

Anu Pramila

READING WATERMARKS WITH A CAMERA PHONE FROM PRINTED IMAGES

UNIVERSITY OF OULU GRADUATE SCHOOL;
UNIVERSITY OF OULU,
FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING;
INFOTECH OULU



ACTA UNIVERSITATIS OULUENSIS
C Technica 644

ANU PRAMILA

**READING WATERMARKS WITH
A CAMERA PHONE FROM 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 IT116, Linnanmaa, on 23 February 2018, at 12 noon

UNIVERSITY OF OULU, OULU 2018

Copyright © 2018
Acta Univ. Oul. C 644, 2018

Supervised by
Professor Tapio Seppänen

Reviewed by
Professor Jiyang Zhao
Professor Andreas Uhl

Opponent
Associate Professor Joni Kämäräinen

ISBN 978-952-62-1804-5 (Paperback)
ISBN 978-952-62-1805-2 (PDF)

ISSN 0355-3213 (Printed)
ISSN 1796-2226 (Online)

Cover Design
Raimo Ahonen

JUVENES PRINT
TAMPERE 2018

Pramila, Anu, Reading watermarks with a camera phone from printed images.

University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering; Infotech Oulu

Acta Univ. Oul. C 644, 2018

University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

There are many reasons for sharing a photo of a printout. The intention might be to copy the image for personal use or experience an interesting ad with friends. With watermarking, the images can also carry side information and with specialized watermarking methods the information can be read with a mobile device camera.

In digital image watermarking, information is hidden on an image in such a way that a computer can read the hidden information but a human cannot discern it. The aim of this thesis is to research the process in which the watermarked image is printed and then read with a digital camera or a camera phone from the printed image. In order to survive the process, the watermark must survive multiple attacks. Some of the attacks occur during printing as the image is halftoned, others when the image is recaptured with a camera, in which case the camera might be rotated around multiple axis. These attacks may cause a loss of synchronization of the watermark and make the extraction impossible.

The main objective of the thesis is thus to develop methods that are robust to the printing and capturing process, especially for the situations when the capturing angle is large. This problem contains the circumstances in which the synchronization is lost and the camera lens is not focused properly.

In this work, research on digital image watermarking, computational photography and mobile phones are combined. The contributions of this thesis lie in two main parts: First, two print-cam robust methods are proposed, one based on a frame and the other on autocorrelation for synchronization. These two are then used as a basis for an algorithm that recovers the watermark even after camera rotation and image blurring caused by the narrow depth of focus of the lens. The algorithm is later refined and implemented for a mobile phone. The results show that the method is highly robust to capturing the watermark without errors in angles up to 60° with processing times acceptable for real-life applications.

Keywords: all-in-focus imaging, digital image watermarking, focal stack optimization, print-cam, print-photo, print-scan, watermark robustness, watermark synchronization

Pramila, Anu, Vesileimojen lukeminen tulostetuista kuvista käyttäen puhelimen kameraa.

Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähkötekniikan tiedekunta; Infotech Oulu

Acta Univ. Oul. C 644, 2018

Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

Tiivistelmä

On olemassa useita syitä tulosteesta otetun valokuvan jakamiseen. Aikomuksena voi olla kopioida kuva omaan käyttöön tai jakaa mielenkiintoinen ilmoitus ystävien kanssa. Vesileimauksessa kuvaan voidaan sijoittaa lisätietoa ja erityisillä menetelmillä tieto voidaan myöhemmin lukea mobiililaitteen kameralla.

Digitaalisten kuvien vesileimauksen tavoite on piilottaa tietoa kuvaan siten, että tietokone pystyy lukemaan piilotetun informaation, siinä missä ihminen ei pysty sitä havaitsemaan. Tämän väitöskirjan tavoitteena on tutkia prosessia, missä vesileimattu kuva tulostetaan ja vesileimataan digitaalisella kameralla tai kamerapuhelimella tulosteesta. Selvytyäkseen tästä prosessista, vesileiman on kestävä useita hyökkäyksiä. Osa hyökkäyksistä esiintyy tulostuksen aikana, kun kuva rasteroidaan, ja osa valokuvatessa, jolloin kamera voi olla kiertynyt. Näiden hyökkäysten seurauksena vesileiman synkronointi voi kadota, jolloin vesileiman lukeminen ei enää onnistu.

Väitöskirjan päätavoitteena on siis kehittää tulostuksen ja valokuvauksen kestäviä vesileimausmenetelmiä erityisesti niitä tilanteita varten, jolloin kuvauskulma on suuri. Tämä ongelma sisältää olosuhteet, joissa synkronointi menetetään, ja kun kameran linssi ei ole kohdistunut oikein.

Työssä yhdistetään digitaalinen kuvien vesileimaus, laskennallinen valokuvaus ja matkapuhelimet. Tutkimus voidaan jakaa kahteen osa-alueeseen: Ensimmäisessä kehitetään kaksi tulostuksen ja valokuvauksen kestäväää menetelmää, joista toinen perustuu kehukseen ja toinen autokorrelaatioon synkronoinnin säilyttämiseksi. Toisessa osassa näitä menetelmiä hyödynnetään algoritmissa, joka kykenee vesileiman lukemiseen myös silloin kun kameran kiertymisen on voimakasta ja objektiivin kapea tarkennussyvyys aiheuttaa sumeita alueita kuvassa. Tutkimustyön lopussa tätä algoritmia viedään eteenpäin ja testataan matkapuhelinalustalla. Tulokset osoittavat menetelmän kestävän kameran kiertymistä 60°:seen saakka suoritusajoilla, jotka ovat hyväksyttäviä sovelluskäyttöön.

Asiasanat: all-in-focus -kuvantaminen, digitaalinen kuvan vesileimaus, focal stack optimointi, print-cam, print-scan, tulostus-valokuvaus, vesileiman kestävyys, vesileiman synkronointi

Aili-tädille

Acknowledgements

The work spanned the years 2007-2017 during which the research group changed its name and configuration. However, the important people stayed the same.

I would like to thank my supervisor, Professor Tapio Seppänen, for helping on each step of the thesis. I would also like to thank all those people working in MediaTeam Oulu research group back when I started my research. Not the least, for giving me a chance to delve into this interesting topic. I am also grateful for the personnel of Biosignal Processing Team for inspiring work conditions.

I also wish to thank Dr. Anja Keskinarkaus for the invaluable role on advising, co-operation and simply discussing the topic when needed. I still miss our Friday afternoon conference. I also own thanks to M.Sc. Angelos Fylakis for all the discussions, whether they were related to the research or not.

I would like to thank collectively the amazing people on our IRC channel. You helped not only in giving advice when needed but also in keeping everything in perspective. A thank you goes also to the bioteam coffee group. You taught me to drink alcohol and my resolve on never liking coffee is crumbling. You did well.

The work of official reviewers, Professor Andreas Uhl and Professor Jiying Zhao is gratefully acknowledged. In addition, I want to thank my follow-up group members Dr. Jukka Komulainen, Professor Guoying Zhao and Professor Vassilis Kostakos for their input.

I am grateful for financial support received from GETA graduate school, Finnish Cultural Foundation, Emil Aaltonen foundation, Walter Ahlström foundation, Kaute, Nokia foundation, Tauno Tönning foundation and Jenny and Antti Wihuri foundation.

I am eternally grateful for my parents and brother for all the support and everything they have done for me. Thank you. Finally, I wish to thank Valteri for being there for me and pushing me forward, even when I did not believe in myself. I also appreciate all my friends for giving me a glimpse of life outside the university. Your support means a lot.

Anu Pramila
Oulu, 2018

List of symbols and abbreviations

B	Binary sharpness map
δ_1, δ_2	Watermark strengths
f	f -values in diopters
\mathbf{F}	Frame detection filter
G, G_i	Gaussian kernel processed binary sharpness maps
\mathbf{H}	Scale matrix
I	Captured image
\hat{I}	Captured and scaled image
I'	Registered and blurred image
I_i	i th image on the focal stack
$JND(x,y)$	JND value at pixel (x,y)
k	Number of blocks
L	Laplacian of an image
N	Number of images in the focal stack
M	Number of images in the optimized focal stack
Q	Sharpness mask
r	A radius in Fourier domain
\hat{r}	An approximation of radius in Fourier domain
$\hat{\mathbf{R}}_j$	An approximation of the j th registration matrix
S	Sharpness map
σ	Standard deviation
$\hat{\mathbf{T}}$	An approximation of an transformation matrix for rectifying an image
θ	An angle
$\hat{\theta}$	An approximation of angle
X_i	i th block of an image
Y	Watermarked image
Y_i	i th block of an watermarked image
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
DA/AD	Digital to analog / analog to digital
DCT	Digital Cosine Transform

DFT	Digital Fourier Transform
DWT	Discrete Wavelet Transform
GHz	Gigahertz
HVS	Human Visual System
IMU	Inertial Measurement Unit
JND	Just Noticeable Difference
JPEG	Joint Photographic Experts Group
MHz	Megahertz
MP	Megapixel
MSSIM	Mean Structural Similarity
PSNR	Peak Signal to Noise Ratio
QR	Quick Response
RFID	Radio Frequency IDentification
RGB	Red, green, blue
RST	Rotation, scale and translation
SDG	Subjective difference grade
SIFT	Scale Invariant Feature Transform
TIFF	Tagged Image File Format
VGA	Video Graphics Array

List of original publications

This manuscript is based on the following articles, which are referred to in the text by their Roman numerals (I–V):

- I Pramila A, Keskinarkaus A & Seppänen T (2008) Multiple domain watermarking for print-scan and JPEG resilient data hiding. Proc. 6th International Workshop on Digital Watermarking (IWDW 2007), Guangzhou, China, Springer Berlin Heidelberg: 279-293.
- II Pramila A, Keskinarkaus A & Seppänen T (2008) Watermark robustness in the print-cam process. Proc. IASTED Signal Processing, Pattern Recognition, and Applications (SPPRA 2008), Innsbruck, Austria, ACTA Press Anaheim, CA, USA: 60-65.
- III Pramila A, Keskinarkaus A & Seppänen T (2012) Toward an interactive poster using digital watermarking and a mobile phone camera. Signal, Image and Video Processing 6(2): 211-222.
- IV Pramila A, Keskinarkaus A, Takala V & Seppänen T (2016) Extracting watermarks from printouts captured with wide angles using computational photography. Multimedia Tools and Applications. 75(15): 16063-16084.
- V Pramila A, Keskinarkaus A & Seppänen T (2018) Increasing the capturing angle in print-cam robust watermarking. Journal of Systems and Software 135: 205-215.

Contents

Abstract	
Tiivistelmä	
Acknowledgements	9
List of symbols and abbreviations	11
List of original publications	13
Contents	15
1 Introduction	17
1.1 Background	17
1.2 Research problem and objectives	18
1.3 Research scope and approach	20
1.4 Contributions and summary of original publications	22
2 Literature review	25
2.1 Digital image watermarking	25
2.2 Robust watermarking	27
2.2.1 RST robustness	27
2.2.2 Print-scan robustness	30
2.2.3 Print-cam robustness	33
2.2.4 The future of the print-cam robust watermarking	37
3 Research contributions	39
3.1 A print-scan robust watermarking method	39
3.2 Print-cam robust watermarking methods	45
3.2.1 A frame based method	46
3.2.2 A directed-grid based method	48
3.3 Focusing issues in print-cam robust watermarking	56
3.3.1 An approach based on computational photography	56
3.3.2 Toward faster implementation for camera phones	63
3.3.3 Execution times of the algorithms	66
4 Discussion	69
4.1 Significance of the results	69
4.2 Limitations and generalizability	70
5 Summary and conclusions	73
	15

References	75
Original publications	81

1 Introduction

1.1 Background

The topic of this research is to study digital image watermarking in the context of camera phones and printed media. In digital image watermarking, data is embedded in the image in such a way that a human cannot see the data but a computer can read it. The extraction of this hidden information with a camera phone is not yet thoroughly studied even though an efficient method could open multiple application areas from games and recreation to various security related fields such as authentication.

Smartphones are changing how we interact with the world and spend our time. It was reported in 2015 that 94% of the 16-45 year old Finnish people had a smartphone (Official Statistics of Finland 2015). Later, it was seen that 92% of the people under 45 years had used the internet on their mobile phone outside home or work (Official Statistics of Finland 2016). Evidently, phones are not only used for holding conversations but also accessing content online regardless of location.

One of the methods for narrowing the gap between the old analogue world and the new digital world are barcodes, as shown in Fig. 1. Possibly the most famous of these codes are QR (Quick Response) codes which were released in Japan in 1994 and gained publicity in the beginning of 2000 as mobile phones with QR code -reading feature were launched (Denso Wave n.d.). To the United States and other western markets, the QR codes arrived almost a decade later when the first applications for reading QR codes were released (Acofino 2009).



Fig. 1. Examples of using barcodes for commercial purposes (Images from Flickr.com by –Slavin, markguim and cote <https://www.flickr.com/photos/sash77/galleries/72157628971986707> CC BY 2.0)

Nowadays, the barcodes can be seen in games and newspaper adverts and they might be placed on top of packages of bread in order to persuade users to participate in various competitions. People are getting accustomed to using barcodes and mobile services initiated by them.

Watermarks relate to barcodes on the level of techniques. A simple form of a watermark could be viewed as an invisible barcode. The advantages of barcodes include high robustness: The barcode can be captured with a camera fairly carelessly and it works. However, they are eye-catching and easily removed, a fact that is not desirable in all applications, especially if any level of security is required.

Security and discretion are needed especially in healthcare technology, which is now the largest high technology area of export in Finland (Teknologiateollisuus 2016). In many health care applications, a lot of data is being stored and transferred constantly. Especially medical documents on paper are in danger of getting lost or damaged or even stolen. There is a need for strict security requirements as data must be protected, e.g., against attacks against integrity and tampering.

From an early stage on, watermarking has been designed to answer some of these demands. With watermarking, the additional information is carried within the content discreetly. Depending on the application, the watermark can be designed to be fully removable, so that the original data does not get disturbed, or that the data is corrupted if content is changed in any way. The technology is also highly transparent, meaning that it does not conflict with other security measurements, nor does it need any specific equipment of embedding or extraction, as is the case with, for example, RFID (Radio Frequency IDentification) tags. These properties make image watermarking suitable to be used as a connecting step between printed materials and camera phones.

1.2 Research problem and objectives

In this research, we look at the problem of reading hidden information, a watermark, from printed images, as illustrated in Fig. 2. In order to read the watermark from the printed image and to transform the information back in digital format, the image is scanned or photographed. We shall refer to the process of printing the watermarked image and then extracting the watermark with a scanner as the print-scan process. The process when the printed image is captured with a camera is referred to as the print-cam process. The words *extract* and *read* are used here interchangeably meaning the procedure of recovering the embedded information.

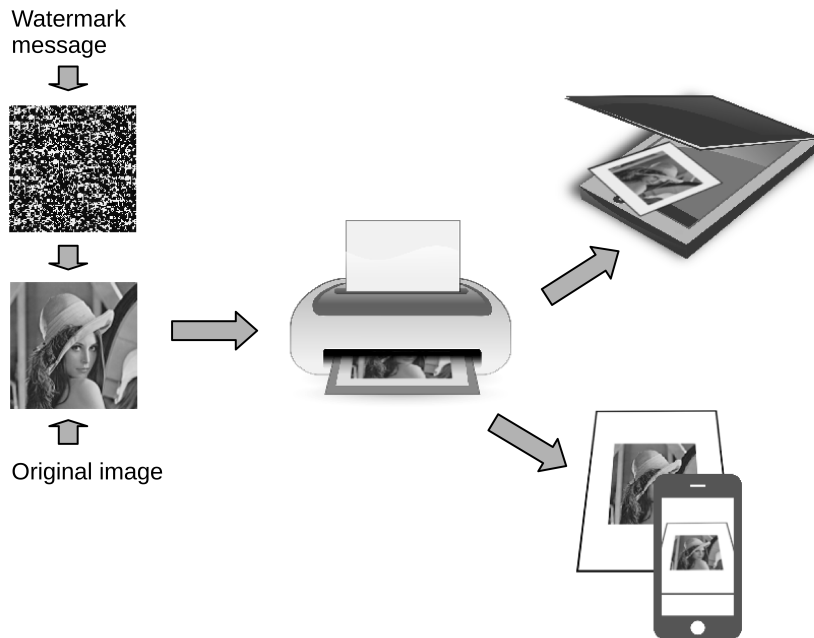


Fig. 2. The image is watermarked and the watermarked image printed. The watermark is read from the printed image with a scanner or a camera phone.

Most of the work about digital watermarking in the literature so far has focused on the images distributed electronically. Some research has been done on the print-scan robust watermarking systems, but few papers discuss the possible methods to read watermarks with a digital camera or a camera phone. Out of these methods, most are either too fragile or too visible for commercial use.

When an image is printed and scanned, the watermark must survive, not only digital to analog and analog to digital (DA/AD) transformation, but also rotation, scale and translation distortions due to the scanning. These still occur on a two-dimensional plane, but when the image is captured with a digital camera, the image might be rotated in three dimensions. All of these could lead to the synchronization of the watermark to be lost and to problems in extraction. In other words, the correspondence between the coordinates of the watermarked image and the embedded watermark could be lost. Image compression, paper quality, lens focusing issues and darkness of the surroundings might bring additional problems.

