (See Fig. 16B). The central area of the autocorrelation is the noisiest area, and masked out. Thresholding is adaptive, to ensure robustness from a varying image area. It takes advantage of the fast operation of bare calculation of the number of peaks to give a rough estimate of the threshold $\bar{\gamma}$. Then, the iterative call of Hough transform is used to find such a $\gamma$ that there are enough peaks for detecting lines exceeding a predetermined length. This way, also the accuracy of angle detection (rotation estimation) from lines is preserved.
In the experiments, both the embedding and extraction parameters were fixed. The angle detection accuracy and precision were measured with the Lena image, using two printers and paper material, with a varying background of the image. The test indicated the capacity of 6 bits/block, with the chosen parameters. A larger set of experiments was realized on 16 color images (512×512). In tests, the boundaries for robust extraction were searched through increasing distortion while extraction finally fails. As an example of the results, performance boundaries for five famous test images are shown in Table 5 in the case when 6 bits/block are embedded.

Table 5. Limits for robust message extraction (6 bits/block).

<table>
<thead>
<tr>
<th>Image</th>
<th>PSNR (dB)</th>
<th>PS+ rot(°)</th>
<th>PS+ crop(%)</th>
<th>PS+ AR change</th>
<th>PS+ x_shear</th>
<th>PS+ y_shear</th>
<th>JPEG QF</th>
<th>PS+ trans</th>
<th>PS+ scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splash</td>
<td>35.6</td>
<td>20</td>
<td>8</td>
<td>1.0.98</td>
<td>2</td>
<td>2</td>
<td>90</td>
<td>10</td>
<td>68</td>
</tr>
<tr>
<td>Tiffany</td>
<td>36.9</td>
<td>20</td>
<td>20</td>
<td>1.0.98</td>
<td>2</td>
<td>1</td>
<td>95</td>
<td>8</td>
<td>68</td>
</tr>
<tr>
<td>Mandril</td>
<td>29.9</td>
<td>6</td>
<td>6</td>
<td>1.0.98</td>
<td>1</td>
<td>2</td>
<td>90</td>
<td>6</td>
<td>85</td>
</tr>
<tr>
<td>Lena</td>
<td>35.1</td>
<td>14</td>
<td>14</td>
<td>1.0.99</td>
<td>1</td>
<td>0.8</td>
<td>95</td>
<td>5</td>
<td>75</td>
</tr>
<tr>
<td>Peppers</td>
<td>34.6</td>
<td>16</td>
<td>8</td>
<td>1.0.98</td>
<td>2</td>
<td>2</td>
<td>90</td>
<td>5</td>
<td>68</td>
</tr>
</tbody>
</table>

Tests also indicated that non-uniform attacks like Stirmark random bending distort the image so that angle detection accuracy decreases, and consequently, capacity decreases. For illustration, in Fig. 17 are presented performance limits and capacity for an example image against uniform attacks, rotation and cropping, as well as for non-uniform attacks, x_shear and y_shear, aspect ratio change and Stirmark random bending.

The method extends the usage of a periodic pattern to carry a multibit message. Also, due to coding of the message as the direction of the periodic pattern, the additional synchronization search caused by translation and cropping can be avoided. Consequently, there is no need to use exhaustive search algorithms or edge detection. The experiments with two printers, two printout materials, and several background variations, had no significant effect on performance. The proposed method was shown to be effective on a compound effect of a fair amount of rotation, translation, cropping, and other distortions on geometry combined with a print-scan attack. Depending on the severity of the distortions, the capacity of 32 bits to 48 bits was achieved.
Fig. 17. Images attacked with print-scan combined with an additional attack. The first row shows a 40 bit message and the last row a 32 bit message. In all cases, the message is extracted without errors.