The main research question then follows as: *How to extract watermark information from a printed image with a hand held camera device when the capturing angle is highly variable?* The research focuses especially on the camera capturing process and the angle at which the image is captured. In most of the literature until now, the camera is placed perpendicularly to the printed image and the angle of capture has not been taken into account.

The main objective of the thesis is therefore to develop methods for print-cam robust watermarking when the capturing angle is large. This means solving not only the problem of synchronization of the watermark but also situations when the camera has not focused properly due to the large capturing angle. In short, the aim of the work is to introduce methods for increasingly robust extraction of the watermarks with hand held devices, surpassing those presented in the literature without sacrificing imperceptibility.

1.3 Research scope and approach

Generally, the research of watermarking is focused around three properties of the watermark: capacity, imperceptibility and robustness. Capacity is the amount of information that is possible to be embedded in the image with the given method, imperceptibility tells how visible the watermark is and robustness, in its turn, describes how well the watermark resists attacks. These properties depend heavily on the application and because the properties are conflicting to some extent, some trade-offs are unavoidable (Fig. 3).

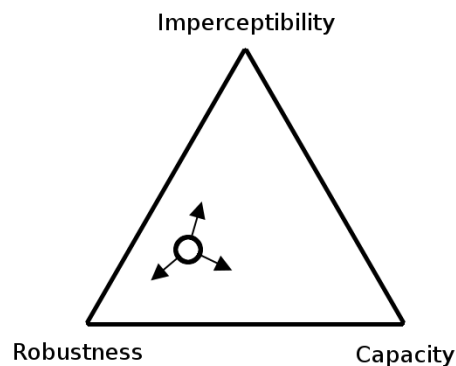


Fig. 3. The trade-off between imperceptibility, capacity and robustness.

The thesis focuses mostly on the robustness of the watermark and especially on the robustness against camera capture induced distortions. These include the robustness to rotations in three dimensions due to the varying angles of capture, lens focusing issues, and lens distortions. Some of these distortions occur because of human interaction. It is assumed here that the user has some knowledge of his/her camera phone but not about the technological aspects of watermarking.

Security, that is, how well the watermark survives malicious attacks, is not considered here. It is assumed that the user finds the watermarks to be beneficial and robustness against malicious attacks is left as a future work. Attacks to the physical object, such as ripping the image, are not considered either. The scope of the research is limited in natural color images only. The computer generated art is left outside the scope. All the data was generated for the research from the beginning as there were no databases available and simulations would not cover the scope of the problem.

A possible use case scenario is presented in Fig. 4, in which the watermark is extracted by capturing the image with a camera phone. This inflicts various distortions to the image and the watermark. Those need to be countered for successful watermark extraction.



Fig. 4. The watermark, here resembling a two-dimensional barcode, is embedded in the image which is then printed. The user can read the watermark with a camera phone and the content is shown according to the watermark information. Here, an augmented reality application is launched in which the application launches a view according to the watermark, in this case, an animation of a frog.

Fig. 5 illustrates the relationship of the original publications included in this thesis. To approach the problem, it makes sense to start with a simplified scenario, which in this case means scanning the image instead of using a camera, and later generalize the method. With this approach, it is possible to identify the main challenges in print-cam process and address them separately.

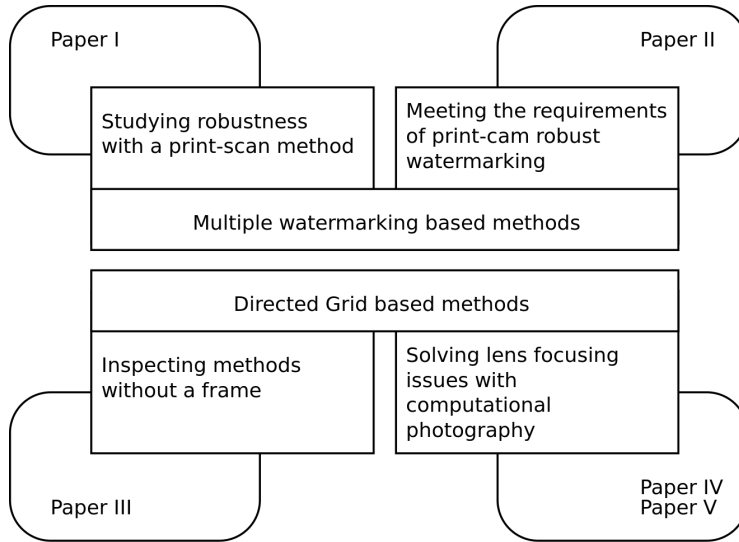


Fig. 5. The relationship between original publications.

1.4 Contributions and summary of original publications

As a pre-step towards the final goal of print-cam robustness, a print-scan robust watermarking method was developed in Paper I. The method was based on the concept of multiple watermarking and consisted of two watermarks for recovering synchronization after geometrical transformations and one watermark for carrying the message. One of the synchronization watermarks was used for inverting rotation and scale and the other was used for inverting translation. The method was then modified to meet the requirements of print-cam robustness in Paper II. A frame was placed around the watermarked image so that the geometrical distortions in three dimensions could be inverted. The rotation and scale inverting watermark was no longer needed, but the translation inverting watermark and the message watermark were utilized. In both of the papers, the author was responsible for algorithm design, development and testing. Dr. Keskinarkaus contributed to the message watermark design.

Because having a frame around the watermarked image is not always advantageous, a method based on autocorrelation was designed in Paper III. The method was a modification from a print-scan robust watermarking approach by Keskinarkaus *et al.* (2010). The modified method was ported on a mobile phone and a demonstration system was also presented in the paper. The algorithm design and testing were done jointly

with Dr. Keskinarkaus. The implementation of the embedding part was done by Dr. Keskinarkaus, whereas the design and implementation of the extraction part was done by the author. The implementations of the extraction part on a camera phone and a server were both done by the author.

For high usability, the designed methods should be robust and fast. The next paper, Paper IV, studied robustness and camera lens focusing the problem with the aid of computer vision. The capturing angle was increased until the narrow depth of view of the camera failed to keep the whole image in focus. The problem was solved with computational photography and the watermark extraction was shown to be robust. The method developed in Paper IV was enhanced in Paper V, in which also a camera phone implementation was presented. In both publications, the author was primarily responsible for the study design, development and implementation of algorithms and analysis of results. In Paper IV, M.Sc. Takala advised in the computer vision section.

The author was also the principal manuscript writer in papers I, II, IV and V. Paper III was written jointly with Dr. Keskinarkaus. Professor Tapio Seppänen contributed to all publications as a supervisor and participated in the revision of the manuscripts.

2 Literature review

This chapter will look into the literature surrounding the thesis. The first section introduces the digital image watermarking in general. Out of the three properties of a watermark, robustness, imperceptibility and capacity, the robustness is the most interesting one within the scope of this thesis. Hence, Section 2.1 investigates the general watermarking themes and the second section, Section 2.2, will look into robust watermarking methods in more detail.

2.1 Digital image watermarking

Digital watermarking can be seen as a sub-field of data hiding (Cox *et al.* 2002) although the definition is not exact. In contrast to (Cox *et al.* 2002), Hartung & Kutter (1999) defined steganography as a collection of techniques for secret communication and watermarking as techniques with an additional notion of robustness against attacks. They define data hiding as separate techniques in between steganography and watermarking.

Cox & Miller (2002) list various application areas for watermarking. Concerning this thesis, the most interesting is the "device control" which includes applications for linking "traditional media to the Web". This resembles the original application area throughout this thesis and thus it is justified to use the word *watermark* here.

The generic flow of the watermarking process as explained by Hartung & Kutter (1999) illustrated in Fig. 6. The watermark embedding process takes as an input an image, in which the watermark will be embedded, and the actual watermark. The input image is often called the host image or cover image. Some watermarking methods also take as an input a public or secret key, which is used in enforcing security. The watermark message can be any digital content, which is transformed into the actual watermark. As an output, the system creates the watermarked image.

The extraction process is an inverse of the embedding process. As an input, the process takes the watermarked image that has gone through an information channel and has possibly been attacked. Depending on the watermarking method, the process can also take as an input the key, the watermark or even the original unwatermarked image. In the latter case, the method is called non-blind in contrast to a blind method when the original image is not required. The output is the extracted watermark message or a confidence measure whether the watermark is present or not (Hartung & Kutter 1999).

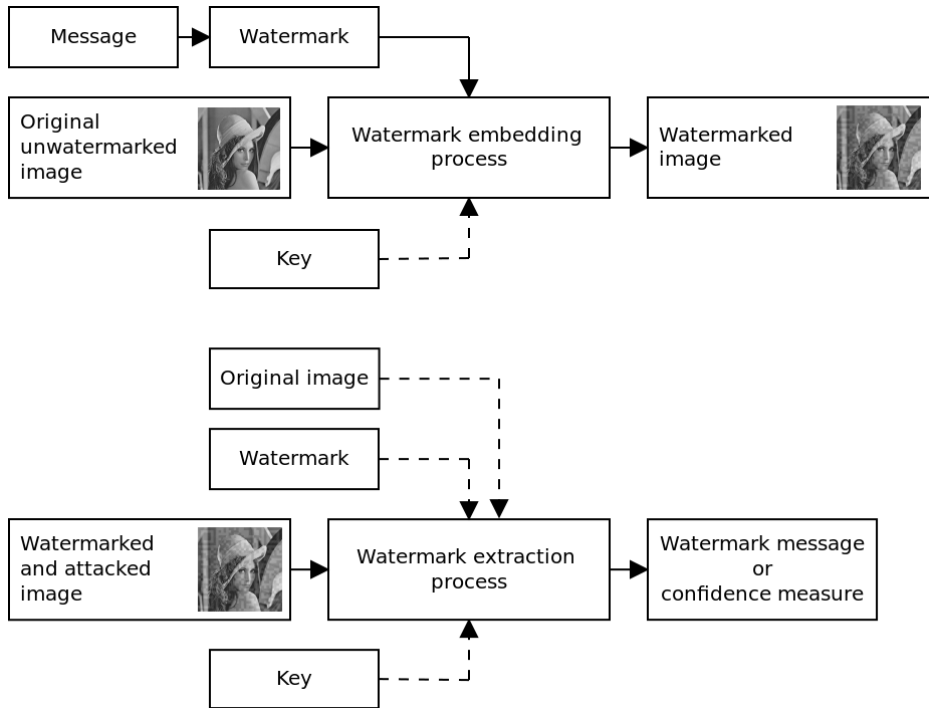


Fig. 6. The basic watermarking system.

Although watermarking was at first developed mostly for copy- and copyright protection (Hartung & Kutter 1999), it was quickly seen that copy- and copyright control might not be feasible with watermarking (Cox & Miller 2002). Since then, the field has moved away from the traditional application area of watermarking. In 2011, the de-facto conference on digital watermarking, IWDW (International Workshop on Digital Watermarking), changed its name to "International Workshop on Digital Forensics and Watermarking" (Ho *et al.* 2009, Shi *et al.* 2012, 2017), reflecting the ongoing changes in the field. The topics of the accepted papers have moved towards forensics, authentication and steganography.

What is common for all of these more recent application areas is that the watermark does not need to be comprehensively robust as with copy- and copyright protection. As (Cox *et al.* 2002) discuss, it is often enough to design a fragile system, in which the watermark is meant to be broken if the content is corrupted. Just the fact that the watermark is missing indicates that an attack has occurred.

Attacks on watermarked images are often divided into intentional and unintentional attacks. The reasons for intentional attacks are nefarious and the aim is to either destroy the watermark or cheat the application into believing that nothing is wrong (Hartung *et al.* 1999). Unintentional attacks, however, consist of general signal processing activities, such as JPEG (Joint Photographic Experts Group) image compression or scaling. The user has no intention of affecting the watermark. What is considered an attack depends on the application, therefore affecting the watermark design.

In this thesis, only unintentional attacks are considered in the print-cam setting. It is assumed that the user does not want to remove the watermark intentionally although severe unintentional attacks must be considered. In the next section, robustness, especially against geometrical distortions, is discussed, eventually reaching print-cam robustness.

2.2 Robust watermarking

Voloshynovskiy *et al.* (2001b) and Kutter *et al.* (2000) divide the attacks against watermarks into removal attacks, geometrical attacks, cryptographic attacks and protocol attacks. In this work, only unintentional attacks are considered that, in the aforementioned classification of attacks, can be considered as a mix of removal attacks and geometrical attacks. The watermark should be robust against common signal processing operations such as lossy compression and DA/AD conversions. In addition, in the print-cam process, the watermark will be required to be robust against strong global geometrical attacks. This literature review of robust watermarking begins from rotation, scale and translation (RST) robust methods, moving then to print-scan robustness and finally to print-cam robust methods.

2.2.1 RST robustness

As was mentioned by Kutter *et al.* (2000), geometrical attacks can be malicious or unintentional, yet their effect is not that of watermark removal but loss of synchronization. As a result, the watermark cannot be detected or extracted, even though the watermark is still present.

Seo & Yoo (2006) divided RST robust watermarking schemes into four categories: non-blind schemes, invariant transform based schemes, embedding-based synchronization schemes and content-based synchronization schemes. What is left outside of the

classification are methods based on exhaustive search. Unless the search space can be limited in somehow, these methods are computationally expensive and prone to false positive errors (Barni 2005, Lichtenauer *et al.* 2003). This division is illustrated in Fig. 7. The non-blind schemes are not either considered here as they require the original image for synchronization.

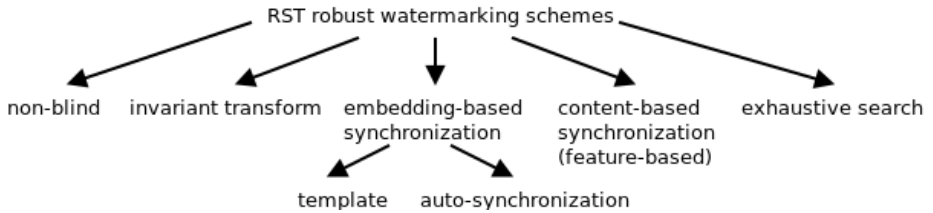


Fig. 7. Division of RST robust watermarking methods.

Invariant transform based methods differ from others in that the synchronization is preserved through RST and inverse transformation is not needed. O’Ruanaidh & Pun (1997) developed a method that took advantage of image invariants and the RST robustness was achieved with Fourier-Mellin transformation. However, they reported some implementation issues that, according to Lin *et al.* (2001), stem from strong invertibility assumption. To solve the issues, Lin *et al.* (2001) applied a non-invertible extraction function. They proposed to represent the watermark as a one-dimensional projection of the image space, which reduced the computational costs. The image was transformed with log-polar mapping of the Fourier magnitudes and then summed along the log-radius axis to obtain the one-dimensional representation. The method was translation and scaling invariant, with rotation handled through exhaustive search.

In addition to Fourier-Mellin transformation, several other invariant domains have been proposed. For example, Coltuc & Bolon (1999) applied histogram specification, while Cedillo-Hernández *et al.* (2014) proposed a hybrid method based on Digital Fourier Transform (DFT) domain and two-dimensional histogram modification.

Unfortunately, the proposed invariant domain methods have tended to be vulnerable to cropping and/or aspect ratio changes. Coronel *et al.* (2016) proposed a method, based on moment invariants, that was robust to RST and additionally to shearing. The watermark generation was based on Hermite transform that is a technique for signal decomposition. The watermark itself was embedded in a normalized image with spread spectrum techniques.

Zong *et al.* (2016) addressed the vulnerability of moment invariant based watermarking methods to cropping. Their method is based on the probability density functions of the pixel value distribution, which was reshaped to construct a two-dimensional image. The moment invariants were then calculated from this image for watermark embedding.

Invariant transform based methods have also been successfully mixed with content-based synchronization methods. Kim & Lee (2003) used Zernike moments to achieve rotational invariance and achieved scale and translation invariance by normalization through image moments. Zernike moments and histograms are definitely invariant domains but image moments can be considered as part of content dependent synchronization. Alghoniemy & Tewfik (2000) proposed a solution to RST robustness by detecting a watermark with geometric moments. The image was normalized before embedding the watermark with the moments and restored to original orientation and scale afterwards. Dong & Galatsanos (2002) continued the work by embedding a multibit message in the Discrete Cosine Transform (DCT) coefficients.

Kutter *et al.* (1999) calls the content dependent watermarking methods the second generation watermarking schemes. According to them the features used for watermarking should be invariant to noise, covariant to geometrical transformations and localized. They proposed a method in which feature points were located by using Mexican-Hat wavelets. The detected feature points were used in segmenting the image using Voronoi diagrams. Each segment was watermarked with a spread spectrum watermark using the feature location as the origin.

The methods used in selecting the feature points as well as segmenting the image vary considerably. Bas *et al.* (2002) used Harris point detection and Delaunay tessellation. Instead using tessellation, Seo & Yoo (2006) embed the watermark in an elliptical region around the feature point. The watermark was transformed before embedding in an elliptical pattern according to the shape of the region.

One weakness of the feature based watermarking methods is finding exactly the same features after the image has gone through geometrical distortions and noise addition. Embedding based methods, methods based on templates or periodic insertion of the watermark, do not suffer from this although in general they are more vulnerable on malicious attacks such as template removal (Herrigel *et al.* 2001).

Fleet & Heeger (1997) embedded sinusoidal signals in the image that acted as a grid while detecting the watermark providing a coordinate frame. The sinusoids appeared as peaks in the frequency domain and could be used in automatically scaling and aligning the images.

Pereira & Pun (2000) relied on a Fourier domain template. The template was embedded pseudo-randomly between two frequencies and detected later by first detecting local peaks and exploiting the fact that the template points have been embedded along two lines. After the template was found, the message, located also in the Fourier domain, could be read.

Kutter (1999) used the watermark signal itself for synchronization. The watermark was embedded repeatedly by tiling it at different, horizontally and vertically shifted locations. The watermark was extracted with an autocorrelation function that showed peaks at watermark locations from which the distortion parameters could be determined and inverted.

Voloshynovskiy *et al.* (2000) also relied on periodicity but on Fourier magnitude spectrum. Later, they expanded the work to cover local geometrical transformations (Voloshynovskiy *et al.* 2001a). Deguillaume *et al.* (2002) modified the work by Voloshynovskiy *et al.* (2000) into a method based on a self-reference watermark. They embedded the watermark with a large number of repetitions, in order to form a grid of peaks in autocorrelation function. The grid was represented with two vectors indicating the axes and vector norms corresponding to the breaks. These vectors were then be used in determining the affine transformation that had been applied to the image.

2.2.2 Print-scan robustness

Intuitively, many of the RST robust watermarking methods are also print-scan robust if the embedding strength is slightly increased. Some of the RST robust methods referred to in the previous section have also been proved to be print-scan robust although they have not been designed as such (O’Ruanaidh & Pun 1997, Lin & Chang 1999, Bas *et al.* 2002). Yet, some differences remain. In addition to RST, a print-scan processed image goes through multiple other distortions such as resampling and filtering.

Lin & Chang (1999) were one of the firsts to research the print-scan process. They began by modelling the print-scan process on a pixel level and analysing more carefully the geometrical distortions. In the print-scan process, the image is first printed and then placed on a scanner flatbed by the user and scanned. The printers are based generally on the process of halftoning, compiling the image of thousands of small dots of different areas, as shown in Fig. 8. The exact pattern depends on the halftoning method that is used. The effect is based on lowpass characteristics of the Human Visual System (HVS) (Lin & Chang 1999).

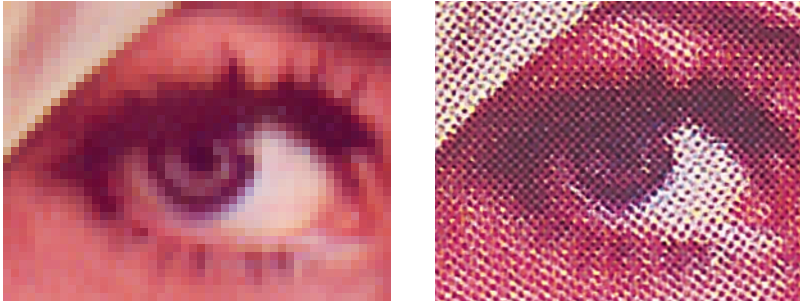


Fig. 8. A digital image of a magnified part of "Lena" on the left and printed and scanned version of the same location on the right.

Solanki *et al.* (2006) studied the effect of halftoning process further and explained that halftoning can be seen as the quantization of the image and adds coloured high-frequency noise to the image. According to Solanki *et al.* (2006), when the image is printed with halftoning, the image can appear darker than the original due to a phenomenon called dot gain. In addition, the image might have been gamma corrected so that the printed image appears to be as similar as possible to the image on the monitor. On the other hand, when the image is scanned, the printed image is again gamma compensated to appear similar on the monitor. Additionally, the image is digitized, the process of which can cause distortions.

In essence, the watermarked image goes through a DA/AD transformation. Furthermore, the image is likely compressed for storing, the image placing on the scanner flatbed and selection on the scanner program is imperfect causing geometrical distortions, edges of the image might get cropped, or the areas around the image show the surrounding paper that might not be blank.

Solanki *et al.* (2004) did tests on printed and scanned images and discovered four trends in DFT coefficients that align with notes by Lin & Chang (1999) and potentially affect watermark robustness:

1. The low and mid frequencies are preserved better than the high frequencies.
2. On these low and mid frequencies, the coefficients with low magnitudes see higher noise than their neighbours with high magnitudes.
3. Coefficients with higher magnitudes see roughly unity gain.
4. Slightly modifying the high magnitude low frequency coefficients does not cause perceptual distortions.

He & Sun (2005) continued the work and introduced the following three more properties:

5. Most textures can be preserved but the magnitudes of individual coefficients may vary
6. The dynamic range of intensity values is reduced from 0-255 to 70-220.
7. The distributions of pixel values appear as a spindle.

Both, Solanki *et al.* (2004) and He & Sun (2005), used these observations for proposing print-scan robust watermarking methods. Solanki *et al.* (2004) based their method on DFT magnitudes and hid the information in dynamically selected low frequency coefficients. The rotation caused by the scanning process is estimated and undone with the help of the halftoning pattern induced by the printer. This renders the method unusable on the digital domain but saves capacity if the image is printed.

He & Sun (2005) also employed the DFT domain but on block-by-block basis. The image was divided into blocks and each block was classified into smooth or textured type. Based on the block type, the watermark was embedded either in the mid-band of DFT coefficients or in a linear band on the spatial domain. The watermark synchronization was handled by detecting the boundaries of the printed image with Hough transform. Yu *et al.* (2005) also took advantage of the image boundaries by placing a frame around the image. The frame was detected with Sobel and/or Prewitt edge detectors.

Lefebvre *et al.* (2001) chose to use a template in the DFT domain and embed the watermark in the spatial domain. The template in DFT domain was embedded in the middle frequencies with a predetermined key and was used for rotation and scale robustness. The watermark itself was a two-dimensional cyclic code that was embedded in the spatial domain through a psycho-visual mask.

Inverting the rotation and scale was not necessary in the model of Chiu *et al.* (2006) in which the watermark was embedded in the Fourier domain. The message was embedded in DFT magnitudes in circular bands on the middle frequencies and one of the peaks outside of the bands was used for synchronization. Nevertheless, the capacity of the method was relatively low.

The watermarked image can also be printed and scanned several times as was stated by Chen *et al.* (2006). The proposed method was based on a periodic template that was recovered in the extraction phase with an autocorrelation function. The watermark itself was embedded as a spread spectrum signal.

As in RST robust watermarking, feature points have also been successfully applied to the print-scan problem. Keskinarkaus *et al.* (2012) employed Harris corner detector for

detecting feature points and Delauney tessellation for dividing the image into triangles in which the watermark was embedded.

The recent research focuses not only on where to embed the watermark but on which format the watermark is embedded. For example, embedding the watermark as a digital hologram image means that it can potentially be reconstructed from a cropped, geometrically distorted, and noise-corrupted hologram (Wang *et al.* 2010).

Wang *et al.* (2010) embedded the watermark in DCT coefficients, whereas Xie *et al.* (2016) based their algorithm on quaternion DFT and Discrete Wavelet Transform (DWT). However, the methods were not highly robust to shear transform and required a separate synchronization method on the print-cam process.

2.2.3 Print-cam robustness

The print-cam process instils heavy distortions on the captured image, and in addition, the watermark is read on a device with restricted processing power and memory. This restricts the watermark extraction methods to those that can be calculated on reasonable time and with limited resources. As Perry *et al.* (2002) noted, high reliability is a fundamental requirement for a print-cam application. Additionally, consumers demand quick responses and ease of use.

The print-cam robustness differs from the print-scan most notably in that distortions occur in three dimensions, as shown in Fig. 9, in which case recovering the watermark synchronization is even more difficult. Other distortions include lens distortions, such as barrel distortions, lighting variations, shadows and user induced distortions such as the shaking of the camera and focusing issues (Pramila *et al.* 2007, Perry *et al.* 2002).

In spite of these obstacles, the print-cam applications gained commercial interest from early on. Alattar (2000) explained the Digimarc MediaBridge solution, in which a Fourier domain template was used in resolving scale, orientation and origin of the watermark signal with the message embedded in the spatial domain. The Fourier domain is widely used in the print-scan robust methods, as was seen in the previous subsection, but it is not as suitable for geometrical distortions in three dimensions. As a result, the MediaBridge application required the image to be as perpendicular as possible to the camera. Instead of robustness, MediaBridge aimed for fast watermark extraction so that the watermark could be attempted to be read multiple times.

Horiuchi *et al.* (2009) embedded the watermark also in the DFT domain but on concentric circles. The outermost circle was used for synchronization, whereas the

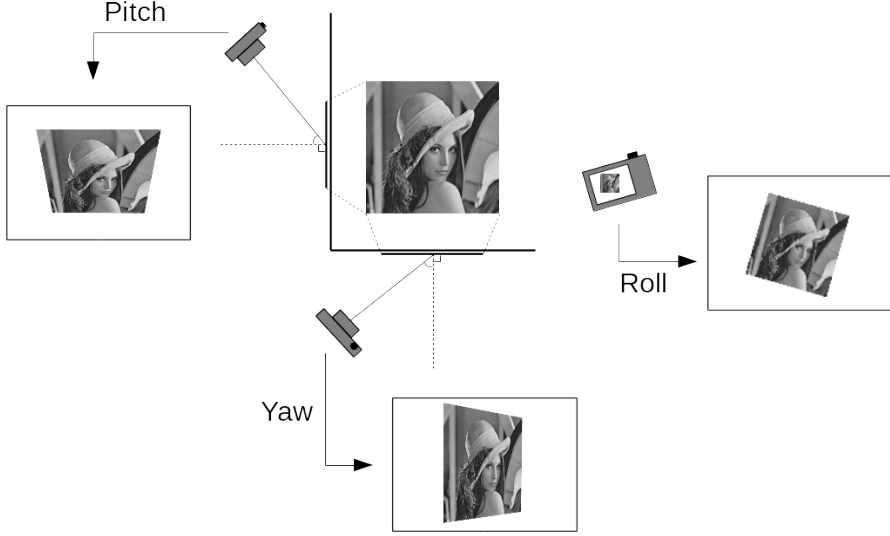


Fig. 9. Camera orientation versus the watermarked image and effects of yaw, pitch and roll.

message was embedded in lower frequencies by varying the amplitude and spread of the peaks. Similarly to Alattar (2000), strong geometrical distortions were not considered in the paper.

Nonetheless, robustness against strong geometric distortions is a natural requirement for the print-cam robust system. At the other end of the scale are picture embedding barcodes such as methods by Huang & Mow (2013) and Garateguy *et al.* (2014), the aim of which is to make barcodes visually more appealing. These methods use barcodes as the basis and are designed to be highly robust.

Katayama *et al.* (2004) and Nakamura *et al.* (2004) proposed a watermarking method that resembled the picture embedding barcodes although the embedding pattern was not a barcode but a sinusoidal pattern. A frame was used for synchronization with following equations:

$$\begin{aligned} x' &= \frac{a_1x + b_1y + c_1}{a_0x + b_0y + 1} \\ y' &= \frac{a_2x + b_2y + c_2}{a_0x + b_0y + 1}, \end{aligned} \quad (1)$$

in which (x', y') are the original picture positions and (x, y) are the camera picture positions. They mentioned that utilizing a frame is not a problem as it shows the user

that a hidden message is present. However, a frame is vulnerable to cropping and may restrict the image shape and size.

Liu & Shieh (2011) continued the work by Katayama *et al.* (2004) and Nakamura *et al.* (2004), by introducing a perceptual model and increasing capacity by decreasing the size of the watermark blocks. Liu & Shieh (2011) also experimented with two different position-detection patterns inspired by two-dimensional barcodes but concluded that a frame is the most efficient way for the synchronization of a watermark signal.

Takeuchi *et al.* (2005) used the image borders for watermark synchronization. The message was embedded with guided scrambling techniques and lens distortions corrected before extraction with pre-calculated coefficients. Also Gourrame *et al.* (2016) used the image borders for synchronization as the selected scenario was verifying identity images. The watermark itself was embedded in the magnitudes of the DFT domain along a preselected radius. Simulated robustness of $\pm 10^\circ$ of the tilt of the optical axis was reported. Likewise, Moritani *et al.* (2016) used Sobel edge detector to detect the edges of the image in order to correct the perspective distortion. First, they embedded markers in the DFT domain to indicate resolution and number of blocks in which the watermark was embedded. The image was divided into blocks and the watermark was embedded in DCT transformed blocks.

As was seen with RST robust watermarking, another way for synchronization is to use self-synchronization and autocorrelation. Kim *et al.* (2006) eliminated the need for a separate frame by embedding the watermark as a pseudo-random vector which was tiled repeatedly. The watermark was read with an autocorrelation based method. The results were limited, however: The amounts of rotation, scale, translation and tilt of the optical axis were minimized by using a tripod and resizing and cutting the image by hand to its original dimensions.

Nuutinen & Oittinen (2008) embedded the watermark also in the spatial domain on a block-by-block basis but not by tiling. A bit was embedded by modifying intensity values between two adjacent blocks. The bit was extracted by comparing the mean intensity values of the neighbouring blocks. The method was simple but not robust to strong distortions. The authors reported a shooting distance of 10 cm and the image was captured perpendicularly. Their aim, however, was not only designing the watermarking method, but also testing the method in different color spaces and annoyance/perceptibility of the watermark in the said color spaces. They concluded that although the Y-channel of the YCbCr transformed image is the most robust, blue

channel of RGB (Red, Green, Blue) works the best when imperceptibility is taken as a factor.

Similar deductions were made by Takimoto *et al.* (2010) who noted that HVS is least sensitive to the blue color. They proposed a circular synchronization template, which was embedded in the blue channel. The method was tested with a camera phone but no information about test setting or capturing angles was provided. Likewise Thongkor & Amornraksa (2014) proposed a print-cam robust watermarking method in which the watermark was embedded in the blue channel of the image on selected positions. However, the synchronization of the watermark was done by registering the image with the original.

In order to get rid of synchronization pattern and preserve the quality of the image, Yamada & Kamitani (2013) embedded the information only in some locations in the image. The watermark was embedded with spread spectrum techniques and read from the video feed by trying to find the watermark from each frame in turn. Time was saved when only those parts of the image that contain watermarks were geometrically corrected. Nevertheless, the method required the user to keep the camera near perpendicular to the watermark at the specified range.

While most of the print-cam robust methods seem to work in the spatial domain, Delgado-Guillen *et al.* (2013) operated their method in the log-polar Fourier domain. They claimed the method to be resistant to $\pm 5^\circ$ of rotation due to the hand movements and inclination of the mobile device.

Thongkor & Amornraksa (2013) focused in their paper on a specific problem with the print-cam applications, that is, glass reflections. The scenario presented by the authors was such that an image had been copied and the copy exposed in a photo gallery without the permission of the owner. The owner wished to check the watermark of the image that was located behind glass. Thongkor & Amornraksa (2013) proposed to use gradient fields to reduce the reflection, but the proposed synchronization method was non-blind and was based on aligning the original watermarked image with the camera captured image.

In addition, there exists a method for print-cam robustness in binary images (Pramila *et al.* 2009). The method was later converted to work with holograms (Pramila *et al.* 2011) in which the shiny surface causes difficult problems.

A summary of the discussed watermarking methods is presented in Table 1. It is clear that some consider print-cam robustness merely an extension for 2D barcodes and some choose to identify one issue in which they are focusing on. It can be seen from the

table that the methods vary greatly in capacity, imperceptibility and robustness. The robustness is often affected by the embedding strength, and capacity is affected by the image size, and consequently the values reported here are but directional. Quality was often reported with Peak Signal to Noise Ratio (PSNR). In addition, it is often difficult to discern the true robustness of the methods as the angle information is not measured or reported in general.

2.2.4 *The future of the print-cam robust watermarking*

The methods reviewed above do not, however, solve all the problems occurring. For example, lighting conditions, paper quality, camera focusing issues and text or other images around the watermarked image affect the watermark extraction process. The effects of these must be researched before the method can be used in real world applications.

What is more, most of the proposed print-cam robust watermarking methods have been tested in relatively constricted settings. Most of the methods assume that the user is able to point the camera straight in relation to the watermark in such a way that the distortions are minimized. This means that the users need to be trained in the use of the system or the requirement of keeping the camera perpendicular might cause frustration. These methods rely on the fact that the watermark extraction can fail a few times, but the user experience does not suffer because the method is fast enough.

With the advance of modern camera phones with high processing power, it is now possible to design more robust methods that are at the same time fast to compute. In addition, the cameras themselves have evolved and have more resolution and fewer lens distortions. From the phone used by Katayama *et al.* (2004) with 100 MHz operating frequency and less than VGA (Video Graphics Array) resolution, to the phone used by Yamada & Kamitani (2013) with 1.5 GHz Quad-core processor and 8 MP camera, the phones have evolved a lot in less than a decade.

Table 1. Summary of the print-cam robust watermarking methods referred to in this chapter. (Marked (-) if not reported or unclear.)