3.4 Value adding application with the aid of a mobile phone camera

When the study of print-scan resilient methods started, around 2000, also the somewhat magical idea of bridging print media to the Internet with watermarking was first mentioned. Since that time, these linking applications have been often listed as a possible watermarking application. However, although it is quite easy to imagine a vast amount of possible uses, the development of methods which withstand the technical and practical problems have been slow. The disturbance due to printing and capture process is high, the context may cause troubles as the image does not exist in a white background. Most importantly, there is a human using the mobile phone, so the method should withstand some degree of freedom when taking the picture, as shown in Fig. 18A. In Paper IV, autocorrelation and a directed periodic pattern based watermarking method robust to print-cam process is presented and evaluated. Also the algorithm is used to develop a linking application where the watermarked image in a wall poster acts as a link to a website. In addition to directing the user to the right web address, the non-
watermarked and watermarked images can be distinguished, which is important in a practical application. The usage scenario is presented in Fig. 18.

Fig. 18. Interactive poster usage scenario.

The embedding method is subtractive-additive, where the embedded message is first error coded and Gray coded. The cause of projective distortion is that the message may be misinterpreted, and this two-level coding increases the robustness to the tilt of the camera. In the embedding side, the host image is first preprocessed using the equation

\[
I_{\text{pre}}(x,y) = \begin{cases} 
I_{\text{wiener}}(x,y), & \text{when } r(x,y) = 1 \text{ and } (I(x,y) - I_{\text{wiener}}(x,y)) > 0, \\
I(x,y), & \text{otherwise}
\end{cases}
\]  

(33)

where \(I_{\text{wiener}}(x,y)\) is Wiener-filtered image and \(r\) is a matrix with uniformly distributed values of 0,1 with a probability(1) + probability(0) = 1. The calculated \(I_{\text{wiener}}(x,y)\) for images tends to be substantial in very textured image areas, which with a purely addition based watermark embedding approach will cause disturbance in watermark extraction. With preprocessing, the effect of the host image is anticipated and partly reduced.

In addition to using noise reduction, more robustness is attained with a modified JND-model where the distortion due to print-cam process is taken into account. With a modified JND-model watermark, embedding strength is enhanced along the details of the image. Additionally, the embedding has a way to adjust strength of the watermark in flat regions versus in textured regions by parameter \(\delta_1\) and \(\delta_2\)

\[
Y(x,y) = X(x,y) + \delta_1 \ast JND(x,y) \ast W(x,y) \\
+ \delta_2 \ast (1 - JND(x,y)) \ast W(x,y)
\]  

(34)
where $W_i^{\theta}$ represents the coded information, $X_i$ is the preprocessed image and $Y_i$ the watermarked block of the image.

Print-cam involves several distortions, caused by user interaction as well as the ones caused by the devices and air interface, which are taken into account in the watermark extraction algorithm design. Autocorrelation function of the Wiener estimate $\hat{W}(x,y)$, which is used for detecting the peak orientation is severely distorted and to enhance peak detection, rotationally symmetric Laplacian of Gaussian filtering operation is performed. The grid image $G(u,v)$ is attained without iterative thresholding to reduce computational complexity, which is important in mobile applications. As before, masking is used and additionally morphological operation is employed to reshape the peaks as explained in Paper IV.

The message extraction process is preceded with watermark detection. The reference block of the watermarked image contains a periodic pattern $W_{\theta}$, where $\theta = 0^\circ$. This can be efficiently taken advantage of to determine if the image is watermarked. The extracted peak pattern should show properties, which appear as regularity when the peak structure is projected perpendicular to the angle of the pattern. The message extraction does not proceed from reference block evaluation, if the grid structure is not clear enough or when there is no watermark. The inequality is defined by

$$\sum_{i=1}^{P} p > a \sum_{i=1}^{P} p,$$

where $p$ holds peaks sorted by their size, $a = 0.7$ is an experimental threshold and $P$ is the total amount of peaks, determines if a watermark is present.

It is shown with various experiments that a multibit message can be robustly embedded and extracted from an image captured with a mobile phone camera. In tests, five images were chosen, which form the interactive elements in the final demonstration prototype of an interactive poster. The method was proven to be robust to systematical distortions related to the devices (printer, mobile phone camera), JPEG compression, for a fair amount of geometric distortions such as perspective distortion, cropping or change of distance of the camera. In Fig. 19, is shown the best shooting range (12–24 cm) for robust extraction, when each block contains four bits of data and the strength of watermark in equation 34 is $\delta_1 = 60$ and $\delta_2 = 6$. 