Authors	Synchronization	Capacity	Image quality	Camera rotation requirement	Other
Alattar (2000)	DFT template	length of an URL or less	(-)	perpendicular	Aimed for fast watermark extraction
Nakamura <i>et al.</i> (2004)	Frame	16 bits	variable (PSNR 37 dB-26 dB)	(-)	
Takeuchi <i>et al.</i> (2005)	Image borders	128 bits	satisfying (PSNR ~33 dB)	$\pm 10^\circ$	A tripod was used
Kim <i>et al.</i> (2006)	autocorrelation	64 bits	good (PSNR ~38 dB)	perpendicular	Aim was to study color models
Nuurinen & Oittinen (2008)	(-)	(-)	(-)	perpendicular	
Horiuchi <i>et al.</i> (2009)	DFT template	10 kb	(-)	perpendicular	
Takimoto <i>et al.</i> (2010)	B-channel template	(-)	high (user test)	(-)	
Liu & Shieh (2011)	Frame	~1000	(-)	(-)	
Delgado-Guillen <i>et al.</i> (2013)	log-polar Fourier	12 bits	good (PSNR ~31-37 dB)	$\pm 5^\circ$	Aimed for barcode beautification
Huang & Mow (2013)	As in 2D barcode	large	low	(-)	
Yamada & Kamitani (2013)	correlation	64 bits	high	perpendicular	Aimed for fast watermark extraction
Garateguy <i>et al.</i> (2014)	As in 2D barcode	large	low	(-)	Aimed for barcode beautification
Gourrame <i>et al.</i> (2016)	Image borders	(-)	good (PSNR 40 dB)	$\pm 10^\circ$	Results simulated
Moritani <i>et al.</i> (2016)	Image borders	7 bits	good (PSNR 37-38 dB)	(-)	

3 Research contributions

The main research contributions of the original Publications I–V are summarized in this chapter. The research began with the introduction of the print-scan robust method presented in Paper I, which was used as a pre-step towards the print-cam robust method presented in Paper II. A different approach to the synchronization of the watermark was presented in Paper III. The approach was based on autocorrelation function instead of a frame. In both papers, II and III, it was noticed that one of the most probable reasons for the watermark extraction to fail was incorrect camera focus. Thus the focusing issue was taken under consideration in the next two papers, papers IV and V. In Paper IV, a method that takes advantage of focal stack optimization and all-in-focus imaging was proposed. In Paper V, the method was made more efficient and a camera phone implementation was presented as well. It should be noted that some of the symbols used in this chapter may differ from the ones used in the publications. This choice was made in order to have a clear and straightforward presentation of the equations.

3.1 A print-scan robust watermarking method

As discussed earlier, the most serious attacks against the watermark in the print-scan process occur from geometrical distortions and JPEG compression. The watermarked and printed image is placed on a scanner bed and the user defines the scanning area on the user interface of the scanner, as illustrated in Fig. 10. The selected area will contain some outside areas of the image and the watermark is rotated, scaled and translated.

As the aim of the research was to later develop a print-cam robust watermarking method, special care was placed on the robustness of the method against geometrical distortions. Here, multiple watermarking techniques were employed, that is, embedding of multiple watermarks in the same image in such a way that the watermarks do not disturb each other. The simplest way to achieve this is to use orthogonal domains: Fourier domain magnitudes are practically translation invariant, whereas the spatial domain retains location information and the wavelet domain has gained interest as a multi-resolution representation to resist the format conversions, especially JPEG.

The watermarks were embedded on the luminance channel of YCbCr transformation. Nuutinen & Oittinen (2008) showed that the Y-channel is the most robust although the blue channel would give better overall results. However, this research is mostly



Fig. 10. A scanning area selected by the user. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

concerned about the robustness of the watermark and the Y-channel is used throughout the research.

First, a circular template was embedded in the Fourier domain in order to determine rotation and scale. A second template was embedded in the spatial domain to find translation. Lastly, the message was embedded in the wavelet domain. This process is visualized in Fig. 11.

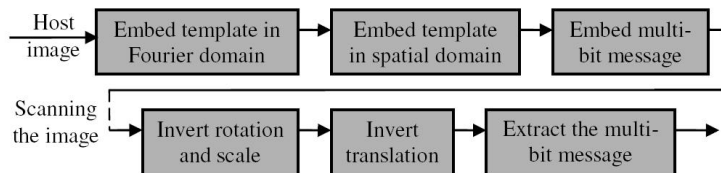


Fig. 11. The block diagram of the proposed method. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

The message was embedded last, so that it would not be affected by the synchronization templates. By employing synchronization templates, use of exhaustive search was

avoided. In Fourier domain, translation of the image needs not to be considered, and after rotation and scale have been inverted, translation is found efficiently.

Fourier domain template

Fig. 12 illustrates the embedding process of the Fourier template watermark. The template was embedded in the mid frequencies at radius r_{orig} . As Solanki *et al.* (2004) observed, the low and mid frequencies are preserved better than the high frequencies. High frequencies are especially susceptible to JPEG compression. In addition, low frequencies contain most of the information on the image and therefore changes in low frequencies are the most visible. The template consists of a pseudorandom sequence p of 0's and 1's arranged around the origin symmetrically in such a way that 1's form peaks and 0's appear as gaps. The angles of the peaks were $\theta_j = \pi j/20$, $j = 0 \dots 19$.

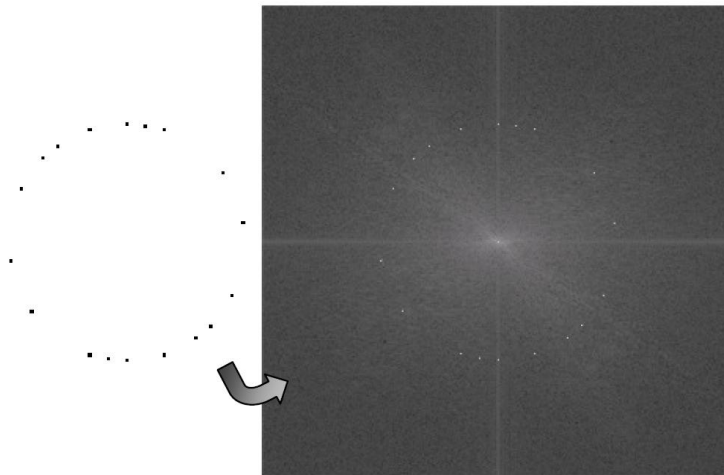


Fig. 12. Embedding a pseudorandom sequence in the Fourier domain of an image as a template. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

The Fourier domain template was extracted with cross-correlation from an annulus between two predefined frequencies, r_1 and r_2 , around the origin. First, each frequency band between r_1 and r_2 was transformed into a one-dimensional signal. A cross-covariance value was calculated with the signal and the pseudorandom sequence p that

was used in embedding. An approximation of the radius \hat{r} was found at the maximum value of the cross-covariances.

A more exact value for the scale was found when the approximated radius and two pixels width from it were searched more accurately for the peaks. The peaks were detected by locating local maximums and thresholding, after which all the points that were at an angle other than $\pi/20$ from the others were discarded. The peak locations were represented as a set of $\{\hat{r}_i, \hat{\theta}_i : i = 1 \dots n\}$, where n is the number of peaks. The trimmed mean of half of the peaks was selected as the final scaling factor r_{final} . The rotation angle was then computed by first cross-correlating the peaks with the pseudorandom sequence p and selecting the maximum that gives the rotation angle in a multiple of $\pi/20$. The final rotation angle was computed by taking a median from $\theta_i - \hat{\theta}_i$ and summing to it the detected multiple.

Translation template

As the amount of translation cannot be determined with the Fourier domain template, a spatial domain template was introduced. The shape of the template is presented in Fig. 13. The template is formed by repeating of a pseudorandom sequence horizontally and vertically. The embedding strength was calculated with a JND method by Chou & Li (1995).

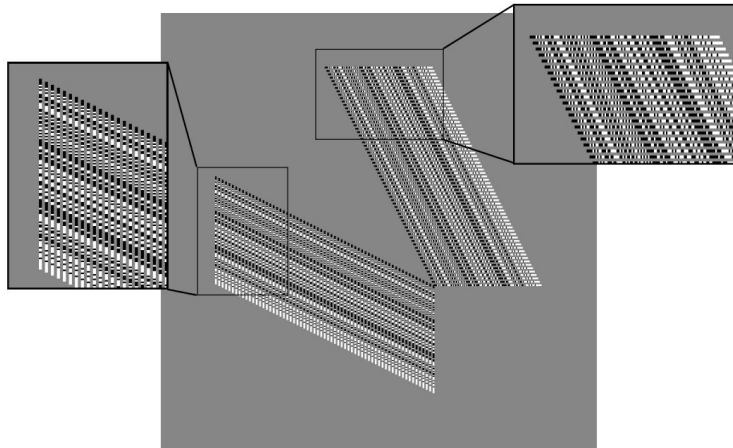


Fig. 13. The template embedded for robustness against translation. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

The extraction was done first in the horizontal and then in the vertical direction. A cross-correlation was calculated for every other line and the results were shifted to be on line with each other. The cross-correlations were added together to strengthen the result and therefore the watermark could be embedded with relatively weak strength.

Multibit message

The multibit message was embedded in the Haar wavelet transform domain with spread spectrum techniques (Keskinarkaus *et al.* 2006). The message was embedded after the Fourier domain template and the spatial domain template had already been embedded in order to preserve message robustness. The watermark was embedded with

$$\begin{cases} Y^{Cm}(n) = Y^C(n) + \beta \cdot m(k), & \text{messagebit} = 1 \\ Y^{Cm}(n) = Y^C(n) - \beta \cdot m(k), & \text{messagebit} = 0 \end{cases}, \quad (2)$$

where m is an m -sequence, Y^C is the approximation coefficients or detail coefficients of the wavelet transformed image with the templates, and β is a scaling coefficient.

The watermark was extracted by cross-correlating the same m -sequence and thresholding the result. If the cross-correlation value was above the threshold, 1 was detected and otherwise 0.

The results

The method was tested both by embedding a message first in the approximation coefficients of the wavelet domain and then to detail coefficients. The message was error coded with (15,7) BCH (Bose-Chaudhuri-Hocquenghem), which is capable of correcting 2 error bits, and the error coded message of size 135 bits was embedded in the image.

The image quality was examined with PSNR values. The PSNR was 40.5 dB when the watermark was embedded in the approximation coefficients and 38.4 dB when detail coefficients were used. It was concluded that the qualities of the images stayed high after watermarking.

Each image was compressed with various JPEG quality factors, i.e., compression ratios. The watermarked and compressed images were printed with two different printers, HP ColorLaserJet 5500 DTN and HP ColorLaserJet 4500 DN. As seen in Fig. 14, the other printer produces significantly darker images.



Fig. 14. A watermarked image printed with two different printers and scanned. The left-most image was printed with HP LaserJet 5500 DTN printer, the other with HP LaserJet 4500 DN printer. Images from Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

The printed images were scanned with Epson GT-15000 scanner. Each image was scanned a hundred times with 150 dpi setting and a hundred times with 300 dpi setting. The obtained images were saved as uncompressed TIFF (Tagged Image File Format) -files. The scanning area was selected by hand and the images were rotated randomly between $\pm 45^\circ$.

Two measurements were taken: success ratio and BER (Bit Error Rate). The success ratio in Table 2 shows the percentage of times when the message was extracted correctly. Table 3 shows the respective BER values. The values in parentheses indicate BER after error correction coding. The results show that the method is robust against high JPEG compression, as well as the print-scan process, including rotation, scale and translation.

Table 2. Success ratio with different JPEG quality factor and scanning settings. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

Quality factor	Approx. coefficients		Detail coefficients	
	300 dpi	150 dpi	300 dpi	150 dpi
100	98%	98%	100%	99%
80	97%	94%	100%	99%
60	97%	91%	98%	98%
40	49%	46%	90%	85%

The results indicate that the method is more robust against JPEG when the message watermark was embedded in detail coefficients. Paper I also includes the respective test

Table 3. BER with different JPEG quality factor and scanning settings. Paper I 2007 International Workshop on Digital Watermarking. Reprinted with permission from Springer.

Quality factor	Approx. coefficients		Detail coefficients	
	300 dpi	150 dpi	300 dpi	150 dpi
100	1.9% (0.6%)	1.4% (0.1%)	0.8% (0%)	1.2% (0.5%)
80	2.6% (1.0%)	2.9% (1.0%)	0.7% (0%)	1.0% (0.5%)
60	3.0% (0.6%)	5.0% (2.8%)	1.8% (0.6%)	1.8% (1.0%)
40	8.3% (4.3%)	8.7% (4.0%)	6.2% (3.6%)	6.8% (4.2%)

for JPEG2000 robustness and the results differ only in that the method was shown to be more robust against JPEG2000 when the message was embedded in the approximation coefficients of the wavelet transform.

Some tests were also done in Paper I on the previously mentioned two different printers. Those results indicate that the printer has an effect on the watermark robustness and some of that effect can be mitigated in the extraction process, e.g., by applying super-resolution in refining the peak detection of the Fourier domain template. In essence, the rotation and scale were determined more accurately and the success ratio increased, e.g., from 80% to 99% when scanned with 150 dpi.

3.2 Print-cam robust watermarking methods

One of the differences between the print-scan and print-cam methods is the JPEG compression, which in print-cam occurs on two levels: first when the content owner releases the watermarked image and second when the user captures the image. Nevertheless, it can be assumed that the content owner wants the image to be as high quality as possible. And although there will be some JPEG compression that is pre-installed by the phone manufacturer, it can also be assumed that reading the watermark has been somehow initiated on the phone and the images taken are as high quality as possible. Consequently, the watermark system should be robust to small amounts of JPEG compression.

The other differences from the print-scan process include the geometrical distortions that in the print-cam process need to be considered in three dimensions. In the next two subsections, two print-cam robust watermarking methods are presented. In the first one, a frame is placed around the image and the corner points are used in watermark extraction. The second method is based on autocorrelation and no frame is required.

3.2.1 A frame based method

In the print-scan publication, Paper I, it was observed that the message watermark was more robust to JPEG compression when the message was embedded in the detail coefficients of the wavelet transform of the image. Therefore, in Paper II, a decision was made to use the same message watermarking method and embed the watermark in the detail coefficients. The aim was not only to develop a print-cam robust watermarking method but also to see whether an existing watermarking method, which is not designed to be robust against the print-cam process, could be used in such circumstances.

The watermarking method and frame detection

The block diagram of the method is shown in Fig. 15. As a Fourier domain template would not be robust to three-dimensional distortions, a visible frame was set around the image. The corner points of the frame were used in inverting the geometrical distortions. The frame was similar to the one used by Katayama *et al.* (2004): a blue rectangle around the image with a small space between the frame and the image border. However, the frame was found to be too inaccurate for determining the translation of the image and so the translation watermark from Paper I was also employed. In addition, barrel distortions were inverted with a method by Kannala & Brandt (2006) after the picture was captured.

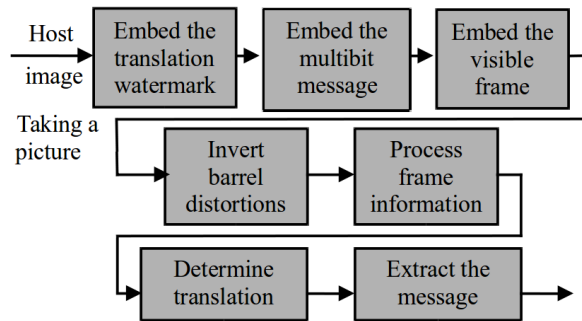


Fig. 15. A block diagram of the print-cam robust watermarking method. Paper II 2008 Signal Processing, Pattern Recognition, and Applications. Reprinted with permission from ACM.

In the captured image, the process of searching the frame was begun by taking a crosswise line dissecting the image in half. This line through the middle of the image

was used in determining the width of the frame and then the width of the frame was used in forming a frame detector filter. The filter was formed by differentiating pixel intensities in the crosswise direction and calculating the distance of the maximum and minimum values on the first third of the line. The distance l was used as the width of the filter and used in building a $3 \times l$ filter \mathbf{F} , so that sides of the matrix consisted of -2 's and the center was filled with 5 's. The frame was then detected with

$$FrameValue = \sum_{i=1}^3 \sum_{j=1}^l I(i, j) \mathbf{F}(i, j), \quad (3)$$

in which I is the captured image.

The computations were continued up and down along the frame edge as illustrated in Fig. 16. On each row of the image, the filter was slid one pixel to the left and right from the current position in order to find the frame. The maximum filter value was selected as the frame location and the next row was iterated. The intersections of the detected frame show the approximate locations of the corner points of the frame. The exact location of the corner was found by correlating the small area with a cross shaped template. The image was then rectified with Eq. 1.

Determining and refining the translation with the template was done as in Paper I, so that the watermark location is determined faster and with better accuracy than by using exhaustive search.

Likewise, the watermark extraction proceeded as presented in Paper I.

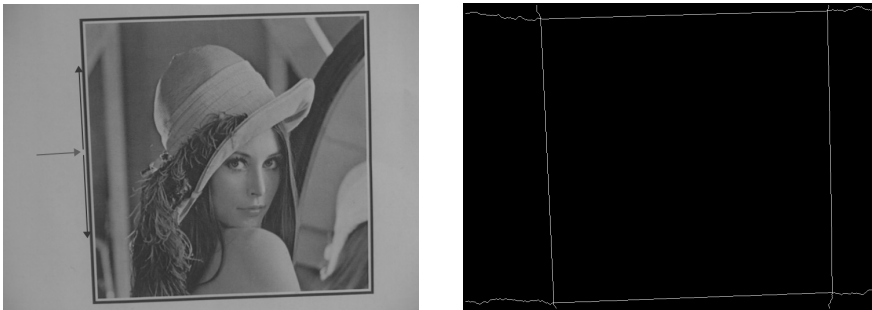


Fig. 16. The frame is determined by searching along a crosswise line and advancing up and down the side of the frame. The second image shows the detected frame.