77
The effect of tilting was inspected through tests, where perspective distortions were simulated for a perpendicularly taken image from the distance of 18 cm (Fig. 19B). The experiments included extraction from images in a white background with two strengths $\delta_1 = 60$, $\delta_2 = 6$ and $\delta_1 = 50$, $\delta_2 = 5$ and also from a poster with strengths $\delta_1 = 60$, $\delta_2 = 6$. Average results in Table 6 show how much perspective distortion in degrees the method is robust for.

**Table 6. The average of the robustness in degrees to the tilt of the images.**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Tilt backward</th>
<th>Tilt forward</th>
<th>Tilt left</th>
<th>Tilt right</th>
</tr>
</thead>
<tbody>
<tr>
<td>50,5,18 cm</td>
<td>7.6°</td>
<td>7.2°</td>
<td>9.2°</td>
<td>8.8°</td>
</tr>
<tr>
<td>60,6, 18 cm</td>
<td>12°</td>
<td>12°</td>
<td>16.2°</td>
<td>10.5°</td>
</tr>
<tr>
<td>60,6, 18 cm poster</td>
<td>16°</td>
<td>11.4°</td>
<td>17.8°</td>
<td>15.8°</td>
</tr>
</tbody>
</table>

The application prototype was tested with a group of fifteen actual users, who also evaluated the quality of the watermarked images subjectively. Accordingly, using SDG (Subjective Difference Grade) measures, derived from ITU (2003), the image quality was rated sufficient, with $0.1 < \text{SDG} < 0.9$ for all of the images. The robustness experiments with real users showed that the largest individual problem in extracting a watermark, was the focusing problems with an unfamiliar mobile phone camera. Otherwise, it was noticed that the algorithm can handle a reasonable amount of distortions caused by the human taking the picture freehandedly.

The objective of the work was a robust algorithm, where visible frames are not used, and the algorithm developed turned out to be robust to background variation and insertion of additional objects, like logos on top of images; in other words, using the watermarked images naturally as they are used in print media in real life seems possible. Tests indicated success also in this sense. Algorithm was
functioning well with two phone models. The experiment has shown that the image resolution, as well as other camera properties has an impact on performance.

### 3.5 Content identification with feature point based synchronization

Once a hardcopy of the image is produced, the metadata included in any header files is lost permanently, including header information that would be used for identifying the content. Such content identification applications have been of growing interest in the watermarking community. The potentiality in relation to being able to communicate where the image comes from, where to attain further details, or even to authenticate the image, can be seen. For these purposes, watermarks can be encrypted and secured so that only authorized reading devices can detect and access the data.

As well as print-scan attack effects on watermark detection/message decoding, print-scan also deteriorates feature point detection. So although the second generation watermarking seems as a logical choice to resolve the synchronization problem, applying it is not straightforward. In Paper V, a method basing synchronization on feature detection is presented. Watermarks can be extracted with a correct key from printed and scanned images, also when the image has undergone some other changes in geometry. Experiments show that the method provides a robust and blind extraction of information for an authorized reader after a print-scan attack and a set of compound attacks.

In the first iteration, the information about the orientation of the feature points is embedded. Then, a multibit message which has been broken to fixed length segments is embedded iteratively one segment at a time. The steps to embed information are as follows:

1. Use convex polygon to tile the image to \( k \) non-overlapping areas.
2. Use Delauney tessellation to divide polygonal areas into triangles.
3. Use random permutation to select a set of triangles to be watermarked.
4. Detect feature points.

For feature detection, Harris detector (Equation 10) is used as a basis. The two “best” features will be used to build a coordinate system. The objectives related to the watermarking method are that the feature detection is robust to print-scan operation and criteria for how to select the features exist. A
robustness descriptor $Rob$ is determined to measure the robustness of the feature points as

$$Rob = \frac{\sum_{i \in \textbf{R}} R_i}{\max(R)}$$

(36)

where response $R_i$ is the Harris response in Level $i$, where each level simulates different scale and contrast conditions. Simultaneous operations as explained in paper V are used for reducing computation complexity. The calculated robustness descriptor $Rob$ gives a measure of the robustness: features which give a strong response in a small neighborhood in normalized image scale and have a long lifetime in scale-contrast-space have a strong value of $Rob$.