The results

The method was tested by embedding a (15,7) BCH error coded message of 135 bits in an image as in Paper I. The PSNR value of the watermarked image was measured to be 39.0 dB. The watermarked image was compressed with various JPEG ratios and printed with HP ColorLaserJet 5500 DTN printer. The images were then placed on the wall and pictures were captured with a Nokia N90 mobile phone, which had a 2 MP camera. The images were taken with two different resolution setting and the obtained results are collected in Table 4. The camera was held in hand perpendicularly to the wall while the images were captured but no external equipment, such as a tripod, was used. The movement of the camera was approximately $\pm 5^\circ$ and the distance from the camera to the wall was around 20 ± 5 cm.

Table 4. Success ratio and BER with different JPEG quality factor and camera resolution settings.

Quality factor	Success ratio		BER	
	800x600	1600x1200	800x600	1600x1200
100	98%	99%	0.52% (1.6%)	0.05% (1.5%)
80	100%	98%	0.0% (1.5%)	0.6% (1.8%)
60	87%	96%	0.6% (3.9%)	1.1% (3.4%)
40	49%	72%	7.5% (12.1%)	3.7% (7.6%)

Table 4 shows that the method was robust against JPEG compression, tilt of the optical axis, lens distortions and geometric attacks. However, the watermarking method on the wavelet domain was deemed to be quite fragile in a sense that the camera had to be held near perpendicularly. This restricts the amount of use cases. Nevertheless, the capacity and imperceptibility measures were higher than in the previous methods by Katayama *et al.* (2004) and Takeuchi *et al.* (2005).

3.2.2 A directed-grid based method

Although the method in Paper II worked quite well, it came apparent that the wavelet domain based message watermarking method is too fragile for many use cases. In Paper III, a method was proposed that is more robust to small synchronization errors and does not, in fact, require the frame. The method is based on autocorrelation and especially on the alignment and the direction of the autocorrelation peaks.

Watermark embedding

The watermark embedding process is presented in Fig. 17 and consists of two tracks: The leftmost track handles the image to be watermarked and the rightmost prepares the message. The message is error correction coded and encoded as rotational angles and the watermark is embedded as a series of rotated two-dimensional pseudorandom patterns. The patterns are embedded block-by-block by using a JND model to enhance imperceptibility.

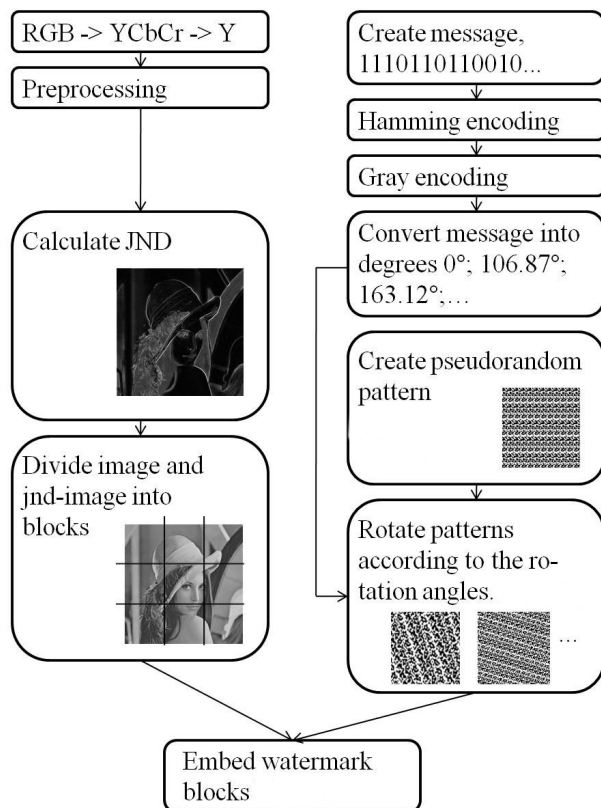


Fig. 17. The embedding process. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.

The watermark was embedded in the Y-channel of the YCbCr transformation. The aim of the preprocessing step was to break some naturally occurring periodicities in the image by applying Wiener filtering on random pixels of the image. In order to make

the watermark more imperceptible, the JND was calculated with a modification of a method by Chou & Li (1995). The method by Chou & Li (1995) is based on computing the background luminance values and spatial masking, and designed for the digital distribution of the images. In their method, the strongest of the two was selected as the JND value. Here, in order to improve robustness against print-cam process and to better take into account the small details of the image, the method was slightly modified. The values were summed together as in

$$JND(x,y) = \lambda_1 * (f_1(bg(x,y),mg(x,y)) + \lambda_2) + f_2(bg(x,y)), \quad (4)$$

where f_1 is the spatial masking component, $bg(x,y)$ and $mg(x,y)$ are average background luminance and maximum weighted average of luminance differences around the pixel (x,y) , respectively, as explained by Chou & Li (1995). The visibility threshold due to background luminance was given by function f_2 . λ_1 and λ_2 are scaling factors and values 2.0 and 3.0 were used. The JND values were then scaled between 0 and 1.

The image was divided into $k = 9$ blocks out of which the first one was reserved for synchronization and watermark detection. Each remaining block contained four bits and the final message length to be embedded was 32 bits. The message was first protected with error correction coding and Gray coding. Each four-bit sequence was transformed into an angle between 0° and 180° . The angles were quantized and each of the angles were assigned a sequence of bits. The quantization angle was determined with

$$\alpha = 180^\circ / 2^a, \quad (5)$$

in which a is the amount of bits embedded in each block, in here four.

The watermark pattern was formed by repeating a small rectangular pseudorandom sequence until it formed a two-dimensional pattern. The pattern was rotated according to the message angle and cut to the size of the block. The blocks were embedded in the image with

$$Y_i(x,y) = X_i(x,y) + \delta_1 * JND(x,y) * W_i^{\theta_i}(x,y) + \delta_2 * (1 - JND(x,y)) * W_i^{\theta_i}(x,y), \quad (6)$$

where Y_i is the i th watermarked image block, X_i is the i th preprocessed image block, $W_i^{\theta_i}$ is the two-dimensional pattern that has been rotated according to the i th angle θ_i , and δ_1 and δ_2 are scaling factors of JND values.

Watermark extraction

The watermark was extracted by first dividing the captured image into blocks. The division was done blindly and it was assumed that the watermarked image lies close to the center of the captured image. Each block was processed separately by filtering and calculating autocorrelation functions, as illustrated in Fig. 18 and 19. A set of peaks was revealed that could then be used in determining the direction and angle of the embedded pseudorandom pattern.

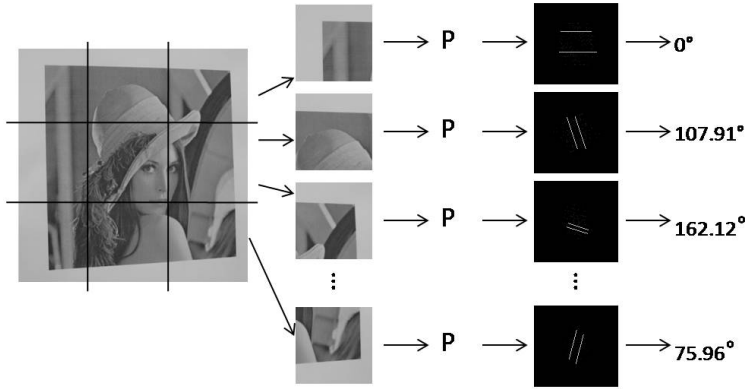


Fig. 18. The message extraction process. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.

Each block was Wiener filtered in order to remove the effect of the cover image from the watermark. The autocorrelation function was then calculated over the Wiener estimate. However, due to the print-cam process, the autocorrelation function of the Wiener estimate \tilde{W}_i is distorted and need to be preprocessed for the optimal result. In order to enhance peak detection, the autocorrelation function was filtered with a rotationally symmetric Laplacian of Gaussian filtering operator. The enhanced autocorrelation peaks were thresholded and a binary grid was formed:

$$G(u, v) = \begin{cases} 1, & \text{when } M(u, v) \times R_{\tilde{W}_i \tilde{W}_i}^{**}(u, v) \geq \gamma \\ 0, & \text{when } M(u, v) \times R_{\tilde{W}_i \tilde{W}_i}^{**}(u, v) < \gamma \end{cases} \quad (7)$$

The center of the autocorrelation function $R_{\tilde{W}_i \tilde{W}_i}^{**}$ is most likely filled with noise and it was filtered out with a circular masking operator M . γ is the threshold and selected such that 99.7% of the data were below the threshold.

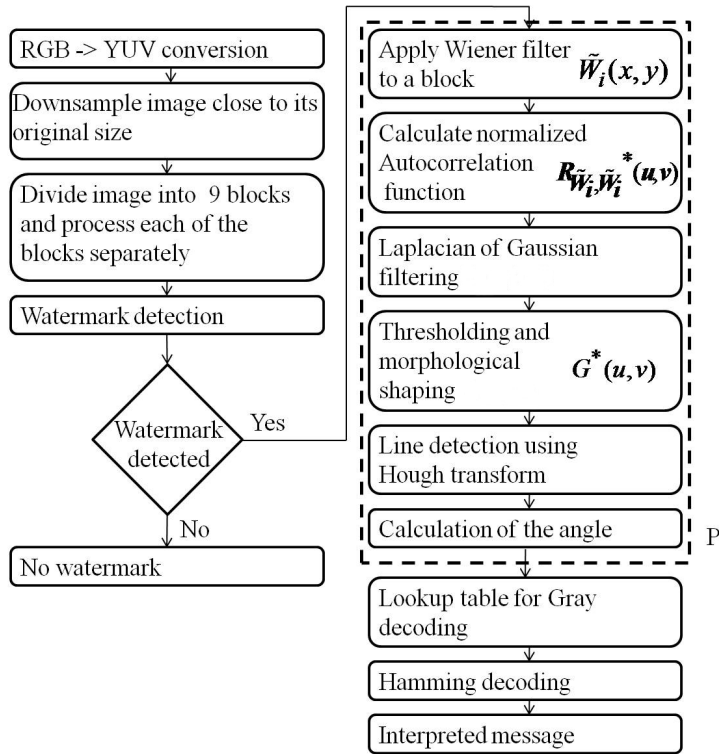


Fig. 19. Extraction process in detail. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.

Capturing the image affects the shape of the peaks. In order to reshape the peaks, the binary grid was dilated with a small disk-shaped structuring element. In this way small errors were allowed in the peak locations while determining line directions.

The angle was detected from the binary grid G with Hough transform and the message read from the slope of the detected lines. Due to the Hough transform properties, false peaks had little or no effect to the line detection. The message was decoded from the angle information in reverse order to the embedding.

The results

For the experiments, five images were used. The images are listed in Fig. 20. Each image was watermarked with two different embedding strengths: first, with embedding values of $\delta_1 = 50$, $\delta_2 = 5$, and then with $\delta_1 = 60$ and $\delta_2 = 6$. The images were then

printed with HP Color LaserJet 4650 PCL printer with print size of 10.5 cm × 10.5 cm and placed on the wall.



Fig. 20. The test images. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.

The qualities of the watermarked images were evaluated with subjective tests. 10 persons were asked to evaluate images without them knowing which of the images were watermarked. The persons rated the images with 5-point impairment scale. Subjective Difference Grade (SDG) was calculated with

$$SDG = Score_{image_under_test} - Score_{reference_signal} \quad (8)$$

in which the ratings for the unwatermarked signals worked as a reference. Resulting SDG scores had a mean of -0.4 for both watermarking strengths and therefore the qualities were deemed sufficient for the intended use case.

The method was tested first against the distance variations of the camera to the wall. The tests were done with Nokia N82 mobile phone, which has a 5 MP camera. The data was collected by capturing images from the watermarked image at each distance and computing the average accuracy of the detected rotation angles of the blocks. The results were collected in Fig. 21. The angle 5.6° indicates the theoretical limit at which the reading of the watermark is still reliable if four bits are embedded in each block.

These results showed how the capacity and embedding strength affect robustness. More bits per block means lower quantization step size and the possibility for misinterpreting the rotation angle information increases. The results showed also that the optimum shooting range for the test images when four bits were embedded was 12-24 cm with the stronger embedding strength and 14-22 cm with the lower embedding strength. Fig. 22 shows as an example of how the pictures look when taken at the limits of the optimum shooting range.

Similarly, robustness against the tilt of the optical axis, namely, yaw and pitch, were tested. Naturally, the method was more robust with stronger embedding strengths but for

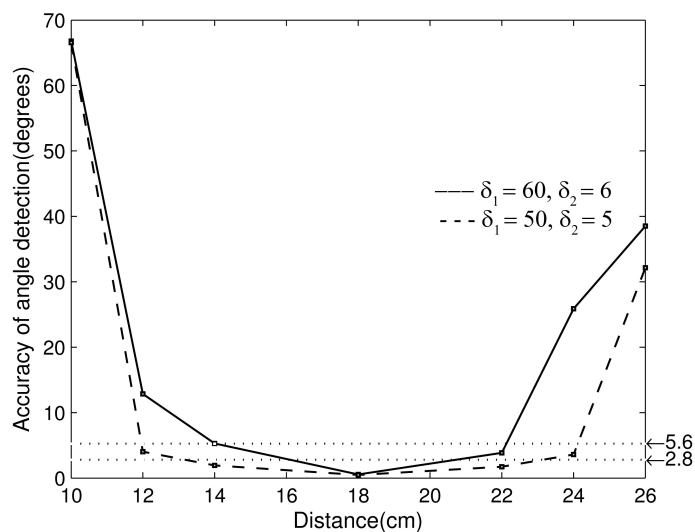


Fig. 21. Effect of distance on the accuracy of the angle detection. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.



Fig. 22. The left image is taken at distance of 12 cm whereas the picture on the right is taken at distance of 24 cm. Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer.

all images and directions, extraction was robust on average 10° of tilt, 6° on minimum and 20° at the maximum.

Encouraged by the results, the images were placed on a poster layout for additional testing. The poster is shown in Fig. 23 and includes coloured and textured background, logos on top of the images and one image that is not rectangular. Surprisingly, the results showed that the method was robust on average 15° of tilt, 10° on minimum and

20° at the maximum. Therefore the watermark was more robust on the poster than on normal paper despite additional distortions such as shiny paper. This was probably because of the better printing quality of the poster printer.

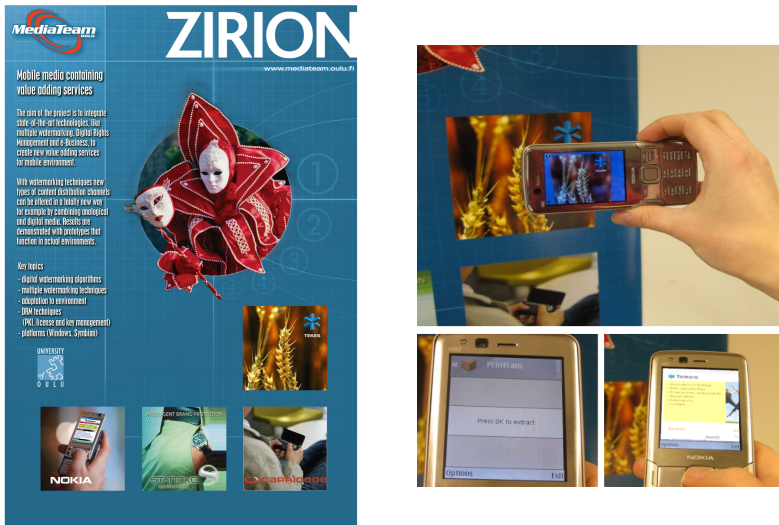


Fig. 23. On the left: The poster with watermarked images on Paper III 2012 Signal, Image and Video Processing. Reprinted with permission from Springer. On the right: an example of a scenario.

In addition to the distance variations and the tilt of the optical axis, some tests were also conducted with different mobile phone cameras and camera settings. Two phones were used in conducting random tests, Nokia N82 and N90. Images were captured free handedly, 50 times from each image. On average, the BER for 5 MP camera of N82 was 1.66, for 2 MP image of N82 average BER was 2.5 and for 2 MP camera of N90 the average BER was 3.8. This indicates that the camera has a discernible effect to robustness. Most probably the lens distortions on the older model, N90, were the biggest factor in the obtained results.

In order to validate the method further, a prototype was implemented on Symbian C++ and installed on the N82. The aim of the application was to direct the user to a website, the address of which was stored as a watermark. Each image contained information for a different address. Fifteen users were asked to take pictures of the poster and test the application. The users were in general unaccustomed to the camera phone model and rarely took pictures with a camera phone. The largest individual problem

seemed to be a difficulty of focusing the camera properly for watermark extraction. Out of 15 test subjects, 14 were directed to the correct website at the first attempt and the one test subject on the second attempt.

Ultimately, the aim of the research was to build a method that did not rely on frames and would be more robust to small local changes. It was shown with extensive tests that the method worked as intended, was robust to additional distortions and worked even with round images.

3.3 Focusing issues in print-cam robust watermarking

The two previous works led to a realization that one of the biggest problems in the print-cam robust watermarking was focusing the camera. In addition, the methods in the literature have constraints for how straight the image must be captured. The following research was done in order to bend the limits of watermark robustness and propose a solution for the focusing issues.