5. Represent the watermark location in the coordinates system.

The location of the watermark is defined in a coordinate system defined by two best features. Criteria are based on the $Rob$ value, as well as to distance between points. The coordinates of the permuted triangles are calculated through Helmert transformation as

$$
\begin{bmatrix}
X' \\
Y'
\end{bmatrix} = \mu \begin{bmatrix}
\cos \theta_f & -\sin \theta_f \\
\sin \theta_f & \cos \theta_f
\end{bmatrix} \begin{bmatrix}
X \\
Y
\end{bmatrix} + C,
$$

(37)

where $\mu$ is the scale factor, and $\theta_f$ is the angle that a line drawn through the feature points forms with x-axis. This process is illustrated in Fig. 20. Location of the watermark segments in the new coordinate frame is stored in a secret key.
6. Embed one segment of the watermark.

   The watermark is embedded in triangles with

   \[
   Y_i^*(x,y) = X_i(x,y) + \lambda_i JND(x,y, W_{j}^{(0)},\phi(x,y)),
   \]

   where the \( W_{j}^{(0)} \) represents the coded information, \( X_i \) is the corresponding area in the preprocessed image and \( Y_i \) the watermarked triangle of the image. For preprocessing, Wiener filtering (Equation 33) is used. The periodicity \( N_i \) in \( W_i \) is determined adaptively, in order to make unauthorized peak estimation difficult. Periodicity is defined with the maximum radius of the incircle of Delauney tessellation triangles by

   \[
   N_i > \frac{2A}{a + b + c},
   \]

   where \( A \) is the area of the triangle, and \( a, b \) and \( c \) are the lengths of the sides.

In print-scan process, geometric distortions cannot be avoided. In Paper V, the property that feature points move along with the geometric distortions is taken advantage of to synchronize the extraction of the watermark. However, the inaccuracy of location of the feature points, as well the effect of the print-scan
process to Harris feature point detector is paid attention to. Steps to extract information are the following:

1. Feature points are detected using a similar method as during embedding.
2. Built up a coordinates system defined by two best features.
   Criteria are based on the Rob value, as well as to the distance between points.
3. Locate the watermark.
   The secret key identifies the location of the watermark from which the information can be extracted. This is illustrated in Fig. 21A.
4. Assemble the polygon from the triangles.
   As the information is scattered, the extraction process involves assembling process. This is illustrated in Fig. 21B. Assembling the polygonal area \( \tilde{W}_k(x, y) \) from triangular areas \( \tilde{W}_j(x, y) \) is realized on the Wiener estimate \( \tilde{W}(x, y) \) of the whole attacked image. Autocorrelation, filtering and masked thresholding reveal a peak structure to be examined. Here, masking, which reduces noise bases itself similarly in geometrical properties as the adaptive periodicity \( N_1 \) in \( W_j \) during embedding. The same equation 39 as during embedding is utilized. Morphological shaping furthermore reshapes the grid structure to radius one disks, which increases robustness (accuracy of the angle detection) from the peak alignment.
5. Ensure the correctness of the feature pair.

In the first iteration, the extraction algorithm ensures that the feature point pair is the correct one, with interplay with watermarking. This is illustrated in Fig. 22.

6. Proceed to extract the whole message.

After finding the correct feature pair, the extraction iteratively proceeds to extract one segment of the information at a time, which completes the extraction process.

In the experiments, a variety of compound attacks together with print-scan process was tested, to find the performance limits for the developed feature based watermarking technique. Altogether sixteen images were used in tests. The image test set was identical to the test set used in Paper III. As an example of the encouraging results, in Table 7 is given an insert of the test results. For the five well known test images, the number of correctly retrieved bits for a 32 bit message is presented.
In tests, the robustness for extraction against print-scan attack and print-scan attack combined with an additional attack were tested. Tests indicated that generally a 32 bit message can be extracted without errors under a variety of attacks. Previously proposed content based watermarking methods are vulnerable to even small changes in aspect ratio. An encouraging result was that using the proposed method, the message also withstands print-scan combined with a small amount of aspect ratio change. From images, the Baboon image with highly textured areas was more vulnerable to combined attacks.