The problem of camera phones is their narrow depth of field which means that, if the image is captured at a large angle, all of the image is not in focus. The solution proposed here is based on a field of computational photography, namely, all-in-focus imaging. In all-in-focus imaging, a series of images are captured at several different focus distances and the images are combined to form one sharp image. The initial method was proposed in Paper IV and the work was refined and implemented on a mobile phone in Paper V.

3.3.1 An approach based on computational photography

When the image is captured in a large angle in respect to the printout, the depth of focus of the camera might not be deep enough to capture the whole scene in-focus: some parts of the image may be unfocused and the watermark extraction fails. Traditionally, to increase the depth of focus, the size of the aperture is increased and subsequently more lighting is required. With camera phones, changing the aperture is generally not possible and, regardless, arranging more lighting is often impractical.

In Paper IV, a method was proposed that improves the focusing by providing an overall sharper image through computational photography and especially through all-in-focus imaging techniques. Computational photography overcomes the limitations of optics by capturing and processing images digitally. In the all-in-focus imaging, the scene is captured by taking multiple pictures of the same scene with varying depth of

focus. This way a focal stack is built and by combining all or part of the images in the focal stack, a sharp version of the scene can be reconstructed.

On a mobile phone, the usage of the whole focal stack is not feasible. Traditionally, the selection of images from the focal stack is done by hand, which would not be practical in a mobile phone setting. The advantage of selecting only a few of the images for reconstruction is twofold: First, if the camera moves between images in the focal stack, there is need for image registration, and the more there is a need for registration, the more the risk of erroneous registration increases. Secondly, image registration is a computationally expensive operation and selecting an optimal amount of images for further processing will save processing time and power.

Unfortunately, most of the proposed all-in-focus imaging methods do not take into account the movement that occurs when the image is captured freehandedly and even fewer have been proposed for automated image selection. None of the methods have been used in combination with watermarking.

Vaquero *et al.* (2011) proposed a method for Linux based mobile phones that used FCam programmable camera software stack (Adams *et al.* 2010). They developed a method for sweeping the focus of the lens and selecting the optimal amount of pictures to be taken based on the sharpness maps of the scene. Solh (2014) selected three predetermined focal distances and the frames at these distances were aligned and fused. Zhang *et al.* (2013) selected the whole focal stack but removed first the blurriest of the images from the stack by using the IMU (Inertial Measurement Unit) of the phone. The remaining images were then registered with SIFT (Scale Invariant Feature Transform). Sakurikar & Narayanan (2014) divided the view finder into 16 blocks and directed the autofocus routine of the camera to focus to each block in turn.

The algorithm for focal stack optimization presented here was inspired by the method of Vaquero *et al.* (2011) and further developed with watermarking application in mind. The basic method, shown in Fig. 24, begins with focal stack processing and generation of an all-in-focus image before the extraction of the watermark message.

Focal stack optimization

The focal stack was built by taking pictures of the watermarked image at distances that were determined with

$$f_{next} = 1.0 / ((1.0 / f_{original}) - (3.0 * f_{step}) + (f_{step} * (i - 1))), \quad (9)$$

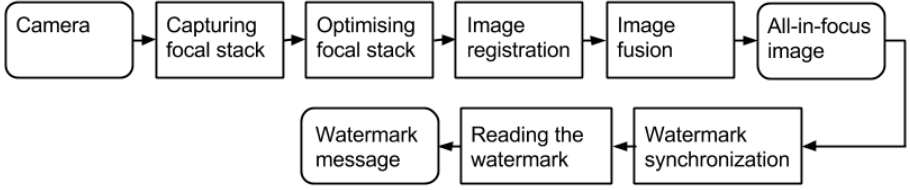


Fig. 24. Overall view of the all-in-focus image acquisition and watermark extraction process. Paper IV 2016 Multimedia Tools and Applications. Reprinted with permission from Springer.

where f -values are given in dioptres with f_{step} being $1.0/100.0$ and $i = 1 \dots N$. The captured images in the focal stack are denoted as I_i , $i = 1 \dots N$. The sharpness maps were then built from the captured images by taking absolute values of Laplacian as in

$$L_i = \left| \frac{\partial^2 I_i}{\partial^2 x} + \frac{\partial^2 I_i}{\partial^2 y} \right|. \quad (10)$$

L_i , $i = 1 \dots N$ were divided into blocks and each block averaged so that each sharpness map S_i is of size 96×72 pixels. The maps were then normalized between 0 and 1.

The foreground and background areas were identified from the sharpness maps. Each sharpness map $S_i(u, v)$ element was classified as foreground if standard deviation

$$\sigma > 0.1 \times \sigma_{max}, \quad (11)$$

where 0.1 was determined experimentally.

Next, out of the foreground elements, the sharp regions were identified. An element at i^{th} sharpness map was determined as sharp if $S_{max}(u, v) == S_i(u, v)$, or $S_{max}(u, v) - S_i(u, v) < S_{max} \times T$ and the element in the neighbouring map was sharp, i.e., element $S_{i-1}(u, v)$ or $S_{i+1}(u, v)$ was sharp. The threshold T was determined as an approximate number of images that contain valuable information about the scene, i.e., the number of images that contain largest amount of the foreground regions.

This sharpness information was collected on binary maps B_i . However, in real life, sharpness of a scene usually changes more gradually and for this reason the binary maps were processed with a small 3×3 Gaussian kernel g with

$$G_i(u, v) = \max_{(l,n) \in g} \{g(l, n), B_i(u+l, v+n)\}. \quad (12)$$

The optimal set of images for the all-in-focus image was selected with a greedy algorithm described in Fig. 25. The starting point of the algorithm was selected with $m = \operatorname{argmax}_{i \in N} \sum_{u,v} G_i(u,v)$ and each of the remaining maps was compared with

$$\operatorname{sum}_i = \sum_{u,v} \max\{G_m(u,v), G_i(u,v)\}, \quad (13)$$

so that the index m' that maximizes sum was selected and the map $G_{m'}$ was combined with G_m to build a new combined map $G_m = \max_{u,v}\{G_m(u,v), G_{m'}(u,v)\}$. The algorithm was iterated until at least 95% of the foreground regions were selected.

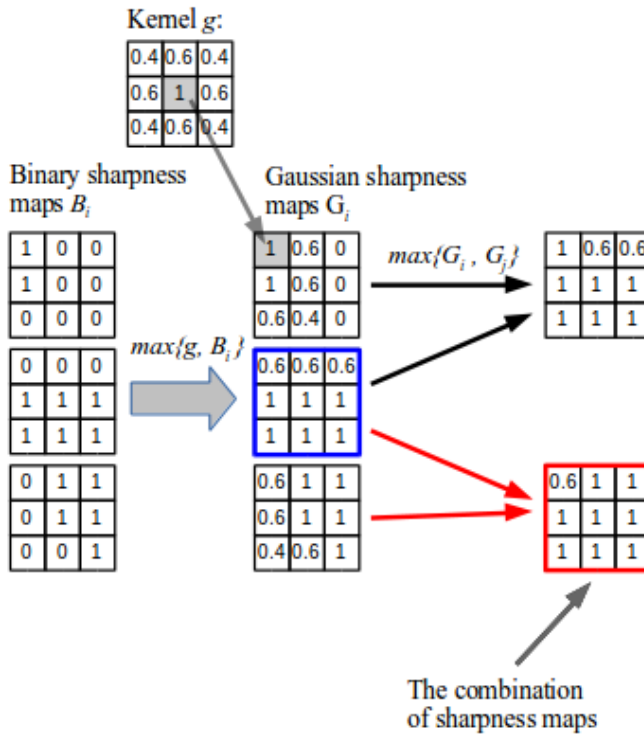


Fig. 25. An algorithm for optimizing focal stack. Paper IV 2016 Multimedia Tools and Applications. Reprinted with permission from Springer.

Image registration and blending

The M images selected from the focal stack were registered by using Accelerated Kaze features (Alcantarilla *et al.* 2013). The A-Kaze features were selected because they are blur-invariant and significantly faster to compute than, e.g., SIFT-features. An example of selected and registered sub-stack with $M = 3$ is shown in Fig. 26.

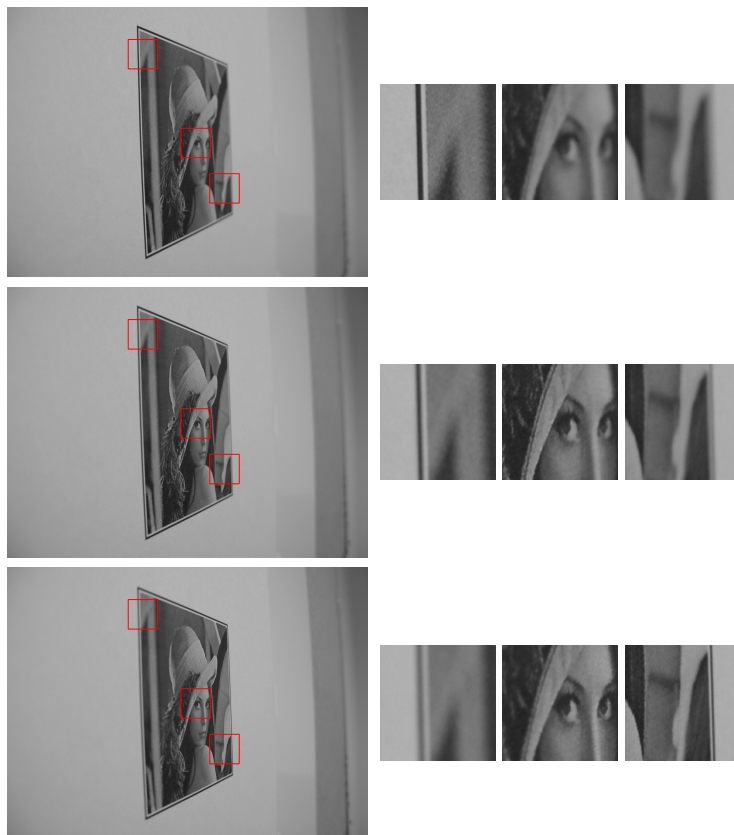


Fig. 26. An example of selected and registered sub-stack with sharp regions on left, middle and right respectively. Corresponding parts are magnified and placed next to each image. Paper IV 2016 Multimedia Tools and Applications. Reprinted with permission from Springer.

The registered images were blended with Laplacian pyramid blending (Burt & Adelson 1983) with a sharpness mask as the alpha mask. The sharpness map was calculated by first applying Laplacian filter to each image and taking the absolute value

of the filtering as in Eq. 10. The values were then smoothed with 5×5 averaging filter and the sharpness mask Q was calculated with

$$Q(x, y) = \operatorname{argmax}_{j \in M} I_j^r(x, y), \quad (14)$$

where I_j^r indicates the registered and filtered images. Fig. 27 depicts the sharpness mask and the final result after blending.

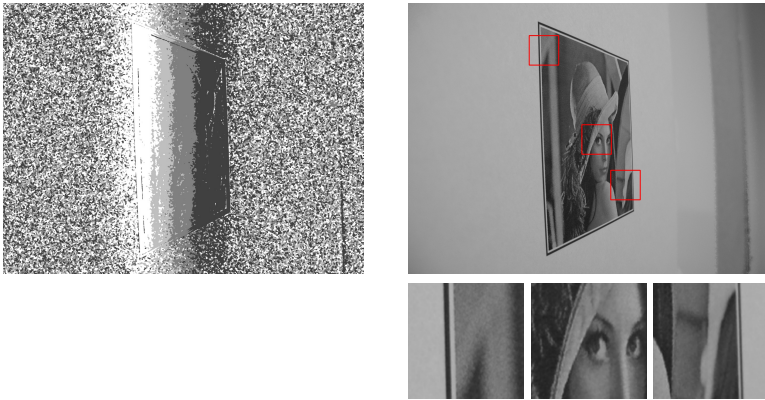


Fig. 27. On the left: Sharpness mask in which the shade of each pixel indicates the index of the image which was sharpest at that pixel. On the right: Final result after blending. Paper IV 2016 Multimedia Tools and Applications. Reprinted with permission from Springer.

Watermarking method

The watermark method used was practically the same as the one presented in Paper III. However, two main differences discern the method in Paper III from the one in Paper IV. First, the capacity was increased to 60 bits by dividing the image into 16 blocks instead of nine. Second, the watermark was synchronized by using a frame. Although the watermarking method chosen is robust to the print-cam process and some tilt of the optical axis, a frame was added for further robustness. After all, the method was tested with angles $> 30^\circ$ so that the depth of focus comes into play.

The frame was detected by first smoothing the image and thresholding it with an adaptive thresholding method. The contours were found in the thresholded image and the contours translated into polygons, which were then simplified. The largest polygon with four corners was assumed to be the frame.

The results

The method was tested with a Canon G7 digital camera by rotating the camera around the printed and watermarked image. Tests were done at angles of 0° , 20° , 40° , 60° and 70° . Angles larger than 70° were omitted due to practical reasons as the camera was too close to the wall.

The six test images, shown in Fig. 28, were watermarked with two strengths: first with values $\delta_1 = 100$, $\delta_2 = 10$ and then with $\delta_1 = 120$, $\delta_2 = 12$. No error correction coding was used. The printed image size was $6.5 \text{ cm} \times 6.5 \text{ cm}$, which is significantly less than at Paper III. Decreasing the size of the printed image affects the watermark visibility in such a way that the embedding strength could be increased without affecting the quality of the watermarked image. The qualities were validated with a method inspired by Eerola *et al.* (2009, 2010) and was based on MSSIM (Mean Structural Similarity) Wang *et al.* (2004). All the measured MSSIM values approached 1 and the image qualities were therefore sufficient for the intended use case.



Fig. 28. The test image. Paper IV 2016 Multimedia Tools and Applications. Reprinted with permission from Springer.

The main results are collected in Tables 5, 6, 7 and 8. The robustness was tested at two distances, 15 cm and 20 cm. At each distance, the camera was turned either yaw or pitch direction and pictures were captured with 10 MP resolution and 2.5 MP resolution. Each captured focal stack contained approximately 15 images. Tables 5 and 6 are collected from the average values of all the test images. However, the complementary tests on pitch were made with only "Lena" image, as shown in Tables 7 and 8.

The method was shown to be robust up to angles of 50° and perform well with angles of 60° . Unsurprisingly, the method is more robust with the stronger watermarking strength but the difference is quite small. In addition, scaling of the images to 2.5 MP seems to have little or no effect. However, the increase in distance together with the reduction in resolution decreases robustness but more tests would need to be done to find the limits.

Table 5. BER(%) at different yaw angles with 10 MP images.

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 15 \text{ cm}$	0.6	0.3	0.8	1.7	3.0	14.7
$\delta_1 = 120, \delta_2 = 12, 15 \text{ cm}$	0.0	0.0	0.3	0.8	1.4	10.6
$\delta_1 = 100, \delta_2 = 10, 20 \text{ cm}$	0.3	1.7	1.4	1.7	5.0	25.8
$\delta_1 = 120, \delta_2 = 12, 20 \text{ cm}$	0.0	0.3	0.0	1.7	2.5	13.3

Table 6. BER(%) at different yaw angles with 2.5 MP images.

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 15 \text{ cm}$	0.6	0.3	2.2	1.7	2.5	12.5
$\delta_1 = 120, \delta_2 = 12, 15 \text{ cm}$	0.0	0.0	0.3	1.1	1.4	8.6
$\delta_1 = 100, \delta_2 = 10, 20 \text{ cm}$	1.7	0.8	1.4	0.8	7.5	28.1
$\delta_1 = 120, \delta_2 = 12, 20 \text{ cm}$	0.3	0.0	0.0	0.8	2.8	18.6

Table 7. BER(%) at different pitch angles with 10 MP images (Lena).

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 15 \text{ cm}$	0.0	0.0	0.0	0.0	3.3	6.7
$\delta_1 = 120, \delta_2 = 12, 15 \text{ cm}$	0.0	0.0	0.0	0.0	0.0	6.7
$\delta_1 = 100, \delta_2 = 10, 20 \text{ cm}$	0.0	0.0	0.0	0.0	1.7	13.3
$\delta_1 = 120, \delta_2 = 12, 20 \text{ cm}$	0.0	0.0	0.0	0.0	0.0	13.3

Table 8. BER(%) at different pitch angles with 2.5 MP images (Lena).

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 15 \text{ cm}$	0.0	0.0	0.0	0.0	0.0	11.7
$\delta_1 = 120, \delta_2 = 12, 15 \text{ cm}$	0.0	0.0	0.0	0.0	0.0	3.3
$\delta_1 = 100, \delta_2 = 10, 20 \text{ cm}$	0.0	0.0	0.0	0.0	1.7	16.7
$\delta_1 = 120, \delta_2 = 12, 20 \text{ cm}$	0.0	0.0	0.0	0.0	0.0	15.0

3.3.2 *Toward faster implementation for camera phones*

In Paper V, the method presented in the previous subsection was improved for mobile phone use. The overall flow of the algorithm is illustrated in Fig. 29. Scaled versions of the focal stack images were used when applicable and approximations of transformation matrices were used. It was shown with experiments that this did not decrease the robustness of the method.