Table 7. Robustness to attacks with 32 message (PS = print-scan).

<table>
<thead>
<tr>
<th>Image</th>
<th>PS &amp; rot 10°</th>
<th>PS &amp; rot 260°</th>
<th>PS &amp; trans 5%</th>
<th>PS &amp; crop I 7%</th>
<th>PS &amp; crop II</th>
<th>PS &amp; scale x = 1.1, y = 1.1</th>
<th>PS &amp; AR x = 0.98, y = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splash</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
</tr>
<tr>
<td>Tiffany</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
</tr>
<tr>
<td>Baboon</td>
<td>32/32</td>
<td>24/32</td>
<td>28/32</td>
<td>28/32</td>
<td>28/32</td>
<td>28/32</td>
<td>24/32</td>
</tr>
<tr>
<td>Lena</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
</tr>
<tr>
<td>Pepper</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
<td>32/32</td>
</tr>
</tbody>
</table>

Additional tests included the effect of expanding the message length to 40 bits and examined the execution time. A variety of combined attacks were tested
which showed how effective preprocessing can improve robustness for images with highly textured areas or images with large areas of bright or dark intensities.

In Paper V, a robust feature point pair is used to form a coordinate system. Watermark information is scattered to the image and the location is stored with a key represented in the formed coordinate system. In the extraction, the robustness is ensured through interplay with watermarking and feature point extraction. An authorized user with a key can access the eight number code protected from errors with a checksum from a printout with a fair computation time using a standard workstation tested with an Intel Pentium 2.66 GHz processor: average of 27.2 seconds.
4 Discussion

In the beginning of this thesis, a question was set: “How to realize a watermarking method robust to synchronization error in printed image applications?” In the thesis, especially the following sub-problems were considered:

1. What kind of methods can be used to ensure robust watermarking against low-pass type attacks, and especially robust extraction from a printout?
2. How to ensure robustness of the synchronization?
3. How to embed a multibit watermark robust to extraction from printout?
4. How to meet application specific demands; robust and secure identification with a scanner/secondly value adding application with the aid of a mobile phone camera?

One of the essentials is the robustness of the actual watermark message against low-pass type attacks and especially to print-scan or print-cam operations. Methods to increase watermark extraction robustness with perceptual weighting was suggested. Paper I presents a spatial spread spectrum method with perceptual shaping, which improves watermark robustness against compression attack without causing visible distortions. The model is furthermore utilized in Papers II, III, IV and V, all of which consider specially message extraction from a printout. Depending on the case, print-scan or print-cam, perceptual shaping is further fine-tuned by taking into account the low pass type distortions caused by the devices, affecting the details of the images. In Paper II, is further considered how to share the available JND between a synchronization watermark and the actual message watermark.

To be able to extract the watermark, the watermark reading process has to be properly synchronized. Methods to robustly synchronize the extraction of a multibit message from a printout were suggested. In Paper II, a multilevel approach is taken. Due to efficient JND usage and filtering and noise reduction methods, the synchronization template is robust to print-scan operation. Accordingly, estimates for RST parameters make possible message extraction after inverting affine transformation. In Paper III, only a portion of the image is used for synchronization purposes. Several techniques, such as adaptive thresholding, are suggested to improve robustness. Similarly in Paper IV, a portion of the image is used for detecting whether the image is watermarked or not, and for reference information about the orientation of the image. In Paper V,
image features are used to build up a coordinate system, and the location of the watermark is tight with this coordinate system. As a consequence, message extraction is possible after geometrical attacks and print scan attack.

It was seen that there was a need of a method, which withholds some inaccuracies during inversion, or does not necessarily need an inversion process at all. A method to encode a multibit message utilizing directed periodic patterns and a method to decode the message after attacks was developed. The developed method, in Paper III, takes advantage of the autocorrelation properties of periodic patterns and encodes the multibit information in the angle information of the periodic pattern. In Paper IV, it was also shown that, with the necessary modifications due to the strong signal distortion, the method is workable also in the presence of perspective distortions.

In Paper IV, a linking application, a demonstrator of an interactive poster, was developed and tested with real users. A watermark in a printout is used to direct the user of a mobile phone to some specific web address. The security requirement is nonexistent as the watermark is useful for the users. Nevertheless, the robustness requirement is very high in order to get acceptance from the users.

In printing, all metadata associated to the images will be lost, so identifying the owner or source or otherwise identifying content using associated information will be difficult. Watermarking offers a potential alternative to digital signatures (fingerprinting) for content identification. An embedded watermark can uniquely identify each specific item or instance of content. A key based robust and secure identification method from printout was developed. The method in Paper V relies on an image features based coordinate system. Location of the watermark is stored on a key, which has to be available in order to read the embedded number code and checksum.

Overall, a set of algorithm level methods to overcome the problems related to watermarking printouts were introduced and verified. Examples in Fig. 23 represent cases where a watermark was correctly extracted. The human factor, namely, the fact that there is a person scanning or taking the picture, shows in the example images, as well as the impact of additional elements like logos and background. These are examples of practical problems that an application should withstand to get wider interest, both from the industry and from the actual users.

Paper II proposes a multilevel watermarking method. When considering performance against the state of the art, similarly as the other template based methods proposed simultaneously or before the year 2006, the method is not robust to cropping. Still, it gives a good ground for how to improve robustness of
a synchronization template and how to expand the properties of a watermarking algorithm against a print-scan attack using a multilevel approach.

Fig. 23. Upper row; example images captured with a scanner. Lower row; example images captured with a mobile phone camera.

Most of the print-scan resilient watermarking methods have restrictions on robustness to RSTC attacks. The method in Paper III is proven to be robust to a combined attack of print-scan and a moderate attack on geometry, which is an improvement over the state of the art. The clear advantage of the presented message coding with periodic patterns is furthermore shown in Paper IV, where distortions are even more severe and geometric distortions are in three dimensions.

Watermarking algorithms can be compared also from the application viewpoint. Then, also application specific requirements must naturally be considered. In Paper V, the analysis of distortions caused by printing and scanning process is accompanied by offering methods to make the embedded data confidential. In the case of autocorrelation based methods, the embedded template, as well as the message encoded, as suggested in Paper III, can be easily estimated from regularities in the autocorrelation. Similarly, all template based methods are vulnerable to estimation. For securing the watermark extraction process, the location of the watermark information is tight to the coordinate frame derived
from image features. Accordingly, the key for reading is unique for each image. Using triangular areas from which watermark information is gathered through composition process, makes attempts to unauthorized estimation of regularities difficult. The approach adds up some complexity, but is a necessary step to secure the multibit watermark information in a content identification application. The approach in Paper V does not give answers for how to maintain a key database, which would be necessary for a practical application. The issue is however, superficially covered also in the state-of-the-art watermarking literature. Malicious attacks, trying to destroy the watermark, are not considered, as in the application, the content is no more in a digital format.

Content identification with watermarking has some compelling approaches, from which the basic properties of watermarking, digital fingerprints and visible codes are compared in Table 8. From the table, it can be seen that the ability to distinguish between different instances of the same original content, as well as an ability to directly embed some extrinsic data are the most important advantages of the watermarking approach. Digital fingerprints do not change the content, which is their most important advantage. (Digimarc 2010). In all approaches, robustness is highly dependent on the choice of algorithms, and as such, hard to compare. Nevertheless, intuitively, visible information is easier to interpret.

Table 8. Properties of compelling techniques.