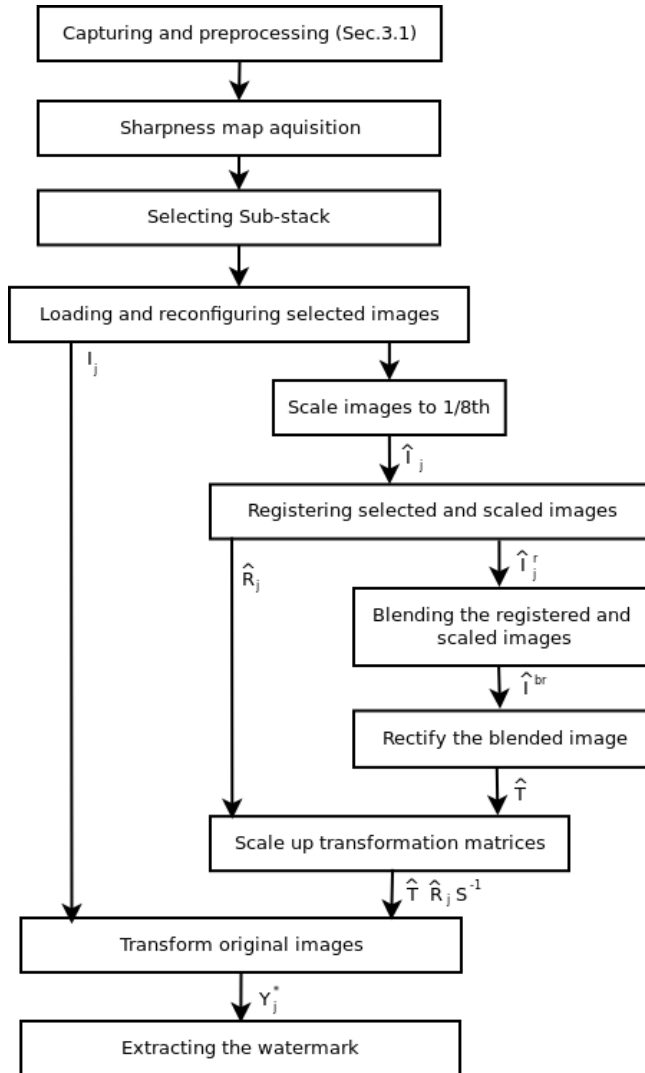


Fig. 29. Overall view of the all-in-focus image acquisition and watermark extraction process. Paper V 2018 Journal of Systems and Software. Reprinted with permission from Elsevier.

The algorithm for watermark extraction

In Paper V, the building and optimization of the focal stack was done as presented in Paper IV. The focal stack was built by first determining the initial focal point with the camera lens autofocus routine and then applying the equation 9. The focal stack size N

was selected to be 10 so that the focal stack would cover the whole distance from the initial focal point to the furthest point of the image.

Unlike in Paper IV, in Paper V, each image in the stack was scaled into size of 816×612 in order to save resources and reduce processing times. The full sized images I_i were saved in memory for later processing. The sharpness maps $S_i, i = 1 \dots N$ were built from the scaled images and M images were selected from the stack. The M full sized images were then reloaded. The full sized images $I_j, j = 1 \dots M$ were filtered with a small Gaussian kernel to smooth out artefacts that originate from the printer halftoning process. In order to save processing time later the images were then to $1/8^{th}$ of the size with a scale matrix \mathbf{H} .

Next, the scaled images $\hat{I}_i, i = 1 \dots M$ were registered and subsequently approximations of the registration $\hat{\mathbf{R}}_j, j = 1 \dots M$ relative to the full sized images were obtained. The images were then blended and a matrix $\hat{\mathbf{T}}$ for rectifying the image was computed from the corner locations of the frame around the image.

The transformation matrices $\hat{\mathbf{T}}, \hat{\mathbf{R}}_j$ and \mathbf{H} were then applied to the full sized images with

$$\mathbf{p}^* = \hat{\mathbf{T}}\hat{\mathbf{R}}_j\mathbf{H}^{-1}\mathbf{p}, \quad (15)$$

where \mathbf{p} denotes a pixel in the original image I_j and \mathbf{p}^* denotes a pixel in the image Y_j^* , $j = 1 \dots M$ from which the watermark could be extracted.

Finally, in order to minimize the effect of small registration errors, the images were not blended but all the M images were divided into $k = 16$ blocks. For each block k , the watermark was read from the sharpest of the M blocks.

The results

It was indicated in Paper IV that the method could be improved with error correction coding and so a (15,8) Reed-Solomon error correction coding (Reed & Solomon 1960) was applied here. Otherwise, the same images were used as in Paper IV. Similarly, the tests were conducted with the Canon G7 camera but in addition the algorithm was implemented for an Android mobile phone with an 8 MP camera. Because of the difference in the field of view of the two cameras, different distances were selected for both test cases. The distances were selected such that the relative sizes of watermarked images in both cases were the same.

The obtained results for watermark robustness are collected at the following tables and contain BER at different angles, at different distances and with different watermark strengths. Table 9 and 10 contain results for the digital camera and mobile phone, respectively. The values in parentheses indicate BER without error correction coding. It can be seen that the mobile phone offered almost the same robustness as the digital camera although it has slightly fewer megapixels and inferior lens specifications.

When compared with the previous method in Paper IV, the new method performed noticeably better. This was mostly due to the different approach on watermark extraction as the artefacts due to the blending operation did not occur. The registration might not have been as accurate but this was not an impediment as the watermarking method was inherently robust to small distortions.

Table 9. BER(%) at different yaw angles with error correction coding. Images captured with a digital camera.

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 15 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.8)	1.6 (6.9)
$\delta_1 = 120, \delta_2 = 12, 15 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (1.4)	0.0 (3.1)
$\delta_1 = 100, \delta_2 = 10, 17.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (1.1)	0.0 (1.7)	9.9 (9.2)
$\delta_1 = 120, \delta_2 = 12, 17.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.8)	0.0 (0.6)	0.0 (3.3)
$\delta_1 = 100, \delta_2 = 10, 20 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.3)	0.0 (1.9)	0.0 (2.5)	5.2 (9.7)
$\delta_1 = 120, \delta_2 = 12, 20 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	8.9 (10.6)

Table 10. BER(%) at different yaw angles with (and without) error correction coding. Images captured with a phone camera.

	0°	20°	40°	50°	60°	70°
$\delta_1 = 100, \delta_2 = 10, 12.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (1.9)	3.6 (10.6)
$\delta_1 = 120, \delta_2 = 12, 12.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.3)	1.6 (5.6)
$\delta_1 = 100, \delta_2 = 10, 14.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (2.2)	4.2 (13.3)
$\delta_1 = 120, \delta_2 = 12, 14.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.8)	1.0 (5.6)
$\delta_1 = 100, \delta_2 = 10, 16.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.2)	0.0 (0.6)	0.0 (5.0)	7.3 (16.9)
$\delta_1 = 120, \delta_2 = 12, 16.5 \text{ cm}$	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (0.0)	0.0 (1.9)	7.8 (15.6)

3.3.3 Execution times of the algorithms

Table 11 shows the performance comparison of the two methods, the initial method on Paper IV and the refined method in Paper V. The initial algorithm in Paper IV took over

six seconds to compute whereas the new algorithm was over six times faster. There was therefore no reason for implementing the first method on a mobile phone. The method on Paper V, however, seemed promising and eventually took only five seconds to run on a mobile phone with equal robustness. That is, the new version is faster on a phone than the old one on a computer. Most of the processing time was eventually spent on the watermark extraction and accessing the full sized images from memory.

Table 11. Execution times of the algorithms.

Sub-stack size	Paper IV on comp.		Paper V on comp.		Paper V on phone	
	1	3	1	3	1	3
handling images	0.10 s	0.10 s	0.10 s	0.10 s	0.37 s	0.36 s
sub-stack	0.01 s	0.01 s	0.01 s	0.01 s	0.07 s	0.04 s
reconfigure images	0.10 s	0.25 s	0.09 s	0.26 s	0.37 s	1.23 s
registering	-	4.19 s	-	0.04 s	-	0.30 s
blending	-	1.17 s	-	0.02 s	-	0.14 s
synchronization	0.29 s	0.28 s	0.01 s	0.02 s	0.23 s	0.28 s
extract watermark	0.37 s	0.37 s	0.37 s	0.38 s	2.63 s	2.73 s
Total	0.87 s	6.37 s	0.58 s	0.83 s	3.69 s	5.08 s

4 Discussion

4.1 Significance of the results

The aim of the thesis was to answer the question: *How to extract watermark information from a printed image with a hand held camera device when the capturing angle is highly variable?* The question was approached by first studying the print-cam robust methods and later the issues concerning the focusing of the lens. In Paper I, the research towards the print-cam robust watermarking begun within a constricted setting: A print-scan robust watermarking method was proposed with emphasis on robustness against geometrical distortions. In papers II and III, print-cam robust methods utilizing a frame and autocorrelation function, respectively, were proposed. In Paper IV, the issue of focusing the camera lens was studied and a method relying on computational photography was proposed. This method was further improved in Paper V and a mobile phone implementation was presented.

Robustness against geometrical distortions is a key element in the print-cam robust watermarking. In order to solve the challenges in print-cam robustness, it makes sense to start with a controlled setting in which the rotations, scale and translation occur only in two dimensions. The research at Paper I aimed at high robustness against the print-scan process, by taking advantage of multiple watermarking. With multiple watermarks, it was possible to direct effort in solving the exact problems very accurately. The proposed method was robust against rotation, scale and translation, but also against JPEG compression, which is important to note considering the print-cam robustness.

The research was continued in Paper II and the results of Paper I were taken into consideration. The results of Paper I showed that the message watermark is more robust on the detail coefficients of the wavelet domain and so the watermark was embedded in those coefficients in Paper I. A frame was placed around the image for synchronization. It was shown that even simple and relatively fragile watermarking methods survive the print-cam process if the synchronization is done properly. The method was robust to the print-cam process, JPEG, and lens distortions.

A more advanced method based on autocorrelation was proposed in Paper III. The method did not rely on a frame or image borders for the synchronization as many of the previous print-scan and print-cam robust methods did. The watermark was encoded in the angles of a pseudorandom signal. The method was shown to be robust, not only to

the print-cam process and JPEG compression, but also to various disturbances around and on top of the image. The method was also implemented on a mobile phone and tested to be functional with user experiments.

The previous methods were proven robust to the print-cam process but with limitations on capturing angles. In the next study, the capturing angles were increased and the effects of narrow depth of focus were studied. A method was proposed in Paper IV that increased the depth of focus through computational photography and was able to read the watermark even with angles up to 60° . The algorithm was then taken further in Paper V in which a mobile phone implementation was presented. In Paper V, the algorithm was modified to better take advantage of the inherent features of the watermarking method and camera phone properties. In the end, the algorithm was made significantly faster without sacrificing robustness.

In comparison to the methods discussed in Chapter 2 and specifically in Table 1, the methods presented here are very robust. The approach of Paper II performs well with it's higher than average image quality and large capacity, whereas the methods of Papers III-V offer superior robustness. Although, straight comparison of the methods is difficult due to different use cases and design goals. Thus, making the triangle shown in the Fig. 3 all the more relevant.

4.2 Limitations and generalizability

Although the methods presented were deemed highly robust to the print-cam process, the printing process was regarded as a black box and similar printers were used throughout the study. It would undoubtedly be worthwhile to study different printing techniques. Especially the halftoning process should be studied more in relation to the print-cam process as the halftoning pattern was noticeable in the captured images that were taken.

In addition to the printing process, also the lighting was kept relatively similar in all study cases. Although in real life, the lighting may vary drastically and mobile phone cameras are specifically sensitive to lighting variations.

A third constant in the research was the original image size. In Paper III, the method was tested also with a circular image but the watermark size was roughly the same as in the square images. In papers IV and V, the printed image size was decreased from 10.5 cm in Paper III to 6.5 cm without changing the resolution of the original images. This can be considered as a scaling issue, for which the methods are indeed robust but the effects must nevertheless be studied to be certain of the overall performance.

Regarding testing the images in different conditions, one of the limitations include the small amount of different images with which the methods were tested. Ultimately testing with different conditions and various images and settings comes down to the question of resources at hand. The methods implemented are not dependent on the image content apart from predefined constraints, such as use of natural color images. In this regard, use of a small amount of test images is justified. Nevertheless, it is a limitation that need to be considered.

In addition, the security of the watermarks was not considered during the research either. This might limit the applicability of the methods and is an important research subject for future work.

The research spanned multiple years during which the specifications of mobile phones advanced significantly. The research of the print-cam robust watermarking methods depends not only the methodologies but also on the target of implementation, the mobile devices. For example, the first mobile devices had lenses with noticeable lens distortions whereas the later models do not suffer from similar limitations. Although, the improving specifications and processing powers reduce limitations, they do not solve the main question of this thesis, that is, how to design a watermarking method robust to geometrical distortions in three dimensions.

Despite the limitations, the results obtained in this research show that the methods are feasible and can be generalized as such for commercial use. For a commercial watermark application, the method must be fast and robust, the very two features, which were already demonstrated to be achievable in this thesis.

5 Summary and conclusions

In this thesis, the print-cam robustness of the digital image watermarks is researched. Particularly, the thesis focuses on situations in which the camera is held at a large angle in relation to the printed and watermarked image. The thesis was initiated with a print-scan method and then divided into two parts. First, two print-cam robust watermarking methods were presented, one based on a frame and another on autocorrelation function. Second, computational photography was applied in designing an algorithm that is robust to a large tilt of the optical axis.

A print-cam robust watermarking method should be robust to multiple distortions, the most severe one being rotation in three dimensions, i.e., the tilt of the optical axis. The goal of the first paper was strong robustness against the print-scan process so that later the method could be developed into a print-cam robust watermarking method. The second publication took this method further and included a frame around the image to solve the synchronization issues. However, the watermarking method was relatively fragile and in the third publication a more robust watermarking method was proposed that employed autocorrelation function.

During the research of the two print-cam robust watermarking methods, it was observed that one of the most common ways for watermark extraction to fail was an incomplete focusing of the camera. The next two papers proposed solutions for the problem by applying computational photography techniques, first, with a digital camera, and then through an implementation on a camera phone. The methods take advantage of all-in-focus imaging and the inherent features of the watermarking method. Robustness of each of the methods was shown with extensive testing with and without user inputs.

This thesis shows that digital image watermarking can be successfully used in connecting the printed analog world to the digital. In the future, it would be advantageous to look into security issues in relation to the print-cam process, as well as variable lighting conditions. This would increase the number of possible applications and bring the print-cam robust watermarking closer to consumers and content providers.

References

- Acohino B (2009) New '2d barcodes' puts info at the tip of your camera phone. Posted online 19.5.2009. URI: usatoday30.usatoday.com/money/industries/technology/2009-05-19-2d-barcodes-camera-phones_N.htm. Online; accessed 6.3.2017.
- Adams A, Talvala EV, Park SH, Jacobs DE, Ajdin B, Gelfand N, Dolson J, Vaquero D, Baek J, Tico M, Lensch HPA, Matusik W, Pulli K, Horowitz M & Levoy M (2010) The frankencamera: An experimental platform for computational photography. *ACM Trans. Graph.* 29(4): 29:1–29:12.
- Alattar AM (2000) Smart images using digimarc's watermarking technology. *Proc. of the Electronic Imaging, International Society for Optics and Photonics*, 264–273.
- Alcantarilla PF, Nuevo J & Bartoli A (2013) Fast explicit diffusion for accelerated features in nonlinear scale spaces. *Proc. of the British Machine Vision Conf. (BMVC)*.
- Alghoniemy M & Tewfik AH (2000) Geometric distortion correction through image normalization. *Proc. of the 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Latest Advances in the Fast Changing World of Multimedia*, 3: 1291–1294.
- Barni M (2005) Effectiveness of exhaustive search and template matching against watermark desynchronization. *IEEE Signal Processing Letters* 12(2): 158–161.
- Bas P, Chassery JM & Macq B (2002) Geometrically invariant watermarking using feature points. *IEEE Transactions on Image Processing* 11(9): 1014–1028.
- Burt P & Adelson E (1983) The laplacian pyramid as a compact image code. *IEEE Transactions on Communications* 31(4): 532–540.
- Cedillo-Hernández M, García-Ugalde F, Nakano-Miyatake M & Pérez-Meana HM (2014) Robust hybrid color image watermarking method based on dft domain and 2d histogram modification. *Signal, Image and Video Processing* 8(1): 49–63.
- Chen P, Zhao Y & Pan JS (2006) Image watermarking robust to print and generation copy. *Proc. of the First International Conference on Innovative Computing, Information and Control - Volume I (ICICIC'06)*, 1: 496–500.
- Chiu YC, Tsai WH *et al.* (2006) Copyright protection against print-and-scan operations by watermarking for color images using coding and synchronization of peak locations in frequency domain. *Journal of information science and engineering* 22(3): 483–496.
- Chou CH & Li YC (1995) A perceptually tuned subband image coder based on the measure of just-noticeable-distortion profile. *IEEE Trans. Cir. and Sys. for Video Technol.* 5(6): 467–476.
- Coltuc D & Bolon P (1999) Robust watermarking by histogram specification. *Proc. of the 1999 International Conference on Image Processing*, 2: 236–239.
- Coronel SLG, Ramírez BE & Mosqueda MAA (2016) Robust watermark technique using masking and hermite transform. *SpringerPlus* 5(1): 1830.
- Cox IJ & Miller ML (2002) The first 50 years of electronic watermarking. *EURASIP Journal on Advances in Signal Processing* 2002(2): 820936.
- Cox IJ, Miller ML & Bloom JA (2002) *Digital Watermarking*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.
- Deguillaume F, Voloshynovskyy S & Pun T (2002) Method for the estimation and recovering from general affine transforms in digital watermarking applications. *Proc. of the SPIE Photonics West, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, 4675: 313–322.