<table>
<thead>
<tr>
<th>Method</th>
<th>Visibility</th>
<th>Capacity</th>
<th>Payload</th>
<th>Content identification</th>
<th>Linking application</th>
<th>Database connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watermarking</td>
<td>Invisible</td>
<td>Low-medium</td>
<td>Contains extrinsic data</td>
<td>Can distinguish between different instances of the same original content</td>
<td>Freedom of design</td>
<td>Not necessary</td>
</tr>
<tr>
<td>Digital fingerprints</td>
<td>Invisible</td>
<td>Carries no additional data</td>
<td>Derived from content</td>
<td>Are the same for all instances of the same content</td>
<td>Freedom of design</td>
<td>Needed</td>
</tr>
<tr>
<td>Barcodes, QR codes etc</td>
<td>Visible</td>
<td>Highest</td>
<td>Contains extrinsic data</td>
<td>Not tight to the content itself</td>
<td>Requires a certain area in the print</td>
<td>Not necessary</td>
</tr>
</tbody>
</table>

In linking applications, similarly, all of the methods presented in Table 8 are feasible. The main distinguishing factor between QR codes, watermarking and digital fingerprints is that the database search is not necessary with watermarking
and QR codes. In the linking application context, usage of QR codes must be considered in the overall print layout design, which can be restrictive in the sense of design freedom. A practical example of an application integrating different techniques for interaction is Digimarc’s Discover (Digimarc 2012), an application with which interactive magazine content can be created and used with a mobile phone application. In Paper IV, the watermark payload is an extrinsic multibit message. The clear advantage of the algorithm is its robustness to tilt, addition of for example logos on top of watermarked images, and extraction of the message without the need of a frame, original image or the embedded message, all of which give design freedom for usage in different applications.
5 Summary

Commonly, in the literature, print-scan has been considered as an individual attack and experiments are restricted to images printed on a white background. In this thesis, robustness of the synchronization/message extraction to print-scan process, as well to combined attacks is considered. High robustness to a variety of attacks on geometry combined with print-scan process is proven. Also, a method to secure the watermarking process, particularly in print-scan process, so that only authorized reading devices can detect and access the data is presented.

Similarly, the scientific literature covering print-cam resilient watermarking algorithms is narrow. Only a few methods have been proposed and most of them utilize a visible frame around the image. Although a frame can indeed be an indicator of the presence of additional information for the user, it still is quite restrictive in an aesthetic/application sense.

In this thesis, an effort was put on development of a method, where frame information is not needed and which allows to the user some flexibility in how the camera is placed relative to the printout considering tilt, cropping and distance. The emphasis was on robustness on print-scan and print-cam processes while maintaining visual quality. With concentration on blind, multibit methods, the aim was to push the technology forward so that neither original image nor the embedded watermark is needed for extraction. Such self-contained images can facilitate the creation of new innovative watermarking applications and ease the management of content. Innovative new methods for multibit message embedding were suggested and verified.

The goal of this thesis was to bring forward problems related to print-scan and print-cam resilient watermarking. In designing watermarking applications, the algorithm developer always struggles with conflicting requirements of capacity, robustness and imperceptuality. In mobile phone applications, an additional struggle comes from algorithm complexity. In this sense, the fast development of the phones and their processing power will aid the acceptance of more robust algorithms. As far as capacity is concerned, the application will dictate the number of needed bits. Nevertheless, capacity analysis and optimization remains an interesting future research question.

Currently, the research of image watermarking applications, where the watermarked images appear in a printed format, has been restricted to flat surfaces. Nevertheless, printed images are also used in various other contexts than magazines or posters. The robustness of the developed algorithms indicates
potentiality of usage also in somewhat curved surfaces, which could widen the scope of possible application areas.
References


List of original publications


Reprinted with permission from IWDW2002 organizing committee (I), Springer (II, IV) and Elsevier (III, V).

Original publications are not included in the electronic version of the dissertation.


428. Landaburu-Aguirre, Junkal (2012) Micellar-enhanced ultrafiltration for the removal of heavy metals from phosphorous-rich wastewaters: From end-of-pipe to clean technology


432. Wang, Meng (2012) Polymer integrated Young interferometers for label-free biosensing applications


436. Ossiannilsson, Ebba (2012) Benchmarking e-learning in higher education: Lessons learned from international projects

437. Pouttu, Ari (2012) Performance Analysis of mMCSK-mMFSK modulation variants with comparative discussion

438. Kupiainen, Laura (2012) Dilute acid catalysed hydrolysis of cellulose—extension to formic acid


Book orders:
Granum: Virtual book store
http://granum.uta.fi/granum/
Anja Keskinarkaus

DIGITAL WATERMARKING TECHNIQUES FOR PRINTED IMAGES