- Delgado-Guillen LA, Garcia-Hernandez JJ & Torres-Huitzil C (2013) Digital watermarking of color images utilizing mobile platforms. Proc. of the IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), 1363–1366.
- Denso Wave (n.d.) History of qr code. URI: <http://www.qrcode.com/en/history/>. Online; accessed 6.3.2017.
- Dong P & Galatsanos NP (2002) Affine transformation resistant watermarking based on image normalization. Proc. of the International Conference on Image Processing, 3: 489–492.
- Eerola T, Kämäräinen JK, Lensu L & Kälviäinen H (2009) Framework for applying full reference digital image quality measures to printed images. Proc. of the 16th Scandinavian Conference on Image Analysis, Springer-Verlag, Berlin, Heidelberg, 99–108.
- Eerola T, Lensu L, Kälviäinen H, Kämäräinen JK, Leisti T, Nyman G, Halonen R & Oittinen P (2010) Full reference printed image quality: Measurement framework and statistical evaluation. Journal of Imaging Science and Technology 54(1): 10201–1.
- Fleet DJ & Heeger DJ (1997) Embedding invisible information in color images. Proc. of the International Conference on Image Processing, 1: 532–535.
- Garateguy GJ, Arce GR, Lau DL & Villarreal OP (2014) Qr images: Optimized image embedding in qr codes. IEEE Transactions on Image Processing 23(7): 2842–2853.
- Gourrame K, Douzi H, Harba R, Ros F, El Hajji M, Riad R & Amar M (2016) Robust print-cam image watermarking in fourier domain. Proc. of the 7th International Conference Image and Signal Processing, ICISP 2016, Springer International Publishing, 356–365.
- Hartung F & Kutter M (1999) Multimedia watermarking techniques. Proceedings of the IEEE 87(7): 1079–1107.
- Hartung FH, Su JK & Girod B (1999) Spread spectrum watermarking: Malicious attacks and counterattacks. Proc. of the Electronic Imaging'99, International Society for Optics and Photonics, 147–158.
- He D & Sun Q (2005) A practical print-scan resilient watermarking scheme. Proc. of the IEEE International Conference on Image processing, 2005. ICIP 2005., IEEE, 1: 1–257–60.
- Herrigel A, Voloshynovskiy SV & Rytsar YB (2001) Watermark template attack. Proc. of the Photonics West 2001-Electronic Imaging, International Society for Optics and Photonics, 394–405.
- Ho ATS, Shi YQ, Kim HJ & Barni M (eds) (2009) Digital Watermarking: 8th International Workshop, IWDW 2009, Guildford, UK, August 24–26, 2009. Springer Berlin Heidelberg.
- Horiuchi T, Wada M, Saito R & Tominaga S (2009) Improvement on information capacity of watermarked images by using multi-valued area of embedded signals. Proc. of the APSIPA ASC 2009: Asia-Pacific Signal and Information Processing Association, Annual Summit and Conference, 765–768.
- Huang W & Mow WH (2013) Picode: 2d barcode with embedded picture and vicode: 3d barcode with embedded video. Proc. of the the 19th Annual International Conference on Mobile Computing & Networking, ACM, 139–142.
- Kannala J & Brandt SS (2006) A generic camera model and calibration method for conventional, wide-angle, and fish-eye lenses. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(8): 1335–1340.
- Katayama A, Nakamura T, Yamamuro M & Sonehara N (2004) New high-speed frame detection method: Side trace algorithm (sta) for i-appli on cellular phones to detect watermarks. Proc. of the 3rd International Conference on Mobile and Ubiquitous Multimedia, ACM, 109–116.

- Keskinarkaus A, Pramila A & Seppänen T (2010) Image watermarking with a directed periodic pattern to embed multibit messages resilient to print-scan and compound attacks. *J. Syst. Softw.* 83(10): 1715–1725.
- Keskinarkaus A, Pramila A & Seppänen T (2012) Image watermarking with feature point based synchronization robust to print–scan attack. *Journal of Visual Communication and Image Representation* 23(3): 507–515.
- Keskinarkaus A, Pramila A, Seppänen T & Sauvola J (2006) Wavelet domain print-scan and jpeg resilient data hiding method. *Proc. of the the 5th International Conference on Digital Watermarking*, Springer-Verlag, Berlin, Heidelberg, 82–95.
- Kim HS & Lee HK (2003) Invariant image watermark using zernike moments. *IEEE Transactions on Circuits and Systems for Video Technology* 13(8): 766–775.
- Kim Wg, Lee SH & Seo Ys (2006) Image fingerprinting scheme for print-and-capture model. *Proc. of the 7th Pacific Rim Conference on Advances in Multimedia Information Processing*, Springer-Verlag, Berlin, Heidelberg, 106–113.
- Kutter M (1999) Watermarking resistance to translation, rotation, and scaling. *Proc. of the Photonics East (ISAM, VVDC, IEMB)*, International Society for Optics and Photonics, 423–431.
- Kutter M, Bhattacharjee SK & Ebrahimi T (1999) Towards second generation watermarking schemes. *Proc. of the 1999 International Conference on Image Processing*, 1: 320–323.
- Kutter M, Voloshynovskiy SV & Herrigel A (2000) Watermark copy attack. *Proc. of the Electronic Imaging*, International Society for Optics and Photonics, 371–380.
- Lefebvre F, Gueluy A, Delannay D & Macq B (2001) A print and scan optimized watermarking scheme. *Proc. of the 2001 IEEE Fourth Workshop on Multimedia Signal Processing*, 511–516.
- Lichtenauer JF, Setyawan I, Kalker T & Legendijk RL (2003) Exhaustive geometrical search and the false positive watermark detection probability. *Proc. SPIE* 5020: 203–214.
- Lin CY & Chang SF (1999) Distortion modeling and invariant extraction for digital image print-and-scan process. *Proc. of the International Symposium on Multimedia*.
- Lin CY, Wu M, Bloom JA, Cox IJ, Miller ML & Lui YM (2001) Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on Image Processing* 10(5): 767–782.
- Liu JC & Shieh HA (2011) Toward a two-dimensional barcode with visual information using perceptual shaping watermarking in mobile applications. *Optical Engineering* 50(1): 017002–017002–11.
- Moritani Y, Yoshihara A, Jinda N & Muneyasu M (2016) Data detection method from printed images with different resolutions using tablet device. *Proc. of the 2016 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 1–6.
- Nakamura T, Katayama A, Yamamuro M & Sonehara N (2004) Fast watermark detection scheme for camera-equipped cellular phone. *Proc. of the 3rd International Conference on Mobile and Ubiquitous Multimedia*, ACM, 101–108.
- Nuutinen M & Oittinen P (2008) Digital watermarking technologies based on color modulation for linking applications. *Graphic Arts in Finland* 37(2-3): 1–14.
- Official Statistics of Finland (2015) More mobile internet use, more personal devices. Use of information and communications technology by individuals. Helsinki: Statistics Finland. URL:http://www.stat.fi/til/sutivi/2015/sutivi_2015_2015-11-26_tie_001_en.html. Online; accessed 26.1.2017.
- Official Statistics of Finland (2016) Finnish residents use the internet more and more often. Use of information and communications technology by individuals. Helsinki: Statistics Finland.

- URI: http://tilastokeskus.fi/til/sutivi/2016/sutivi_2016_2016-12-09_tie_001_en.html. Online; accessed 26.1.2017.
- O’Ruanaidh JJK & Pun T (1997) Rotation, scale and translation invariant digital image watermarking. *Proc. of the International Conference on Image Processing, ICIP’97*, 1: 536–539.
- Pereira S & Pun T (2000) Robust template matching for affine resistant image watermarks. *Trans. Img. Proc.* 9(6): 1123–1129.
- Perry B, MacIntosh B & Cushman D (2002) Digimarc mediabridge: The birth of a consumer product, from concept to commercial application. *Proc. of the SPIE Security and Watermarking of Multimedia Contents IV, Society of Photo-Optical Instrumentation Engineers*, 4675: 118–123.
- Pramila A, Keskinarkaus A, Rahtu E & Seppänen T (2011) Watermark recovery from a dual layer hologram with a digital camera. *Proc. of the 17th Scandinavian Conference on Image Analysis, Springer-Verlag, Berlin, Heidelberg*, 146–155.
- Pramila A, Keskinarkaus A & Seppänen T (2007) Camera based watermark extraction-problems and examples. *Proc. of the Finnish Signal Processing Symposium*.
- Pramila A, Keskinarkaus A & Seppänen T (2009) Reading watermarks from printed binary images with a camera phone. *Proc. of the 8th International Workshop on Digital Watermarking, Springer-Verlag, Berlin, Heidelberg*, 227–240.
- Reed IS & Solomon G (1960) Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics* 8(2): 300–304.
- Sakurikar P & Narayanan PJ (2014) Dense view interpolation on mobile devices using focal stacks. *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, IEEE Computer Society*, 138–143.
- Seo JS & Yoo CD (2006) Image watermarking based on invariant regions of scale-space representation. *IEEE Transactions on Signal Processing* 54(4): 1537–1549.
- Shi YQ, Kim HJ & Perez-Gonzalez F (eds) (2012) *Digital Forensics and Watermarking: 10th International Workshop, IWDW 2011, Atlantic City, NY, October 23-26, 2011*. Springer Berlin Heidelberg.
- Shi YQ, Kim HJ, Perez-Gonzalez F & Liu F (eds) (2017) *Digital Forensics and Watermarking: 15th International Workshop, IWDW 2016, Beijing, China, September 17-19, 2016, Revised Selected Papers*. Springer International Publishing.
- Solanki K, Madhow U, Manjunath BS & Chandrasekaran S (2004) Estimating and undoing rotation for print-scan resilient data hiding. *Proc. of the International Conference on Image Processing, ICIP ’04.*, 1: 39–42.
- Solanki K, Madhow U, Manjunath BS, Chandrasekaran S & El-Khalil I (2006) ‘print and scan’ resilient data hiding in images. *IEEE Transactions on Information Forensics and Security* 1(4): 464–478.
- Solh M (2014) Real-time focal stack compositing for handheld mobile cameras. *Proc. of the IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics*, 9020: 90200Z–90200Z–6.
- Takeuchi S, Kunisa A, Tsujita K & Inoue Y (2005) Geometric distortion compensation of printed images containing imperceptible watermarks. *Proc. of the 2005 Digest of Technical Papers. International Conference on Consumer Electronics, ICCE.*, 411–412.
- Takimoto H, Yoshimori S, Mitsukura Y & Fukumi M (2010) Invisible calibration pattern based on human visual perception characteristics. *Proc. of the 2010 20th International Conference on Pattern Recognition*, 4210–4213.

- Teknologiaeollisuus (2016) Terveysteknologia jälleen ennätyslukemiin. Announcement 5.4.2016 URI: <http://teknologiaeollisuus.fi/fi/ajankohtaista/uutiset/terveysteknologia-jalleen-ennatyslukemiin>. Online; accessed 6.3.2017.
- Thongkor K & Amornraksa T (2013) Image watermark extraction for captured image with partially glass reflection. Proc. of the 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 1–6.
- Thongkor K & Amornraksa T (2014) Robust image watermarking for camera-captured image using image registration technique. Proc. of the 14th International Symposium on Communications and Information Technologies (ISCIT), IEEE, 479–483.
- Vaquero D, Gelfand N, Tico M, Pulli K & Turk M (2011) Generalized autofocus. Proc. of the IEEE Workshop on Applications of Computer Vision (WACV), IEEE Computer Society, 511–518.
- Voloshynovskiy S, Deguillaume F & Pun T (2000) Content adaptive watermarking based on a stochastic multiresolution image modeling. Proc. of the 2000 10th European Signal Processing Conference, 1–4.
- Voloshynovskiy S, Deguillaume F & Pun T (2001a) Multibit digital watermarking robust against local nonlinear geometrical distortions. Proc. of the 2001 International Conference on Image Processing, 3: 999–1002.
- Voloshynovskiy S, Pereira S, Iquise V & Pun T (2001b) Attack modelling: towards a second generation watermarking benchmark. Signal Processing 81(6): 1177–1214.
- Wang S, Huang S, Zhang X & Wu W (2010) Hologram-based watermarking capable of surviving print-scan process. Applied optics 49(7): 1170–1178.
- Wang Z, Bovik AC, Sheikh HR & Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Transactions on Image Processing 13(4): 600–612.
- Xie Y, Tan H & Wang K (2016) A novel color image hologram watermarking algorithm based on qdft-dwt. Proc. of the 2016 Chinese Control and Decision Conference (CCDC), 4349–4354.
- Yamada T & Kamitani M (2013) A method for detecting watermarks in print using smart phone: Finding no mark. Proc. of the 5th Workshop on Mobile Video, ACM, New York, NY, USA, 49–54.
- Yu L, member) XNI & Sun S (2005) Print-and-scan model and the watermarking countermeasure. Image and Vision Computing 23(9): 807 – 814.
- Zhang C, Bastian JW, Shen C, van den Hengel A & Shen T (2013) Extended depth-of-field via focus stacking and graph cuts. Proc. of the 2013 IEEE International Conference on Image Processing, 1272–1276.
- Zong TR, Xiang Y, Elbadry S & Nahavandi S (2016) Modified moment-based image watermarking method robust to cropping attack. Int. J. Autom. Comput. 13(3): 259–267.

Original publications

- I Pramila A, Keskinarkaus A & Seppänen T (2008) Multiple domain watermarking for print-scan and JPEG resilient data hiding. Proc. 6th International Workshop on Digital Watermarking (IWDW 2007), Guangzhou, China, Springer Berlin Heidelberg: 279-293.
- II Pramila A, Keskinarkaus A & Seppänen T (2008) Watermark robustness in the print-cam process. Proc. IASTED Signal Processing, Pattern Recognition, and Applications (SPPRA 2008), Innsbruck, Austria, ACTA Press: 60-65.
- III Pramila A, Keskinarkaus A & Seppänen T (2012) Toward an interactive poster using digital watermarking and a mobile phone camera. *Signal, Image and Video Processing* 6(2):211-222.
- IV Pramila A, Keskinarkaus A, Takala V & Seppänen T (2016) Extracting watermarks from printouts captured with wide angles using computational photography. *Multimedia Tools and Applications*. 75(15): 16063-16084
- V Pramila A, Keskinarkaus A & Seppänen T (2018) Increasing the capturing angle in print-cam robust watermarking. *Journal of Systems and Software* 135: 205-215.

Reprinted with permission from Springer (I,III,IV), Association for Computing Machinery (ACM) (II) and Elsevier (V).

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

628. Pargar, Farzad (2017) Resource optimization techniques in scheduling : applications to production and maintenance systems
629. Uusitalo, Pauliina (2017) The bound states in the quantum waveguides of shape Y, Z, and C
630. Palosaari, Jaakko (2017) Energy harvesting from walking using piezoelectric cymbal and diaphragm type structures
631. Mononen, Petri (2017) Socio-economic impacts of a public agency – enhancing decision support for performance management
632. Kärkkäinen, Marja-Liisa (2017) Deactivation of oxidation catalysts by sulphur and phosphorus in diesel and gas driven vehicles
633. Viittala, Harri (2017) Selected methods for WBAN communications : FM-UWB and SmartBAN PHY
634. Akram, Saad Ullah (2017) Cell segmentation and tracking via proposal generation and selection
635. Ylimäki, Markus (2017) Methods for image-based 3-D modeling using color and depth cameras
636. Bagheri, Hamidreza (2017) Mobile clouds: a flexible resource sharing platform towards energy, spectrum and cost efficient 5G networks
637. Heikkinen, Kari-Pekka (2018) Exploring studio-based higher education for T-shaped knowledge workers, case LAB studio model
638. Joshi, Satya Krishna (2018) Radio resource allocation techniques for MISO downlink cellular networks
639. Shashika Manosha Kapuruhamy Badalge, (2018) Convex optimization based resource allocation in multi-antenna systems
640. Koskela, Pekka (2018) Energy-efficient solutions for wireless sensor networks
641. Vuokila, Ari (2017) CFD modeling of auxiliary fuel injections in the blast furnace tuyere-raceway area
642. Vallivaara, Ilari (2018) Simultaneous localization and mapping using the indoor magnetic field
643. Kaparulina, Ekaterina (2018) Eurasian Arctic ice sheets in transitions – consequences for climate, environment and ocean circulation

S E R I E S E D I T O R S

A
SCIENTIAE RERUM NATURALIUM
University Lecturer Tuomo Glumoff

B
HUMANIORA
University Lecturer Santeri Palviainen

C
TECHNICA
Postdoctoral research fellow Sanna Taskila

D
MEDICA
Professor Olli Vuolteenaho

E
SCIENTIAE RERUM SOCIALIUM
University Lecturer Veli-Matti Ulvinen

E
SCRIPTA ACADEMICA
Planning Director Pertti Tikkanen

G
OECONOMICA
Professor Jari Juga

H
ARCHITECTONICA
University Lecturer Anu Soikkeli

EDITOR IN CHIEF
Professor Olli Vuolteenaho

PUBLICATIONS EDITOR
Publications Editor Kirsti Nurkkala

ISBN 978-952-62-1804-5 (Paperback)
ISBN 978-952-62-1805-2 (PDF)
ISSN 0355-3213 (Print)
ISSN 1796-2226 (Online)

